LANDTAG VON BADEN-WÜRTTEMBERG Drucksache 9 / **4015**

9. Wahlperiode 31. 12. 86

Mitteilung

der Landesbeauftragten für den Datenschutz

Siebter Tätigkeitsbericht
der Landesbeauftragten für den Datenschutz

Schreiben der Landesbeauftragten für den Datenschutz vom 30. Dezember 1986 Nr. C 2310:

Anbei übersende ich Ihnen meinen 7. Tätigkeitsbericht, den ich nach § 16 Abs. 2 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 31. Dezember 1986 zu erstatten habe.

Dr. Ruth Leuze

Eingegangen: 31. 12. 86 / Ausgegeben: 14. 01. 87

Siebter Tätigkeitsbericht der Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

	Seite
1. Teil: Zur Lage	6
1. Amtsverständnis	6
2. Die Leitbildfunktion des Bundes	8
2.1 Das Gesetzespaket	8
2.2 Der Wartestand	9
3. Der Übergangsbonus	10
4. Die Kontrollpraxis	11
5. Was wird?	13
2. Teil: Landessystemkonzept	14
1. Reaktionen auf den 6. Tätigkeitsbericht	14
2. Der Technische Fortschritt im Jahre 1986	16
3. Was wurde aus dem landeseinheitlichen Netz?	17
3.1 Die Entwicklung im allgemeinen	17
3.2 Das Landesverwaltungsnetz – Teil Umwelt	19
3.3 Auf dem Weg zum Landesrechenzentrum?	20
4. Bürokommunikation	21
5. Zur Unzulänglichkeit der rechtlichen Rahmenbedingungen	22
3. Teil: Volkszählung 1987	23
1. Zur Situation	23
1.1 Das Gesetz	23
1.2 Sein Vollzug	24
2. Die Probleme	26
2.1 Die Abschottung: wasserdicht oder lückenhaft?	26
2.1.1 Erhebungsstelle: Gemeinde oder Landkreis?	26
2.1.2 Die Mitarbeiter	28
2.2 Die Wohnung der Zähler – 150000 Zwischenlager	30
2.3 Korrektur falscher Angaben	30
2.4 Einsatz der EDV in der Erhebungsstelle	31
2.5 Nachzählung durch die Meldebehörden?	32
3. Resümee	32
4. Teil: Öffentliche Sicherheit	33
1. Hiroshima-Forum	34
2. Die Speicherpraxis der Polizeidirektion Tübingen	36
2.1 Die Verlängerungspraxis	37
2.2 Speicherung von Senioren	40
2.3 Speicherung von Kindern	41

Seite

3. Sicherheitsüberprüfungen 42

3.1 Sicherheitsüberprüfungen für Angehörige des öffentlichen Dienstes 43

3.2 Sicherheitsüberprüfung aus Anlaß von „Wintex-Cimex 87" 44

4. Datenmißbrauch bei der Polizei 45

4.1 Merkwürdiges Zusammenspiel 46

4.2 Der allwissende Geschäftsführer 46

4.3 Falsche Gefälligkeit 47

5. Schlamperei 47

6. Eingaben 49

6.1 Die „Verbrecherkartei" 49

6.2 Personenauskunftsdatei contra Bundeszentralregister 50

6.3 Der perfekte Staat? 50

5. Teil: Kriminologische Forschung 51

1. Personenbezogen oder anonym? 52

1.1 Projekt „Strafzumessung" 52

1.2 Projekt „Jugendstrafvollzug" 53

2. Die Einwilligung 54

3. Das verlängerte Sozialgeheimnis 57

4. Nachfolgeuntersuchungen 58

5. Tübinger Langzeituntersuchung 59

6. Der Forscher und der Computer 61

6.1 Forschungsdokumentation 61

6.1.1 Kriminologisches Institut der Universität Heidelberg 62

6.1.2 Institut für Rechtstatsachenforschung – Bereich Kriminologie – der Universität Konstanz 62

6.2 Der Forscher und das Rechenzentrum 62

6.2.1 Universität Konstanz 63

6.2.2 Universität Heidelberg 64

6.3 Konsequenzen für Forscher und Rechenzentren 65

6. Teil: Datenschutz im Krankenhaus 66

1. Auf dem Weg zum vollautomatisierten Krankenhaus 66

1.1 Krankenhäuser Sindelfingen und Leonberg 67

1.2 Kreiskrankenhaus Reutlingen 68

2. Externe Rechenzentren 68

3. Diagnosestatistik 70

4. Der Doktorand und der Patient 71

5. Auskünfte an der Pforte 72

6. Der Gesetzgeber ist gefordert 74

Seite

7. Teil: Soziale Leistungen 76

1. Essensgutscheine an Nichtseßhafte 77
2. Nachbar hört mit 77
3. Das Bürgermeisteramt als Anlaufstelle 78
4. Das Erziehungsgeld 79
5. Amtshilfe durch Krankenkassen 80
6. Das Jugendamt und der Regreß 81
7. Die Auskunftspflicht des Arbeitgebers 82
8. Reha-Entlaßberichte 83

8. Teil: Das Rathaus – ein Umschlagplatz von Daten 84

1. Computer auf dem Rathaus 84
2. Die Schwarzfahrerdateien 85
   - 2.1 Wie befragen die Kontrolleure die Fahrgäste? 85
   - 2.2 Was Verkehrsbetriebe über Personen ohne gültigen Fahrausweis speichern 86
   - 2.3 Wie lange bleibt ein Schwarz- oder Graufahrer gespeichert? 87
3. Das kommunale Archiv und die zeitgeschichtliche Forschung 88
4. Das Finanzamt als Datenlieferant 90
5. Forschungsvorhaben „Gemeinderäte" 91

9. Teil: Sorgen der Bürger 92

Ausblick 97

1. Teil: Zur Lage

1. Amtsverständis

Der letzte Tätigkeitsbericht war für die CDU-Landtagsfraktion Anlaß, grundsätzliche Kritik an meiner Arbeit und ihrer Darstellung im Tätigkeitsbericht zu üben. Hatte ihr rechtspolitischer Sprecher noch in einer ersten Reaktion gegenüber der Presse von einer „gewohnt gediegenen und gründlichen Arbeit" gesprochen, so sollte sich dies im Lauf der Beratungen des Berichts im Landtag grundlegend ändern. Gewiß, auch dort lobten ihre Sprecher den „Fleiß und die Arbeit", die hinter dem Bericht stecken, bescheinigten meinen Mitarbeitern und mir vor Ort gute Arbeit und bedankten sich dafür. Zur gleichen Zeit aber glaubten sie, mir vorwerfen zu müssen, daß ich in weiten Teilen des Berichts, „wenn es um allgemeine und gesetzgeberische Fragen gehe, zum Sprachrohr der Opposition geworden sei" und deren Arbeit verrichte – ja sogar gaben sie zu verstehen, ich würde nicht „parteipolitisch unabhängig Bericht erstatten". Darüber hinaus meinte ein Sprecher, er wolle nicht im Rahmen von Gesetzgebungsvorhaben „einen Datenschutzbeauftragten zu Rate ziehen, der dann nach der Beratung in seinem Bericht wieder Watschen austeile, weil er sich nicht in allen Punkten wiedergefunden habe". Ein anderer Sprecher ließ wissen, anders als bei der Landesbeauftragten für den Datenschutz sei es Pflicht des Parlaments, dafür zu sorgen, daß beim Datenschutz „das Gleichgewicht mit anderen öffentlichen Aufgaben gewahrt bleibe". Ihm mißfiel im übrigen u. a. auch die Darstellung von Mißbrauchsfällen im Tätigkeitsbericht. Solche Fälle dürften nicht so dargestellt werden: „Weil sich ein Beamter falsch verhalten hat, ist die Behörde, ist die Regierung, ist die Fraktion der CDU gegen den Datenschutz" [1].

Diese Kritik geht von einem Verständnis meines Amtes und seiner Aufgaben aus, das ich nicht teilen kann:

- Zu meinem gesetzlichen Auftrag gehört neben der Kontrolle des Verwaltungshandelns auch die Beratung von Parlament und Regierung in Fragen des Datenschutzes; § 16 Abs. 1 Satz 2 des Landesdatenschutzgesetzes sagt dies ausdrücklich. Diesem Beratungsauftrag würde ich gewiß nicht gerecht, wenn ich mich ausgerechnet in einer Zeit passiv verhalten würde, in der sich zum einen die moderne Informations- und Kommunikationstechnik rasant fortentwickelt und in der zum anderen infolge des Volkszählungsurteils des Bundesverfassungsgerichts vom 15. Dez. 1983 die entscheidenden Weichen für ein verfassungskonformes, die hohen Risiken dieser Technik eingrenzendes Datenschutzrecht gestellt werden müssen. Ich sehe es vielmehr wie meine Kollegen im Bund und in den anderen Ländern als unerläßlich an, meine Kenntnisse, Erfahrungen und Überlegungen in die öffentliche Diskussion einzubringen und auf diese Weise dazu beizutragen, daß die Verantwortlichen bei ihren anstehenden wichtigen Entscheidungen den damit verbundenen Auswirkungen auf die Freiheitssphäre aller Bürger in der gebotenen Weise Rechnung tragen. Dabei kann es selbstverständlich nicht ausbleiben, daß ich Pläne, Vorschläge und Entscheidungen der Regierung oder der sie tragenden Partei anders bewerte als diese selbst und

[1] Pressemitteilung der CDU-Fraktion vom 10. 1. 1986, Beschlußempfehlung und Bericht des Ständigen Ausschusses vom 9. 5. 1986, LT-Drs. 9/3072, S. 2 f.; Protokoll über die 57. Sitzung des Landtags am 16. 10. 1986, S. 4624 f. u. 4632.

darauf auch deutlich hinweise. Daraus aber abzuleiten, ich würde „ständig parteipolitische Bewertungen" abgeben und mich damit zum Sprachrohr der Opposition machen, hieße, die Sache auf den Kopf zu stellen. Meine Aufgabe ist, mein Amt unabhängig, unvoreingenommen, rein sachbezogen und unbeeinflußt von jedermann wahrzunehmen. Darum bemühe ich mich, seit mich 1980 der Landtag einmütig auf Vorschlag der Landesregierung in dieses Amt berief. Nicht Lob oder Tadel, nicht politische Strömungen oder parlamentarische Mehrheiten, nicht der viel beschworene Zeitgeist, sondern allein die Verpflichtung auf die Sache des Datenschutzes so, wie sie die Verfassung vorgibt, darf Richtschnur meines Handelns sein.

- Mit ihrem Argument, das Parlament habe anders als ich für eine Wahrung des Gleichgewichts zwischen dem Datenschutz und anderen öffentlichen Aufgaben zu sorgen, erweckt die CDU-Landtagsfraktion den Eindruck, ich würde einseitig dem Datenschutz vor anderen öffentlichen Aufgaben Vorrang geben. Dies ist nicht richtig. Bei der Schaffung datenschutzrechtlicher Vorschriften sind genauso wie bei ihrem Vollzug die verschiedensten Interessen sorgfältig gegeneinander abzuwägen und zu gewichten. Dies kann überhaupt keine Frage sein. Deshalb muß selbstverständlich auch ich als Datenschutzbeauftragte solche Überlegungen anstellen; sie gehören seit jeher zu den elementaren Voraussetzungen meiner Arbeit. In keinem Fall darf ich nur das Interesse des einzelnen Bürgers sehen, sondern muß stets insbesondere auch die möglicherweise entgegenstehenden Belange der Allgemeinheit in Rechnung stellen und diese genauso gegeneinander abwägen, wie es Parlament und Regierung tun müssen. Davon ging ich in der Vergangenheit bei meiner Arbeit stets aus. Wie hätte ich sonst, um nur wenige Beispiele zu nennen, auf den Erlaß eines Landesarchivgesetzes drängen können, das den Archiven mehr Unterlagen gibt als sie bislang bekommen dürfen? Wie hätte ich sonst an der Realisierung des Modellversuchs „Leistungs- und Kostentransparenz in der gesetzlichen Krankenversicherung" maßgeblich mitwirken können, der die Datenbestände bei den beteiligten gesetzlichen Krankenkassen erheblich vergrößert? Warum sonst hätte ich nach neuen Wegen gesucht und mein Amt neue Anonymisierungsmethoden entwickelt, wenn ich nicht dem Landtag die Schaffung eines landesweiten Krebsregisters und der Landesregierung die Durchführung ihres Landesprogramms zur Weiterentwicklung der außerstationären psychiatrischen Versorgung ermöglichen wollte, die zunächst an der Hürde der unverzichtbaren ärztlichen Schweigepflicht zu scheitern drohten?
- Für unberechtigt halte ich auch die Kritik an der Darstellung der Mißbrauchsfälle im Tätigkeitsbericht. Ihr liegt eine Vorstellung zugrunde über das, was in einem Tätigkeitsbericht zu stehen hat, die ich nicht teilen kann. Der Tätigkeitsbericht ist ein Rechenschaftsbericht. Aus ihm sollen das Parlament, aber auch Regierung, Verwaltung und Öffentlichkeit ersehen können, womit ich mich im Berichtsjahr beschäftigte, welche Probleme und Fragen sich mir stellten, welche Anliegen an mich herangetragen wurden, welche Haltung ich dazu einnahm, welche Reaktion meine Arbeit hervorrief und welche Probleme mich in absehbarer Zukunft beschäftigen werden. Dazu gehört auch, über einzelne Mißbrauchsfälle zu berichten, auf mögliche Fehlerquellen hinzuweisen, die den Mißbrauch ermöglichten oder erleichterten, und die dafür verantwortlichen Stellen zu nennen. Gerade darum bemühte ich mich in meinem letzten Tätigkeitsbericht wegen der gestiegenen

Zahl an Mißbrauchsfällen besonders. Vor allem wollte ich auch deutlich machen, daß das, was oft verkannt oder gar Ausrede ist, nicht zutrifft: Datenmißbrauch ist keineswegs bloß eine Privatsache des agierenden Bediensteten, sondern in hohem Maße auch Sache der betroffenen Behörde, da die absichtliche Zuwiderhandlung gegen die Grundsätze des Datenschutzes eine der schwersten Formen denkbarer Regelverletzungen darstellt, die sich in einer Behörde ereignen können. Wenn mir ungeachtet all dessen der Sprecher der CDU-Fraktion unterstellt, ich hätte in meiner Darstellung der Mißbrauchsfälle den Eindruck erweckt, die Behörde des Beamten, die Regierung und die Fraktion der CDU sei gegen den Datenschutz, dann ist dies eine durch nichts gerechtfertigte Fehlinterpretation. Der mögliche Ärger darüber, daß ich in einer Reihe von Fragen im Bereich des Datenschutzes andere Vorstellungen als die CDU-Fraktion und die Landesregierung habe und mir erlaube, dies auch deutlich zum Ausdruck zu bringen, sollte doch den Blick für eine objektive Betrachtung der Sachdarstellung im Tätigkeitsbericht nicht trüben.

2. Die Leitbildfunktion des Bundes

Der Gesetzgeber und nicht die Verwaltung muß entscheiden, welche Informationen der Staat über seine Bürger sammeln, nutzen und weitergeben darf. Er darf solche Maßnahmen nur zulassen, wenn sie das überwiegende Allgemeininteresse gebietet. Dies ist die wichtigste Konsequenz aus dem Volkszählungsurteil des Bundesverfassungsgerichts. Obwohl inzwischen schon drei Jahre vergangen sind, sind wir leider von diesem Idealzustand noch weit entfernt. In vielen Bereichen ist der Verfassungsauftrag nicht erfüllt. Noch immer stützt sich die Verwaltung auf Rechtsgrundlagen, die vielleicht einer Zeit angemessen waren, als man noch mit Ärmelschoner und Federhalter arbeitete, die aber gewiß nicht mehr der Gegenwart entsprechen, in der die Risiken der modernen Kommunikations- und Informationstechniken in der öffentlichen Verwaltung immer mehr zunehmen.

2.1 Das Gesetzespaket

Mit einem Gesetzespaket, den „Sicherheits- und Datenschutzgesetzen", sollte auf Bundesebene 1986 der entscheidende Schritt nach vorn getan werden. Doch schnell zeigte sich, daß sein Inhalt nicht hielt, was seine Verpackung versprach. Von vielen Seiten, nicht nur von den Datenschutzbeauftragten, hagelte es zu Recht Kritik. Allzusehr waren die Gesetzentwürfe von dem Bestreben geleitet, den status quo nach Möglichkeit festzuschreiben, der Verwaltung einen an ihren Wünschen ausgerichteten, nicht kneifenden Maßanzug zu verschaffen und den Flurschaden zu begrenzen, den das Volkszählungsurteil in den Augen vieler angerichtet hatte. Zu wenig berücksichtigte das Gesetzespaket, daß die zulässigen Informationseingriffe im überwiegenden Allgemeininteresse geboten, also notwendig sein müssen, und daß dies nicht nur behauptet, sondern bewiesen werden muß. Aus diesem Grund war es ein, wenn auch bescheidener Teilerfolg, daß der Bundestag das Gesetzespaket aufschnürte und sein Inhalt großteils nicht den Weg ins Bundesgesetzblatt fand. Unbefriedigend bleibt aber auch so die Bilanz für den Datenschutz allemal: Der maschinenlesbare Ausweis kommt, ohne daß seine Befürworter nachgewiesen hätten, daß ein solcher Ausweis maschinenlesbar sein muß.

Dies wiegt um so schwerer, weil immer noch ausreichende Regelungen für die Informationsverarbeitung durch die Sicherheitsbehörden fehlen, obwohl gerade diese Regelungen der ganze deutsche Bundestag einst als unerläßliche Voraussetzung für die Einführung eines maschinenlesbaren Personalausweises ansah. Dasselbe verfassungsrechtliche Manko haftet – abgesehen von anderen Defiziten – der soeben verabschiedeten Regelung über die Nutzung der Datensammlungen des Kraftfahrtbundesamts, dem sog. ZEVIS-Gesetz, an. Auch vermag die – zwar noch in letzter Minute etwas verbesserte – Vorschrift über die Schleppnetzfahndung nicht zu befriedigen, weil sie den Abgleich von Schleppnetzdateien mit anderen Datenbeständen voraussetzungslos zuläßt und damit in Kauf nimmt, daß völlig außer Kontrolle geraten kann, was mit den Daten völlig harmloser Bürger in einer Schleppnetzdatei geschieht.

2.2 Der Wartestand

Nahezu absolute Funkstille herrschte bei der Datenschutzgesetzgebung im Lande. Man begnügte sich mit einigen, für sich gesehen sicherlich begrüßenswerten Regelungen im Beihilferecht der öffentlichen Bediensteten und im Personalvertretungsrecht. Im übrigen wartet man noch immer auf Bonn. Der Innenminister beschwor die Leitbildfunktion des Bundes. Die Landtagsmehrheit schloß sich bei der Beratung eines Gesetzentwurfs der SPD-Fraktion zur Änderung des Landesdatenschutzgesetzes dieser Argumentation an. Es erklang das hohe Lied der Rechtseinheit im Bundesgebiet; von der sonst zu Recht immer wieder betonten Eigenständigkeit der Länder war nichts zu hören. Das Bemühen um ein einheitliches Datenschutzrecht im Bundesgebiet verdient gewiß auch aus mancher Sicht Unterstützung. Wenn aber der Bund dabei seiner Leitbildfunktion nicht gerecht wird, darf dies nicht dazu führen, daß auch in den Ländern die notwendigen Entscheidungen unterbleiben. Vor allem kann eine solche Situation kein Grund sein, sich von der öffentlichen Diskussion über die Zukunft des Datenschutzrechts auszuschalten. Genau dies aber ist kennzeichnend für das Vorgehen der Landesregierung. Die beteiligten Ministerien nehmen zwar durchaus aktiv Einfluß auf die Erarbeitung der Gesetzentwürfe im Bund und in Bund/Länder-Gremien, tun aber gleichzeitig alles, um ja eine öffentliche Erörterung ihrer dabei eingenommenen Positionen im Land zu verhindern. So warte ich beispielsweise heute noch vergebens auf eine sachliche Auseinandersetzung des Innenministeriums mit meinen ausführlichen Stellungnahmen zur Novellierung des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes sowie zu den verschiedenen Gesetzentwürfen über die Informationsverarbeitung bei den Sicherheitsbehörden. Wenn überhaupt eine Reaktion erfolgte, dann erschöpfte sie sich in einer Bestätigung des Empfangs und der Zusage, die Stellungnahme in die weiteren Beratungen einzubeziehen. Wer die konkrete Haltung der Landesregierung Baden-Württemberg zu den einzelnen Gesetzesvorhaben in Erfahrung bringen will, dem bleibt nur übrig, Einblick in die Protokolle des Bundesrats und seiner Ausschüsse zu nehmen. Dann wird er freilich schnell feststellen, daß die Ministerien dort gewissermaßen unter Ausschluß der Öffentlichkeit durchaus in der Lage sind, dezidiert Positionen zu vertreten und sich dabei keineswegs in Zurückhaltung üben. Natürlich ist dieser Weg für die Ministerien

der bequemere: Er enthebt sie der Notwendigkeit, gegenüber der kritischen Öffentlichkeit ihre Haltung näher zu begründen, und eröffnet ihnen nach Verabschiedung der Bundesgesetze die Möglichkeit, bei der Beratung der entsprechenden Landesregelungen mit dem Hinweis auf die notwendige Bundeseinheitlichkeit etwaigen Gegenargumenten zu begegnen und etwaige abweichende Vorstellungen abzulehnen. Doch bleibt die bohrende Frage, ob sich ein Land von der Bedeutung Baden-Württembergs einen solchen Mangel an Eigenständigkeit, wie er in dieser Verfahrensweise zum Ausdruck kommt, leisten kann.

3. Der Übergangsbonus

Auch wer wenig mit dem Datenschutz im Sinn hat, muß zugestehen, daß die Verwaltung gegenwärtig vielfach Informationen über Bürger erhebt, nutzt und weitergibt, ohne sich dabei auf Rechtsgrundlagen stützen zu können, die den verfassungsrechtlichen Anforderungen entsprechen:

- So geben z. B. die Justizbehörden, also die Gerichte und Staatsanwaltschaften, in großem Stil Entscheidungen an andere Behörden und Stellen weiter. Für diesen umfangreichen Mitteilungsdienst gibt es bisher keine gesetzliche Grundlage. Er stützt sich vielmehr ausschließlich auf von der Justizverwaltung erlassene Verwaltungsvorschriften, nämlich die Anordnung über Mitteilungen in Strafsachen (Mistra) und die Anordnung über Mitteilungen in Zivilsachen (Mizi).
- So speichert z. B. die Polizei in ihrem landesweiten automatisierten Informationssystem, der Personenauskunftsdatei (PAD), Personen, gegen die ein Ermittlungs- oder Strafverfahren anhängig war, sehr häufig auch dann weiter, wenn dieses Verfahren nicht zu einer Verurteilung führte. Voraussetzung für die weitere Speicherung ist im wesentlichen allein, daß in den Augen der Polizei ein sog. Restverdacht blieb. Eine Entscheidung des Gesetzgebers, die einen solchen Eingriff in die Rechte des betroffenen Bürgers erlaubt, existiert nicht.

Neben den Fällen, für die überhaupt keine gesetzlichen Grundlagen bestehen, gibt es aber auch Vorgehensweisen, die sich auf den Grundsätzen des Volkszählungsurteils eklatant zuwiderlaufende Rechtsvorschriften stützen. Zu erwähnen ist hier insbesondere § 10 des Landesdatenschutzgesetzes. Diese Bestimmung läßt eine Datenweitergabe an andere Behörden und öffentliche Stellen allein schon dann zu, wenn der Empfänger die Information zur Erfüllung seiner Aufgaben benötigt. Eine solche Regelung ist schlechterdings unvereinbar mit der Feststellung des Bundesverfassungsgerichts, daß zwangsweise erhobene Daten grundsätzlich nur für den Zweck verwendet werden dürfen, für den sie erhoben wurden.

Die Diskrepanz zwischen dem, was eigentlich die Verfassung erlaubt, und dem, was tagtäglich praktiziert wird, stellt die Verwaltung, aber auch die unabhängige Datenschutzkontrolle bei ihrer täglichen Arbeit vor schwierige Fragen. Ist es angesichts dieses Auseinanderklaffens von Sollen und Sein vertretbar, bis zum Tätigwerden des Gesetzgebers so zu tun, als gäbe es das Volkszählungsurteil des Bundesverfassungsgerichts nicht, oder müssen alle bisher praktizierten Informationseingriffe, für die es keine verfassungskonforme Rechtsgrundlage gibt, ab sofort unterbleiben – selbst dann, wenn sie tatsächlich im überwiegenden Allgemeininteresse geboten sind? Diese Fragen werden um so dringender, je länger der Gesetzgeber untätig bleibt. Einstweilen verfährt die Verwaltung noch wie gewohnt. Soweit sie über-

haupt ein Problem sieht, beruft sie sich auf das Zauberwort „Übergangsbonus". Hinter diesem Begriff verbirgt sich folgendes: Das Bundesverfassungsgericht billigte in einer Reihe von Entscheidungen dem Gesetzgeber und der Verwaltung eine Übergangsfrist zu, wenn verfassungsrechtlich ursprünglich unbedenkliche Maßnahmen aufgrund einer gewandelten Rechtsauffassung verfassungsrechtlich bedenklich wurden. Auf diese Weise hat der Gesetzgeber die Chance, eine neue verfassungsmäßige Regelung zu erlassen. Obgleich sich sehr wohl darüber streiten läßt, ob tatsächlich erst das Volkszählungsurteil den Wandel in der verfassungsrechtlichen Beurteilung von Informationseingriffen herbeigeführt hat, gehe ich bei meiner Prüfungspraxis davon aus mit der Folge, daß die höchstrichterliche Rechtsprechung zum Übergangsbonus grundsätzlich anwendbar ist. Auch Datenschutzbeauftragte huldigen also nicht dem Wahlspruch: „Fiat justitia et pereat mundus". Das kann jedoch nicht bedeuten, daß die Verwaltung ihre bisherige Praxis uneingeschränkt bis zum St. Nimmerleinstag fortsetzen darf. Zu bedenken ist vielmehr folgendes:

- Das Bundesverfassungsgericht konzidiert eine solche Übergangsfrist nur, um eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen zu vermeiden, die der verfassungsgemäßen Ordnung noch ferner stünde als der bisherige Zustand. Aus diesem Grunde dürfen auch innerhalb der Übergangsfrist nur solche Informationseingriffe ohne ausreichende Rechtsgrundlage erfolgen, die zur Sicherstellung dieses Zustands unerläßlich sind. Insbesondere muß die Behörde jeweils prüfen, ob nicht eine bislang nicht übliche, aber schonendere Maßnahme ausreicht, um die Funktionsfähigkeit sicherzustellen. Dem Grundsatz der Verhältnismäßigkeit kommt hier also ganz wesentliche Bedeutung zu.
- Die Übergangsfrist kann keineswegs unendlich sein. Die Gesetzgeber in Bund und Land sind in Pflicht genommen. Sie können sich dieser Aufgabe nicht durch Abwarten entziehen, sondern sind gehalten, in angemessener Zeit darüber zu entscheiden, was künftig noch zulässig sein soll und was nicht. Wollen die Gesetzgeber nicht das Risiko des Fristablaufs beim Übergangsbonus eingehen, müßten sie auf alle Fälle in der nächsten Legislaturperiode von Bundestag und Landtag die erforderlichen Beschlüsse fassen.

4. Die Kontrollpraxis

Für ein Kontrollorgan ist es wichtig, die Verwaltungspraxis immer wieder vor Ort mit eigenen Augen zu sehen und sich nicht nur aus dem oft zeitraubenden und umfangreichen Schriftwechsel mit den verschiedensten Behörden und Stellen ein Bild zu verschaffen. Erfreulicherweise konnten meine Mitarbeiter und ich im vergangenen Jahr ca. 60 Informations- und Kontrollbesuche durchführen und uns direkt bei den Behörden die notwendigen Informationen holen. Im Vordergrund standen dabei Überprüfungen einzelner konkreter Vorgehensweisen und nicht so sehr allgemeine, die gesamte Tätigkeit der aufgesuchten Behörden umfassende Kontrollen. Die besuchten Stellen spiegeln das weite Feld wider, in dem die öffentliche Hand Datenverarbeitung betreibt: Bürgermeisterämter und Polizeipräsidien, eine Sonderschule und ein Gesundsheitsamt, das Landesamt für Verfassungsschutz, Landeskriminalamt und mehrere Justizvollzugsanstalten, Universitätsverwaltungen und Universitätsrechenzentren, Kriminologische Institute von Universitäten und die drei Oberfinanzdirektionen im Lande, das Gemeinschaftsrechenzentrum des Landes und ein Regionales Rechenzentrum, das

Statistische Landesamt, der Onkologische Schwerpunkt beim Klinikum der Stadt Karlsruhe und nicht zuletzt die Landesanstalt für Schweinezucht zählten dazu.

Alle Stellen zeigten – auch wenn teilweise gravierende Mängel festzustellen waren – eine erfreuliche Kooperationsbereitschaft. Diese Erfahrung bestätigt meinen Eindruck, daß die Verwaltung des Landes inzwischen im allgemeinen gegenüber der Datenschutzkontrolle aufgeschlossen ist und sie bei ihrer Arbeit unterstützt. Dafür sprechen auch die zahlreichen schriftlichen und telefonischen Anfragen von öffentlichen Stellen und einzelnen ihrer Mitarbeiter, in der sie um Rat und Unterstützung bei der Lösung datenschutzrechtlicher Probleme bitten. Diese positive Entwicklung läßt freilich nicht den Schluß zu, an der Datenschutzfront herrsche eitel Freude. Denn auch im vergangenen Jahr gab es unbefriedigende Ereignisse und Vorgehensweisen:

- Die Notwendigkeit, sich mit den Erfordernissen des Datenschutzrechts auseinanderzusetzen, mag manchmal unbequem sein. Dies darf jedoch nicht dazu führen, sich dieser Auseinandersetzung durch Tricks zu entziehen. Nur so kann ich aber eine Anordnung des Kultusministeriums an die Schulen bewerten, ihre Lehrerdateien nicht für Mitteilungen an Dritte zu benutzen, sondern dann, wenn solche Mitteilungen notwendig werden, auf die Personalhilfsakten zurückzugreifen. Diese erstaunliche Regelung hat folgende Vorgeschichte: 1984 hatte ich bei Kontrollbesuchen festgestellt, daß die Schulen vielfach über ihre Lehrer mehr Daten als benötigt erheben und in ihren Lehrerkarteien speichern. Diesen Befund teilte ich dem Kultusministerium mit. Anstatt sich mit meinen dabei gestellten detaillierten Fragen auseinanderzusetzen, behauptete es daraufhin, die Schulen würden aus den Lehrerkarteien keine Auskünfte erteilen, diese seien daher sog. interne Dateien im Sinne von § 1 Abs. 2 LDSG; die Schulen müßten folglich nach § 8 LDSG nur darauf achten, daß die Karteien gegen unbefugte Einsichtnahme und Wegnahme geschützt sind. Nachdem ich das Kultusministerium darauf aufmerksam gemacht hatte, daß diese Sicht der Dinge ganz und gar nicht der Realität entspricht, sondern die Schulen aus ihren Lehrerkarteien sehr wohl auch Informationen an Dritte weitergeben, nahm es sich zunächst einmal längere Zeit und entschloß sich dann zur Vorwärtsverteidigung: es erließ die bereits erwähnte Anordnung. Erreicht ist damit folgendes: benötigt ein Schulleiter für seine Kontakte mit anderen Behörden, Eltern oder privaten Organisationen Informationen über einzelne Lehrer, muß er diese jeweils mühsam in den Akten suchen. Er kann sie nicht wie bisher schnell und unkompliziert der Lehrerkartei entnehmen. Da die Schulen die Beweggründe des Kultusministeriums für diese merkwürdige neue Anordnung nicht kennen, müssen sie annehmen, eine solch ineffektive Arbeitsweise verlange der Datenschutz. Daß der Datenschutz damit in Mißkredit geraten kann und daß auf diese Weise das eigentliche Problem – nämlich die Frage, welche Informationen ein Lehrer seinem Schulleiter zukommen lassen muß und was dieser damit anfangen darf – nicht gelöst ist, kümmert das Kultusministerium offensichtlich nicht. Ihm ging es bloß darum, einen Weg zu finden, wie es sich der Auseinandersetzung mit meinem Amt über die Notwendigkeit des Erhebens und Speicherns von Lehrerdaten an Schulen entziehen kann.
- Ein anderes leidiges Problem tritt bedauerlicherweise immer wieder auf: bis mir Behörden auf schriftliche Anfragen antworten, vergeht oft sehr lange Zeit. Besonders unbefriedigend ist dies, wenn ich deren Stellungnahme benötige, um Eingaben von Bürgern zu beantworten. So mußte mein Amt zwei

Mahnschreiben schicken und ich noch persönlich den Oberbürgermeister anschreiben, bis mir die Stadtverwaltung Albstadt auf meine Anfrage vom Januar 1986 wegen einer Eingabe aus dem Bereich der Sozialhilfe im Juli 1986 schließlich ihre Stellungnahme übermittelte. Arg schwer tut sich manchmal auch die Stadt Stuttgart: so ließ ihre Antwort trotz wiederholter schriftlicher und fernmündlicher Erinnerungen durch die ganze städtische Verwaltungshierarchie hindurch bis hin zu einem persönlichen Brief an den Oberbürgermeister im September 1986 auf eine Anfrage, die ich wegen der Eingabe eines ausländischen Mitbürgers im März 1986 an die Stadtverwaltung gerichtet habe, neun Monate auf sich warten.

- Offensichtlich nicht auszumerzen ist auch die Neigung, Auskünfte mit dem Hinweis auf den Datenschutz zu verweigern, obwohl die Behörde in Wirklichkeit aus ganz anderen Gründen etwas nicht sagen will. So lehnte beispielsweise der Leiter einer Berufschule die Bitte einer Kreistagsfraktion, Unterlagen über die Lehrerversorgung an den Schulen zu erhalten, mit der Begründung ab, die Schulen seien bei einer früheren Direktorenkonferenz gebeten worden, „aus Gründen des Datenschutzes keine statistischen Unterlagen direkt auszugeben, sondern jeweils auf das Oberschulamt und das Statistische Landesamt zu verweisen". In Wirklichkeit enthielten die erbetenen Unterlagen überhaupt keine Angaben über Personen, so daß schon allein deshalb der Datenschutz ihrer Herausgabe nicht entgegenstand. Das wahre Motiv war auch ein ganz anderes: man hielt aus organisatorischen Überlegungen das Oberschulamt für den geeigneteren Ansprechpartner.

Diese Liste negativer Erfahrungen ließe sich natürlich noch fortschreiben. Gleichwohl meine ich: die Schwierigkeiten des Datenschutzes liegen gegenwärtig weniger im Vollzug als im Mangel an datenschutzfreudlichen Entscheidungen des Gesetzgebers.

5. Was wird?

Wer gegenwärtig die Berichterstattung in den Medien unbefangen verfolgt und dabei hört und sieht, wie sich Minister, Staatssekretäre, Abgeordnete, Landespolizeipräsidenten und andere Vertreter der Sicherheitsbehörden in Bund und Ländern zum Thema Datenschutz äußern, der kann nicht optimistisch in die Zukunft sehen. Gewiß, nicht jeder ist gleich so radikal wie die Frankfurter Allgemeine Zeitung, die am 30. Oktober 1986 zur Schlachtung der „Heiligen Kuh Datenschutz" aufrief. Doch die Tendenz ist eindeutig: der Datenschutz wird wieder einmal zum Sündenbock erklärt. Viele nutzten die nur allzu verständliche Bestürzung über die Opfer sinnloser Gewaltverbrechen dazu, Stimmung gegen den Datenschutz zu machen. Pauschalurteile werden gefällt; Vereinfachungen und Schlagworte beherrschen das Feld; sorgfältiges Analysieren, Abwägen und Differenzieren ist zur Mangelware geworden. Mehr Befugnisse der Sicherheitsbehörden beim Sammeln und Verarbeiten von Informationen über Bürger setzen viele automatisch gleich mit mehr Sicherheit. Während es seit langem ganz selbstverständlich ist, beim Erlaß von Gesetzen, die den Bürger zu Geldleistungen – seien es noch so geringe Beträge – verpflichten, deren Notwendigkeit nachzuweisen, gilt das bei Eingriffen in das Grundrecht der Bürger auf Selbstbestimmung offenbar nicht. Hier wird aus welchen Gründen auch immer die Beweislast umgekehrt: wer sich gegen weitere Eingriffsbefugnisse wendet, muß nachweisen, daß diese keine Vorteile bringen und auch die Effektivität der Strafverfol-

gung nicht steigern. Auf völliges Unverständnis stößt gar vielfach, wer zu bedenken gibt, daß die Schaffung weiterer Eingriffsbefugnisse für die Sicherheitsbehörden auch nachteilige Auswirkungen auf unsere Gesellschaft haben kann, und deshalb dafür eintritt, nicht nur die möglichen Vorteile, sondern auch die zu befürchtenden Nachteile in die Überlegungen einzubeziehen und angemessen zu gewichten. Die Risiken, die sich aus dieser Stimmungslage ergeben, kann man nicht hoch genug veranschlagen. Denn die eigentliche Bewährungsprobe für den Datenschutz steht noch aus: zum einen entwickeln sich die modernen Informations- und Kommunikationstechniken nach wie vor rasant weiter; zum anderen müssen spätestens in der nächsten Legislaturperiode des Deutschen Bundestags die grundlegenden Weichen für ein verfassungskonformes Datenschutzrecht gestellt werden, das auch diese Risiken auffängt. Eine solch schwierige Aufgabe läßt sich nur in einem Klima der Vernunft und der Sachlichkeit leisten. Emotionen, Vorurteile und Einseitigkeiten sind fehl am Platz. Notwendig sind kühle Köpfe und nicht heiße Nadeln.

2. Teil: Landessystemkonzept

1. Reaktionen auf den 6. Tätigkeitsbericht

Wer weiß, wie sehr sich die Landesregierung der Idee verschrieben hat, möglichst rasch in allen Büros der Landesverwaltung das High Tech-Zeitalter einzuläuten, den kann nicht verwundern, daß meine Ausführungen zum Landessystemkonzept im letzten Tätigkeitsbericht ein lebhaftes Echo hervorriefen. Der Herr Ministerpräsident diagnostizierte „voreilige Vorwürfe", die CDU-Landtagsfraktion sprach von einem „Horror-Szenario, das mit der Wirklichkeit nicht übereinstimmt" und die Landesregierung meinte sogar, mir in ihrer offiziellen Stellungnahme zu meinem Tätigkeitsbericht vorwerfen zu müssen, ich hätte die Ziele des Landessystemkonzepts nicht richtig dargestellt. Dabei hatte ich doch nur in verständlicher Sprache das zu Papier gebracht, was den damals über das Landessystemkonzept vorhandenen, im EDV-Jargon geschriebenen Unterlagen mit den üblichen Interpretationsmethoden zu entnehmen war und was die voraussehbare Entwicklung der Informations- und Kommunikationstechnik erwarten ließ. Anders als meine Kritiker hatte ich dabei aber sehr wohl zwischen den konkreten Zielen der Einzelszenarien des Landessystemkonzepts und den technischen Möglichkeiten und Risiken unterschieden, die bei der Verfolgung dieser Ziele entstehen können.

Bemerkenswert an der Reaktion von Landesregierung und Regierungsfraktion war auch ein weiteres: beide beteuerten unisono, daß bei der Realisierung des Landessystemkonzepts selbstverständlich der Datenschutz beachtet werden müsse. So erfreulich diese Aussagen für sich gesehen sind, so fraglich ist zugleich, ob sie mit Datenschutz wirklich das meinen, was er nach unserer Verfassung tatsächlich ist: nämlich die Summe der rechtlichen, technischen und organisatorischen Vorkehrungen, die zum Schutze des Grundrechts des Bürgers, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu entscheiden, notwendig sind. Sowohl die Stellungnahme der Landesregierung zu meinem letzten Tätigkeitsbericht als auch sonstige Äußerungen aus ihren Reihen, der Regierungsfraktion

und des Staatsministeriums [1] lassen vielmehr vermuten, daß Datenschutz beim Landessystemkonzept nur als Datensicherheit, im wesentlichen also als technischer und organisatorischer Datenschsutz verstanden wird. Dieser ist gewiß beim Landessystemkonzept ein ganz wichtiger Aspekt, aber eben keineswegs der einzige.

Schließlich war noch eine weitere Reaktion zu verzeichnen. Auf Wunsch der CDU-Fraktion bat mich die Landesregierung, im Landessystemausschuß mitzuwirken. Aufgabe dieses von ihr 1985 ins Leben gerufenen Gremiums ist, den Einsatz der Informations- und Kommunikationstechnik in der Landesverwaltung zu koordinieren und grundsätzliche Entscheidungen des Kabinetts auf dem Gebiet der Informations- und Kommunikationstechnik vorzubereiten. Ich entsprach der Bitte um Beratung und erklärte mich bereit, als Gast an den Sitzungen des Landessystemausschusses teilzunehmen. Anders als die nebenbei gemachte Bemerkung des Sprechers der CDU-Fraktion bei der Aussprache über meinen letzten Tätigkeitsbericht, es hätte nicht der „50 Seiten benötigt, um darzulegen, daß ich hinein will" vermuten läßt, tat ich dies nicht leichten Herzens. Denn ich wußte sehr wohl, daß es für mich als unabhängiges Kontrollorgan durchaus problematisch ist, sich schon so frühzeitig an der Planung für den Einsatz der Informations- und Kommunikationstechnik zu beteiligen; allzu leicht könnten dabei spätere Kontrollmaßnahmen präjudiziert werden. Auch fragte ich mich, ob der falsche Schein entstehen könnte, durch meine Teilnahme an den Sitzungen des Landessystemausschusses sei der Datenschutz bei der Realisierung des Landessystemkonzepts in ausreichendem Maße gewährleistet. Gerade diese Befürchtung erwies sich in der Folgezeit leider als sehr real: wer auch immer seitdem wann auch immer Kritik am Landessystemkonzept übte, bekam von der Landesregierung und CDU-Fraktion zu hören, durch meine Mitarbeit im Landessystemausschuß sei der Datenschutz gewahrt [2]. Ich halte eine solche Vereinnahmung meiner Person für sehr bedauerlich. Natürlich bemühe ich mich nach Kräften, Einfluß auf eine datenschutzgerechte Realisierung des Landessystemkonzepts zu nehmen. Doch sollte man sich dabei keinen falschen Vorstellungen über meine Möglichkeiten hingeben: Allein schon wegen der Fülle der zu erwartenden Probleme und der beschränkten Personalkapazität meines Amtes ist es völlig ausgeschlossen, umfassend auf alle auftretenden Probleme des Datenschutzes einzugehen. Zudem betritt die Landesregierung mit ihrem Landessystemkonzept Neuland, so daß ich selbstverständlich nicht in Anspruch nehme, schon jetzt alle möglicherweise auftretenden Risiken und Probleme zu erkennen und dafür Lösungsvorschläge parat zu haben. Vor allem aber kümmert sich der Landessystemausschuß nur um eine Seite der Medaille, die Datensicherheit; überhaupt nicht befaßt er sich mit der weiteren Grundvoraussetzung für die Realisierung des Landessystemkonzepts, der Schaffung eines verfassungskonformen Datenschutzrechts, das den Risiken von High Tech angemessen begegnet. Und last not least: die eigentlichen Entscheidungen über die Realisierung des Landessystemkonzepts fallen überhaupt nicht im Landessystemausschuß, sondern andernorts – vornehmlich im Kabinett, durch Ressortabsprache oder Ministerweisung; daran wirke ich in keiner Weise mit. Was folgt aus alledem? Schlicht eines: Sollten Landesregierung und Regie-

[1] z. B. StAnz. Nr. 8 v. 25. Jan. 1986, S. 1; Pressemitteilung des Landtags Nr. 31 v. 13. Mai 1986; StAnz. Nr. 41/42 v. 24. Mai 1986, S. 4.

[2] z. B. Protokoll über die 54. Sitzung des Landtags am 24. Sept. 1986, S. 4350 ff. (4361); StAnz. Nr. 80 v. 4. Okt. 1986; Protokoll über die 57. Sitzung des Landtags v. 16. Okt. 1986, S. 4624.

rungsfraktion weiterhin alle berechtigten Fragen nach dem Datenschutz beim Landessystemkonzept mit dem Hinweis auf meine Mitwirkung im Landessystemausschuß abwehren, sehe ich keinen Grund, weshalb ich noch länger an den Sitzungen dieses Gremiums teilnehmen soll. Ich bin nicht bereit, als Alibi herzuhalten.

2. Der Technische Fortschritt im Jahre 1986

Um die Jahreswende 1985/86 verfügte die Informationstechnik trotz ihres hohen Standards nicht über die erforderlichen Techniken für eine datenschutzgemäße Realisierung des Landessystemkonzepts; dies schilderte mein letzter Tätigkeitsbericht ausführlich. Die damals auf dem Markt angebotenen Produkte konnten zwar Datennetze zu einem Universalnetz zusammenschließen, waren jedoch nicht in der Lage, seine Datenflüsse von vornherein so zu lenken, daß niemand mehr oder andere Informationen erhält, als für ihn bestimmt sind. Auch war keines der auf dem Markt befindlichen Bürokommunikationssysteme in der Lage zu registrieren, wer wann welchen Text inwieweit verfaßt, korrigiert, gebilligt und unterschrieben hat, und sicherzustellen, daß niemand nachträglich diesen Text verfälscht. Diese Funktionen sind aber unabdingbare technische Voraussetzungen, um die Behörden des Landes in einem Universalnetz zusammenzuschließen und Bürokommunikation in der Landesverwaltung generell einzuführen. Der Beschluß der Landesregierung von 1985, trotz dieser technischen Defizite beide Vorhaben im Rahmen ihres Landessystemkonzepts so schnell wie möglich zu realisieren, steuerte deshalb automatisch auf den Konflikt mit dem Datenschutz zu. Denn Datenschutz ohne Datensicherheit ist undenkbar.

Heute, ein Jahr später, sieht die technische Landschaft etwas anders aus. Erste Entwürfe neuer Techniken, die für die Datensicherheit in Netzen von Bedeutung sind, kamen auf den Markt: verschiedene Firmen präsentierten 1986 nämlich erstmals Konzepte, wie in einem nach dem Industrie-Standard Systems Network Architecture (SNA) betriebenen landeseinheitlichen Netz ein geordneter Datenfluß zu erreichen sein könnte. Für das Landessystemkonzept ist diese Entwicklung von besonderem Interesse, weil die Landesregierung alle künftigen Netze nach diesem Standard betreiben will. Die Grundidee der neuen Konzepte ist überall dieselbe: ein spezielles Kontrollprogramm soll die bislang völlig freien Datenflüsse im Netz so sicher lenken, daß in Zukunft jeder der vielen an das Netz angeschlossenen Benutzer tatsächlich nur auf die für ihn bestimmten Daten zugreifen kann. Mit Hilfe zweier Hauptfunktionen soll dies erreicht werden:

- Anhand einer Berechtigungstabelle soll das Kontrollprogramm feststellen, ob der Benutzer eines bestimmten Terminals die gewünschte Verbindung zu einem bestimmten Programm in einem bestimmten Computer bekommen darf. Nur solche Verbindungen stellt es her, die in der Berechtigungstabelle eingetragen sind; alle anderen Verbindungswünsche weist es ab.
- Um eine nachträgliche Kontrolle der Vorgänge im Netz zu ermöglichen, insbesondere um etwaige Mißbrauchsversuche erkennen zu können, soll das Kontrollprogramm bis ins Detail protokollieren, welche Verbindungen es wann zwischen welchen Kommunikationspartnern aufgebaut und welche gewünschten Verbindungen es abgewiesen hat.

Neben diesen Hauptfunktionen soll das Kontrollprogramm zur Erhöhung der Sicherheit im Universalnetz noch weiteres kön-

nen, nämlich: Verbindungen automatisch abbauen, wenn an einem Terminal längere Zeit keine Eingabe erfolgte, und Terminals außer Betrieb setzen, wenn von ihnen hintereinander mehrfach die Herstellung unzulässiger Verbindungen gewünscht wurde.

Auf der Grundlage dieser Konzepte kamen 1986 bereits auch erste Versionen solcher Netzkontrollprogramme auf den Markt: zum einen sind die Verbindungscomputer des neuen Programms SNA Netzwork Interconnection (SNI), Gateways genannt, zu nennen, die nicht nur einzelne, voneinander unabhängige SNA-Netze miteinander verbinden, sondern zugleich kontrollieren können, wer aus einem SNA-Netz mit wem aus einem anderen SNA-Netz Verbindungen aufbauen will. Zum zweiten wurde ein neues Programm vorgestellt, das zur Steuerung des Aufbaus von Verbindungen innerhalb ein und desselben SNA-Netzes bestimmt ist. Beide Programme sind ein Schritt in die Richtung von mehr Datensicherheit in SNA-Netzen. Ob sie aber in dem von der Landesregierung angestrebten landeseinheitlichen Netz zum Einsatz kommen und ob sie dabei halten, was man sich von ihnen verspricht, läßt sich heute noch nicht sagen. Fest steht dagegen, daß beide Programme bestenfalls eine der beiden Hauptfunktionen des konzipierten Kontrollprogramms erfüllen – nämlich die Steuerung des Verbindungsaufbaus –, daß sie aber die zweite Hauptfunktion, alle Aktivitäten detailliert zu protokollieren, noch nicht beherrschen.

Bei der Bürokommunikation waren vergleichbare technische Fortschritte nicht zu verzeichnen. Positiv zu vermerken ist freilich der 1986 eingetretene Umdenkungsprozeß in Fachkreisen. Während Ende 1985 noch das Problembewußtsein für die technischen Unzulänglichkeiten der Bürokommunikationssysteme beim Einsatz in der öffentlichen Verwaltung nahezu völlig fehlte, ist dies inzwischen allgemein anerkannt. Anders als bei der Wirtschaft eignen sich für die öffentliche Verwaltung nur Bürokommunikationssysteme, die das komplizierte Gefüge von Berechtigungen und Zuständigkeiten der Bediensteten beherrschen, eine Abbildung des herkömmlichen Geschäftsgangs auf die Maschinen erlauben und Fälschungen elektronischer Akten verhindern. Dafür aber ist – sieht man von wenigen spärlichen Ansätzen ab – noch kein Konzept in Sicht, geschweige denn ein geeignetes Produkt auf dem Markt.

Fazit von alldem ist: Die Sicherheitstechnik für Kommunikationsnetze wurde erheblich verbessert. Demgegenüber tat sich bei den Bürokommunikationssystemen praktisch nichts.

3. Was wurde aus dem landeseinheitlichen Netz?

Die Pläne der Landesregierung, ein landesweites Netz aufzubauen, nahmen 1986 deutlich konkretere Formen an; zum Teil setzte sie diese auch bereits in die Tat um. Mitte 1986 gab die Landesregierung ihre ursprüngliche Absicht auf, die bestehenden Teilnetze so rasch wie möglich Schritt für Schritt in ein landeseinheitliches Netz zu integrieren. Jetzt heißt die Devise: so rasch wie möglich eine neues, landesweites Sondernetz Umwelt schaffen, in das später einmal die bestehenden Teilnetze integriert bzw. über SNI angekoppelt werden sollen.

3.1 Die Entwicklung im allgemeinen

Noch Ende 1985 gab die Landesregierung den Startschuß für den Aufbau eines landeseinheitlichen Netzes, über das sich in Zukunft die gesamte Kommunikation der Landesbehör-

den abspielen soll. In einem Kabinettsbeschluß legte sie die technischen Regeln, darunter den SNA-Standard für die Datenfernverarbeitung, fest, nach denen in Zukunft im landesweiten Netz die zu versendenden Informationen aufgebaut und transportiert werden sollen. Die Landesregierung wollte also die bislang voneinander getrennten Datennetze der Landesverwaltung – mit Ausnahme der Netze der Polizei, der Hochschulen und des Landesamts für Umweltschutz – rasch auf SNA-Basis umstellen und damit die Voraussetzung für einen Zusammenschluß schaffen. Was dafür im einzelnen zu tun ist, sollte das Staatsministerium in die Wege leiten. Es erhielt zugleich den Auftrag, für das landesweite Netz ein Datensicherungskonzept zu erarbeiten.

Dieser Kabinettsbeschluß war alarmierend. Denn mit ihm stellte die Landesregierung die entscheidenden Weichen für eine Realisierung des landesweiten Netzes ohne die gebotenen Datensicherungsmaßnahmen: Mit den damals verfügbaren Techniken ließ sich ein solches Datennetz nicht sicher betreiben. Sie kannten noch keine zuverlässige Methode, in einem so großen und komplexen Netz sicherzustellen, daß jede Behörde und jeder ihrer Mitarbeiter jeweils nur die Informationen erhalten und verarbeiten kann, die seinem Aufgabenbereich entsprechen. Insbesondere konnte sie nicht verhindern, daß der Netzverwalter, der die Datenflüsse im Netz zu lenken und zu überwachen hat, durch ein paar Handgriffe den Mitarbeitern einer Behörde den Zugriff auf die Daten vieler anderer Behörden öffnet und daß Unbefugte die transportierten Daten während ihrer Zwischenspeicherung in einem Netzcomputer auswerten oder verfälschen. Diese technischen Schwächen haften zwar im Prinzip auch den verschiedenen, bereits seit Jahren betriebenen Teilnetzen an. Da diese Netze jedoch erheblich kleiner sind, bislang keine Bürokommunikation enthalten und vom vorhandenen Personal noch überschaut werden können, ist ihr Betrieb – einmal von den vielen von mir festgestellten Sicherheitsmängeln abgesehen – grundsätzlich vertretbar. Anders bei dem landeseinheitlichen Netz: der Kabinettsbeschluß lief darauf hinaus, daß die Landesverwaltung von einer weniger riskanten Form der Datenverarbeitung auf eine unvergleichlich riskantere Form umsteigen sollte. Ein solches Vorgehen aber wäre mit § 8 LDSG unvereinbar.

Ich bat deshalb das Staatsministerium Anfang 1986 dafür zu sorgen, daß der Kabinettsbeschluß einstweilen nicht vollzogen wird. Hierzu war das Staatsministerium nicht bereit. Es meinte zum einen, die vorhandene SNA-Technik reiche aus. Damit verkannte es die ungleich höheren Risiken eines landesweiten Netzes – eine Tatsache, die es, wenn auch nicht ausdrücklich, inzwischen akzeptiert. Zum anderen verwies das Staatsministerium auf das beabsichtigte EUREKA-Projekt „Datenschutz in offenen Netzen", das angeblich bereits in zwei Jahren Lösungen anbieten könne. Damit waren meine Sorgen freilich keineswegs entkräftet. Denn alles sprach um die Jahreswende 1985/86 dafür, daß die Umstellung der Einzelnetze auf SNA relativ rasch abgeschlossen ist und der Betrieb des landesweiten Netzes, wenn das Kabinett dafür den Startschuß gibt, eher aufgenommen werden kann, als die erforderlichen Datensicherungsmaßnahmen – sei es durch ein EUREKA-Projekt oder auf andere Weise – vorliegen.

Im Laufe der Monate bahnte sich dann aber ein Sinneswandel des Staatsministeriums an: Die von ihm in Auftrag gegebene Studie, wie der Zusammenschluß der bislang getrenn-

ten Netze der Landesverwaltung im einzelnen technisch erfolgen soll, wies in großer Deutlichkeit auf das hohe Gefahrenpotential des damit entstehenden Landesverwaltungsnetzes und die Notwendigkeit hin, deshalb spezielle neue, noch zu entwickelnde Sicherheitstechniken einzusetzen. Kein Wunder, daß ich diese seit Juli 1986 vorliegende Studie erst Monate später als die anderen Ressorts und zudem erst nach wiederholter Aufforderung vom Staatsministerium erhielt. Sicherlich trugen aber die Aussagen in dieser Studie mit dazu bei, daß das Staatsministerium der Datenzentrale im Spätherbst den Auftrag erteilte, ein Datenschutz- und Sicherheitskonzept für ein Landesverwaltungsnetz zu erarbeiten. Erste Ansätze auf dem Weg in die richtige Richtung sind damit erkennbar.

3.2 Das Landesverwaltungsnetz - Teil Umwelt

Weniger die ungenügende Technik der Datensicherung als die negativen Erfahrungen mit dem unzulänglichen Meldedienst im Lande während der Reaktorkatastrophe von Tschernobyl waren für die Landesregierung Anlaß, ihr Konzept zum Aufbau des landeseinheitlichen Netzes entscheidend zu ändern. Ziel der Landesregierung ist jetzt, vordringlich ein landesweites Spezialnetz Umwelt zu schaffen, an das aber nicht nur Landesbehörden, z. B. die Landesanstalt für Umweltschutz, Gewerbeaufsichtsämter, Gesundheitsämter, medizinisches Landesuntersuchungsamt, sondern auch die Kommunen angeschlossen sind. Die Landesregierung will dieses Spezialnetz so auslegen, daß die verschiedensten Meßstellen im Lande ihre Meßwerte dem „Umweltministerium" jederzeit melden und das Ministerium die Auswertung dieser Meßdaten und andere wichtige Umweltinformationen möglichst rasch an nachgeordnete Behörden bis hinunter zu den Gemeinden und diese wiederum Nachrichten nach oben senden können. Über dieses Umweltnetz sollen nicht nur Meßwerte, z. B. Daten zur Beschaffenheit von Luft, Wasser und Boden, und andere Sachinformationen fließen, sondern auch – ganz anders, als es lange Zeit aus dem Staatsministerium zu hören war – Personendaten. Außerdem will die Landesregierung von Anfang an im Umweltnetz Bürokommunikation einsetzen.

Eine, wenn nicht die Hauptschwierigkeit dieses Vorhabens für den Datenschutz ist die geplante Einbeziehung der Gemeinden in das Netz. Wenn auch der dafür einzuschlagende Weg noch nicht festgelegt ist, läuft alles darauf hinaus, daß die bislang getrennten Netze der 10 kommunalen Rechenzentren an das neue Umweltnetz des Landes angeschlossen werden. Ein solches staatlich/kommunales Netz wäre in seinen Dimensionen vergleichbar mit dem geplanten landeseinheitlichen Netz für die Landesverwaltung: Da sich nämlich nahezu alle der 1111 Gemeinden, dazu noch eine Reihe von Landkreisen und Zweckverbänden der Dienste der kommunalen Rechenzentren für die unterschiedlichsten Aufgaben bedienen, entstünde auch hier ein Netz mit einem komplizierten, technisch noch nicht beherrschbaren Gefüge von Berechtigungen und Zuständigkeiten der Bediensteten. Daraus resultiert die Gefahr, daß aus dem Umweltnetz des Landes auf die Vielzahl höchst sensibler Daten der Kommunen – z. B. der Zulassungsstellen, Krankenhäuser, Sozialämter und Einwohnermeldeämter – in den kommunalen Netzen zugegriffen wird. Ebenso wäre nicht ausgeschlossen,

daß dann Benutzer eines kommunalen Netzes auf die Daten eines anderen kommunalen Netzes zugreifen. Deshalb darf man einen solchen Zusammenschluß – wenn überhaupt – allenfalls dann ins Auge fassen, wenn es spezielle Datensicherungstechniken gibt, die diese Risiken von vornherein ausschließen und sicherstellen, daß jeder Benutzer weiterhin nur die Daten verarbeiten kann, die seinem Aufgabenbereich entsprechen.

Auch die Landesregierung weiß, daß der Anschluß der Gemeinden an das Umweltnetz des Landes kurzfristig auf keinen Fall zu erreichen ist. Deshalb will sie das Umweltnetz zunächst auf die Landesverwaltung beschränken und die nötigen Umweltinformationen an die Kommunen über den Telexdienst der Bundespost abwickeln; im Notfall soll es ergänzend dazu „tägliche Lagebesprechungen" mit den Gemeinden geben, weil hier auch der „persönliche Kontakt" wichtig sei – so heißt es in einer vom Ministerrat gebilligten Kabinettsvorlage des Ernährungsministeriums. Recht und gut: hätte die Landesregierung nicht den Plan, auch auf ihrem auf die Landesverwaltung beschränkte Sondernetz Umwelt die Bürokommunikation einzusetzen, wäre dieses Sondernetz für den Datenschutz kein besonderes Problem. Denn selbst wenn Personendaten darüber fließen, läßt sich ein solches Netz mit den herkömmlichen Mitteln der Datensicherung hinreichend sicher betreiben. Sobald aber die Bürokommunikation hinzukommt, stellen sich auch hier im Prinzip alle ungelösten Datenschutzprobleme bei deren Einsatz, die ich im letzten Tätigkeitsbericht beschrieb.

3.3 Auf dem Weg zum Landesrechenzentrum?

Ob die Landesregierung mit ihrem Ziel, ein zentral betriebenes landeseinheitliches Netz zu schaffen, zugleich auch die gesamte Datenverarbeitung der Landesverwaltung zentralisieren will, liegt bislang im Dunkeln. Jedenfalls ist die Beibehaltung der verschiedenen Rechenzentren in der Landesverwaltung für die Landesregierung alles andere als eine ausgemachte Sache. Zum einen ist das Staatsministerium zur Zeit dabei, mit Hilfe eines Unternehmensberaters die gegenwärtige Struktur der Rechenzentren im staatlichen Bereich zu analysieren und Vorschläge für die künftige Gestaltung zu erarbeiten. Zum anderen kommt kein Ministerium – welches auch immer eines der Rechenzentren in seinem Geschäftsbereich ausbauen will – so recht voran: das Staatsministerium schiebt allem mit dem Hinweis auf die laufende Untersuchung einen Riegel vor. So konnte z. B. das Ernährungsministerium nicht einen neuen Großrechner für sein Rechenzentrum beschaffen. Zum dritten sind gegenwärtig im Auftrag der Landesregierung Datenverarbeitungssysteme in Vorbereitung, die sich ohne zentrale Datenhaltung kaum realisieren lassen: so ist ein erklärtes Ziel, mit Hilfe des Haushalts-Management-Systems – einem wesentlichen Teil des Landessystemkonzepts – jederzeit den Ausgabenstand bei jeder Landesbehörde, auch wenn sie im hintersten Winkel des Landes liegt, für die anstehenden Regierungsentscheidungen abrufen zu können. Dies geht – so auch die Ansicht des Finanzministeriums – nur, wenn alle Haushaltsdaten in einem Rechenzentrum zusammenfließen. Zum anderen richtete die Landesregierung im Gemeinschaftsrechenzentrum des Landes, das Sozial-, Justiz-, Wirtschafts-, Finanz- und Innenministerium gemeinsam betreiben, das

Netzwerk Management-Zentrum für Kontrolle und Steuerung des Umweltnetzes ein und installierte dafür jüngst eigens einen neuen Großrechner. Wie nun auch die Entscheidung der Landesregierung über die Struktur der Rechenzentren ausfallen mag, eines muß jetzt schon gesagt sein: Ein zentrales Rechenzentrum der Landesverwaltung, in dem im Prinzip alle Landesbehörden ihre Daten speichern und verarbeiten lassen müßten, wäre – selbst wenn z. B. die Polizei ihr Rechenzentrum im Landeskriminalamt behielte – mit ungleich höheren Risiken behaftet als die derzeit betriebenen Rechenzentren:

- Eine einzige Schwachstelle im Sicherheitsprogramm eines solchen Landesrechenzentrums könnte sich dann auf die Sicherheit aller Daten auswirken – ganz gleich, ob es Steuerdaten der Finanzämter, Lehrerdaten der Oberschulämter, Daten aus anderen Personalverwaltungssystemen, Angaben gerichtlicher Mahnverfahren oder gar die vielen Personendaten für Zwecke der Statistik bis hin zu den Volkszählungsdaten sind.
- Die einzelnen Verwaltungen, z. B. die Oberfinanzdirektionen oder das Statistische Landesamt, hätten praktisch keinen unmittelbaren Einfluß mehr auf die Verarbeitung ihrer Daten im Landesrechenzentrum. Dieses könnte nämlich grundsätzlich jedem beliebigen Teilnehmer am Netz den Zugriff auf jedes beliebige Einzeldatum erlauben, ohne daß dies der Besitzer der Daten verhindern kann. Es könnte beispielsweise irgendeinen beliebigen Benutzer eines Terminals – sei er im Ministerium, beim Finanzamt oder Statistischen Landesamt – berechtigen, auf alle im Landesrechenzentrum gespeicherten Daten zuzugreifen. Mit den heutigen technischen Methoden gelänge es nicht einmal in jedem Fall, einen solchen Mißbrauch nachträglich nachzuweisen.

Es gilt deshalb, jeder Entwicklung rechtzeitig entgegenzusteuern, an deren Endpunkt ein Landesrechenzentrum mit seinem geballten Wissen über Bürger des Landes stehen könnte.

4. Bürokommunikation

Während die Landesregierung in ihrer Stellungnahme zu meinem letzten Tätigkeitsbericht behauptete, die technischen und organisatorischen Probleme beim Einsatz der Bürokommunikation in der öffentlichen Verwaltung seien so, wie ihn die Landesregierung anpeilt, bereits mit der vorhandenen Technik lösbar, sieht es jetzt anders aus: inzwischen wissen die High-Tech-Verfechter, daß der Einsatz der Bürokommunikation in der Verwaltung nicht so einfach geht wie in der Wirtschaft, und sehen, daß die auf dem Markt befindlichen Systeme den Anforderungen der öffentlichen Verwaltung nicht genügen. Das Staatsministerium erarbeitete deshalb einen ersten Anforderungskatalog und will nun Hersteller bewegen, auf dessen Basis ihre Produkte so weiter zu entwickeln, daß sie sich mit der Zeit auch für den Einsatz in der öffentlichen Verwaltung eignen. Zunächst ist dabei allerdings nur an eine Teilfunktion gedacht, die elektronische Post.

Auch die Realisierung des Szenarios „Büroautomation bei den Regierungspräsidien" des Landessystemkonzepts läuft langsamer als geplant. Das Innenministerium weiß noch nicht einmal, mit welchem System es dieses Projekt durchführen lassen will. Es ist gerade dabei, durch einen Test der auf dem Markt befind-

lichen Produkte herauszufinden, welches sich am ehesten für den Erprobungsversuch bei den Regierungspräsidien mit seinen reduzierten Anforderungen eignet. Wie sich das Innenministerium auch entscheiden wird, auf alle Fälle muß gelten: Weil die Regierungspräsidien nach den Vorstellungen des Innenministeriums das ausgewählte System anhand der täglichen Arbeitsabläufe – also nicht mit Hilfe von Testmaterial – erproben sollen und dabei auch viele Informationen über Bürger und Bedienstete anfallen, müssen sie bei dem Projekt von Anfang an die Regeln des Datenschutzes beachten. Zum einen sind die nach § 8 LDSG erforderlichen Datensicherungsmaßnahmen zu ergreifen, z. B. zu protokollieren, wer wann welche Informationen eingab. Darüber hinaus sind aber auch zusätzlich Sicherheitsvorkehrungen erforderlich, um den besonderen Risiken der Bürokommunikationssysteme zu begegnen. Insbesondere ist notwendig,

- durch Abschottungsmaßnahmen sicherzustellen, daß niemand unzulässig Informationen über Bürger zusammenführt,
- dafür zu sorgen, daß Systemverwalter und Wartungstechniker nicht ohne weiteres auf Personendaten zugreifen können und
- die Systemverwalterfunktionen, z. B. die Vergabe von Berechtigungen, besonders zu schützen und im einzelnen zu protokollieren.

Sollte dies in dem eng begrenzten Bereich, in dem die Regierungspräsidien die Bürokommunikation erproben wollen, technisch nicht möglich sein, müssen sie darauf verzichten, mit Echtdaten über Bürger zu arbeiten. Unabhängig davon haben sie sicherzustellen, daß die bei der Erprobung des Bürokommunikationssystems zwangsläufig anfallenden automatischen Aufzeichnungen über die Tätigkeit der einzelnen Mitarbeiter nicht zu deren Verhaltens- und Leistungskontrolle verwendet werden.

5. Zur Unzulänglichkeit der rechtlichen Rahmenbedingungen

Wer diese Entwicklung seit dem letzten Tätigkeitsbericht betrachtet, muß zugeben, daß die Landesregierung inzwischen die Einsatzmöglichkeiten der neuen Kommunikations- und Informationstechnik nüchterner und realistischer sieht. Von mancher „Fehleinschätzung" mußte nicht ich, sondern sie Abschied nehmen [1]. Die Probleme der Datensicherung, also der technischen und organisatorischen Vorkehrungen zum Schutz gegen eine unbefugte Verwendung von Informationen, nimmt sie inzwischen ernster. Man setzt sich damit auseinander und bemüht sich um Lösungen.

Um so bedauerlicher ist andererseits, daß für die Landesregierung die Realisierung des Landessystemkonzepts und die Schaffung eines verfassungskonformen modernen Datenschutzrechts immer noch zwei Paar Stiefel sind. Immer noch verschließt sie die Augen vor dem unmittelbaren Zusammenhang zwischen Technik und Recht. Sie will nicht anerkennen, daß es für die Beurteilung des Landessystemkonzepts ganz entscheidend auch darauf ankommt, welche Stellen welche Informationen zu welchem Zweck erheben, speichern, auswerten und weitergeben dürfen. Gerade aber davon hängt nicht zuletzt auch ab, ob und welche technischen und organisatorischen Schutzvorkehrungen faktisch getroffen werden müssen. Wie soll es möglich sein, die Unbedenklichkeit von Netzen und Kommunikationssystemen zu bescheinigen, wenn noch garnicht präzise festgelegt ist, was dort eigentlich geschehen darf, was verhindert werden muß und nach welchen Spielregeln das Erlaubte abzulaufen hat. Der

1) vgl. Pressemitteilung der CDU-Landtagsfraktion vom 14.1.1986

Staat ist eben nicht, wie die Landesregierung immer wieder meint, mit einem privaten Wirtschaftsunternehmen vergleichbar. Dort können die Daten zwischen den Mitarbeitern frei fließen, weil das Datenschutzrecht einen solchen Betrieb als Einheit bewertet. Die Aufgaben des Staates nehmen dagegen sehr viele einzelne, voneinander organisatorisch und funktional getrennte Stellen wahr. Jede von ihnen ist zur Wahrung der Grundrechte der Bürger verpflichtet und darf deshalb Informationen über einzelne Bürger ohne oder gegen deren Willen nur dann registrieren, nutzen und an andere Stellen weitergeben, wenn ihr ein Gesetz dies ausdrücklich gestattet. Die gegenwärtig geltenden Rechtsvorschriften über die Informationsverarbeitung werden diesem Verfassungsgebot bei weitem noch nicht gerecht. Nicht nur die überfällige Novellierung der allgemeinen Datenschutzgesetze steht noch aus; ebenso fehlen noch für viele Bereiche - etwa Polizei, Verfassungsschutz und Gesundheitswesen - bereichsspezifische Vorschriften, die den dort auftretenden besonderen Risiken für das Grundrecht der Bürger auf Datenschutz Rechnung tragen. Auf dieser absolut unbefriedigenden Gesetzeslage eine umfassende Automatisierung und Vernetzung der Landesverwaltung voranzutreiben, ist nicht verantwortbar. Nach wie vor gilt, was ich bei der Vorstellung meines letzten Tätigkeitsberichts sagte: Die Landesregierung läuft Gefahr, mit ihrem Vorhaben in Gegensatz zu unserer Verfassung zu gelangen.

3. Teil: Volkszählung 1987

1. Zur Situation

Am 25. Mai 1987 wird das Volk gezählt. So will es das Volkszählungsgesetz 1987, das der Deutsche Bundestag am 8. Nov. 1985 mit den Stimmen von CDU/CSU, SPD und FDP gegen die Stimmen der Grünen beschloß. Immer wieder fragen mich Bürger, ob das jetzige Gesetz verfassungsgemäß ist. Sie haben nicht vergessen, daß das Bundesverfassungsgericht 1983 die damals unmittelbar bevorstehende Volkszählung ausgesetzt und bald danach das Volkszählungsgesetz 1983 in Teilen für verfassungswidrig erklärt hat.

1.1 Das Gesetz

Der Deutsche Bundestag war sichtlich bemüht, beim Volkszählungsgesetz 1987 den Vorgaben des Bundesverfassungsgerichts zu entsprechen. Andererseits zeigte er aber keinerlei Neigung, auch nur einen Schritt in Richtung auf mehr Datenschutz zu tun. Nur zweierlei zum Beleg:

- Sehr ernst nahm er es mit dem vom Bundesverfassungsgericht betonten Grundsatz der Trennung von Statistik und Verwaltungsvollzug, dem sog. Abschottungsgebot. Dem Bundestag war klar, daß es hier keine problematischen Regelungen geben durfte, wußte er doch: nur wenn die Bürger wirklich vertrauen können, daß ihre Volkszählungsdaten vor der Verwaltung sicher sind, werden sie bereit sein, wahrheitsgemäße Angaben zu machen. Deshalb entschied er sich für ein striktes Abschottungsgebot und erteilte damit den Forderungen der kommunalen Spitzenverbände nach einer Lockerung, die der Bundesrat und mit ihm die Landesregierung Baden-Württemberg bereit-

willig unterstützt hatten, eine klare Absage. Freilich hatte es der Bundestag in dieser Frage letztlich einfach. Er mußte keine konkreten Lösungen präsentieren, sondern konnte dies alles den Ländern überlassen. So sieht es die Regelung der Gesetzgebungskompetenzen im Grundgesetz vor.

- Zu kurz kam dagegen im Bundestag die Methodendiskussion: das Problem, ob es wirklich notwendig ist, daß jeder Bürger jede Frage des Volkszählungsbogens beantworten muß, wischte man mit dem Hinweis vom Tisch, die Totalerhebung habe das Verfassungsgericht wegen des gegenwärtigen Erfahrungs- und Erkenntnisstands in der amtlichen Statistik und Sozialforschung noch für zulässig gehalten. Keine Neigung bestand auch, meine in der Sachverständigenanhörung aufgeworfene Frage nach dem Umfang der Regelungsbefugnis des Bundesgesetzgebers zu vertiefen. Für mich ist es noch keine ausgemachte Sache, daß der Bund trotz seiner auf die „Statistik für Bundeszwecke" beschränkten Gesetzgebungskompetenz eine Totalerhebung für einzelne Merkmale bloß deshalb vorschreiben darf, weil eine solche für Zwecke der Länder und der Kommunen erforderlich ist, während für Zwecke des Bundes eine Stichprobenerhebung ausreichen würde. Die Aussagen des Bundesverfassungsgerichts sind insoweit nicht eindeutig.

Wie dem auch sei: Das Volkszählungsgesetz 1987 fiel jedenfalls so aus, wie es das Bundesverfassungsgericht vorgab. Außer dem Abschottungsgebot legt es fest, daß und wie die auskunftspflichtigen Bürger über ihre Rechte zu belehren sind, verlangt eine Trennung und frühzeitige Löschung der Identifizierungsmerkmale und setzt für den Einsatz der Zähler Grenzen. Es macht ferner einen Vergleich der Volkszählungsdaten mit dem Melderegister unmöglich und läßt die Weitergabe von Einzelangaben aus der Volkszählung an Ministerien des Bundes oder der Länder nicht mehr zu; die Weitergabe an Gemeinden für statistische Zwecke knüpft es an strenge Voraussetzungen.

1.2 Sein Vollzug

Damit ist freilich die Kuh noch nicht vom Eis: Für das Gelingen der Volkszählung ist genauso entscheidend, wie die Landesregierung die Vorgaben des Volkszählungsgesetzes 1987 umsetzt und wie die Bevölkerung bei der Zählung mitmacht.

- Die Abschottung

  Die Gretchenfrage an die Landesregierung lautete von Anfang an, wie sie es mit dem Trennungsgebot von Statistik und Verwaltungsvollzug in der kritischen Erhebungsphase halten will. Sie reicht von der Auswahl und dem Einsatz der Zähler über das Austeilen der leeren und Einsammeln, Sichten und Ordnen der ausgefüllten Volkszählungsbogen in der Erhebungsstelle bis hin zu deren Zuleitung an das Statistische Landesamt. Rasch stand fest: die Landesregierung bleibt im Prinzip bei der Organisationsform früherer Volkszählungen. Die Städte und Gemeinden sollen wie eh und je die Zählung vor Ort durchführen; nur an Stelle kleiner Gemeinden sollen erstmals die Landkreise treten. Pate bei dieser Lösung stand keineswegs bloß der Datenschutz. Andere, für die Beziehungen zwischen Land und Kommunen viel wichtigere Probleme beeinflußten zumindest unterschwellig den Entscheidungsprozeß:

- Zum einen fühlen sich die Gemeinden und Landkreise für ihre Mitwirkung bei der Volkszählung vom Land nicht ausreichend entschädigt. Vor allem schmerzt es die Gemeinden, daß man sie nicht mehr wie früher außer mit Geld auch mit Volkszählungsdaten entschädigt, die sie zur Bereinigung ihrer Einwohnermelderegister und für andere eigene Zwecke nutzen durften. Denn diesem begehrten Datenfluß schob das Volkszählungsurteil einen Riegel vor.
- Zum anderen plagt die Städte und Gemeinden mehr als früher die Sorge um ihre Einwohnerzahl. Diese muß das Statistische Landesamt aufgrund der Ergebnisse der Volkszählung 1987 neu festsetzen. Sie ist auf Jahre hinaus Grundlage für den Finanzausgleich und die Aufteilung des Steueraufkommens zwischen Bund, Ländern und Gemeinden. Jeder bei der Volkszählung „vergessene" Einwohner kann für eine Gemeinde Jahr für Jahr einen Einnahmeausfall in der Größenordnung von bis zu 1000,– DM bedeuten.

Bei den meisten Gemeinden überwiegt trotz ihrer veränderten Einstellung zur Volkszählung zwar immer noch das Interesse, an der Zählung mitzuwirken, um nicht bei der Ermittlung der Einwohnerzahl ganz abseits zu stehen. Das verringerte Eigeninteresse der Gemeinden ist aber andererseits sicher mit ein Grund, warum sich die Landesregierung für die Wünsche der kommunalen Seite so aufgeschlossen zeigte. Nicht immer war dies gut für den Datenschutz.

– Akzeptanz

Wie die Volkszählung 1987 bei der Bevölkerung ankommt, weiß heute noch keiner so recht. Natürlich höre ich immer wieder auch kritische Stimmen: viele sind durch die hektischen Auseinandersetzungen der letzten Jahre immer noch verunsichert; gerade ältere Menschen haben wenig Vertrauen in das Vorhaben. Andere irritiert, daß sie praktisch dieselben Fragen beantworten müssen, wie sie der Volkszählungsbogen 1983 vorsah, und fragen enttäuscht, was eigentlich der Karlsruher Richterspruch bewirkt hat. Schon deshalb wäre es gut gewesen, wenn der Gesetzgeber dem Rat mancher Sachverständigen gefolgt und sein Erhebungsprogramm reduziert hätte. Natürlich war auch das monatelange Gerangel zwischen Land und Kommunen wegen der Kostenerstattung nicht vertrauensbildend. Erhebliche Irritationen löste die dabei gemachte Äußerung des Stuttgarter Oberbürgermeisters und gleichzeitigen Präsidenten des Städtetags aus, er gäbe eine erneute Verschiebung der Volkszählung zu erwägen. Unbehagen ruft auch der Plan mancher Städte und Gemeinden hervor, die EDV zur Kontrolle des Rücklaufs der ausgefüllten Volkszählungsbogen einzusetzen und deshalb die Namen und Anschriften aller auskunftspflichtigen Bürger in Rechenzentren zu speichern. Schließlich gibt es erklärte Gegner der Volkszählung, die bereits wieder zum Boykott aufrufen. Ob die im Gegenzug gestartete Informationskampagne der Statistischen Ämter des Bundes und der Länder geglückt ist, mag jeder für sich entscheiden. Ebenso muß sich erst zeigen, ob sie die gegenläufigen Strömungen auffangen kann. Auffallend war, wie die Vertreter der amtlichen Statistik immer wieder versuchten, die Datenschutzbeauftragten für ihre Werbeaktion zu vereinnahmen.

2. Die Probleme

Die Weichen für die Organisation der Volkszählung in Baden-Württemberg stellten Landesregierung und Finanzministerium durch die Verordnung zur Durchführung des Volkszählungsgesetzes vom 30. Juni 1986 (GBl. S. 245) und zwei Verwaltungsvorschriften dazu – die eine vom 1. Okt. 1986 (GABl. S. 945), die andere nicht veröffentlichte vom 9. Okt. 1986. Weitere Verwaltungsvorschriften sollen folgen. Befriedigen können die bisher erlassenen Regelungen nur begrenzt. Man gab mir zwar im allgemeinen Gelegenheit, zu den Entwürfen Stellung zu nehmen, hörte sich in zahlreichen Besprechungen unsere Vorstellungen an, nahm auch die schriftlichen Äußerungen entgegen. Doch in den entscheidenden Punkten bewirkte dies alles so gut wie nichts; hier hatten die kommunalen Landesverbände und die Statistiker das Ohr des Finanzminsters.

2.1 Die Abschottung: wasserdicht oder lückenhaft?

Damit die Volkszählungsdaten nicht in Verwaltungsmaßnahmen einfließen – seien es beispielsweise Bescheide des Finanz-, Sozial-, Wohnungs-, Einwohnermeldeamts und Maßnahmen der Polizei –, müssen die Erhebungsstellen von anderen Verwaltungsstellen räumlich, organisatorisch und personell strikt getrennt sein. So verlangt es das Volkszählungsgesetz 1987. Die Regelungen der Landesregierung über die räumliche und organisatorische Trennung der Erhebungsstelle entsprechen diesem Gebot; auch dürfte es im allgemeinen keiner Behörde Schwierigkeiten bereiten, sie zu beherzigen. Anders verhält es sich mit der personellen Trennung: sie bedeutet, daß Mitarbeiter der Erhebungsstelle nicht gleichzeitig irgendwelche Verwaltungsaufgaben wahrnehmen dürfen. Will eine Behörde für ihre Erhebungsstelle nicht eigens neue Mitarbeiter einstellen, muß sie bereits vorhandene Mitarbeiter aus ihrem Aufgabengebiet herauslösen und von ihren üblichen Aufgaben völlig freistellen. Kleine Ämter mit wenig Mitarbeitern tun sich damit schwer; manchen wird es objektiv unmöglich sein. Dieser Situation mußte die Landesregierung bei ihrer Entscheidung, wo die örtlichen Erhebungsstellen einzurichten sind, gerecht werden.

2.1.1 Erhebungsstelle: Gemeinde oder Landkreis?

Ihre Entscheidung fiel so aus: Erhebungsstellen sind aufgrund von § 3 Abs. 1 DVO alle Gemeinden mit mehr als 8000 Einwohnern – es sind 263 im Land –, im übrigen die Landkreise. Bereits dieser Einwohnerschnitt ist unbefriedigend, weil in der Regel nur Gemeinden ab etwa 20 000 Einwohnern so viele Mitarbeiter haben, daß sie einige davon für die Dauer der Volkszählung von ihren üblichen Aufgaben völlig freistellen und der Erhebungsstelle zuweisen können. Ich hatte deshalb stets eine Anhebung der Einwohnergrenze gefordert, freilich leider vergeblich.

Doch damit nicht genug: Die Landesregierung ermächtigte in § 3 Abs. 4 DVO außerdem die Landkreise, auch Gemeinden unter 8000 Einwohnern oder Verwaltungsgemeinschaften zur Erhebungsstelle zu bestimmen, wenn diese bis 15. Aug. 1986 einen Antrag stellen und dabei nachweisen, daß bei ihnen die Trennung der Erhebungsstelle von der übrigen Verwaltung gewährleistet ist. Noch ehe die Verordnung verkündet war, emp-

fahl der Landkreistag mit Rundschreiben vom 2. Juli 1986 den Landkreisen, ihre Gemeinden zu ermuntern, selbst die Aufgabe der örtlichen Erhebungsstelle zu übernehmen. Damit ja auch alles reibungslos laufen kann, fügte er ein vom Statistischen Landesamt entworfenes Erklärungsmuster bei. Rasch kam die Lawine ins Rollen; ihre Wirkung war enorm: die Landratsämter bestimmten nicht weniger als 659 der insgesamt 848 Gemeinden unter 8000 Einwohner zu Erhebungsstellen; für 46 weitere Gemeinden übertrugen sie diese Aufgabe der Verwaltungsgemeinschaft. 13 der 35 Landkreise in Baden-Württemberg sind infolgedessen für keine einzige ihrer Gemeinden mehr Erhebungsstelle. Damit war die Regelung des § 3 Abs. 4 DVO ins Gegenteil verkehrt und das Gebot der personellen Trennung der Erhebungsstelle vom Verwaltungsvollzug in Gefahr. Schon als sich diese alarmierende Entwicklung abzuzeichnen begann, entschloß ich mich, durch eine Umfrage bei den Landkreisen vom 1. Sept. 1986, die der Landkreistag gerne unterbunden hätte, zu untersuchen, in welchem Umfang die Landkreise die Aufgaben der Erhebungsstelle auf die Gemeinden delegiert und welchen Maßstab sie dabei im einzelnen an den Nachweis der personellen Trennung angelegt hatten. Was die große Zahl der Delegationen schon anzeigte, bestätigte sich: längst nicht alle Landkreise setzten sich ernsthaft mit den Schwierigkeiten auseinander; viele machten es sich einfach und begnügten sich mit der formularmäßigen Versicherung der Gemeinde, es habe alles seine Ordnung. Diese Verfahrensweise rechtfertigten die Landkreise z. B. mir gegenüber so:

> „Das Landratsamt geht grundsätzlich davon aus, daß selbständige Gemeinden in Baden-Württemberg auch dazu in der Lage sind, die rechtlichen Bestimmungen im Zusammenhang mit der Volkszählung 1987 einzuhalten und umzusetzen. Eine besondere Prüfung der Einhaltung der Datenschutzbestimmungen wurde deshalb nicht für erforderlich gehalten."

> „Die Gemeinden ... mußten schriftlich bestätigen, daß die räumliche, organisatorische und personelle Trennung der örtlichen Erhebungsstellen von den anderen Verwaltungsstellen der Gemeinden nach Maßgabe des § 4 der Verordnung ... gewährleistet ist. Da das Landratsamt aufgrund der bisherigen Zusammenarbeit mit den Gemeinden des Landkreises keinen Grund hatte, an der schriftlichen Bestätigung der Bürgermeister zu zweifeln, wurde diesen Gemeinden die örtliche Durchführung der Volkszählung übertragen."

> „Im jetzigen Stadium halten wir es noch nicht für sinnvoll, konkrete Überprüfungen vorzunehmen."

Von Nachweis der personellen Trennung kann hier keine Rede sein. Ich wandte mich deshalb am 24. Okt. 1986 an den Herrn Finanzminister und den Herrn Innenminister, die zusammen für die Durchführung der Volkszählung im Lande verantwortlich sind, und bat sie dafür zu sorgen, daß die notwendige Korrektur so rasch wie möglich im Wege der Rechtsaufsicht erfolgt. Die Antwort der Ressorts vom 17. Dez. 1986 befriedigt nicht. Obwohl ihre Recherchen meine Feststellungen zur Praxis der Landratsämter bestätigten, fühlten sie sich in keinem einzigen Fall bemüßigt, die Zuständigkeitsübertragung rückgängig zu machen. Sie begnügten sich vielmehr damit, die Landratsämter auf ihre Pflicht hinzuweisen, bei den Gemeinden die Beach-

tung des Abschottungsgebots zu überprüfen. Dadurch sind meine Bedenken gewiß nicht ausgeräumt. Die Frage, ob wirklich in jedem Fall einer Delegation die Erhebungsstelle richtig abgeschottet wird, steht nach wie vor unbeantwortet im Raume. Dabei kann auch nicht der Hinweis des Finanzministeriums weiterhelfen, die Nachbarländer Hessen und Bayern hätten ebenfalls kleine Gemeinden zu Erhebungsstellen bestimmt. Abgesehen von der unterschiedlichen kommunalen Struktur in den einzelnen Bundesländern könnte doch ein Sündenfall in einem Land nicht Gleiches im anderen rechtfertigen.

2.1.2 Die Mitarbeiter

Wenn sich schon nicht vermeiden läßt, daß Gemeinden und Landkreise örtliche Erhebungsstellen sind und dahin einen Teil ihrer Mitarbeiter abstellen müssen, dann muß man wenigstens dafür sorgen, daß alles, was diese Mitarbeiter in der Erhebungsstelle erfahren, nicht doch irgendwie in Maßnahmen der Verwaltung einfließt:

- Interessenkollisionen möglich

  Mit dem Erlaß von § 4 Abs. 4 DVO tat die Landesregierung einiges, aber leider nicht alles, was dazu notwendig gewesen wäre. Nach dieser Vorschrift müssen die Mitarbeiter der Erhebungsstelle zuverlässig und verschwiegen sein; sie dürfen während ihrer Tätigkeit für die Erhebungsstelle keine anderen Verwaltungsaufgaben wahrnehmen; vor allem ist ihnen auch untersagt, ihre Erkenntnisse über Bürger aus der Volkszählung später in Verwaltungsentscheidungen einfließen zu lassen. Nicht verbietet die Regelung dagegen, in der Erhebungsstelle auch solche Mitarbeiter einzusetzen, bei denen infolge der Art ihrer beruflichen Tätigkeit oder aus anderen Gründen die Gefahr besteht, daß sie ihr Wissen aus den ausgefüllten Volkszählungsbogen eines Tages gegen den Bürger verwenden. Solche Interessenkonflikte können vor allem bei Mitarbeitern auftreten, die üblicherweise im Einwohnermelde-, Sozial-, Steuer- oder Ordnungsamt der Gemeinde arbeiten. Meine nachhaltige Forderung, in der Durchführungsverordnung diesen Personenkreis von einer Tätigkeit in der Erhebungsstelle ausdrücklich auszuschließen, fand leider kein Gehör. Nach einigem Hin und Her empfahl das Finanzministerium lediglich den Gemeinden in seiner Verwaltungsvorschrift, in der Erhebungsstelle keine Mitarbeiter aus dem Bereich des Einwohnermeldewesens einzusetzen, „sofern dies die personelle Ausstattung der Körperschaft zuläßt". Dies reicht nicht aus. Diese letztlich unverbindliche Empfehlung gibt keine Garantie, daß nichts aus den ausgefüllten Volkszählungsbogen in Verwaltungsentscheidungen einfließt. Das gesetzliche Verwertungsverbot allein vermag dies nicht sicher zu verhindern. Denn in die Verwaltungsentscheidungen eines Mitarbeiters werden immer auch seine beruflichen Erfahrungen mit einfließen – ganz gleich, ob ein solches Verwertungsverbot besteht oder nicht. Wie schrieb mir doch einmal ein Oberbürgermeister, als es um ein Verwertungs-

verbot in anderem Zusammenhang ging: „Beim besten Willen ist es mir nicht gelungen, bis heute zu vergessen, was mein Gedächtnis beim Durchlesen ... bemerkt hat." Deshalb gilt es, bereits bei der Auswahl der Mitarbeiter der Erhebungsstelle solchen Situationen vorzubeugen. Dies verlangt das Volkszählungsgesetz 1987 bei der Auswahl der Zähler ausdrücklich, obwohl diese nur einen Bruchteil der Erhebungsunterlagen zu Gesicht bekommen, mit denen die Mitarbeiter der Erhebungsstelle umgehen.

- Kein Hin und Her

Wer meint, in § 4 Abs. 4 DVO sei klargestellt, daß Mitarbeiter einer Gemeinde nicht je nach Arbeitsanfall zwischen ihrem Arbeitsplatz in der Erhebungsstelle und ihrem üblichen Arbeitsplatz hin und her pendeln können, irrt. Obwohl gerade das Verbot eines Pendelbetriebs die personelle Trennung ausmacht, unterläuft das Finanzministerium inzwischen die von ihm selbst erarbeitete Rechtsnorm: Anstatt in seiner Verwaltungsvorschrift von Anfang an klipp und klar zu sagen, daß es weder einen tageweisen noch einen stundenweisen Wechsel eines Mitarbeiters zwischen Erhebungsstelle und üblichem Arbeitsplatz geben darf, schließt es in Nr. 1.3 VwV-VZG 1987 lediglich den stundenweisen Wechsel ausdrücklich aus. Meinem Hinweis, zum tageweisen Wechsel sei eine entsprechende Aussage nötig, folgte es nicht - in voller Absicht, wie sich inzwischen herausstellte. Einem Rundschreiben des Landkreistags vom 4. Aug. 1986 mußte ich nämlich zu meiner Überraschung entnehmen:

> „Das Finanzministerium hält ... einen tageweisen Wechsel zwischen Erhebungsstelle und übriger Verwaltung für zulässig. Wir begrüßen diese Auffassung, welche die personelle Disposition wesentlich erleichtert."

Auf meine Nachfrage, ob dies tatsächlich die Haltung des Finanzministeriums sei, ließ es mich wissen, es halte einen tageweisen Wechsel mit dem personellen Abschottungsgebot für vereinbar, da „eine hinreichende zeitliche Zäsur zwischen der Tätigkeit in der Erhebungsstelle und der in anderen Verwaltungsstellen gewährleistet ist" - ganz so, als ob der Mitarbeiter am nächsten Morgen nicht mehr weiß, was er tags zuvor in der Erhebungsstelle erfahren hat. Hält man es mit dem Finanzministerium, könnten sich beispielsweise die Mitarbeiter des Einwohnermelde-, Sozial-, Steuer- und Ordnungsamts im täglichen Wechsel in der Erhebungsstelle ablösen. Eine solche Verfahrensweise würde das Gebot der personellen Trennung zur Makulatur machen. Daran ändert auch nichts, wenn das Finanzministerium infolge meines Protestes nunmehr erwägt, die kommunalen Landesverbände auf den Ausnahmecharakter eines tageweisen Wechsels besonders hinzuweisen. Denn eigentlich sollte das Finanzministerium doch auch wissen, daß der deutsche Bundestag bei den Beratungen des Volkszählungsgesetzes 1987 den Versuchen der kommunalen Seite, das personelle Trennungsgebot aufzuweichen, eine strikte Absage erteilte und Ausnahmen ausschließen wollte. Doppelbödiger geht es kaum mehr: einerseits der

klare Wortlaut des § 4 Abs. 4 Satz 2 DVO, auf den sich immer offiziell verweisen läßt, andererseits der verstohlene Wink an die kommunale Seite, man brauche es nicht so genau zu nehmen.

2.2 Die Wohnung der Zähler – 150 000 Zwischenlager

Bürger, die ihre ausgefüllten Erhebungsbogen dem Zähler mitgeben, sollten eigentlich darauf vertrauen können, daß dieser sie sofort dorthin bringt, wo sie zunächst am sichersten sind – nämlich in der Erhebungsstelle. Dem ist jedoch nicht so: nach § 7 Abs. 1 DVO sind die Zähler lediglich verpflichtet, „unverzüglich nach Abschluß der Erhebung" die ausgefüllten Erhebungsbogen abzuliefern. Abgeschlossen ist die Erhebung für den Zähler aber erst, wenn er in seinem Bezirk alle ausgefüllten Erhebungsvordrucke, die die Bürger nicht direkt der Erhebungsstelle zuleiten, eingesammelt hat. Dies kann mehrere Wochen dauern. Bis es soweit ist, muß der Zähler die bereits eingesammelten Erhebungsvordrucke so sicher aufbewahren, daß niemand davon Kenntnis erlangt. Auf jeden Fall wird das – ganz gleich, wie die noch ausstehende Zähleranleitung des Finanzministeriums sonst ausfällt – darauf hinauslaufen, daß der Zähler die ausgefüllten Bogen in seine Wohnung mitnimmt. Damit ist aber, so gewissenhaft der Zähler auch sein mag, ein zusätzliches und zudem unnötiges Risiko für die Volkszählungsdaten verbunden. Längst nicht jeder Zähler kann nämlich in seiner Wohnung die Volkszählungsbogen so sicher aufbewahren, wie es die Erhebungsstelle infolge der sehr detaillierten Regelung in § 4 Abs. 6 DVO über die Sicherung ihrer Räume und die Zutrittsbeschränkungen und -kontrollen kann und muß. Trotzdem war das Finanzministerium nicht bereit, in der Durchführungsverordnung oder wenigstens in den Verwaltungsvorschriften festzuschreiben, daß die Zähler die Erhebungsvordrucke zumindest wöchentlich bei der Erhebungsstelle abliefern müssen.

2.3 Korrektur falscher Angaben

Jeder Bürger ist verpflichtet, die Fragen zur Volkszählung wahrheitsgemäß, vollständig und fristgerecht zu beantworten. Doch was tut die Erhebungsstelle, wenn er absichtlich oder versehentlich einige Fragen nicht oder falsch beantwortet? In jedem Fall kann sie sich an die Faustregel halten: zunächst mit dem Bürger sprechen. Führt dies aus welchen Gründen auch immer nicht zum Erfolg, fragt sich, ob die Erhebungsstelle seinen Volkszählungsbogen selbst ergänzen oder abändern kann. Für den Fall, daß Angaben fehlen, gibt § 11 Abs. 1 VZG die Antwort: Die Erhebungsstelle darf nur in ganz begrenztem Umfang Angaben – nämlich über Straße und Hausnummer, Haupt- und Nebenwohnung, Geburtsjahr und -monat, Geschlecht oder Staatsangehörigkeit – eintragen, damit der Auskunftspflichtige bei der Volkszählung als Einwohner mitgezählt werden kann. Sie darf diese Angaben den Unterlagen entnehmen, die ihr das Einwohnermeldeamt ohnehin zur „Organisation der Zählung" übermitteln mußte. Zur Frage der Berichtigung von Angaben durch die Erhebungsstelle schweigt dagegen das Volkszählungsgesetz 1987. Im Entwurf der VwV-VZG 1987 des Finanzministeriums (Stand: Juli 1986) hieß es dazu: „Die Berichtigung von nicht offensichtlich falschen Angaben darf nur im Einverständnis mit dem Auskunftspflichtigen erfolgen". Das Finanzministerium wollte also zulassen, daß die Erhebungsstellen offen-

sichtlich falsche Angaben von sich aus berichtigen können. Ich bin mir alles andere als sicher, daß dies geht: Nach dem Volkszählungsgesetz sollen die Angaben des Bürgers und nicht die der Erhebungsstelle in die Statistik einfließen. Wenn man gleichwohl erwägt, eine Berichtigung durch die Erhebungsstelle zuzulassen, dann kann die Berichtigungsbefugnis nicht weitergehen als die Ergänzungsbefugnis nach § 11 Abs. 1 VZG. Auf keinen Fall kann es angehen, daß die Erhebungsstelle überhaupt nicht den Kontakt mit dem auskunftspflichtigen Bürger sucht. Gerade Letzteres schwebte dem Finanzministerium für die Fälle offenkundiger Unrichtigkeit vor. Es gab dann aber infolge meines Vetos den Plan, dies in seiner Verwaltungsvorschrift zu sagen, zumindest vorläufig auf. Wie es nun endgültig über die Angelegenheit denkt, weiß ich nicht.

2.4 Einsatz der EDV in der Erhebungsstelle

„Ihr Name wird nicht auf elektronischen Datenträgern gespeichert" versprach das ursprüngliche Muster des Volkszählungsbogens, das dem Bundestag bei seinen Beratungen zum Volkszählungsgesetz vorlag. Es versprach zuviel: Übersehen hatten die Statistischen Ämter des Bundes und der Länder, daß ihre Aussage mit den Plänen vieler Städte und Gemeinden, die EDV in der örtlichen Erhebungsstelle einzusetzen, nicht vereinbar war. Denn diese wollen mit Hilfe der EDV vor allem den Rücklauf der ausgefüllten Volkszählungsbogen überwachen; das aber geht nicht, ohne daß der Name des auskunftspflichtigen Bürgers gespeichert wird. Obwohl die Statistischen Ämter über Monate hinweg das ursprüngliche Vordruckmuster bei ihrer Öffentlichkeitsarbeit verwandten und Presse und Behörden dies weit streuten, entschloß man sich, den Widerspruch durch eine Änderung des Volkszählungsbogens auszuräumen. Seit Anfang Oktober 1986 lautet der die Sache reichlich verschleiernde Satz: „Ihr Name hilft lediglich, die Vollzähligkeit der Erhebung zu gewährleisten; er wird nicht zusammen mit Ihren Angaben aus dem Personenbogen oder dem Wohnungsbogen auf elektronischen Datenträgern gespeichert". Dieser Vorgang wird das Vertrauen der Bürger in amtliche Versprechungen bei der Volkszählung kaum erhöhen. Mancher wird sich auch fragen, wie es mit der Gewährleistung des Datenschutzes beim Einsatz von Computern für die Arbeit der Erhebungsstelle steht. Die Antwort hängt mit davon ab, ob die Erhebungsstelle einen eigenen Personal Compter einsetzen oder das städtische oder regionale Rechenzentrum für sich arbeiten lassen will:

- Der Einsatz eines eigenen Personal Computers in der Erhebungsstelle trägt dem Gebot der räumlichen, organisatorischen und personellen Trennung voll Rechnung. Fraglich ist jedoch, ob beim Einsatz eines Personal Computers auch die in § 8 LDSG gebotene Datensicherheit gewährleistet werden kann. Notwendig ist z. B. eine ausreichende Protokollierung, die nachvollziehbar macht, welcher Mitarbeiter der Erhebungsstelle welche Daten, z. B. über die Rückläufe ausgefüllter Volkszählungsbogen, wann eingegeben, verändert oder abgerufen hat oder ob ein Mitarbeiter unzulässigerweise den Datenbestand ganz oder teilweise, z. B. die Rücklaufdatei, kopiert hat. Auch können Bedienungsfehler schlimme Folgen für den Datenbestand haben, z. B. die Rücklaufdatei löschen. Gewiß bieten schon die Sicherheitsvorkehrungen, die für die Erhe-

bungsstelle wegen des Abschottungsgebots getroffen werden müssen, einen gewissen Schutz gegen eine mißbräuchliche Nutzung der gespeicherten Daten; erforderlich ist jedoch noch mehr.

- Solche Risiken gibt es bei den großen städtischen oder regionalen Rechenzentren in der Regel nicht. Die Preisfrage hier ist dagegen, ob sich der Einsatz eines zentralen Rechners für Zwecke der Erhebungsstelle mit dem Abschottungsgebot vereinbaren läßt. Der Wortlaut von § 9 Abs. 1 VZG und § 4 DVO, wonach die Erhebungsstellen räumlich, organisatorisch und personell von anderen Verwaltungsstellen zu trennen sind, spricht dagegen. Denn bei Inanspruchnahme des Rechenzentrums speichert die Erhebungsstelle ihre Daten außerhalb ihrer Räume; zudem kann sie über diese Daten nicht mehr allein bestimmen, sondern ist auf das Bedienungspersonal des Rechenzentrums angewiesen. Das Bedienungspersonal des Rechenzentrums wiederum hat nicht nur Zugriff auf die Daten der Erhebungsstelle, sondern führt gleichzeitig seine üblichen Arbeiten im Rechenzentrum für andere Verwaltungsstellen, z. B. das Sozial-, Einwohnermelde- oder Steueramt, durch. Es dient also gleichzeitig zwei Herren.

Wie man sieht: keiner der beiden denkbaren Wege ist ohne Probleme. Wird schon der Personal Computer in der Erhebungsstelle bei manchen Bürgern Vorbehalte auslösen, so dürfte die Speicherung ihrer Daten in einem Rechenzentrum, das auch eine Fülle von Verwaltungsdaten verarbeitet, erst recht Mißtrauen und Unsicherheit auslösen. Dies alles spricht eher dafür, vom Einsatz der EDV für die Erhebungsstelle die Finger zu lassen.

2.5 Nachzählung durch die Meldebehörden?

Die Gemeinden sorgen sich nicht nur darum, daß die Volkszählung die richtige, möglichst hohe Einwohnerzahl bringt. Sie befürchten zudem, daß sie das Statistische Landesamt nach der Volkszählung nicht richtig fortschreibt. Nicht ohne Grund: Zieht ein Einwohner, der in mehreren Gemeinden Wohnungen hat, um, kann nach den Fortschreibungsmodalitäten folgendes passieren: er wird nicht der Gemeinde abgezogen, die ihn bislang zählte, sondern einer anderen. Verständlich ist deshalb, daß die kommunale Seite ein Verfahren fordert, das solche Ungereimtheiten ausschließt; schlechterdings unverständlich aber, auf welche Weise sich das Finanzministerium die Lösung vorstellte: das Einwohnermeldeamt sollte jeden Bürger, der nach der Volkszählung umzieht und mehrere Wohnungen hat, bei der Anmeldung befragen, welche Wohnung am Stichtag der Volkszählung seine Hauptwohnung war. Faktisch lief dieser Vorschlag darauf hinaus, daß die Bürger nachträglich hätten offenbaren müssen, welche Angaben sie bei der Volkszählung zur Haupt- und Nebenwohnung machten. Das Innenministerium lehnte ab, solches in die Tat umzusetzen – freilich erst nach meinem Widerspruch.

3. Resümee

Die Volkszählung 1987 wird die Gemüter weiter bewegen. Auch ihre Kritiker sollten anerkennen, daß sich der Deutsche Bundestag Mühe gab, den Vorgaben des Bundesverfassungsgerichts zu entsprechen. Nicht so positiv kann ich die Landesvorschriften

zur Durchführung der Volkszählung in Baden-Württemberg bewerten. Ihr neuralgischster Punkt ist § 3 Abs. 4 DVO, also die Regelung über die Bestimmung der Erhebungsstelle. Sie bietet keine Garantie, daß jede Erhebungsstelle von vornherein so abgeschottet ist, wie es das Volkszählungsgesetz verlangt. Um so mehr gilt es jetzt darauf zu achten, wie die Dinge vor Ort im einzelnen laufen. Hier sind in erster Linie die Kommunen gefordert. Vieles hängt davon ab, wie ernst sie es mit den erforderlichen Schutzvorkehrungen nehmen. Da lassen sich gewiß nicht alle Gemeinden über einen Kamm scheren; generelle Vorbehalte gegen ihre Mitwirkung scheinen mir deshalb nicht angebracht. Gleichwohl besteht wegen der fragwürdigen Haltung des Finanzministeriums und des Innenministeriums und wegen des ständigen Bemühens der kommunalen Verbände, strikte Vorgaben zur Sicherung der Abschottung zu verhindern, Grund zur Aufmerksamkeit. Jeder Bürger, der das örtliche Geschehen genau verfolgt, trägt mit dazu bei, daß die Erhebungsstelle seines Wohnorts die Volkszählung tatsächlich so durchführt, wie es das Volkszählungsgesetz verlangt. Sollten Bürger Anhaltspunkte in andere Richtung haben, bin ich gerne bereit, dem vor Ort nachzugehen. Alles in allem: erst während der Zählung wird sich erweisen, ob das Abschottungsgebot in der Praxis hält, was das Volkszählungsgesetz verspricht.

4. Teil: Öffentliche Sicherheit

Wer geglaubt hatte, man würde 1986 in Baden-Württemberg so, wie es gute demokratische Art ist, öffentlich über die erforderlichen Regelungen zur Datenverarbeitung der Sicherheitsbehörden des Landes diskutieren, wurde eines Besseren belehrt. Das erklärte Ziel des Innenministeriums war, möglichst auch 1986 jede Sachdiskussion zu diesem Thema zu vermeiden. Zwar wirkte es kräftig dabei mit, die Weichen für die künftigen gesetzlichen Regelungen zu stellen; doch tat es dies unter Ausschluß der Öffentlichkeit in Arbeitskreisen, Ausschüssen und anderen Gremien. Einer öffentlichen Auseinanderseztung ging es wie eh und je aus dem Weg. Nicht genug: die Verantwortlichen hielten es statt dessen für richtig, Stimmung zu machen, Emotionen zu wecken und dabei den Datenschutz anzuschwärzen. Anstelle von Sachargumenten, die in der Tat ja auch schwerlich zu finden gewesen wären, begnügte man sich mit primitiven Schlagworten wie „Menschenschutz vor Datenschutz" und „Datenschutz darf nicht Terroristenschutz werden". Diese Taktik wirkte sich natürlich auch auf meine Arbeit aus. Eine sachliche Erörterung von Grundsatzproblemen fand im Sicherheitsbereich praktisch nicht statt. Alles, was ich bereits 1985 dazu verlautbarte, ist nach wie vor ohne Antwort.

Im Mittelpunkt meiner Tätigkeit im Sicherheitsbereich standen 1986 die Überprüfung konkreter Vorgehensweisen der Polizei und des Verfassungsschutzes. Dabei zeigte sich eine aus der Sicht des Datenschutzes wenig erfreuliche Tendenz: Während es 1985 noch möglich war, bei der Behandlung von Blockierern in Mutlangen oder Heilbronn in persönlichen Gesprächen mit dem Herrn Innenminister zu einer gemeinsamen, immerhin vertretbaren Lösung zu gelangen, sind diese Zeiten inzwischen vorbei. Die Kritik aus Polizeikreisen an der Kooperationsbereitschaft des Herrn Innenministers zeigte Wirkung. Inzwischen hat sich in der Polizei eine einheitliche Linie durchgesetzt: man nimmt auf Anfrage schriftlich Stellung und beschränkt sich dabei auf das rechtliche Minimum.

Meinen Vorschlägen trägt die Polizei nur dann Rechnung, wenn es überhaupt nicht anders geht. Die unabhängige Datenschutzkontrolle ist für sie eine lästige, im Grunde überflüssige, aber nun einmal vorhandene Institution, die es eben – wenn man sie schon nicht mehr abschaffen kann – zu ertragen gilt. Zu dieser Linie gehört, daß wieder viel häufiger als in letzter Zeit vorgesetzte Behörden – seien es Innenministerium, Landeskriminalamt oder Landespolizeidirektionen – anstelle der von mir angesprochenen „speichernden" Polizeidienststellen die angeforderte Stellungnahme abgeben oder diese sich zumindest vorab ihre Äusserungen von oben absegnen lassen. Abweichungen von der Generallinie werden auf diese Weise vermieden. Daß meine Ansprechpartner nach dem Landesdatenschutzgesetz primär die „speichernden" Polizeidienststellen sind, wird dabei geflissentlich übersehen. Diese Entwicklung ist nicht gut: manch guter Wille bei den Polizeibeamten vor Ort, auf den ich immer wieder stoße, wird dadurch unnötig verschüttet. Zugleich nützen die Sicherheitsbehördern das für sie günstige Klima, ihre Informationssysteme im Lande tatkräftig auszubauen. Dringlicher denn je sind deshalb intensive Kontrollen. Dazu ist es notwendig, nicht nur die Stellungnahmen der kontrollierten Stellen entgegenzunehmen und sie rechtlich zu bewerten, sondern sich selbst durch ein umfassendes Aktenstudium ein Bild vor Ort von dem zu bewertenden Sachverhalt zu machen. Das aber erfordert einen enormen Zeitaufwand, den mein Amt in seiner jetzigen Besetzung keineswegs immer leisten kann: So wäre es längst nötig, das neue bundesweite polizeiliche Informationssystem „APIS" beim Landeskriminalamt zu überprüfen. So war es, als kürzlich das Landesamt für Verfassungsschutz wegen seiner Aktivitäten in Ravensburg in die Schlagzeilen geriet, trotz dessen Unterstützung in zwei Kontrollbesuchen nicht annähernd möglich, die Fülle der dabei zutage getretenen Probleme abschließend zu klären. Was haben beispielsweise Einträge wie „Teilnahme an genehmigter Demonstration ‚Stoppt Strauß' in ..." in den Karteien des Verfassungsschutzes zu suchen? Welchen Sinn machen Sicherheitsüberprüfungen, wenn das Landesamt für Verfassungsschutz meint, aus Gründen des Geheimschutzes nichts mitteilen zu können? Diese und andere Grundsatzfragen stellten sich bei diesen Kontrollbesuchen zuhauf. Wollte ich alle bis ins Detail gewissenhaft abklären, wären wochenlange Überprüfungen vor Ort nötig. Diese konnte mein Amt infolge seiner ungenügenden Ausstattung 1986 nicht leisten; auch besteht wenig Hoffnung, daß dies 1987 möglich sein wird. Eine solche Situation ist für eine Datenschutzbeauftragte, die es mit ihrem gesetzlichen Auftrag ernst nimmt, bedrückend.

1. Hiroshima-Forum

„Verfassungsschutz sammelt systematisch Material über führende Politiker", „Vor allem Spitzenpolitiker aus Baden-Württemberg im Visier" lauteten eines Tages die Schlagzeilen von Zeitungen. Dazu hieß es weiter: ein Staatssekretär im Bonner Innenministerium habe beim Bundesamt für Verfassungsschutz einen Bericht über die kommunistischen Beeinflussungsversuche demokratischer Parteien angefordert und an Journalisten seines Vertrauens verteilen lassen. In diesem Bericht waren u. a. auch die Namen von Abgeordneten und Gewerkschaftsvertretern aus Baden-Württemberg genannt. Deshalb informierte ich mich durch einen Kontrollbesuch beim Landesamt für Verfassungsschutz über dessen Aktivitäten in dieser Sache. Dabei stellte ich fest:

Am 20. Juli 1985 fand in Heilbronn zur Mahnung an die Folgen des Abwurfs der ersten Atombomben vor 40 Jahren ein Hiroshima-Tag statt. Träger dieser Veranstaltung war das sog. Hiroshima-Forum. Ihm gehörten Vertreter verschiedener demokratischer Organisationen, aber auch Vertreter einiger kommunistisch be-

einflußter Gruppierungen an, die – so das Landesamt für Verfassungsschutz – auf die am Hiroshima-Tag beteiligten demokratischen Organisationen und die Friedensbewegung Einfluß zu gewinnen versuchten. Deshalb beobachtete das Landesamt für Verfassungsschutz Vorbereitung, Durchführung und Auswertung dieser Veranstaltung und legte darüber eine Akte mit den verschiedensten Unterlagen an. In diesen waren auch die Namen zahlreicher Personen – darunter von Parlamentariern und Gewerkschaftsführern – aufgeführt, die auch nach Auffassung des Landesamts für Verfassungsschutz in keiner Weise mit extremistischen Bestrebungen in Zusammenhang gebracht werden können. Am 21. Aug. 1985 übersandte das Landesamt für Verfassungsschutz unaufgefordert dem Bundesamt für Verfassungsschutz mit dem lapidaren Anschreiben „Anbei werden in Ablichtung Unterlagen über die im Betreff näher bezeichnete Veranstaltung übersandt" einen Teil dieser Unterlagen in Photokopie, u. a.

- das Flugblatt „Heilbronn mahnt: Nie wieder Hiroshima", in dem die über 100 Mitglieder des Trägerkreises unter ihrem vollen Namen zur Teilnahme an dem Forum aufgerufen hatten,
- Sitzungsunterlagen über den Trägerkreis und seine Untergruppierungen,
- ein Rundschreiben des Trägerkreises an alle Mitglieder mit Zeitungsausschnitten über die Berichterstattung in der Presse; darunter befanden sich auch die nach Meinung des Landesamts für Verfassungsschutz inhaltlich nicht zu beanstandenden Interviews, die ein Abgeordneter und ein führender Funktionär einer Gewerkschaft aus Baden-Württemberg dem kommunistischen Blatt „Unsere Zeit" aus Anlaß des Hiroshima-Tags gegeben hatten.

Zu diesem Vorgehen des Landesamts für Verfassungsschutz ist aus der Sicht des Datenschutzes zu sagen:

- Zum einen hätte das Landesamt für Verfassungsschutz nicht die Namen der zahlreichen völlig „unverdächtigen" Personen, die ihm im Zuge seiner Beobachtung des Hiroshima-Forums bekannt wurden, in seiner Akte festhalten dürfen. Zumindest hätte es deren Namen, soweit sie, wie z. B. bei Flugblättern, wegen der Art der Unterlage nicht ganz entfernt werden konnten, schwärzen müssen. Denn nach der Rechtsprechung des Bundesverfassungsgerichts muß der einzelne Bürger jederzeit wissen können, wer was wann bei welcher Gelegenheit über ihn weiß, und darf auch nicht befürchten müssen, daß er wegen seiner Teilnahme an einer Versammlung oder Bürgerinitiative behördlich registriert wird und ihm daraus Nachteile entstehen können. Gerade aber dies ist der Fall, wenn „harmlose" Bürger aus Anlaß ihrer Teilnahme an einer erlaubten Veranstaltung in die Akten des Landesamts für Verfassungsschutz geraten und dadurch in unmittelbaren Zusammenhang mit extremistischen Bestrebungen gebracht werden.
- Erst recht hätte das Landesamt für Verfassungsschutz die Namen der „unverdächtigen" Personen nicht an das Bundesamt für Verfassungsschutz weitergeben dürfen. Denn § 4 Abs. 2 des Bundesverfassungsschutzgesetzes berechtigt und verpflichtet es nur, solche Informationen weiterzugeben, die das Bundesamt für Verfassungsschutz zur Erfüllung seiner Aufgaben braucht. Dazu gehören ganz gewiß nicht Mitteilungen über Personen, die über jeden Verdacht linksextremistischer Bestrebungen erhaben sind. So sieht es selbst der im Bundestag Anfang 1986 im Rahmen des Gesetzespakets „Sicherheits- und Datenschutzgesetze" eingebrachte neue Entwurf eines Bundesverfassungsschutzgesetzes, der wegen seiner wenig

datenschutzfreundlichen Regelungen vielfach kritisiert wurde und den der Bundestag aus diesem Grunde in dieser Legislaturperiode nicht mehr verabschiedet hat. Das Landesamt für Verfassungsschutz hätte folglich nicht wahllos Photokopien seiner Unterlagen versenden dürfen, sondern selbst einen Bericht formulieren müssen, in dem es nur die Namen der Personen aufführt, die sich tatsächlich extremistisch betätigt hatten. Zumindest hätte es die Unterlagen vor dem Versenden daraufhin durchsehen müssen, ob darin „Unverdächtige" erwähnt sind und, soweit ja, deren Namen schwärzen müssen. Dies gilt selbst dann, soweit die Namen in Presseveröffentlichungen oder Flugblättern enthalten sind. Zwar ist in solchen Fällen das Schutzbedürfnis der Betroffenen geringer: sie mußten damit rechnen, daß durch die Veröffentlichung viele von ihrer Aktivität erfahren. Gibt jedoch der Verfassungsschutz solche Informationen weiter, so erhalten sie darüber hinaus eine zusätzliche Bedeutung: es wird ein Zusammenhang hergestellt zwischen der „unverdächtigen" Person und Aktivitäten, die dem Bereich „Beeinflussung demokratischer Organisationen durch extremistische Gruppierungen" zuzuordnen sind.

Das Landesamt für Verfassungsschutz, das mir bei dem Kontrollbesuch bereitwillig und umfassend Auskunft gab, war für meine Überlegungen aufgeschlossen – anfangs mehr als im Laufe des sich anschließenden Schriftwechels. Es wies seine Mitarbeiter an dafür zu sorgen, daß in Zukunft nach Möglichkeit keine Daten „Unbeteiligter" mehr in Akten des Amtes genannt werden. Soweit dies ausnahmsweise wegen der Gestaltung der gesammelten Unterlagen nicht zu vermeiden sei, untersagte es, diese Informationen amtsintern zu verwenden und an das Bundesamt für Verfassungsschutz weiterzugeben. Meiner Bitte, diese neue Handhabung in einer Dienstanweisung festzulegen, um ein für allemal Klarheit zu schaffen, entsprach es dagegen nicht. Wenig dienlich war auch die Pressemitteilung des Innenministeriums vom 5. Mai 1986 zu den eingangs erwähnten Zeitungsberichten: mit markigen Worten ließ man die Öffentlichkeit wissen, der Verfassungsschutz beobachte systematisch selbstverständlich nur extremistische Bestrebungen, nicht auch Parteien oder Gewerkschaften. Kein Wort verlor man darüber, daß das Landesamt für Verfassungsschutz zahlreiche Namen von über jeden Verdacht erhabenen Personen an das Bundesamt für Verfassungsschutz weitergegeben und damit eine entscheidende Ursache gesetzt hat, daß Politiker und Gewerkschaftsführer aus Baden-Württemberg ihre Namen in dem veröffentlichten Bericht des Bundesamts für Verfassungsschutz über die kommunistischen Beeinflussungsversuche demokratischer Parteien wiederfinden mußten.

2. Die Speicherpraxis der Polizeidirektion Tübingen

Polizeiliche Arbeit ist ohne Erheben und Sammeln von Daten nicht möglich. Die Polizei muß sich aber von ihren Informationen auch wieder trennen können. So will es § 13 des Landesdatenschutzgesetzes; so sehen es die 1981 dazu ergangenen Richtlinien der Polizei vor. Um diese Aufgabe möglichst rationell abwickeln zu können, gab sich die Polizei Regellöschungsfristen. Sie betragen bei Erwachsenen 10 Jahre, im Falle von Bagatelldelikten 3 Jahre. Nur ausnahmsweise darf die Polizei Vorgänge darüber hinaus speichern, nämlich wenn „wegen der Art und Ausführung der begangenen Tat Wiederholungsgefahr besteht oder die Speicherung der Daten aus anderen schwerwiegenden Gründen zur Strafverfolgung oder Abwehr konkreter Gefahren

erforderlich ist". In solchen Ausnahmefällen muß die Polizei die Gründe für die Verlängerung aktenkundig machen. Zweimal im Jahr teilt das Landeskriminalamt den Polizeidienststellen im Lande in Form der sog. „Löschwarnungen" mit, welche Vorgänge zur Löschung heranstehen. Sofern die einzelnen Polizeidienststellen nicht bei einzelnen Vorgängen innerhalb der Ausschlußfrist eine andere Entscheidung treffen, löscht das Landeskriminalamt diese Datensätze. Über die Löschung führt es eine Statistik.

Seiner Löschstatistik über das Jahr 1985 entnahm ich, daß die Polizeidirektion Tübingen, die zugleich die Daten aus dem Bereich der Polizeidirektion Balingen speichert und löscht, beim Löschwarnlauf 1/85 bei insgesamt 1514 Löschwarnungen nur 543 Regellöschungen und beim Löschwarnlauf 2/85 bei insgesamt 1456 Löschwarnungen nur 594 Regellöschungen durchführte. Dies enspricht einer Löschquote von 35% bzw. 40%, während der Landesdurchschnitt dagegen bei 85% bzw. 88% lag. In Wirklichkeit war die Tübinger Löschquote freilich etwas höher: infolge der Eigenart der Tübinger Vorgehensweise hatte nämlich das Landeskriminalamt beim Löschlauf 1/85 206 Löschungen und beim Löschlauf 2/85 397 Löschungen einer anderen Rubrik der Statistik zugeschlagen, anstatt sie bei den Regellöschungen mitzuzählen. Aber auch mit der bereinigten Löschquote liegt die Polizeidirektion Tübingen mit 49,5% beim Löschlauf 1/85 und 68% beim Löschlauf 2/85 immer noch praktisch an unterster Stelle im Lande. Deren Ursachen gingen meine Mitarbeiter und ich in mehreren Kontrollbesuchen nach. Unser besonderes Augenmerk richteten wir gleichzeitig auf die Datenspeicherung von Kindern und Senioren. Das Ergebnis sah so aus.

2.1 Die Verlängerungspraxis

Bei der Durchsicht zahlreicher Datensätze stellten meine Mitarbeiter und ich fest, daß die überaus großzügige Praxis, statt zu löschen die Regelspeicherfristen zu verlängern, vor allem zwei Ursachen hat:

- Entscheidungen der Datenstation

  Anstatt die Entscheidung über eine etwaige Verlängerung den Sachbearbeiter treffen zu lassen, der sich im einzelnen auskennt, entschied die Datenstation „eindeutige" Fälle. Dagegen wäre nichts einzuwenden, wenn es sich tatsächlich bei der Verlängerung um eine Routineentscheidung handeln würde, die nur „Verlängerung der Speicherdauer" lauten kann. Dem ist aber nicht so: gleichwohl ging die Datenstation davon aus. Sie verlängerte die regelmäßige Speicherdauer immer bei Sittlichkeitsdelikten oder wenn INPOL-Bestand – also ein Eintrag im bundesweiten polizeilichen Informations- und Auskunftssystem – vorhanden war. Beides rechtfertigt jedoch eine automatische Verlängerung der Regelspeicherdauer nicht: zum einen geht es nicht an, einfach auf die Art des begangenen Delikts, auch wenn es ein Sittlichkeitsdelikt ist, abzustellen. Wäre dem so, wären die Regelspeicherfristen, welche die deutsche Polizei aufgrund ihrer jahrzehntelangen Erfahrungen für angemessen hielt und deshalb in ihren Richtlinien festschrieb, von vornherein falsch. Das aber trägt selbst die Polizei so nicht vor. Zum anderen rechtfertigt ebensowenig ein INPOL-Bestand eine automatische Verlängerung. Man nehme beispielsweise die Ausschreibung zur Fahndung in INPOL: sie kann sehr unterschiedliche Gründe haben – sei es, daß gegen je-

mand Haftbefehl wegen Totschlags besteht, sei es, daß gegen jemand ein Vorführungsbefehl nach § 230 Abs. 2 StPO erging, weil er nicht hinreichend entschuldigt von einer Hauptverhandlung fernblieb, sei es, weil er an einer übertragbaren Krankheit leidet und sich der gerichtlich angeordneten Unterbringung entzieht. Wer dies weiß, dem leuchtet ein: es kommt immer auf die Ausschreibungsgründe, also auf die Gesamtsituation an. Da man diese allein aus der Ausschreibung in INPOL in der Regel nicht ersehen kann, muß die Polizei vor ihrer Entscheidung über eine etwaige Verlängerung einer Datenspeicherung deshalb weitere Ermittlungen anstellen.

- Ein ungeeigneter Vordruck

  Um sich die Arbeit möglichst zu erleichtern, benützte die Polizeidirektion Tübingen für ihre Entscheidungen auf Verlängerung der Datenspeicherung einen Vordruck. Dieser Vordruck war nicht geeignet, sachgerechte Entscheidungen im Einzelfall herbeizuführen. Denn er machte zum einen nicht hinreichend deutlich, daß die Löschung nach Ablauf der Regelfrist die Regel und die Verlängerung die Ausnahme ist. Zum anderen ersparte er dem Bearbeiter die Auseinandersetzung mit dem konkreten Fall. Dieser mußte lediglich eines der vorgedruckten, relativ nichtssagenden Schlagworte wie z. B. „Wiederholungsgefahr aufgrund von Art und Ausführung der Tat" oder Verlängerung „Aus Gründen der Prävention" ankreuzen. Im zweiten Fall forderte der Vordruck zwar, diese Gründe kurz darzulegen. Sehr oft geschah dies aber, wie die eingesehenen Akten zeigten, nicht und wenn ausnahmsweise, dann so knapp und dürftig, daß damit nichts anzufangen war. Nötig ist, in den Akten zu vermerken, weshalb im konkreten Fall infolge Art und Ausführung der Tat eine Wiederholungsgefahr usw. besteht. Wohin es führt, wenn dies nicht geschieht, zeigen allein schon folgende Fälle:

  - Die Herrenhose
    Ein Mann hatte 1973 aus der Textilabteilung eines Kaufhauses eine Herrenhose im Wert von 25,- DM entwendet. Er ging dabei so vor, daß er zwei Hosen aus einem Regal nahm, in einer Umkleidekabine die eine davon anzog und die andere dann wieder in das Regal legte. Wegen dieses Vorfalls speicherte die Polizei diesen Mann zunächst auf 10 Jahre, obwohl sie eigentlich, da es sich um ein Bagatelldelikt handelte, nur eine Speicherdauer von 3 Jahren hätte eingeben dürfen. Anstatt nach der 10jährigen Speicherung nun die Daten zu löschen, folgte die Verlängerung der Speicherung ohne Angabe konkreter Gründe um weitere 3 Jahre. Im Vordruck waren einfach die Rubriken „Wiederholungsgefahr" und „Gründe der Prävention" angekreuzt. Auf meinen Hinweis, diese Verlängerung sei eindeutig rechtswidrig gewesen, löschte die Polizeidirektion Tübingen den Datensatz des Mannes.
  - Der Ausländer
    Einen Ausländer hatte sie gespeichert, weil er 1972 ein Auto gekauft und eine Anzahlung geleistet, dann aber 1973 die Bundesrepublik verlassen hatte, ohne zuvor die restlichen Raten zu bezahlen. Hier meinte die Polizei 11 Jahre nach der Tat, die Speicherung nochmals um zwei Jahre verlängern zu müssen. Im Vordruck waren wieder, ohne irgend etwas näher zu begründen, die Rubri-

ken „Wiederholungsgefahr" und „Aus Gründen der Prävention" angekreuzt. In Wirklichkeit war diese Tat weder besonders schwer noch zeichnete sie sich durch einen von sonstigen Unterschlagungen abweichenden besonderen modus operandi aus noch gab es Anhaltspunkte für eine erneute Straffälligkeit. Meine Forderung, diesen Datensatz deshalb unverzüglich zu löschen, lehnte die Polizei mit dem Hinweis ab, eine solche Art von Straftat würden besonders häufig Ausländer begehen. Auch könne man auf die Ermittlungsakte noch nicht verzichten, falls der Ausländer wieder einreise; dann könnte sie nämlich für die Abwicklung der zivilrechtlichen Ansprüche des Autoverkäufers u. U. eine Rolle spielen. Bei dieser Argumentation übersieht die Polizei, daß das Verfahren gegen den Ausländer 1981 nach § 170 Abs. 2 StPO, also wegen Fehlens eines hinreichenden Tatverdachts, eingestellt wurde. Auch paßt das Vorgehen des Mannes – selbst wenn Ausländer eher dazu neigen sollten, sich nach Straftaten ins Ausland abzusetzen – nicht in ein solches Bild. Denn der Mann reiste ausweislich der Aktenlage nicht kurzfristig in die Bundesrepublik mit der Absicht ein, eine Straftat zu begehen und dann sofort wieder auszureisen. Vielmehr hielt er sich nach dem Kauf des Autos noch über mehrere Monate hier auf, bis er sich entschloß, in seine Heimat zurückzukehren. Wenn die Polizei trotz alledem glaubt, diesen Vorgang wegen des Vorliegens eines Restverdachts in der Personenauskunftsdatei (PAD) speichern zu dürfen, dann ließ sich dies nur innerhalb der Regelfrist von 10 Jahren rechtfertigen. Eine Verlängerung der Speicherung darüber hinaus bloß zum Zwecke der Beweiserleichterung in zivilrechtlichen Streitigkeiten ist nicht zulässig. Meiner Aufforderung, den Datensatz zu löschen, kam die Polizei bislang nicht nach. Zu hoffen bleibt, daß sie sich noch eines Besseren besinnt und wenigstens jetzt – 14 Jahre nach der Tat – zeigt, daß sie vergessen kann, wie es das Gesetz schon längst verlangt.

Meine Bewertung dieser und anderer Einzelfälle teilte ich der Polizeidirektion Tübingen ebenso wie meine grundsätzlichen Bedenken gegen ihre Verfahrensweise bei der Verlängerung der Regelspeicherfristen mit: Dabei zeigte ich ihr zum einen meine Zweifel auf, ob ein solcher Vordruck überhaupt für die Entscheidung über die Verlängerung der Speicherfrist geeignet ist. Sollte sie an einem solchen Vordruck festhalten wollen, müßte sie ihn auf jeden Fall so ändern, daß er für jeden formatierten Verlängerungsgrund eine individuelle, am Einzelfall orientierte Begründungspflicht vorschreibt. Auch müßte die Verlängerungsentscheidung in jedem Einzelfall ersehen lassen, wer sie wann getroffen hat. Ein schlagwortartiger Vermerk in der Löschwarnung ohne Angabe des Sachbearbeiters und des Zeitpunkts der Entscheidung genüge nicht. Zum anderen ließ ich sie wissen, es wäre zweckmäßig, wenn nicht die Datenstation, sondern stets der mit der Materie viel vertrautere Sachbearbeiter über eine etwaige Fristverlängerung entscheidet. Wenn die Polizeidirektion gleichwohl an einer Entscheidungsbefugnis der Datenstation festhalten wolle, dann müsse sie sicherstellen, daß diese die Entscheidung anhand aller Umstände des Einzelfalls trifft; die Einzelheiten seien in einer Dienstanweisung festzulegen. Anstatt dazu die Meinung der Polizeidirektion Tübingen zu erfahren, zogen die Landespolizeidirek-

tion Tübingen und das Landeskriminalamt den Vorgang an sich. Erstaunt war ich vor allem über das Vorgehen des Landeskriminalamts: nach monatelangem Schweigen stellte es mich nämlich vor vollendete Tatsachen, indem es mir eine Dienstanweisung an die Polizeidienststellen übersandte, die in mancherlei Hinsicht nicht meinen Vorstellungen entspricht.

2.2 Speicherung von Senioren

Weil ältere Menschen seltener straffällig werden und auch längst nicht mehr alle Straftaten verüben können, legt die Polizei an sie einen weniger strengen Maßstab an. Nach ihren Richtlinien werden alle Datensätze von Personen, die das siebzigste Lebensjahr vollendet haben, gelöscht – es sei denn, in den letzten 5 Jahren hätten sich neue Erkenntnisse ergeben, die eine weitere Datenspeicherung in der Personenauskunftsdatei (PAD) rechtfertigen. Bei meinen Kontrollen stellte ich fest, daß die Polizeidirektion Tübingen die Regellöschung der 70jährigen durchweg einhält. Einen zu strengen Maßstab legt sie jedoch zumindest teilweise an, wenn es um die erstmalige Speicherung hochbetagter Personen geht:

- Die Rentnerin

  Eine 85jährige Rentnerin, die sich bislang nie etwas zuschulden kommen ließ, nahm 1982 in einem Kaufhaus eine Handtasche im Wert von 39,90 DM und ein Paket Taschentücher an sich, das sie in die Tasche stopfte. Die Taschentücher bezahlte sie an der Kasse, die Tasche dagegen nicht. Das Verkaufspersonal beobachtete dies, stellte die Frau, die einen verwirrten Eindruck machte, zur Rede und erstattete Strafanzeige. Die Staatsanwaltschaft stellte das Ermittlungsverfahren wegen Ladendiebstahls ein, weil die alte Rentnerin im Augenblick der Tat wegen ihrer geistigen Verwirrung nicht schuldfähig gewesen war. Gleichwohl meinte die Polizeidirektion Tübingen, es sei richtig, die Frau wegen dieses Vorfalls fünf Jahre in der Personenauskunftsdatei zu speichern. Weil es sich bei dem Vorfall jedoch allenfalls um ein Bagatelldelikt handelte und die dafür zulässige Speicherfrist bereits abgelaufen war, forderte ich, die Daten unverzüglich zu löschen. Die Polizei konterte, die Datenspeicherung der inzwischen 89jährigen Frau sei weiterhin erforderlich, da diese Frau infolge ihrer geistigen Verwirrung möglicherweise zwangsweise untergebracht werden müsse. Dafür fehlen jegliche Anhaltspunkte. Weder aus den staatsanwaltschaftlichen Ermittlungsakten noch aus den Unterlagen der Polizei geht irgend etwas hervor, daß von der Rentnerin eine konkrete Gefahr für ihre Umgebung ausgeht, die möglicherweise eine Unterbringung erfordern könnte. Selbst wenn dem so gewesen wäre, könnte dies nicht eine weitere Speicherung des Vorfalls aus dem Jahre 1982 rechtfertigen, da beides miteinander überhaupt nichts zu tun hat. Erst auf diese Hinweise hin war die Polizei bereit, die Daten der Rentnerin zu löschen.

- Der Rentner

  Ein Mieter zeigte seinen Vermieter, einen 85jährigen Rentner, an, weil er ihm eine kleine Dachgeschoßwohnung in Tübingen zu einer Kaltmiete von 800,– DM vermietet hatte; in der Nachbarschaft sei eine größere, allerdings nicht renovierte Wohnung wesentlich preiswerter.

Dies allein genügte für die Polizei, den Rentner wegen Wuchers in der Personenauskunftsdatei zu speichern. Wie das Ermittlungsverfahren bei der Staatsanwaltschaft ausging, überwachte sie nicht, sondern gab einfach die 5jährige Speicherfrist ein. Auf meinen Hinweis, daß es so nicht ginge, löschte die Polizei den Datensatz.

2.3 Speicherung von Kindern

Kinder bis 14 Jahre sind strafunmündig. Erfüllen sie den Tatbestand einer Straftat – sei es Sachbeschädigung oder Diebstahl –, wird dies nicht geahndet. So will es unsere Rechtsprechung aus gutem Grund. Die Polizei interessiert sich jedoch auch für strafunmündige Kinder, weil sich manchmal schon früh der Beginn einer kriminellen Karriere zeige. Diese heikle Frage lösen ihre Richtlinien so: Sie verbieten generell, Kinder unter 7 Jahren in der Personenauskunftsdatei zu speichern, auf die jeder Polizeibeamte aus welchem Anlaß auch immer zugreifen kann; Kinder zwischen 7 und 14 Jahren darf sie nur ausnahmsweise speichern, wenn – was immer dies heißen mag – kein „kindtypisches, entwicklungsbedingtes Verhalten vorliegt und Anhaltspunkte für die Begehung weiterer Straftaten" gegeben sind. Die Speicherung erfolgt dann aber in der Regel nicht wie bei Erwachsenen auf 10, sondern nur auf 2 Jahre. Dann soll die Polizei prüfen, ob sie die Daten löschen und die Akten vernichten kann. Wohin diese unpräzisen Regelungen führen, zeigen folgende Fälle, auf die ich in Tübingen stieß:

- Die verlockenden Süßigkeiten

  Eine Kassenaufsicht eines Kaufhauses beobachtete, wie ein 7jähriges Mädchen Brausepulver und andere kleine Süßigkeiten im Gesamtwert von 2,80 DM in seine Hosentasche steckte. Sie stellte das Kind zur Rede und nahm ihm die Süßigkeiten wieder ab. Das Mädchen sagte ihr, sie habe bereits schon zweimal Süßigkeiten mit nach Hause genommen, diese aber am nächsten Tag wieder zurückgebracht. Die Tübinger Polizei speicherte sodann diesen „Ladendiebstahl" zum jederzeitigen Abruf durch alle Polizeibeamten des Landes in der Personenauskunftsdatei (PAD), obwohl dies weder zur vorbeugenden Bekämpfung von Straftaten erforderlich noch verhältnismäßig war. Auf meinen Vorhalt hin nahm die Polizeidirektion Tübingen die Daten des Kindes aus der landesweiten Speicherung heraus.

- Zwei Hühnerstrolche

  Zwei 11jährige Buben stiegen 1984 über den Zaun in ein Gartengrundstück und drangen dort in das Hühnerhaus ein. Als sie dabei waren, die Hühner mit Hilfe von „Gartenwerkzeugen" in eine Ecke des Gartens zu scheuchen, überraschte sie der Besitzer. Die Buben liefen davon. Gegenüber der Polizei bestritten sie, in Diebstahlsabsicht in den Garten eingestiegen zu sein. Sie hatten eindeutig nichts entwendet; auch war kein Sachschaden entstanden. Gleichwohl speicherte die Polizei sie in der Personenauskunftsdatei wegen eines „besonders schweren Fall des Diebstahls", in Wirklichkeit war es wohl nur ein Hausfriedensbruch. Nicht genug damit: sie verlängerte 1986 diese Speicherung wegen angeblicher Wiederholungsgefahr um weitere drei Jahre. Auf meinen Hinweis, daß dies schlechterdings nicht zu rechtfertigen ist, löschte die Polizeidirektion Tübingen inzwischen die Datensätze der beiden Buben.

- Der verhängnisvolle Klebstoff

  Zwei Buben im Alter von 12 und 13 Jahren entwendeten im Mai 1984 in einem Papiergeschäft Klebstoff zum Preis von 7,– DM. Dabei stand der eine Schmiere, der andere führte die Tat aus. Beim Verlassen des Kaufhauses stellte der Hausdetektiv den einen und nahm den Klebstoff an sich; der andere Bub flüchtete mit dem Fahrrad. Wegen dieses Vorfalls speicherte die Polizei die beiden Buben in der Personenauskunftsdatei wegen Ladendiebstahls für zwei Jahre. 1986 verlängerte sie diese Regelfrist um weitere drei Jahre, indem sie, ohne daß es den geringsten Anhaltspunkt dafür gab, Wiederholungsgefahr unterstellte. Auf meinen Vorhalt hin war die Polizei zunächst nicht bereit, die Daten zu löschen, sondern meinte, die beiden Buben hätten die Tat bis ins Detail geplant: sie seien arbeitsteilig vorgegangen; daß sie nur Klebstoff gestohlen hätten, seien nicht Absicht, sondern Zufall gewesen. Auch erlaube das Umfeld der beiden Jugendlichen keine positive Prognose. Aus den Ermittlungsakten der Staatsanwaltschaft, die ich beizog, ergab sich freilich das Gegenteil: Den beiden Buben ging es von vornherein nur um den Klebstoff, da sie solchen für Bastelarbeiten benötigten. Auch ist das Umfeld der Kinder nicht negativ; im Gegenteil stellte der Jugendsachbearbeiter ausweislich der Akten fest, daß die Familienverhältnisse der Kinder geordnet sind. Schließlich ließ die Polizei bei ihrer Entscheidung völlig außer Betracht, daß ein Ladendiebstahl ein Fall von geringer Bedeutung ist, der selbst bei Erwachsenen eine Regelspeicherfrist von höchstens drei Jahren rechtfertigt. Erst auf diese Vorhalte hin war die Polizei bereit, die Datensätze zu löschen.

- Der Walkman

  Ein 13½ Jahre alter Schüler entwendete Ende 1983 in einem Kaufhaus einen Walkman mit Kopfhörer zum Preis von 39,95 DM. Er gestand den Vorfall und brachte die gestohlene Ware zurück. Die Polizei speicherte ihn zunächst wegen Ladendiebstahls für zwei Jahre. 1986 verlängerte sie die Speicherfrist um weitere drei Jahre wegen Wiederholungsgefahr. Auch hier kreuzte sie in dem Vordruck einfach das Kästchen an; irgendwelche Tatsachen, aus denen sie die Wiederholungsgefahr herleitet, ergeben sich aus den Akten nicht. Auf meinen Vorhalt, daß selbst ein Erwachsener wegen eines solchen Vorfalls in der Regel nur drei Jahre gespeichert würde, löschte die Polizei den Datensatz.

Meine Feststellungen sollten für die Polizei des Landes Anlaß sein, bei der Speicherung von Kindern zurückhaltender zu sein. Auch wäre gut, wenn sie die Fälle der gegenwärtig gespeicherten Kinder – zumindest der 7- bis 10jährigen – überprüft. Immerhin befanden sich ausweislich der mir vom Landeskriminalamt überlassenen Statistiken im Spätherbst 1985 unter den 850 000 gespeicherten Personen mit 2,2 Millionen Straftaten ca. 9100 strafunmündige Kinder zwischen 7 und 14 Jahren.

3. Sicherheitsüberprüfungen

Der Staat muß Vorsorge treffen, daß geheimzuhaltende Informationen nicht in die Hände Unbefugter gelangen. Nur zuverlässige Personen sollen Kenntnis von sicherheitsempfindlichen Unterlagen erhalten können. Um dies zu erreichen, gibt es die sog.

Sicherheitsüberprüfungen. Dabei durchleuchten die Sicherheitsbehörden, vornehmlich der Verfassungsschutz, die Lebensverhältnisse der Personen, die Behörden in sicherheitsempfindlichen Bereichen einsetzen wollen. Sicherheitsüberprüft werden freilich nicht nur Angehörige des öffentlichen Dienstes. So mußte sich z. B. auch ein langjähriger Stadtrat einer solchen Sicherheitsüberprüfung unterziehen, als er Mitglied im Beirat für geheimhaltungsbedürftige Angelegenheiten seiner Stadt werden sollte mit dem Ergebnis, daß ihm das Landesamt für Verfassungsschutz zunächst wegen eines Schwagers in der DDR die für den Beirat notwendige Eignung absprach; Sicherheitsüberprüfungen sind aber auch in der gewerblichen Wirtschaft keine Seltenheit; sicherheitsüberprüft wird beispielsweise auch das Personal kerntechnischer Anlagen. Das hier zutagetretende Bemühen, möglichen Risiken vorzubeugen, ist verständlich. Doch darf darüber nicht außer acht bleiben, daß solche Sicherheitsüberprüfungen gravierende Eingriffe in die Persönlichkeitssphäre der Betroffenen darstellen. Sie können deshalb nur im Rahmen der rechtlichen Grenzen erfolgen, die unsere Verfassung vorgibt.

3.1 Sicherheitsüberprüfungen für Angehörige des öffentlichen Dienstes

In letzter Zeit bezweifeln immer häufiger Beamte und Angestellte in Eingaben, ob sie tatsächlich verpflichtet sind, der Aufforderung des Geheimschutzbeauftragten zu folgen, sich einer Sicherheitsüberprüfung zu unterziehen. Diese Zweifel sind sehr wohl berechtigt:

- Keine ausreichende Rechtsgrundlage bildet § 3 Abs. 2 Nr. 1 des Landesverfassungsschutzgesetzes, wonach das Landesamt für Verfassungsschutz bei der Überprüfung von Personen mitwirkt, denen im öffentlichen Interesse geheimzuhaltende Tatsachen, Gegenstände oder Kenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können. Diese Bestimmung räumt – wenn überhaupt – allenfalls dem Landesamt für Verfassungsschutz und nicht auch den anderen am Überprüfungsverfahren mitwirkenden Stellen, insbesondere nicht dem es einleitenden Geheimschutzbeauftragten Befugnisse ein. In keinem Fall läßt sich aus ihr eine Pflicht der Bediensteten zur Mitwirkung an der Sicherheitsüberprüfung herleiten. Ihr ist lediglich mittelbar zu entnehmen, daß Angehörige des öffentlichen Dienstes unter bestimmten Voraussetzungen sicherheitsüberprüft werden.
- Das Landesbeamtengesetz und das Tarifrecht kann man entgegen der Auffassung einiger Gerichte heute ebenfalls nicht als Rechtsgrundlage für die Überprüfung ansehen. Insbesondere genügen die für Beamten und Angestellte geltenden Vorschriften über die Treuepflicht, die Amtsführung und das Weisungsrecht des Vorgesetzten bzw. die Gehorsamspflicht des Untergebenen hierfür nicht, weil sie den Anforderungen des Volkszählungsurteils nicht gerecht werden. Aus ihnen kann der einzelne nicht entnehmen, unter welchen Voraussetzungen und in welchem Umfang er eine Einschränkung seines informationellen Selbstbestimmungsrechts hinnehmen muß. Darüber geben nur die ebenfalls der Geheimhaltung unterliegenden Richtlinien für die Sicherheitsüberprüfung von Bediensteten des Landes Baden-Württemberg hinreichend klare Auskunft.

Ich meine deshalb in Übereinstimmung mit meinen Kollegen im Bund und in den Ländern, daß nicht nur die Mitwirkung des Verfassungsschutzes an der Sicherheitsüberprüfung im Bundes- und Landesverfassungsschutzgesetz detailliert geregelt werden muß, sondern daß auch bereichsspezifische Vorschriften über die Sicherheitsüberprüfung selbst zu schaffen sind. Standort einer solchen Regelung könnte bei Beamten das Landesbeamtengesetz und bei Angestellten der Bundesangestellten-Tarifvertrag sein. Im Juni 1986 wies ich das Innenministerium auf diese Rechtslage hin und teilte ihm die Punkte mit, die aus meiner Sicht Bestandteil dieser bald zu schaffenden gesetzlichen Regelungen sein müssen. Insbesondere wäre zu regeln,

- welche Bediensteten unter welchen Voraussetzungen in welcher Art von Überprüfung einbezogen werden dürfen,
- inwieweit auch die Ehegatten und Verlobten der Bediensteten überprüft werden,
- daß sich der Umfang der Überprüfung nach den Erfordernissen des Einzelfalls beurteilt,
- welche Stelle die Überprüfung in die Wege leitet,
- welche Befugnisse der Geheimschutzbeauftragte hat,
- daß der zu Überprüfende über Tatsache, Zweck, Rechtsgrundlage und Ablauf der Überprüfung, vor allem über die beteiligten Stellen und die Verarbeitung seiner Daten zu unterrichten ist,
- welche Daten beim zu Überprüfenden erhoben werden dürfen,
- welche Stellen am Überprüfungsverfahren beteiligt und wo die Ergebnisse zusammengefaßt werden,
- wann Bedenken gegen die Beschäftigung in einem sicherheitsempfindlichen Bereich bestehen,
- daß und in welcher Form der Überprüfte über das Ergebnis der Überprüfung zu unterrichten ist,
- daß ihm im Falle von Sicherheitsbedenken grundsätzlich Gelegenheit zur Stellungnahme zu geben ist, insbesondere zu Auskünften von Referenzpersonen, und welche Ausnahmen hiervon bestehen,
- was mit den erhobenen Daten bei den verschiedenen am Verfahren beteiligten Stellen geschehen darf, insbesondere ob und wie lange sie in welcher Form aufbewahrt werden dürfen,
- ob und gegebenenfalls in welchem Umfang ein Einsichtsrecht des Überprüften in die Sicherheitsakten besteht, und
- daß die bei ihm und anderen Personen/Stellen erhobenen Daten strenger Zweckbindung unterliegen.

Außerdem unterbreitete ich dem Innenministerium konkrete Vorschläge darüber, wie es in der Zwischenzeit das Überprüfungsverfahren verbessern kann. Seine Reaktion war mehr als enttäuschend. Das Innenministerium teilte mir lediglich mit, mit der Frage der Rechtsgrundlage für Sicherheitsüberprüfungen würden sich seit geraumer Zeit Bund und Länder beschäftigen. Die Meinungen seien noch uneinheitlich. Es werde erwogen eine gesetzliche Regelung zu finden. Eine konkrete Stellungnahme zu meinen Vorschlägen hielt es bisher für nicht angebracht.

3.2 Sicherheitsüberprüfung aus Anlaß von „WINTEX-CIMEX 87"

Erhebliche Unruhe löste bei nicht wenigen Angehörigen von Behörden, u. a. den Mitarbeitern des Schwarzwald-Baar-Kreises die Aufforderung ihrer Dienststelle aus, sich wegen

der bevorstehenden Stabsrahmenübung „WINTEX-CIMEX 87" einer Sicherheitsüberprüfung durch das Landesamt für Verfassungsschutz zu unterziehen und dazu den für solche Überprüfungen üblichen Fragebogen auszufüllen. Dies hatte folgenden Hintergrund: Das Innenministerium meint, alle Übungsteilnehmer würden im Verlauf der Übung als „Geheim" eingestufte Unterlagen zu Gesicht bekommen und müßten deshalb zum Zugang zu solchen Unterlagen ermächtigt werden, falls sie aufgrund ihrer „zivilen" Tätigkeit nicht bereits dazu ermächtigt seien. Eine solche Ermächtigung ist aber nach den einschlägigen Richtlinien ohne vorherige Durchführung einer Sicherheitsüberprüfung nicht möglich. Eine solche schematische Verfahrensweise begegnet – vom Problem der Rechtsgrundlage einmal abgesehen – Bedenken. Sie berücksichtigt zu wenig die Tatsache, daß die mit einer Verpflichtung bis „Geheim" zwangsläufig verbundene Sicherheitsüberprüfung einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung des zu Überprüfenden darstellt. Dieser Eingriff erfolgt allein zur Durchführung einer zweiwöchigen Übung, bei der der Bedienstete möglicherweise gar kein „Geheim" eingestuftes Material in die Hände bekommt und auch sonst nicht Wissen darüber größeren Umfangs erlangt. Die Sicherheitsüberprüfung dagegen ist für ihn harte Realität. Bei dieser Sachlage verlangt der Grundsatz der Verhältnismäßigkeit, in jedem Einzelfall sorgfältig zu prüfen, ob es tatsächlich zur Durchführung der Übung geboten ist, den Teilnehmer bis zum Geheimhaltungsgrad „Geheim" zu ermächtigen. Differenzierungen sind also erforderlich und nicht pauschale Bewertungen. Von einer solchen Differenzierung gehen auch die der Stabsrahmenübung zugrunde liegenden Rahmenbestimmungen des Bundes aus. Außerdem fordert die „Verschlußsachenanweisung", nach der die Bestimmung des Geheimhaltungsgrades zu erfolgen hat: Kenntnis nur, wenn nötig. Wird dieser Grundsatz tatsächlich beachtet, verbietet sich, alle Übungsteilnehmer bis zum Geheimhaltungsgrad „Geheim" zu ermächtigen. Ich bat deshalb das Innenministerium, die nachgeordneten Behörden darauf hinzuweisen, daß ein differenziertes Vorgehen möglich und notwendig ist.

4. Datenmißbrauch bei der Polizei

Mein Appell im vergangenen Jahr an die Polizeibeamten des Landes, ihre dienstliche Stellung nicht für private Zwecke zu mißbrauchen, stieß leider bei einigen auf taube Ohren. Erneut war ich gezwungen, mich mit Datenmißbrauch zu befassen. Natürlich waren es wiederum nur wenige Einzelfälle; jedoch wäre ein Fehler, sie einfach als isolierte Ausreißer abzutun. Eher von Interesse wäre, einmal zu untersuchen, in welcher Größenordnung sich das Dunkelfeld bewegt. Und noch eine weitere Fehldeutung gilt es aus der Welt zu schaffen: ruft ein Polizeibeamter für private Zwecke – sei es, um sich finanzielle Vorteile zu verschaffen, vor anderen zu prahlen oder Bekannten gefällig zu sein u. a. – Informationen aus den polizeilichen Informationssystemen ab, so ist dies ein schwerer Verstoß gegen den Datenschutz, den sich die Behörde anrechnen lassen muß. Denn sie ist verantwortlich für die Einhaltung der Regeln des Datenschutzes: sie hat die Datenverarbeitungssysteme installiert, sie muß für ihren reibungslosen korrekten Betrieb sorgen und Mißbrauch durch Polizeibeamte verhindern. Hier bekommt die Polizei die Kehrseite der Medaille zu spüren, daß jeder ihrer 28 000

Beamten im Land aus welchem Anlaß auch immer auf die Fülle der gespeicherten Daten im bundesweiten Informations- und Auskunftssystem INPOL, in der landesweiten Datenbank PAD und zudem auch auf die zahllosen Fahrzeughalterdaten im Flensburger Kraftfahrtbundesamt in Sekundenschnelle zugreifen kann. Die Polizei muß alles daran setzen, daß ihre Mitarbeiter solche Systeme nicht unbefugt für polizeifremde Zwecke nutzen. Wird Datenmißbrauch durch Polizeibeamte ruchbar, gilt es alles daran zu setzen, die Vorfälle vollständig und exakt aufzuklären. Deshalb bleibt mir in aller Regel nichts anderes übrig als Strafantrag zu stellen. Das tue ich nicht gern, doch der Gesetzgeber gab mir dieses Instrument bewußt dafür an die Hand.

4.1 Merkwürdiges Zusammenspiel

Ein mehrfach vorbestrafter Versicherungsvertreter, der bereits früher Informand für die Polizei war, gab ihr 1985 den Hinweis, auch die Polizei sei nicht „dicht"; er könne von drei im Bereich der Polizeidirektion Rastatt tätigen Polizeibeamten Informationen erhalten. Die Ermittlungen gestalteten sich infolge der voneinander abweichenden und zudem immer wieder variierenden Aussagen der drei Polizeibeamten und des Anzeigeerstatters recht schwierig. Nach Einsicht in die Ermittlungsakten entschloß ich mich, gegen zwei der drei Polizeibeamten und gegen den Anzeigeerstatter Strafantrag zu stellen. Das Ergebnis der Ermittlungen der Staatsanwaltschaft war: Das Verfahren gegen den Anzeigeerstatter stellte sie ein, weil die zu erwartende Strafe wegen des Datenschutzverstoßes neben der gegen ihn bereits verhängten Freiheitsstrafe von 1 Jahr und 7 Monaten nicht ins Gewicht fiel. Erwartungsgemäß wurde auch das Strafverfahren gegen den Polizeibeamten, gegen den ich keinen Strafantrag gestellt hatte, eingestellt. Das Ermittlungsverfahren gegen den zweiten beteiligten Polizeibeamten endete mit Zahlung einer Geldbuße von 1500,– DM und anschließender Einstellung nach § 153 a StPO. Gegen den dritten Polizeibeamten erhob die Staatsanwaltschaft Anklage beim Schöffengericht. Sie beschuldigt ihn, polizeiliche Informationssysteme nach mehreren Personen abgefragt, zumindest teilweise die dabei erhaltenen Informationen an den Anzeigeerstatter weitergegeben und dafür Geldbeträge zwischen 50,– und 1200,– DM als Gegenleistung entgegengenommen zu haben. Wie das Gericht entscheidet, bleibt abzuwarten. Sicher ist freilich bereits jetzt, daß die Rastatter Vorfälle, über die auch Presse und Rundfunk mehrfach berichteten, dem Ansehen der Polizei nicht zuträglich waren.

4.2 Der allwissende Geschäftsführer

Ein Bürger bewarb sich 1985 bei einer Wach- und Sicherheitsfirma. Es kam zu einem persönlichen Vorstellungsgespräch. Dabei sagte ihm der Geschäftsführer der Firma, das vorgelegte polizeiliche Führungszeugnis sei wertlos, weil darin zu wenig eingetragen werde. Er habe dann das Besprechungszimmer verlassen, sei wenige Minuten später zurückgekehrt und habe ihn gefragt, ob es gegen ihn ein Verfahren wegen Nötigung gegeben habe. Der verdutzte Bewerber erklärte, dies sei 1982 eingestellt worden. Seine Frage, woher der Geschäftsführer dies wisse, beantwortete dieser nicht. Jedoch erklärte der Geschäftsführer, er wisse in wenigen Minuten alles über jemand. Der geschockte Bürger wandte sich an mich.

Beim Kontrollbesuch bei der Polizeidirektion Ludwigsburg stellten wir anhand der in der Datenstation geführten Kontrolliste fest, daß ein Polizeibeamter des Verkehrsdienstes justament zu der Zeit, als das Bewerbungsgespräch stattfand, abfragen ließ, ob über den Bürger im bundesweiten polizeilichen Informationssystem INPOL und in dem landesweiten polizeilichen Informationssystem PAD Daten gespeichert sind. Die INPOL-Abfrage war negativ, die PAD-Abfrage positiv: der Bürger war darin wegen eines 1982 von der Landespolizeidirektion Stuttgart II geführten Ermittlungsverfahrens wegen Nötigung erfaßt. Damals hatte ein Autofahrer den Bürger angezeigt, weil er sich angeblich an einer rot anzeigenden Ampel vor sein wartendes Fahrzeug gestellt und den Weg nicht freigegeben hatte, als die Ampel auf grün umschaltete. Da dieser Vorfall von geringer Bedeutung war und daher nur eine dreijährige Speicherung rechtfertigte, hätte ihn die Polizei zu der Zeit, als der Beamte des Verkehrsdienstes mißbräuchlich die Abfrage über den Bewerber durchführen ließ, gar nicht mehr speichern, geschweige denn weitergeben dürfen. Die Landespolizeidirektion Stuttgart II war deshalb auf meinen Hinweis hin rasch bereit, die gespeicherten Daten zu löschen und die Ermittlungsunterlagen zu vernichten. Erst recht hätte der Polizeibeamte des Verkehrsdienstes den Bürger nicht abfragen dürfen. Dies war schon deshalb unbefugt, weil die Polizei im Auftrag Privater keine derartigen Abfragen durchführen darf. Die Abfrage war aber auch unzulässig, weil sie ein Beamter durchführte, der weder generell noch im konkreten Fall mit der Wahrnehmung solcher Aufgaben betraut ist. Ich stellte deshalb Strafantrag gegen den Beamten des Verkehrsdienstes. Er wurde inzwischen zu einer Geldstrafe von 1400,– DM, der Geschäftsführer zu einer Geldstrafe von 3000,– DM verurteilt. Für den Bürger mag dies eine gewisse Genugtuung sein; die begehrte Stelle freilich erhielt er nicht.

4.3 Falsche Gefälligkeit

Die Staatsanwaltschaft Karlsruhe frug vor kurzem bei mir an, ob ich gegen einen Polizeibeamten bei der Autobahnpolizeidirektion Karlsruhe Strafantrag stelle. Es ging um folgendes: Er hatte Mitte 1986 INPOL und PAD abfragen lassen, um festzustellen, ob der Vater einer seiner Bekannten gesucht werde. Dieser Mann wollte gern wieder in die Bundesrepublik einreisen, hatte jedoch Angst, noch wegen eines früher verursachten Verkehrsunfalls gesucht zu werden. Der Polizeibeamte wurde fündig und gab der Bekannten den Hinweis, sie solle sich wegen des Vorgangs an das Amtsgericht oder die Staatsanwaltschaft Heilbronn wenden. Daneben standen weitere unbefugte Datenabrufe des Polizeibeamten zur Debatte; die Beweislage war jedoch insoweit wegen der voneinander abweichenden Aussagen der Vernommenen unklar. Deshalb stellte ich nur wegen des zuerst genannten Vorfalls Strafantrag. Die Staatsanwaltschaft stellte das Verfahren wegen geringer Schuld des Polizeibeamten inzwischen gegen Entrichtung eines Geldbetrags von 400,– DM an eine gemeinnützige Einrichtung nach § 153 a Abs. 1 StPO ein.

5. Schlamperei

Eines Tages erschien in meiner Dienststelle ein Journalist und legte mir eine Fülle von EDV-Ausdrucken des Landeskriminalamts auf den Tisch. Er berichtete, seiner Redaktion seien diese

Ausdrucke von einem Herrn X zugegangen. Dieser Herr X schrieb in einem Begleitbrief, den mir der Journalist auch vorlegte, erläuternd: Das Landeskriminalamt habe im Zuge eines Ermittlungsverfahrens gegen ihn 1984 eine Hausdurchsuchung durchgeführt und dabei u. a. 17 Aktenordner Geschäftsunterlagen beschlagnahmt. Diese habe es ihm später zurückgegeben. Bei der Durchsicht der Unterlagen habe er dann festgestellt, daß ihm das Landeskriminalamt auch Dateiausdrucke mit Dafen seiner Kunden – darunter eines Abgeordneten des Europäischen Parlaments – übermittelt habe. Das sei für ihn sehr interessant gewesen, habe er doch daraus außer den genauen Personalien seiner Kunden auch deren Vorstrafen bzw. frühere Ermittlungsverfahren ersehen können. In der Tat konnte der Einsender, der aufgrund der gegen ihn geführten Ermittlungen des Landeskriminalamts zu einer längeren Freiheitsstrafe wegen Unterschlagung u. a. verurteilt worden war und diese abgesessen hatte, solches den EDV-Ausdrucken entnehmen:

- 65 der mir insgesamt vorgelegten 73 Ausdrucke über Anfragen des Landeskriminalamts beim Kraftfahrt-Bundesamt enthielten neben den Fahrzeugdaten jeweils Vor- und Nachnamen, gegebenenfalls Geburtsname, Geburtsdatum und Geburtsort sowie die jetzige Anschrift des Kunden;
- in 10 dieser Fälle waren die Ausdrucke des Landeskriminalamts über seine Abfrage im landesweiten Informationssystem, der Personenauskunftsdatei, angefügt. Auf 4 dieser PAD-Ausdrucke war der Tatvorwurf im Klartext vermerkt; es ging um „Urkundenfälschung", „Sachbeschädigung", „Diebstahl Kfz" und „Warenbetrug, mittelbare Falschbeurkundung". In den übrigen Fällen waren die Zahl der gespeicherten Vorgänge und der Tatvorwurf in der Schlüsselzahl angegeben. Da hieß es z. B. „Müller, Peter: 2 T: 630, 224" was im Klartext bedeutete: ein Ermittlungsverfahren wegen Begünstigung und eines wegen Körperverletzung. Daß solche EDV-Ausdrucke nichts in fremden Händen zu suchen haben, zu allerletzt in den Händen von Personen, die bereits mit dem Gesetz in Konflikt gekommen sind, liegt auf der Hand.

Um zu sehen, ob sich die Dinge tatsächlich so zugetragen hatten, führten wir zwei Kontrollbesuche beim Landeskriminalamt durch. Dabei bestätigte sich die Schilderung des Herrn X: Das Landeskriminalamt hatte einst gegen ihn ermittelt, weil er im Verdacht stand, in den USA Fahrzeuge angemietet, in die Bundesrepublik verbracht und hier veräußert zu haben. Etwa 10 der 17 beschlagnahmten Aktenordner mit Geschäftsunterlagen enthielten Offerten amerikanischer Fahrzeuge. Da daraus jedoch nicht zu ersehen war, welche Fahrzeuge Herr X tatsächlich angemietet und in die Bundesrepublik verbracht hatte, führte das Landeskriminalamt anhand der in den Unterlagen vermerkten Fahrzeuggestellnummern ZEVIS-Abfragen beim Kraftfahrt-Bundesamt in Flensburg durch. Auf diese Weise stellte es 250 Fahrzeuge, die inzwischen in der Bundesrepublik zugelassen worden waren, und deren jetzige Eigentümer fest. Da das Landeskriminalamt nicht ausschließen wollte, daß der eine oder andere dieser Autobesitzer mit dem beschuldigten Herrn X gemeinsame Sache machte, hielt es für notwendig, durch eine Abfrage in der Personenauskunftsdatei abzuklären, wer von diesen 250 Autobesitzern wann und weshalb mit der Polizei in Konflikt gekommen und deshalb gespeichert war. Die Dateiausdrucke legte es jeweils in die Ordner an der Stelle ein, an der die Fahrzeugdaten genannt waren. Nach Abschluß des Ermittlungsverfahrens vergaß das Landeskriminalamt, zumindest aus einem Aktenordner die Dateiausdrucke herauszunehmen und zu vernichten. Diesen Ordner händigte es samt Dateiausdrucken dem Vater des Herrn X aus, der sie an seinen Sohn weitergab.

Dies hätte selbstverständlich nicht geschehen dürfen. Um eine solche rechtswidrige Datenweitergabe und die darin liegende Verletzung der schutzwürdigen Belange der abgefragten Kunden des Herrn X zu vermeiden, hätte das Landeskriminalamt geeignete Sicherungsmaßnahmen treffen müssen. Es hätte beispielsweise dafür sorgen müssen, daß solche Dateiausdrucke nicht in Ermittlungsakten, sondern in einen besonders gekennzeichneten Hefter oder Ordner kommen; zumindest hätte es sich vor der Rückgabe der beschlagnahmten Unterlagen sorgfältig davon überzeugen müssen, daß diese keine Dateiausdrukke mehr enthalten. Weil dies nicht geschah, ließ es das Landeskriminalamt an den nach § 8 LDSG erforderlichen Sicherungsmaßnahmen fehlen. Ich beanstandete diesen Vorfall nach § 18 LDSG. Das Landeskriminalamt erließ daraufhin eine Weisung, die sicherstellen soll, daß sich ähnliche Vorfälle nicht wiederholen.

6. Eingaben

Die Zahl der Eingaben, in denen Bürger nicht ohne Grund am Verhalten der Polizei Anstoß nahmen, war 1986 auffallend hoch. Das mag Zufall sein. Nur wenige Beispiele sollen belegen, was Bürgern widerfuhr:

6.1 Die „Verbrecherkartei"

Welcher Liebhaber von Fernsehkrimis kennt nicht die Szene, in der der Kommissar dem Kind, das Zeuge eines Verbrechens geworden war, in der meist vergeblichen Hoffnung auf diese Weise den Täter zu identifizieren, eine Sammlung mit Lichtbildern von Bösewichten vorzeigt. Daß die Führung einer solchen landläufig als „Verbrecherkartei" bezeichneten Lichtbildvorzeigedatei in der Realität ihre Tücken haben kann, zeigt folgender Fall:

Bei einer Auseinandersetzung zweier Wohnungsnachbarn mischte sich die 14jährige Tochter des einen ein und warf dem anderen vor, er stünde ja in der Verbrecherkartei. Sie habe sein Foto bei der Polizei gesehen. Diese Aussage wiederholte das Mädchen auch in der Schule, die auch die Kinder dieses Mannes besuchten. Da er sich diskriminiert fühlte, wandte er sich an mich und bat um Überprüfung. Dabei ergab sich folgendes: Vor acht Jahren ermittelte die Polizei gegen ihn wegen des Verdachts des versuchten sexuellen Mißbrauchs von Kindern. Im Zuge dieses Verfahrens wurde er auch nach § 81 b der StPO erkennungsdienstlich behandelt. Dazu gehört regelmäßig auch die Anfertigung eines Lichtbilds. Obwohl das Ermittlungsverfahren den Tatverdacht nicht bestätigte und die Staatsanwaltschaft es deshalb nach § 170 Abs. 2 StPO einstellte, hielt sich die Polizei dennoch für berechtigt, die erkennungsdienstlichen Unterlagen des Bürgers weiterhin aufzubewahren und sein Lichtbild in die Lichtbildvorzeigekartei aufzunehmen. Sie begründete dies mit dem Bestehen eines Restverdachts. Auf meine Initiative hin erklärte sie sich aber dann doch bereit, die erkennungsdienstlichen Unterlagen einschließlich des Lichtbilds in der Lichtbildvorzeigekartei zu vernichten. Es bleibt freilich die Frage, ob es überhaupt gerechtfertigt war, das Foto unseres Bürgers in die Lichtbildvorzeigekartei aufzunehmen: ich meine nein. Die Aufnahme in eine Lichtbildvorzeigekartei stellt einen so schwerwiegenden Eingriff in die Persönlichkeitssphäre des Betroffenen dar, daß sie in keinem Fall in Frage kommen kann, wenn die Staatsanwaltschaft

nicht einmal den zur Anklageerhebung erforderlichen hinreichenden Tatverdacht bejaht. Dies gebietet allein schon der Grundsatz der Verhältnismäßigkeit. Zudem verlangt auch das Innenministerium in seinen Richtlinien für die Führung der Lichtbildvorzeigekartei aus dem Jahr 1984, daß die Person, die in die Lichtbildvorzeigekartei aufgenommem werden soll, einer rechtswidrigen Tat dringend verdächtig sein muß.

6.2 Personenauskunftsdatei contra Bundeszentralregister

Welche Ungereimtheiten sich ergeben, wenn die Polizei glaubt, ihre Datenverarbeitung nicht an den Regeln über das Bundeszentralregister ausrichten zu müssen, zeigt folgender Fall:

Ein Taxifahrer beantragte im Oktober 1985 die Verlängerung seines Fahrausweises zur Fahrgastbeförderung. Im Rahmen des Erlaubnisverfahrens fragte die Führerscheinbehörde bei der Polizeidirektion Heidelberg an, ob dort „Bedenken gegen die Eignung" bestehen. Daraufhin teilte diese u. a. auch mit, in der Personenauskunftsdatei werde eine Straftat aus dem Jahr 1973 gespeichert. Die Führerscheinbehörde erfuhr auf diese Weise, daß der Taxifahrer im Jahr 1973 einen Polizisten mit den Worten „Sie sind mir viel zu blöd" beleidigt hatte und deswegen zu einer Geldstrafe von 60,- DM verurteilt worden war. Der Taxifahrer, dessen Fahrausweis zur Fahrgastbeförderung trotzdem verlängert wurde, beklagte sich zu Recht über diese Vorgehensweise. Die Datenübermittlung aus der Personenauskunftsdatei war nämlich aus mehreren Gründen rechtswidrig:

- Zum einen hätte die geringfügige Straftat im Zeitpunkt der Anfrage schon längst in der Personenauskunftsdatei gelöscht sein müssen. Daten aber, die die Polizei zu Unrecht speichert, darf sie schon deshalb nicht weitergeben.
- Zum anderen beachtete die Polizei nicht, daß die Verurteilung wegen Beleidigung im Bundeszentralregister schon längst getilgt war. Niemand, auch die Polizei, darf solche getilgten Verurteilungen im Rechtsverkehr verwerten. Dieses vom Bundesgesetzgeber festgelegte absolute Verwertungsverbot muß auch die Polizei bei der Übermittlung von Daten aus ihren Informationssystemen beachten.
- Zum dritten hätte die Polizei unabhängig von all diesen Überlegungen der Führerscheinbehörde die Verurteilung wegen Beleidigung aus dem Jahre 1973 nicht mitteilen dürfen, weil sie ersichtlich ohne jede Bedeutung für die jetzt, 12 Jahre später zu treffende Entscheidung der Führerscheinbehörde war.

Erstaunlich ist, wie das Innenministerium bisher selbst in diesem krassen Fall darauf beharrt, die Polizeidirektion Heidelberg habe recht getan.

6.3 Der perfekte Staat?

Was einem Bürger passieren kann, wenn der Staat auf seinem Recht besteht, zeigt folgender Fall: Eine 72jährige Dame zahlte das gegen sie festgesetzte Bußgeld wegen einer Verkehrssache in Höhe von 100,- DM nicht. Das Amtsgericht ließ nicht mit sich fackeln und ordnete Erzwingungshaft von 3 Tagen an. Nachdem die Frau der Aufforderung zum Antritt der Erzwingungshaft nicht Folge leistete, erließ

die Staatsanwaltschaft einen Vorführungsbefehl und forderte sie auf, sich bei ihrem Polizeirevier zum Antritt der Erzwingungshaft zu melden. Daraufhin überließ die Frau dem Polizeirevier drei ärztliche Atteste, die ihr Haftunfähigkeit bescheinigten, und bat, diese Atteste der Staatsanwaltschaft und dem Amtsgericht vorzulegen. Damit war der Fall allerdings nicht erledigt. Das Polizeirevier nahm die ärztlichen Atteste zum Anlaß, sich an die Führerscheinstelle zu wenden, die einst den Führerschein der 72jährigen Dame ausgestellt hatte, und wies sie darauf hin, die Frau sei erkrankt; deshalb bestünden Bedenken an ihrer Eignung zum Führen von Kraftfahrzeugen. Die angegangene Führerscheinstelle reichte die Mitteilung des Polizeireviers an die für den Wohnsitz der Dame zuständige Führerscheinstelle weiter. Von dort erhielt die Frau dann unter Hinweis auf den Inhalt eines der drei Atteste die Aufforderung, entweder ein ärztliches Attest über ihre Eignung zum Führen von Kraftfahrzeugen vorzulegen oder aber auf den Führerschein zu verzichten. Doch auch das war noch nicht das Ende des Falles: Wenige Tage später teilte das Staatliche Gesundheitsamt der Frau mit, das Amtsgericht habe eine amtsärztliche Untersuchung angeordnet, um ihre Haftfähigkeit zu überprüfen. Bei dieser Aufforderung blieb es dann allerdings. In der Folgezeit verlegte sich die Justiz auf Beitreibungsversuche: nachdem diese ergebnislos blieben und auch eine erneute Ladung zum Antritt der Erzwingungshaft nicht zum gewünschten Erfolg führte, kapitulierte sie schließlich. Auch die Führerscheinsache kam zu einem glücklichen Abschluß: nachdem der Arzt die Eignung der Dame zum Führen von Kraftfahrzeugen bestätigt hatte, teilte ihr die Führerscheinstelle mit, die Angelegenheit habe sich erledigt.

Diese wahre Geschichte hat vielerlei Aspekte. Ich hatte mich mit ihr zu befassen, weil sich die Dame bei mir beklagte, daß das Polizeirevier den Inhalt ärztlicher Atteste zur Überprüfung ihrer Eignung zum Führen von Kraftfahrzeugen an die Führerscheinstelle weitergegeben hat. Sie sieht darin eine Verletzung des Datenschutzes, weil sie die Unterlagen dem Polizeirevier allein zur Weiterleitung an die Staatsanwaltschaft und das Amtsgericht übergeben hat. Mein Versuch, die zuständige Polizeidirektion dazu zu bewegen, die Rechtsgrundlage für das Vorgehen des Polizeireviers und seine Beweggründe zu nennen, blieb erfolglos. Sie berief sich darauf, sie habe die weitergegebenen Informationen über die Frau nicht aus Karteien/Dateien entnommen; deshalb sei meine Kontrollbefugnis nicht gegeben. Damit machte es sich die Polizei wieder einmal recht einfach: hätte sie mir die konkreten Rechtsgrundlagen nennen müssen, wäre die Antwort schwieriger gewesen. Denn ihre Vorgehensweise könnte sie allenfalls auf die ursprünglich für ganz andere Fallgestaltungen geschaffene Generalklausel der §§ 1 und 3 des Polizeigesetzes stützen.

5. Teil: Kriminologische Forschung

Die Kriminologie ist die Wissenschaft vom Verbrechen. Seine Ursache möchte sie ergründen und damit zur Verhütung von Straftaten beitragen. Viele Kriminologen befassen sich deshalb sehr intensiv mit der Person, den Lebensumständen, dem Umgang und dem Verhalten von Straftätern: ihre Aufmerksamkeit gilt daneben

aber auch den in der Strafrechstpflege Tätigen – seien es Straf-, Vollstreckungsrichter, Staatsanwälte oder Bewährungshelfer. Über all dies sammeln die Kriminologen zum Teil eine Fülle von Informationen und werten sie aus. Solche Forschungsvorhaben sind notwendig und wichtig. Doch rechtfertigt ihr guter Zweck allein noch nicht jedes Mittel. Auch hier gilt es die Grenzen zu beachten, die das Datenschutzrecht der Forschung setzt. Dabei macht keinen Unterschied, ob Gegenstand der Forschung jemand mit einer weißen Weste oder ein Straftäter ist. Denn auch Straftäter müssen selbstverständlich das Sammeln und Verarbeiten ihrer Daten ohne oder gegen ihren ausdrücklichen Willen nur hinnehmen, soweit eine Rechtsvorschrift dies dem Forscher ausdrücklich erlaubt. Um zu sehen, wie die Kriminologie mit diesen Vorgaben zurechtkommt, führten meine Mitarbeiter und ich 1986 Kontrollbesuche an den Universitäten Heidelberg, Konstanz und Tübingen durch und überprüften dort 14 kriminologische Forschungsprojekte. Dabei zeigte sich zum einen, daß die einzelnen Forscher sehr unterschiedlich vorgehen, und zum anderen, daß sie zunehmend für ihre Forschung die Möglichkeiten der Computer in den Universitätsrechenzentren nutzen. Eine Reihe wichtiger, teils neuer Fragestellungen für den Datenschutz ergab sich daraus.

1. Personenbezogen oder anonym?

Forschung mit anonymen Daten ist uneingeschränkt möglich; Forschung mit personenbezogenen Daten dagegen nur, soweit sie das Datenschutzrecht erlaubt. Es macht deshalb einen großen Unterschied, ob das Datenmaterial eines Forschungsprojekts noch personenbezogen oder schon anonym ist. Ob das eine oder andere der Fall ist, ist in der Praxis nicht immer einfach zu beurteilen. Auch gehen die Meinungen der Vertreter des Datenschutzes und der Forschung darüber öfter auseinander. So war es auch bei einigen Forschungsvorhaben des Kriminologischen Instituts der Universität Heidelberg; zwei davon seien exemplarisch dargestellt:

1.1 Projekt „Strafzumessung"

Ziel des Projekts ist, die Gründe der unterschiedlichen Strafzumessung trotz gleichgelagerter Situation zu ergründen. Zu diesem Zweck befragte das Kriminologische Institut Heidelberg im Herbst 1979 ca. 525 Strafrichter und Staatsanwälte an den Amts-, Land- und Oberlandesgerichten und Staatsanwaltschaften des Landes Niedersachsen über ihre Arbeit und ihre Einstellung u. a. zum Strafzweck, zur Strafvollstrekkung und zur Todesstrafe. Es verwendete dabei einen Fragebogen, in dem weder nach Name noch Anschrift gefragt war. Um so mehr war aus ihm über den beruflichen Werdegang der Befragten zu ersehen, u. a.

- ob sie als Richter oder Staatsanwalt beschäftigt und Richter oder Beamter auf Zeit oder Probe sind, ob und wie lange sie die Strafrichtertätigkeit am Amts-, Land- oder Oberlandesgericht ausüben und ob sie, sofern sie dem Land- oder Oberlandesgericht angehören, Vorsitzender oder Beisitzer sind,
- ob sie in einer Strafvollstreckungskammer tätig sind oder ob und wie lange als Jugendrichter oder Jugendstaatsanwalt,
- ob ihre Dienststelle ihren Sitz in einer Stadt mit weniger als 50000, mit 50000 bis 250000 oder mit über 250000 Einwohnern hat.

Außerdem gaben die Befragten Geschlecht, Religionszugehörigkeit, ihre Noten in den beiden Staatsexamen und ihr Alter – unter 36, 36 bis 45, 46 bis 55, 56 Jahre und darüber – an. Diese und alle anderen erfragten Angaben speichert das Institut zur Zeit noch auf Lochkarten, Magnetplatten und Magnetband.

Es meint, dieser Datenbestand sei anonym. Diese Auffassung kann ich nicht teilen. Sie stimmt mit der herrschenden Meinung in der datenschutzrechtlichen Literatur, von der auch ich ausgehe, nicht überein. Danach sind Datenbestände nur dann anonym, wenn es faktisch nicht mehr möglich ist, einen Bezug zu der Person, auf die sie sich beziehen, herzustellen. Eine solche faktische Anonymisierung ist gegeben, wenn der Forscher oder andere Personen, denen das Datenmaterial zugänglich ist, den Personenbezug nur noch mit einem völlig unangemessenen und daher nicht zu erwartenden Aufwand herstellen könnten. Nicht kommt es darauf an, ob dies tatsächlich beabsichtigt ist; die objektive Möglichkeit genügt. Legt man diesen Maßstab an, wird rasch klar, daß bei dem gespeicherten Material von Anonymität nicht die Rede sein kann. Das Kriminologische Institut braucht nur das jedermann zugängliche Jahrbuch der Justiz, eventuell noch die Geschäftsverteilungspläne der Gerichte von Niedersachsen zur Hand zu nehmen und zu seinem Datenbestand in Beziehung setzen, dann könnte es gewiß eine Reihe der befragten Personen identifizieren und feststellen, welche Angaben sie machten. Denn es hat einerseits in seinem Datenbestand eine Fülle von Angaben über die richterliche Tätigkeit, die berufliche Stellung, den Sitz des Gerichts, die Art des Gerichts, das Alter und das Geschlecht der Befragten. Im Jahrbuch der Justiz stehen andererseits alle Richter und Staatsanwälte, die zur Zeit der Befragung an den einzelnen Gerichten und Staatsanwaltschaften in Niedersachsen tätig waren, mit Name, Geburtstag und Dienstalter; zudem ist bei den am Land- oder Oberlandesgericht Tätigen zu ersehen, ob sie Vorsitzender oder Beisitzer sind.

Obwohl also das Datenmaterial personenbezogen ist, bedeutet dies nicht, daß die Datenspeicherung von vornherein unzulässig wäre. Denn dem Institut ist das Forschen mit personenbezogenen Daten keineswegs generell verboten. Es darf dies vielmehr im Rahmen der Voraussetzungen des § 20 LDSG tun. Da diese hier gegeben sind, ist gegen die Datenspeicherung als solche nichts einzuwenden. Bloß muß das Institut zum Schutz der gespeicherten Daten noch die erforderlichen Datensicherungsmaßnahmen ergreifen. Außerdem muß es die Daten nach Abschluß seines Projekts entweder löschen oder zumindest faktisch anonymisieren. In diesem Verlangen kann ich entgegen der Meinung des Instituts keinen ungerechtfertigten Eingriff in die Forschungsfreiheit sehen.

1.2 Projekt „Jugendstrafvollzug"

Mit diesem Vorhaben untersucht das Kriminologische Institut Heidelberg über einen Beobachtungszeitraum von ca. 10 Jahren hinweg die Entwicklung von 500 jungen Strafgefangenen, die 1960 aus zwei Jugendstrafanstalten in Nordrhein-Westfalen entlassen wurden. Das Datenmaterial erhielt es von einem Doktoranden der Universität Göttingen. Das Institut speicherte die Angaben auf Lochkarte und Magnet-

platte. Der gespeicherte Datenbestand enthält ca. 230 Datenarten. Diese geben teilweise bis in alle Einzelheiten Aufschluß über den Werdegang der Probanden, ihre Familienverhältnisse und Familienangehörigen, ihre Erkrankungen und Straftaten. Gespeichert ist auch ihr Geburtsdatum, Familienstand, der Tag ihrer Entlassung und die Jugendstrafanstalt, aus der sie 1960 entlassen wurden.

Trotz dieser Fülle höchst sensibler Informationen gehe ich davon aus, daß das Institut – anders als bei seinem Forschungsprojekt „Strafzumessung" – die Probanden nicht identifizeren kann. Es bräuchte dazu ein Zusatzwissen, das es sich – wenn überhaupt – nur unter sehr schwierigen Umständen beschaffen könnte und deshalb nicht zu erwarten ist. Damit ist der Datenbestand freilich noch nicht anonym. Wäre dem so, könnte ihn das Institut jederzeit ohne Verstoß gegen das Datenschutzrecht veröffentlichen oder sonstwie Dritten zugänglich machen. Gerade aber dies darf nicht sein. Denn der eine oder andere verfügt möglicherweise über das erforderliche Zusatzwissen und könnte damit eine Reihe der gespeicherten Personen identifizieren. Deshalb muß das Kriminologische Institut durch geeignete Vorkehrungen sicherstellen, daß niemand anderes als es selbst die gespeicherten Einzelangaben erfährt. Nur dann wäre der gespeicherte Datenbestand tatsächlich anonym. Solche Vorkehrungen hatte das Institut bei meinem Kontrollbesuch noch nicht getroffen. Ich schlug ihm deshalb vor, die gespeicherten Daten wie personenbezogene gegen Zugriff durch Dritte zu schützen, keine fallbezogenen Einzelangaben daraus zu veröffentlichen und das Datenmaterial nach Abschluß der beabsichtigten Auswertungen zu löschen. Denselben Vorschlag unterbreitete ich ihm für andere Projekte mit vergleichbarer Problematik.

2. Die Einwilligung

Muß ein Forscher die Einwilligung seiner Probanden einholen, wenn er Informationen über sie erheben und speichern will? Welche Anforderungen sind an eine solche Einwilligung zu stellen? Diese Fragen stellen sich besonders nachdrücklich beim Forschungsprojekt „Maßregelvollzug" des Kriminologischen Instituts Heidelberg. Mit diesem Projekt will das Institut untersuchen, ob und inwieweit Personen während ihrer Unterbringung in einem psychiatrischen Krankenhaus, die ein Gericht nach § 63 StGB angeordnet hat, in ihren Rechtsschutzmöglichkeiten beeinträchtigt sind. Das Institut bezog in die Untersuchung 146 Probanden ein, die von Ende 1983 bis Anfang Februar 1985 im Psychiatrischen Landeskrankenhaus Wiesloch untergebracht waren. Dabei ging es in mehreren Schritten vor:

- Zunächst nahmen Mitarbeiter des Instituts an der mündlichen Anhörung jedes der 146 Probanden teil, die die Strafvollstrekkungskammer im Rahmen der jährlichen Überprüfung der Fortdauer der Unterbringung durchführen muß. Sie beobachteten dabei die Probanden und Verfahrensbeteiligten und zeichneten die Anhörung auf Tonband auf. Eine schriftliche Einwilligung der Probanden holten die Institutsmitarbeiter nicht ein. Der Projektleiter versicherte mir jedoch, der beauftragte Richter der Strafvollstreckungskammer habe die Probanden jeweils vor Beginn der Verhandlung über das Ziel des Projekts und die beabsichtigte Beobachtung und Tonbandaufzeichnung aufgeklärt und um ihre mündliche Einwilligung gebeten. Diese Einwilligung hätten alle Probanden erteilt.

- Nach der Anhörung trugen die Institutsmitarbeiter jeweils ihre Beobachtungen in ein vorbereitetes, sehr detailliertes Auswertungsschema ein. Außerdem speicherten sie diese Informationen unter einer Probandennummer auf Magnetband und Magnetplatte. In diesem EDV-Bestand sind u. a. Angaben registriert über
  - den emotionalen Zustand und die affektive Reaktion der Probanden während der Anhörung,
  - psychische und physische Auffälligkeiten, die sich bei der Anhörung zeigten,
  - besondere Verhaltensweisen,
  - geäußerte Meinungen, Einstellungen und Erwartungen zu Fragen, die mit der Unterbringung zusammenhängen.
- Dann nahmen die Mitarbeiter des Instituts mit Genehmigung des Kammervorsitzenden bei der Strafvollstreckungskammer Einsicht in die Strafverfahrens- und Vollstreckungsakten der Probanden. Außerdem überließ ihnen die Staatsanwaltschaft mit Einwilligung des Justizministeriums ihre Gnadenakten. Aus all diesen Akten kopierten die Mitarbeiter des Instituts zahlreiche Vorgänge, insbesondere alle psychiatrischen und psychologischen Gutachten. Zusätzlich übertrugen sie den Akteninhalt in ein weiteres umfangreiches Auswertungsschema. Dieses enthält u. a. detaillierte Anfgaben über die Familien- und Lebensverhältnisse, die wirtschaftlichen und gesundheitlichen Verhältnisse sowie über psychiatrische, psychologische und pädagogische Begutachtungen und Behandlungen. All dies geschah, ohne daß zuvor die Gerichte und Staatsanwaltschaften und das Kriminologische Institut die Einwilligung der Probanden zu ihren Vorgehensweisen eingeholt hätten.

  Zur Zeit bewahrt das Institut die Aktenkopien, aus denen auch die Namen der Probanden zu ersehen sind, und die Auswertungsschemata auf. Die Angaben in den letzteren wollte es ursprünglich auch automatisiert speichern. Zur Zeit des Kontrollbesuchs waren deshalb Mitarbeiter des Instituts mit der Erstellung des Datensatzes beschäftigt.

Aus datenschutzrechtlicher Sicht ist zu diesem Projekt folgendes zu bemerken:

- Die Informationen aus der mündlichen Verhandlung

  Die Speicherung aller Informationen, die das Institut während der mündlichen Anhörung erfuhr, ist nicht rechtmäßig, weil es an der dafür erforderlichen Einwilligung der Probanden fehlt. Eine wirksame Einwilligung liegt nämlich nur vor, wenn folgendes beachtet ist: die Einwilligung muß nach § 5, 20 LDSG schriftlich erteilt sein; eine andere Form genügt nur, wenn sie wegen der besonderen Umstände angemessen ist. Darüber hinaus ist der, um dessen Einwilligung ersucht wird, über deren Bedeutung aufzuklären. Ihm muß gesagt werden, wer welche Angaben zu welchem Zweck in welcher Weise und voraussichtlich wie lange speichern will. Nur dann kann er in etwa die Tragweite seiner Entscheidung überblicken. Das wiederum ist eine wichtige Voraussetzung für eine wirksame Einwilligung. All dies beachtete das Kriminologische Institut bei seinem Vorgehen nicht ausreichend: entgegen seiner Meinung konnten die Probanden der Belehrung durch den beauftragten Richter der Strafvollstreckungskammer nicht hinreichend deutlich entnehmen, daß das Institut seine Beobachtungen anschließend für längere Zeit automatisiert speichern wird. Auch war es nicht vertretbar, auf eine schriftliche Einwilligung zu verzichten. Die Schriftform hat der Gesetzgeber ja gerade deshalb geschaffen, daß den Betroffenen besonders

bewußt wird, worauf sie sich einlassen. Die Befürchtung des Instituts, eine ganze Reihe von Probanden hätte wegen ihres psychischen und physischen Zustands nicht eingewilligt, wenn sie dieses schriftlich hätten tun müssen, rechtfertigt ein Abgehen von der Schriftform nicht. Die besondere Situation, in der sich die Probanden bei der Anhörung durch die Strafvollstreckungskammer befinden, hätte vielmehr besonderer Anlaß sein müssen, alles daran zu setzen, ihre Entscheidungsfreiheit unbedingt zu gewährleisten. Ohne umfassende Information, was beabsichtigt ist, und ohne schriftliche Einwilligung war dem nicht so.

Aus alledem folgt: da das Institut das Datenmaterial unzulässig speichert, muß es dieses unverzüglich löschen. Sein Interesse, das Forschungsvorhaben zu Ende zu bringen, muß demgegenüber zurücktreten. Einen Ausweg, auf den ich das Institut hinwies, gäbe es freilich: es müßte sich unverzüglich darum bemühen, die schriftliche Einwilligung aller Probanden in die Fortdauer der Speicherung ihrer Daten zu erhalten. Dabei müßte das Institut sich auch vergewissern, ob die Probanden tatsächlich einwilligungsfähig sind; Zweifel kann es daran geben, weil das Gericht deren Einweisung in das psychiatrische Krankenhaus im Hinblick auf ihre Schuldunfähigkeit bzw. verminderte Zurechnungsfähigkeit angeordnet hatte. Soweit es an der Einwilligungsfähigkeit fehlt, müßte sich das Institut an den gesetzlichen Vertreter wenden. Die Daten all der Probanden, die dem Institut die Einwilligung endgültig verweigern, oder die das Institut überhaupt nicht mehr ansprechen kann, wären unverzüglich zu löschen.

- Auswertung der Akten

  Nicht rechtmäßig war auch die automatisierte Speicherung all der Informationen, die das Institut den Strafverfahrens- und Vollstreckungsakten der Gerichte und den Gnadenakten der Staatsanwaltschaften entnommen hat. Nach § 20 Abs. 1 LDSG wäre dies ohne ausdrückliche schriftliche Einwilligung der Probanden nämlich nur zulässig, wenn man davon ausgehen könnte, daß die Speicherung die schutzwürdigen Belange der Probanden nicht beeinträchtigt. Davon kann aber nicht die Rede sein:

  - Zum einen ist schon fraglich, ob nicht bereits die Art und Weise, wie das Institut an die Informationen kam, die schutzwürdigen Belange der Probanden beeinträchtigt. Gewährt die Justiz nämlich einem Forscher Einsicht in Straf- und Gnadenakten, so liegt darin ein Eingriff in das informationelle Selbstbestimmungsrecht. Sie erlaubt damit nämlich dem Forscher, die nur für Gericht oder Staatsanwaltschaft bestimmten Angaben für einen anderen Zweck, nämlich den der Forschung, zu nutzen. Eine solche Zweckänderung ist nur im überwiegenden Allgemeininteresse und nur aufgrund einer Rechtsvorschrift zulässig; eine solche existiert derzeit nicht. Folglich kann die Justiz nur unter Zuhilfenahme der Rechtsprechung zum „Übergangsbonus" noch für eine gewisse Übergangszeit ohne gesetzliche Grundlage Einsicht in Akten gewähren. Da sie jedoch bereits jetzt soweit wie irgend möglich das Recht des anderen zu beachten hat, selbst über die Verwendung seiner Daten zu bestimmen, darf sie dies in der Regel nicht ohne Einwilligung des Betroffenen tun. Nur wenn dies nicht möglich oder zumutbar wäre, könnte sie darauf verzichten. In dieser Beurteilung der gegenwärtigen Rechtssituation weiß ich mich mit dem Justizministerium im Prinzip einig, mit dem ich die Problematik erörterte.

- Zum anderen beeinträchtigt die automatisierte Speicherung zweifelsohne die schutzwürdigen Belange der Probanden. Denn diese Informationen erhellen praktisch ihren gesamten Lebens- und Intimbereich. Es ist daher schlechterdings ausgeschlossen, solche Daten zu nutzen, ohne damit zugleich die schutzwürdigen Belange der Probanden zu beeinträchtigen. Der Einwand des Instituts, diese Beeinträchtigung müsse wegen des überwiegenden Forschungsinteresses hingenommen werden, zieht nicht. Denn § 20 Abs. 1 LDSG stellt ausschließlich auf die schutzwürdigen Belange ab; es geht nicht an, entgegen seinem klaren Wortlaut, hier die Forschungsinteressen als Rechtfertigungsgrund hineinzuinterpretieren.

Aus alledem folgt: das Kriminologische Institut darf die aus den Justizakten gewonnenen Informationen so lange nicht automatisiert speichern, als es an der Einwilligung der Probanden fehlt. Das Institut teilt diese Meinung zwar nicht, will jedoch gleichwohl von einer automatisierten Speicherung absehen und die Auswertungsschemata lediglich von Hand auswerten. Geht es so vor, findet § 20 LDSG keine Anwendung. Mit den Vorgaben des Bundesverfassungsgerichts im Volkszählungsurteil dürfte eine solche Verfahrensweise gleichwohl nicht zu vereinbaren sein.

3. Das verlängerte Sozialgeheimnis

Nicht selten will die kriminologische Forschung Strafakten auswerten, in denen sich Unterlagen von Sozialleistungsträgern befinden. Dann ergeben sich besondere Probleme, weil solche Schriftstücke dem Sozialgeheimnis unterliegen und daher besonders geschützt sind. Dessen sind sich bislang freilich weder Gerichte noch Forscher so recht bewußt. Deutlich zeigte sich dies am Forschungsprojekt „Erzieherische Maßnahmen im deutschen Jugendstrafrecht", das eine Forschungsgruppe am Institut für Rechtstatsachenforschung der Universität Konstanz durchführt. Sie will damit untersuchen, ob und welche erzieherischen Maßnahmen die Staatsanwaltschaften und Gerichte gegenüber straffälligen Jugendlichen anstelle eines förmlichen Verfahrens anordnen können, für welche Tätergruppen zweckmäßig sind. Für diese Untersuchung übersandten Amts- und Landgerichte aus dem ganzen Bundesgebiet jeweils mit Zustimmung ihres Justizministeriums dem Institut insgesamt 1134 Strafakten über Jugendliche der Geburtsjahrgänge 1961 bis 1966. Die Forschungsgruppe wertete diese Akten aus und speicherte die Fülle der so erhobenen Informationen - pro Person über 360 Datenarten - im Rechenzentrum der Universität Konstanz auf Magnetbändern. Darunter befindet sich auch der Inhalt der in den Strafakten enthaltenen Berichte der Jugendgerichtshilfe; allein dieser Datensatz umfaßt u. a. Angaben über den schulischen Werdegang, die Berufsausbildung, Freizeitgestaltung, das Einkommen des Beschuldigten, seine Vorstrafen, das Ergebnis der Charakterdarstellung des Beschuldigten (positiv, negativ, neutral), Alkohol- und Drogenkonsum, Angaben zur Straffälligkeit in der Familie, besondere Krankheiten physischer und psychischer Art, die Gesinnung (gleichgültig, roh, Reue, unklar) und die Prognose (günstig, ungünstig, ungewiß, unklar).

Gerichte und Staatsanwaltschaften dürfen solche Berichte der Jugendgerichtshilfe aus Strafakten nur unter den Voraussetzungen des § 75 SGB X für Forschungszwecke zur Verfügung stellen. Danach ist eine Herausgabe - vorausgesetzt, daß es unzumutbar ist, die Einwilligung der Betroffenen einzuholen - nur erlaubt

- soweit dies für die wissenschaftliche Forschung im Sozialleistungsbereich erforderlich und
- schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung im Sozialleistungsbereich das Geheimhaltungsinteresse erheblich überwiegt.

Das heißt: das kriminologische Forschungsvorhaben muß zugleich als Forschungsbeitrag im Sozialleistungsbereich zu werten sein. Dies ist beispielsweise der Fall, wenn die Untersuchung auch dazu dienen soll, Erkenntnisse für die Jugendgerichtshilfe zu gewinnen. Bei der weiteren Frage, ob es unzumutbar ist, die Einwilligung einzuholen, sind alle Umstände des Einzelfalls zu berücksichtigen. Die Zumutbarkeit kann man nicht allein schon deshalb verneinen, weil möglicherweise bei einem solchen Vorgehen nicht genügend Probanden ihre Einwilligung erteilen oder einiger Verwaltungsaufwand entsteht.

Diesem Maßstab wird das Forschungsprojekt „Erzieherische Maßnahmen im deutschen Jugendstrafrecht" nicht voll gerecht. Ich verstehe zwar gut, daß die Gerichte wegen der Fülle der ausgewerteten Akten und ihrer Arbeitsüberlastung die Erhebungsbogen nicht selbst ausfüllen konnten. Bloß hätten sie dann statt dessen nicht einfach die Strafakten dem Institut für Rechtstatsachenforschung übersenden sollen, sondern sich zunächst darum bemühen müssen, die Einwilligung der betroffenen Jugendlichen hierzu zu erhalten.

4. Nachfolgeuntersuchungen

Für den Forscher sind Informationen ein wichtiges Kapital. Deshalb ist er bestrebt, sie möglichst lange und intensiv zu nutzen. Auf der anderen Seite setzt diesem Wunsch § 20 Abs. 1 LDSG Grenzen: die Speicherung personenbezogener Daten ist nur für ein bestimmtes Forschungsvorhaben erlaubt. Wegen dieser Situation stellt sich in der Praxis immer wieder die Frage, unter welchen Voraussetzungen ein Forscher Daten noch nach Abschluß eines Forschungsvorhabens für spätere wissenschaftliche Untersuchungen aufbewahren darf. Besonders deutlich trat diese Problematik beim Forschungsprojekt „Mehrfachtäter und Karriereabbruch" zutage, das eine Forschungsgruppe beim Institut für Rechtstatsachenforschung der Universität Konstanz plant. Sie will mit diesem Projekt auf einer früheren Untersuchung aufbauen, in der sie der Frage nachging, bei welchen jugendlichen Tätergruppen die von Staatsanwaltschaft und Gerichten angeordneten erzieherischen Maßnahmen so erfolgreich verliefen, daß der Jugendliche eine weitere straffreie Lebensführung erwarten läßt. Diese Untersuchung ist inzwischen abgeschlossen; die dafür angelegte Namensdatei hat ihren Dienst getan. Gleichwohl will das Institut diese Namesdaten nicht löschen, weil es im Rahmen des geplanten neuen Projekts gerade die Namen dieser Personen benötigt. Es möchte über sie vom Bundeszentralregister erfahren, welche Registereintragungen nach Eintritt der Volljährigkeit erfolgten. Ob und in welcher Weise es diese Registereintragungen erhalten kann, prüft zur Zeit der Generalbundesanwalt. Obwohl dessen Genehmigung noch aussteht, halte ich es für vereinbar mit § 20 Abs. 1 LDSG, wenn das Institut für Rechtstatsachenforschung in der geplanten Weise vorgeht.

Zwar erlaubt § 20 Abs. 1 LDSG eine Datenspeicherung nur für ein bestimmtes Forschungsvorhaben. Will ein Forscher die Daten eines bestimmten Forschungsvorhabens noch nach dessen Abschluß speichern, geht dies folglich nur, wenn er diese Daten

für ein neues bestimmtes Forschungsvorhaben braucht. Wann dies der Fall ist, ist nicht einfach zu entscheiden. Sicher reicht dafür nicht die bloße Absicht des Forschers, die Daten irgendwann einmal für ein noch nicht näher fixiertes Forschungsvorhaben zu verwenden. Solange seine Planungen noch so vage sind, läßt sich nämlich überhaupt nicht feststellen, ob die Voraussetzungen des § 20 Abs. 1 LDSG für eine Speicherung vorliegen. Dafür bedarf es präziserer Vorstellungen über das künftige Projekt. Auf der anderen Seite wäre es aber überzogen zu verlangen, daß jede Phase der Anschlußuntersuchung bereits im Zeitpunkt des Abschlusses des früheren Forschungsprojekts im Detail festliegen und konzipiert sein muß. Sinn und Zweck des § 20 Abs. 1 LDSG ist vielmehr Genüge getan, wenn im Zeitpunkt des Abschlusses des ersten Forschungsvorhabens konkrete nachprüfbare Vorstellungen über das Folgeprojekt bestehen, ein realistischer Zeitplan für dessen Durchführung vorliegt und anzunehmen ist, daß dies auch so mit einiger Wahrscheinlichkeit geschieht.

5. Tübinger Langzeituntersuchung

Eine in ihrer Art in der Bundesrepublik einmalige kriminologische Untersuchung lernte ich beim Kriminologischen Institut der Universität Tübingen kennen: die sog. Tübinger Jungtäter-Vergleichsuntersuchung. Mit dieser Untersuchung begann das Institut bereits Mitte der 60er Jahre - also in einer Zeit, in der der Datenschutz allenfalls ein Thema für einige Experten, aber keineswegs noch für den Gesetzgeber war. Diese Untersuchung zeichnet sich zum einen durch die Fülle an Informationen aus, die das Institut aus allen Lebensbereichen der Probanden zusammentrug. Zum andern ist an ihr bemerkenswert, daß ihr das Institut von Beginn an nicht konkrete wissenschaftliche Fragestellungen zugrunde legte, sondern es bewußt der weiteren Entwicklung überließ, welche Fragen es untersuchen und welche Auswertungen es vornehmen will. Im einzelnen ging das Institut bei der Untersuchung so vor: Zunächst wählte es in den Jahren 1965 bis 1969 je 200 Männer zwischen 20 und 30 Jahren aus den Häftlingen der Vollzugsanstalt Rottenburg und der vergleichbaren Durchschnittsbevölkerung aus dem räumlichen Einzugsbereich dieser Vollzugsanstalt aus. Dabei standen ihr für die Auswahl der Häftlinge (sog. H-Probanden) die Zugangslisten der Vollzugsanstalt zur Verfügung. Die Vergleichsgruppe (sog. V-Probanden) wählte ein Mitarbeiter des Instituts aus den Meldekarteien der Einwohnermeldeämter nach dem Zufallsverfahren aus. Das Institut schrieb die so gezogenen Probanden an und bat sie, an der Untersuchung mitzuwirken und ihre Einwilligung schriftlich zu erklären. Der Vordruck, den ihnen das Institut zukommen ließ, enthielt folgende Erklärung:

> „Hiermit erkläre ich mein Einverständnis, daß ich im Institut für Kriminologie der Universität Tübingen untersucht werde und daß über meine Person Erhebungen bei Behörden und Arbeitgebern durchgeführt werden dürfen. Mir ist ausdrücklich versichert worden, daß die Untersuchung reinen Forschungszwecken dient, die mit der Untersuchung beauftragten Personen über die erhobenen Tatsachen Verschwiegenheit bewahren und über meine Person Dritten gegenüber keinerlei Auskünfte erteilen werden."

Das Institut befragte die Probanden, die diese Erklärung unterschrieben haben, führte psychologische Tests durch und unterzog sie medizinischen Untersuchungen, z. B. einer Chromosomen-Untersuchung. Es zog zudem alle erreichbaren Akten und Befunde bei und wertete sie aus - inbesondere Gerichtsakten, Akten von Strafanstalten, Jugend- und Sozialämtern, Akten des Landeswohlfahrtsverbands und der Bewährungshilfe, Kranken-

geschichten des Psychiatrischen Landeskrankenhauses und anderer Krankenhäuser und Ärzte sowie psychiatrische, psychologische und gerichtsmedizinische Gutachten. Darüber hinaus holte das Institut schriftliche Auskünfte ein bei Schulen, Heimen, Jugendämtern, Bewährungshelfern und Fürsorgern, Bürgermeistern, Pfarrern, Polizei, Krankenkassen, Arbeitsämtern und sonstigen Stellen. Mündlich befragte es neben den Probanden auch ihre Arbeitgeber, Pfarrer, Bürgermeister, Bewährungshelfer und Fürsorger sowie Angehörige und sonstige Bezugspersonen. Das Institut schloß die Datenerhebung im Jahr 1971 ab. Derzeit führt es noch über jeden Probanden eine Akte. Typisierte Einzelangaben aus dem Aktenbestand speichert es auf Lochkarte und in einer automatisierten Datei (Magnetbänder). Auf diesen Datenträgern sind zwar keine Namen gespeichert, wohl aber die den einzelnen Probanden zugeteilten Kenn-Nummern. Die Kenn-Nummer führt das Institut jeweils mit den Adreßdaten der Probanden auch noch in einer Handkartei. Die bisherigen wissenschaftlichen Ergebnisse der Untersuchung sind im wesentlichen in zwei in den Jahren 1983 und 1985 erschienenen Forschungsberichten dargestellt. Für das Institut ist damit allerdings die Untersuchung noch nicht beendet. Es will noch weitere Auswertungen vornehmen. Darüber hinaus beabsichtigt es, alle noch erreichbaren Probanden einer Nachuntersuchung zu unterziehen, um deren langfristige Entwicklung zu erfassen. Aus diesem Grund will es alle über die Probanden in Akten oder auf Lochkarte und Tonband enthaltenen Informationen weiter aufbewahren.

Ob ein Forscher unter heutigem Recht eine solche Langzeituntersuchung überhaupt noch beginnen und durchführen könnte, ist mehr als fraglich:

- Ohne wirksame Einwilligung der Probanden ginge es auf keinen Fall. Denn § 20 Abs. 1 LDSG läßt zwar eine Datenspeicherung ohne Einwilligung für wissenschaftliche Zwecke unter bestimmten Voraussetzungen zu; doch sind diese bei Langzeituntersuchungen der geschilderten Art in keinem Fall gegeben. § 20 Abs. 1 LDSG erlaubt eine Datenspeicherung ohne Einwilligung nämlich nur für ein bestimmtes Forschungsvorhaben und zudem nur dann, wenn dabei eine Beeinträchtigung schutzwürdiger Belange der Betroffenen durch die Art der Daten oder die Art ihrer Verwendung ausgeschlossen werden kann. An all diesen Voraussetzungen fehlt es. Zum einen kann man bei Untersuchungen mit einer solch offenen Fragestellung überhaupt nicht von einem „bestimmten" Forschungsvorhaben sprechen, weil bei Beginn der Speicherung noch nicht einmal annähernd feststeht, welche Auswertungen vorgenommen werden und wie lange Zeit die Datenspeicherung dauern soll. Zum anderen läßt sich bei einer solchen Vorgehensweise keinesfalls eine Beeinträchtigung schutzwürdiger Belange für die Zeit der überhaupt nicht absehbaren Dauer der Speicherung ausschließen. Für Forschungsvorhaben wie die Tübinger Jungtäter-Vergleichsuntersuchung gilt dies in besonders hohem Maße, weil hier über die einzelnen Probanden Persönlichkeitsprofile entstehen, wie man sie sich umfassender und vollständiger kaum vorstellen kann. Alle Lebensbereiche des Probanden werden bis ins letzte Detail erfaßt und bewertet.
- Auch mit wirksamer Einwilligung der Probanden wäre eine solche Untersuchung nicht unproblematisch. Es gibt durchaus ernstzunehmende Stimmen, die meinen, die Menschenwürde verbiete prinzipiell, auch mit Einverständnis der Betroffenen im Rahmen einer solchen Langzeituntersuchung Persönlichkeitsprofile umfassendster Art zu erstellen. In diese

Richtung deutet auch der Hinweis in § 20 Abs. 1 LDSG, daß es sich selbst bei Einwilligung um ein „bestimmtes" Forschungsvorhaben handeln muß. Stellt man diese Bedenken zurück, muß auf jeden Fall als Mindestvoraussetzung die Entscheidungsfreiheit des Probanden, ob er einwilligen will oder nicht, optimal gewahrt sein. Dazu gehört eine umfassende vorherige Aufklärung darüber, woher man welche Informationen einholen und in welcher Weise verarbeiten will. Vor allem sind die Probanden auch darüber aufzuklären, daß die Speicherung ihrer Daten praktisch zeitlich unbegrenzt andauern soll. Nur wenn eine so umfassende Information erfolgte und der einzelne Proband in der Lage ist, die Tragweite seines Handelns zu übersehen, kann man von einer wirksamen Einwilligung i.S.v. § 5 LDSG ausgehen.

Diesen Maßstab des geltenden Rechts kann man allerdings nicht uneingeschränkt an die Tübinger Jungtäter-Vergleichsuntersuchung anlegen, da sie bereits in den 60er Jahren begann und auch die Daten bereits vor Inkrafttreten des Landesdatenschutzgesetzes gespeichert waren. Zwar findet das Landesdatenschutzgesetz grundsätzlich auch auf solche, bei seinem Inkrafttreten „laufende" Vorhaben Anwendung. Doch rechtfertigt die Übergangssituation, die Einwilligungserklärungen, die das Institut einst einholte und die dem damaligen Standard entsprachen, als ausreichende Legitimation für die Fortdauer der Datenspeicherung bis zum Abschluß des Projekts anzusehen. Die zwischenzeitliche Entwicklung des Datenschutzrechts sollte allerdings für das Institut in besonderem Maße Anlaß sein zu prüfen, ob es tatsächlich noch für sein Forschungsprojekt notwendig ist, den gesamten umfangreichen Datenbestand beizubehalten. Uneingeschränkt zu beachten hat das Institut selbstverständlich das geltende Datenschutzrecht, wenn es nunmehr die ins Auge gefaßte Nachuntersuchung der noch erreichbaren Probanden tatsächlich durchführt: dies gilt von der Gewinnung der dafür notwendigen Adreßdaten über die Nachuntersuchungen bis hin zur Speicherung der dabei gewonnenen Erkenntnisse.

6. Der Forscher und der Computer

Bedient sich der Forscher des Computers, muß er die Rechtsvorschriften über die automatisierte Datenverarbeitung beachten. Ob dem so ist, sahen sich meine Mitarbeiter und ich bei unseren Kontrollbesuchen der Universitäten Konstanz und Heidelberg näher an. Dabei stellten wir fest, daß noch vieles im argen liegt.

6.1 Forschungsdokumentation

Führt ein Forscher ein Forschungsvorhaben durch, geht er in der Regel nach einem bestimmten Plan vor. Ein solches planmäßiges Vorgehen ist erst recht notwendig, wenn er dabei den Computer einsetzen will. Dann genügt freilich nicht, daß der Forscher bloß den Plan im Kopf hat, nach dem die Datenverarbeitung ablaufen soll. Er muß vielmehr ihren vorgesehenen Ablauf dokumentieren. Eine solche Dokumentation ist zum einen unentbehrlich, um Fehler bei der Datenverarbeitung zu vermeiden. Zum anderen ist sie notwendig, um feststellen zu können, ob bei ihr die Anforderungen des Datenschutzes tatsächlich beachtet wurden. Nur wenn der vorgesehene Ablauf detailliert aufgezeichnet ist, lassen sich Abweichungen wie z. B. ein unerlaubtes Abgleichen oder Verändern der Daten oder das Anlegen von Kopien nachvollziehen.

6.1.1 Kriminologisches Institut der Universität Heidelberg

Im Zeitpunkt des Kontrollbesuchs hatte das Kriminologische Institut Heidelberg kein einziges seiner laufenden Forschungsvorhaben vollständig dokumentiert. Nur die Datensätze der einzelnen Projekte waren in Code-Plänen beschrieben. Darüber hinaus legte das Institut im Anschluß an meinen ersten Kontrollbesuch noch eine Übersichtsliste über die vorhandenen Dateien, Magnetbänder und Lochkarten an. Die Angaben in dieser Liste waren allerdings nicht fehlerfrei: ein als „leer" bezeichnetes Magnetband enthielt – wie sich später herausstellte – den gesamten Datenbestand eines Forschungsvorhabens. Überhaupt nirgendwo dokumentiert hatte das Institut, welche Programme jeweils eingesetzt wurden und wie es dabei mit dem Datenschutz aussah.

Auf meinen Vorhalt machte das Institut geltend, seine Dokumentation sei keineswegs unvollständig. Sie sei nur weder zentral angelegt noch übersichtlich geführt und auch nicht in jedem Detail aktuell. Mit dieser Stellungnahme verkennt das Institut die Anforderungen, die an eine ordnungsgemäße Dokumentation zu stellen sind. Diese muß in jedem Fall exakt und aktuell sein. Auch muß sie so angelegt sein, daß sie andere, z. B. auch die Datenschutzkontrolle, nutzen und nachvollziehen können.

6.1.2 Institut für Rechtstatsachenforschung – Bereich Kriminologie – der Universität Konstanz

Auch das Institut für Rechtstatsachenforschung hatte im Zeipunkt des Kontrollbesuchs keines seiner laufenden Forschungsvorhaben dokumentiert. So war insbesondere nicht beschrieben,

- zu welchem Projekt welche Dateien und Magnetbänder gehörten,
- welche EDV-Programme überhaupt vorhanden sind,
- welche Daten zu welchen Personengruppen auf welchen Magnetbändern gespeichert sind,
- auf welchem der beiden Computer des Universitätsrechenzentrums die Daten verarbeitet werden und
- welche technischen und organisatorischen Datensicherungsmaßnahmen im Institut und im Universitätsrechenzentrum getroffen wurden.

Ich forderte das Institut auf, diese Mängel bei allen Projekten, die nicht bereits kurz vor dem Abschluß stehen, umgehend zu beheben und bei neuen Projekten von vornherein eine vollständige und verständliche Dokumentation zu erstellen und während der Dauer des Projekts laufend zu aktualisieren. Das Institut hat mit der Realisierung dieser Forderung inzwischen begonnen.

6.2 Der Forscher und das Rechenzentrum

So wichtig ist, daß der Forscher eine vollständige und verständliche Dokumentation erstellt, so sicher ist zugleich, daß dies allein nicht genügt. Verarbeitet er die Daten auf einem Personal Computer im eigenen Institut, muß er zusätzlich die Daten und Programme sichern. Läßt er die Daten dagegen im Universitätsrechenzentrum verarbeiten, ist es des-

sen Aufgabe, diese Daten gegen unbefugten Zutriff zu schützen. Die Praxis sieht leider noch reichlich anders aus:

6.2.1 Universität Konstanz

Die Forschungsgruppe des Instituts für Rechtstatsachenforschung setzte für ihre Datenverarbeitung einen eigenen Personal Computer und die Großrechner des Universitätsrechenzentrums ein. Auf dem Personal Computer des Instituts verarbeitete es überwiegend Identifizierungsdaten, im Rechenzentrum dagegen alle anderen Forschungsdaten. Die Arbeiten auf dem Personal Computer liefen ab, ohne daß der Zugriff auf Daten und Programme durch spezielle Sicherheits-Software kontrolliert wurde. Auch erfolgte keine Protokollierung der einzelnen Datenverarbeitungsvorgänge. Infolgedessen bestand die Gefahr, daß Unbefugte unbemerkt die Daten im Personal Computer abrufen, verändern oder löschen konnten. Auf meinen Hinweis, daß dies nicht mit § 8 LDSG vereinbar ist, entschloß sich das Institut, auf seinem Personal Computer ab sofort keine personenbezogenen Daten mehr zu verarbeiten.

Auch die Datenverarbeitung im Rechenzentrum hatte Mängel:

- Da das Rechenzentrum die Zugriffsmöglichkeiten seiner angeschlossenen Datenstationen in keiner Weise beschränkt hatte, war es technisch möglich, von jeder Datenstation auf die gespeicherten kriminologischen Daten zuzugreifen. Ein Sicherheitskonzept, das dies verhindert hätte, fehlte.
- Das Rechenzentrum bewahrte die ihm vom Institut übergebenen Magnetbänder in seinem Maschinensaal in einem Tresor auf, führte jedoch keine Nachweise über deren Entnahme zum Zweck der Verarbeitung. Das aber hätte es zumindest tun müssen, um belegen zu können, wann wer die Magnetbänder verwendet hat.
- Das Rechenzentrum protokollierte nicht in notwendigem Umfang die Abläufe der Datenverarbeitung bei den einzelnen Forschungsvorhaben. Deshalb ließ sich nicht feststellen, wer wann welche Personendaten eingab, wer welche Dateien wann einrichtete, veränderte oder löschte, wer wann welche Programme erstellte und wann sie zum Ablauf kamen. Nur aber wenn die Protokolle all dies aussagen, ist möglich, mit ihrer Hilfe die Datenverarbeitung exakt nachzuvollziehen.

Auf meinen Hinweis auf diese Mängel hin war die Universität rasch bereit, bei der Archivierung der Magnetbänder Abhilfe zu schaffen. Die anderen Mängel mußte ich dagegen nach § 18 LDSG beanstanden, weil die vom Rechenzentrum der Universität zunächst ins Auge gefaßten Abhilfemaßnahmen nicht ausreichten. Inzwischen bemüht sich jedoch das Rechenzentrum, in Zusammenarbeit mit dem Institut für Rechtstatsachenforschung ein Sicherheitskonzept für die Verarbeitung personenbezogener Daten zu erstellen. Damit ist die Universität auf dem richtigen Weg.

6.2.2 Universität Heidelberg

Das Kriminologische Institut der Universität Heidelberg verarbeitet seine Forschungsdaten in einem der drei Großrechner des Universitätsrechenzentrums. Auch dort zeigten sich bei Kontrollbesuchen verschiedene Schwachstellen:

- Das Universitätsrechenzentrum erlaubt den Universitätsinstituten, an Wochenenden dessen Großrechner selbst zu betreiben. Die interessierten Universitätsinstitute stellen dann jeweils einen Mitarbeiter – häufig eine wissenschaftliche Hilfskraft – dafür ab. Dessen Aufgabe ist, anstelle des unter der Woche eingesetzten Personals des Rechenzentrums für den Betrieb des Großrechners zu sorgen. In aller Regel ist der Institutsmitarbeiter deshalb viele Stunden allein im Maschinensaal des Universitätsrechenzentrums. Dort bewahrt das Rechenzentrum den größten Teil seines mehrere Tausend Magnetbänder umfassenden Archivs offen auf. Darunter befinden sich zum einen alle Magnetbänder mit personenbezogenen Daten, die nicht als solche gekennzeichnet sind, und zum anderen alle Datensicherungsbänder mit einer Fülle personenbezogener Daten. Beispielsweise waren auch Magnetbänder des Kriminologischen Instituts frei zugänglich – insbesondere die Magnetbänder zum Forschungsprojekt „Maßregelvollzug", auf denen sensibelste Angaben über Personen gespeichert sind, die nach § 63 StGB aufgrund richterlicher Anordnung im Psychiatrischen Landeskrankenhaus Wiesloch untergebracht waren. Bei einem so ausgestalteten Wochenendbetrieb ist es möglich, daß der Institutsmitarbeiter einzelne Magnetbänder unerlaubt entfernt oder nach Belieben verarbeitet. Er könnte sogar mit einem fremden Betriebssystem ohne Sicherheitsprogramm die gesamte Datenverarbeitung des Rechenzentrums beeinflussen, z. B. die zentrale Berechtigungsdatei ausforschen und so die Paßwörter der einzelnen Benutzer feststellen.

  Diese Mängel sind ein schwerer Verstoß gegen § 8 LDSG, den ich nach § 18 Abs. 1 LDSG beanstandet habe. Meiner gleichzeitigen Aufforderung, den Wochenendbetrieb umgehend zu ändern, kam das Universitätsrechenzentrum bis jetzt nicht nach. Es meint, es genüge, daß es die Institutsmitarbeiter verpflichtet habe, während ihrer Arbeit im Rechenzentrum keine Datenverarbeitung außerhalb ihres Auftrags zu betreiben, und am Wochenbeginn die Protokolle des Wochenendes durchgesehen würden. Dies reicht jedoch nicht aus. Notwendig ist, zumindest das „Vier-Augen-Prinzip" zu beachten und deshalb nie eine Person allein im Maschinensaal zu lassen sowie die Kontrolle der Datenverarbeitungsvorgänge am Wochenende durch Auswertungsprogramme zu unterstützen.

- Ferner weist das Sicherheitsprogramm des Großrechners, auf dem die Forschungsvorhaben laufen, erhebliche Mängel auf. Es schützt die zentrale Berechtigungsdatei, in der alle Benutzerkennungen und Paßwörter im Klartext gespeichert sind, nicht ausreichend. Durch systematisches Ausprobieren kann man je nach der eingesetzten Methode entwe-

der gleich alle vorhandenen Benutzerkennungen und Paßwörter herausbekommen oder nur die eines einzelnen Benutzers. Hat man aber erst einmal Benutzerkennung und Paßwort, ist es ein Leichtes, die Daten dieses Benutzers zu lesen, zu verändern und zu löschen. Anders gesagt: das Sicherheitsprogramm erkennt weder Eindringungsversuche noch unterbindet sie, ja es kann nicht einmal Eingriffsaktionen im Nachhinein feststellen. Diese Mängel sind nicht zuletzt deshalb besonders riskant, weil mehr als 160 verschiedene Institute, Kliniken, Forschungs- und Verwaltungseinrichtungen und Firmen mit mehr als 3000 Benutzern und Tausenden Benutzerprogrammen und Benutzerdateien auf dem Großrechner arbeiten. Beispielsweise kann ein Heidelberger Forscher, der vorübergehend in Kalifornien tätig ist, über das internationale Computerforschungsnetz EARN (European Academic Research Network) seine im Heidelberger Großrechner gespeicherten Daten verarbeiten. Weil diese Mängel ein erhebliches Risiko für die gesamte Datenverarbeitung auf dem Großrechner darstellen, mußte ich sie nach § 18 LDSG beanstanden. Die Äußerung der Universität darauf, ob und wie sie Abhilfe schaffen will, steht noch aus.

6.3 Konsequenzen für Forscher und Rechenzentren

Der Einsatz des Computers entlastet in der Regel den Forscher bei seiner Arbeit. Nicht entlasten kann er ihn jedoch von der Verantwortung für die Einhaltung der Spielregeln des Datenschutzes. Dies gilt auch dann, wenn der Forscher seine Forschungsdaten in einem Rechenzentrum verarbeiten läßt. Deshalb geht nicht an, daß er einfach seine Datenbestände in den Computer des Rechenzentrums eingibt und dann davon ausgeht, alles Weitere sei Sache des Rechenzentrums. So aber ist leider die Praxis. Notwendig ist ein enges Zusammenwirken zwischen Forscher und Rechenzentrum. Der Forscher muß das Rechenzentrum darüber informieren, ob die gespeicherten Daten personenbezogen sind und welches Schutzbedürfnis für sie besteht. Das Rechenzentrum muß dem Forscher mitteilen, welche Datensicherung es anbieten kann und welcher Schutz damit zu erreichen ist. Forscher und Rechenzentren müssen dann gemeinsam überlegen, ob die vom Rechenzentrum gebotenen Schutzvorkehrungen für die Durchführung des Forschungsvorhabens ausreichen oder nicht. Wenn nein, muß der Forscher auf die Inanspruchnahme des Rechenzentrums verzichten, das Rechenzentrum die Übernahme der Datenverarbeitung ablehnen. Soll es damit nicht sein Bewenden haben, müssen beide gemeinsam überlegen, ob und in welcher Weise sich die Datensicherheit im Rechenzentrum so verbessern läßt, daß einer Verarbeitung der Forschungsdaten den Anforderungen an die Datensicherung nach § 8 LDSG genügt. Dem Forscher wird damit nichts aufgebürdet, was eigentlich nicht seine Sache ist, im Gegenteil: seine Zusammenarbeit mit dem Rechenzentrum liegt auch im Interesse einer effektiven Forschung. Denn diese hängt, wie die Kriminologischen Forschungsprojekte deutlich zeigen, oft ganz entscheidend von der Bereitschaft von Personen ab, sich vom Forscher untersuchen zu lassen und ihm andere persönlichen Daten zur Verfügung zu stellen. Diese Bereit-

schaft wird um so größer sein, je sicherer der Proband sein kann, daß der Forscher mit seinen Daten sorgfältig umgeht. Die vertrauensfördernde Wirkung des Datenschutzes ist hier unverkennbar. Das sollten vor allem auch Forscher, die den Datenschutz eher als Hemmnis empfinden, nicht aus dem Auge verlieren.

6. Teil: Datenschutz im Krankenhaus

1. Auf dem Weg zum vollautomatisierten Krankenhaus

Wer in ein Krankenhaus muß, bemerkt bislang wenig vom Einsatz der EDV. Vielleicht sieht er, wie die Aufnahme seine Daten am Bildschirm eintippt und Adreßetiketten ausdruckt. Vielleicht fällt ihm auch auf, daß der Pförtner nicht mehr lange in Karteikarten sucht, sondern nach einem kurzen Blick auf den Bildschirm Auskunft gibt. Allenfalls bemerkt er noch, daß das Krankenhaus seine Rechnungen über die ambulanten und stationären Leistungen mit Hilfe eines Computers erstellt. Damit hat es aber dann in der Regel schon sein Bewenden.

In der Tat verarbeiteten bis vor kurzem die Krankenhäuser Patientendaten praktisch nur für Abrechnungszwecke mit automatisiertem Verfahren. Sie setzen dafür entweder einen eigenen Computer ein oder bedienen sich eines Rechenzentrums. Letzteres ist weitgehend Praxis im Land - doch der Öffentlichkeit nicht bekannt. Wer beispielsweise in Leonberg oder Sindelfingen, Waiblingen oder Göppingen, Ludwigsburg oder Böblingen ins Krankenhaus muß, ahnt in aller Regel nicht, daß dieses Krankenhaus seine Daten außer Haus gibt und fernab in Stuttgart im Regionalen Rechenzentrum speichern läßt. Die meisten Kommunen des Mittleren Neckarraums bedienen sich dieses Rechenzentrums, lassen dort freilich nicht nur Patientendaten, sondern auch die Melderegister- und Steuerdaten ihrer Einwohner, Angaben über Sozialhilfeempfänger, Wohngeldberechtigte und BaföG-Bezieher sowie Führerscheindaten und Personaldaten ihrer Mitarbeiter speichern. Damit hat es inzwischen nicht mehr stets sein Bewenden: Zusätzlich setzen seit geraumer Zeit einige wenige Krankenhäuser im Land Textsysteme für Arztbriefe und elektronische Laborsysteme ein. Seit Anfang 1986 speichern außerdem die meisten Krankenhäuser des Landes zur Erstellung der neu eingeführten Diagnosestatistik einige medizinische Daten über ihre Patienten.

Doch dabei soll es nicht bleiben. Auch im Krankenhaus soll in den nächsten Jahren High Tech einziehen. Entstehen sollen Informations- und Kommunikationssysteme, die Patientendaten aus den verschiedensten Bereichen des Krankenhauses - beispielsweise aus Labor, Operationssaal, Röntgen und Stationen - sammeln und zum Abruf bereithalten. Die Krankenschwester kann dann Labor- und Röntgenuntersuchungen und physikalische Therapien am Bildschirm anfordern - entweder mit einem tragbaren Gerät unmittelbar während der Visite oder im Anschluß daran an einem stationären Terminal; das Ergebnis einer Blutuntersuchung gelangt dann unmittelbar vom Analyseautomaten in das Informationssystem und steht sofort dem behandelnden Arzt auf der Station zur Verfügung. Kurzum: mit einem solchen Informations- und Kommunikationssystem entsteht im Krankenhaus eine Sammlung höchst sensibler Patientendaten.

Noch ist es nicht soweit. Doch liegen bereits Pläne zum Aufbau solcher Systeme in den Krankenhäusern vor. Darüber hinaus führt die Kommunale Datenverarbeitung Mittlerer Neckar (KDMN) gegenwärtig mit 5 Krankenhäusern im Lande einen Pilotversuch durch. Ihr Ziel ist, ein solches Informations- und Kommunikationssystem zu entwickeln und im Krankenhausalltag zu erproben. Auf weitere Sicht strebt sie an, daß mit Hilfe der Datenzentrale möglichst viele Krankenhäuser im Lande dieses Verfahren einführen. Andere Krankenhäuser, z. B. Heilbronn und Reutlingen, schlugen einen anderen Weg ein und erproben im Alleingang Verfahren zur Verarbeitung von Patientendaten.

Diese sich anbahnende Entwicklung ist nicht ohne Probleme für den Datenschutz. Deshalb führten meine Mitarbeiter und ich 1986 u. a. Kontrollbesuche bei der KDMN und den Krankenhäusern Leonberg, Reutlingen und Sindelfingen durch. Dabei zeigten sich neben den Problemen der Einschaltung externer Rechenzentren und der Erstellung der Diagnosestatistik, die nahezu alle Krankenhäuser im Lande in gleicher Weise betreffen, spezielle Mängel der Datensicherung bei den kontrollierten Krankenhäusern. Davon soll zunächst die Rede sein:

1.1 Krankenhäuser Sindelfingen und Leonberg

Die verschiedenen Bildschirmgeräte und Drucker der beiden Krankenhäuser sind an das Rechenzentrum der KDMN angeschlossen. Dieses speichert und verarbeitet im Rahmen des Pilotversuchs die Patientendaten. Das dabei eingesetzte Verfahren wies so gravierende Mängel auf, daß ich es nach § 18 LDSG beanstanden mußte:

- Die Dokumentation der Datenverarbeitung war unvollständig; insbesondere fehlte ein Sollkonzept zum Aufbau der Patientendatenbank und aktuelle Beschreibungen der Bildschirmmasken. Ohne eine vollständige Dokumentation ist aber eine ordnungsgemäße Datenverarbeitung nicht möglich. Die KDMN und die Krankenhäuser kamen inzwischen meiner Forderung weitgehend nach, die Dokumentation zu vervollständigen.
- Welche Versionen der einzelnen Programme wann im Einsatz waren, und wann das KDMN eine Fehlfunktion beseitigte, teilte es den Krankenhäusern - wenn überhaupt - nur mündlich mit. So stellte z. B. das Städtische Krankenhaus Sindelfingen nur durch Zufall eine weitreichende Änderung am Ablauf der Diagnoseerfassung fest. Weil dies aber die Datensicherheit stark beeinträchtigt, forderte ich von der KDMN, die Programme nur in Absprache mit den Krankenhäusern einzusetzen. Es sagte mir daraufhin zu, in Zukunft nur noch vom Krankenhaus getestete und freigegebene Programme einzusetzen. Dies wird die KDMN künftig auch laufend für das Krankenhaus schriftlich festhalten.
- Die Krankenhäuser gaben an, daß sie beim stunden- oder tageweisen Ausfall der EDV auf herkömmliche Weise anhand von Formularen weiterarbeiten wollen. Das mag solange noch angehen, als sie nicht - wie sie aber planen - die innerhalb des Krankenhauses hin- und hergehenden schriftlichen Unterlagen, vornehmlich die Formulare durch die elektronische Post ihres Kommunikationssystems ersetzen. Dann aber spätestens ist die Notsituation da. Da auch dann die Krankenhäuser auf alle zur Behandlung der Patienten notwendigen Informationen zugreifen

können müssen, ist ein Ausfallkonzept nötig. Darin sind die möglichen Ausfallursachen zu untersuchen und auf die konkrete Situation des Krankenhauses abgestimmte Notfallmaßnahmen festzulegen.

1.2 Kreiskrankenhaus Reutlingen

Auch das Verfahren, das das Kreiskrankenhaus Reutlingen seit Mitte 1984 auf eigenem Computer betreibt, wies bei der Datensicherung Mängel auf:

- Seit 1984 hat es die Paßwörter, welche den einzelnen Mitarbeitern den Zugriff auf die Patientendaten ermöglichen, noch nie geändert; da die Mitarbeiter dafür zudem ihr eigenes Kurzzeichen verwandten, waren die Paßwörter leicht zu erraten. Meiner Forderung, unverzüglich sämtliche Paßwörter auszutauschen und einen regelmäßigen Wechsel vorzusehen, folgte das Krankenhaus.
- Nicht gewährleistet war, daß alle Mitarbeiter des Krankenhauses die Patientendaten nur so verarbeiten konnten, wie es ihren Aufgaben entsprach. So konnten z. B. Bediensteten der Zentralen Aufnahme verschiedene Statistiken ausdrucken, obwohl dafür andere Mitarbeiter zuständig sind. Meinem Hinweis, sämtliche Berechtigungen zu überprüfen und entsprechend den Aufgaben der einzelnen Mitarbeiter zu gestalten, trug das Krankenhaus inzwischen Rechnung.

2. Externe Rechenzentren

Wer die Kommunikation im Krankenhaus will, kommt an der Frage nicht vorbei, ob das Krankenhaus die Patientendaten mit Hilfe eines eigenen Computers verarbeiten soll oder ob es dafür ein externes Rechenzentrum einschalten will. Letzteres ist, um es vorweg zu sagen, mit den Vorschriften zum Schutz der Patientendaten nicht vereinbar. Die rechtlichen Überlegungen, die zu diesem Ergebnis führen, sind ziemlich kompliziert:

Wollen Krankenhäuser Patientendaten verarbeiten, müssen sie neben dem Landesdatenschutzgesetz vor allem das Arztgeheimnis beachten. Dieses ist bekanntlich durch das ärztliche Standesrecht und das Strafrecht abgesichert und verpflichtet nicht nur Krankenhausärzte, sondern alle im Krankenhaus Beschäftigten zum Stillschweigen über den Patienten und seine Krankheit – es sei denn, eine spezielle Offenbarungsbefugnis erlaubt im Einzelfall die Weitergabe der Patientendaten. Unter Offenbaren ist jede Bekanntgabe an andere Personen oder Stellen zu verstehen. Dabei spielt keine Rolle, ob und, wenn ja, welche Rechtsbeziehungen zwischen den anderen Personen / Stellen und dem Krankenhaus bestehen. Deshalb rechtfertigt die Tatsache, daß ein Krankenhaus ein externes Rechenzentrum mit der Durchführung seiner Datenverarbeitung im Rahmen von § 3 LDSG beauftragte, nicht, diesem Rechenzentrum Patientendaten mitzuteilen. Eine solche Offenbarung wäre nur rechtmäßig, wenn sie eine Rechtsvorschrift ausdrücklich zuläßt oder wenn der Patient damit einverstanden ist. An beidem fehlt es:

- Eine gesetzliche Regelung, die eine Weitergabe von Patientendaten an ein externes Rechenzentrum generell erlauben würde, existiert nicht. Das Krankenhausgesetz von Baden-Württemberg enthält, anders als z. B. das bayerische Krankenhausgesetz, dazu keine Aussage.

- Auch kann man nicht vom Einverständnis der Patienten ausgehen, wie es zwei von der KDMN eingeholte Gutachten meinen. Zwar kann ein Patient in die Weitergabe seiner Daten grundsätzlich auch stillschweigend einwilligen. Dies setzt jedoch voraus, daß er in etwa übersieht, an wen welche Informationen über ihn weitergehen und welche Konsequenzen sein Einverständnis damit hat. Hat er von all dem, was geschieht, überhaupt keine Ahnung - und gerade so ist es bei der Einschaltung externer Rechenzentren durch Krankenhäuser –, dann kann von einem stillschweigenden Einverständnis schlechterdings nicht die Rede sein. Seine Annahme wäre eine reine Fiktion. Entgegen der Ansicht der beiden Gutachter gibt der Patient auch nicht bei seiner Aufnahme dem Krankenhaus gewissermaßen freie Hand, mit all seinen Daten so umzugehen, wie es das Krankenhaus für richtig und zweckmäßig hält. Dafür gibt es keinerlei Anhaltspunkte, im Gegenteil: der Patient erwartet in aller Regel Diskretion.

Aus alledem folgt: Gegenwärtig darf ein Krankenhaus allenfalls die Daten an ein externes Rechenzentrum weitergeben, die es für Abrechnungszwecke speichern und verarbeiten muß. Denn inzwischen ist es weitgehend üblich, solche Arbeiten außerhalb des Krankenhauses durchführen zu lassen. Aber schon hier ist die Annahme eines Einverständnisses des Patienten problematisch. In keinem Fall läßt sich darüber hinaus die Weitergabe von Patientendaten an externe Rechenzentren rechtfertigen. Für dieses Ergebnis spricht noch ein anderer Grund: Die Daten der Patienten in Rechenzentren sind schlechter geschützt als solche im Krankenhaus. Die Ärzte des Krankenhauses und das Krankenhauspersonal haben nämlich im Strafverfahren ein Zeugnisverweigerungsrecht; niemand kann sie zwingen, Aussagen über den Patienten zu machen. Ebensowenig darf die Staatsanwaltschaft in einem Strafverfahren ärztliche Unterlagen des Krankenhauses beschlagnahmen. So ist es in §§ 53, 54 und 97 StPO ausdrücklich geregelt. Die Mitarbeiter eines Rechenzentrums dagegen sind zwar verpflichtet, das Datenschutzgeheimnis zu beachten; sie haben aber kein Zeugnisverweigerungsrecht im Strafverfahren. Entgegen der Meinung der beiden Gutachter, kann man sie auch nicht als „Gehilfen" der Krankenhausärzte ansehen und ihnen über diesen Umweg zu einem Zeugnisverweigerungsrecht verhelfen. Die Krankenhausärzte wären sicherlich genauso baß erstaunt wie die Beschäftigten in Rechenzentren, wenn sie von dieser „Gehilfeneigenschaft" hörten - denn sie haben doch schlechterdings miteinander keinerlei Berührung. Das Rechenzentrum könnte folglich auch nicht mit dem Hinweis auf die „Gehilfeneigenschaft" verhindern, daß durch eine Weitergabe seiner Daten an ein externes Rechenzentrum gespeicherte Patientendaten beschlagnahmt werden. Folglich erhöht sich für den Patienten das Risiko, daß andere als behandelnde Ärzte und Pflegepersonal von seiner Erkrankung und ihren näheren Umständen erfahren.

Keine Lösung wäre es, wenn sich die Krankenhäuser infolgedessen in Zukunft entschlössen, stets das ausdrückliche Einverständnis ihrer Patienten zur uneingeschränkten Einschaltung externer Rechenzentren einzuholen. Dreierlei spricht dagegen; zum ersten: Krankenhäuser sind unter bestimmten Voraussetzungen zur Aufnahme eines Patienten verpflichtet; zumindest dann könnten sie die Aufnahme nicht von der Abgabe einer solchen Einwilligung abhängig machen. Zum zweiten hat jeder Patient das Recht, seine Einwilligung jederzeit zu widerrufen. Dem Krankenhaus bliebe deshalb nichts anderes übrig als zwei Verfahren vorzuhalten - eines für die interne und eines für die externe Verarbeitung der Patientendaten. Schließlich befinden

sich nicht wenige Patienten bei ihrer Aufnahme im Krankenhaus in einer Ausnahmesituation: da sie dringend auf Hilfe angewiesen sind, spricht vieles dafür, daß sie in diesem Augenblick überhaupt nicht über die notwendige Entscheidungsfreiheit verfügen.

Weil der Trend erkennbar ist, die Weichen im Lande anders zu stellen, wies ich im August 1986 das Sozialministerium, die kommunalen Landesverbände, die Krankenhausgesellschaft Baden-Württemberg, die Datenzentrale und die Regionalen Rechenzentren auf die Rechtslage hin und bat, sie bei ihren weiteren Planungen zu berücksichtigen. Kommunale Landesverbände, Krankenhausgesellschaft und Datenzentralen teilten mir daraufhin mit, sie könnten meine Beurteilung vorerst nicht teilen, wollten jedoch in Abstimmung mit dem Sozialministerium eine eingehende Stellungnahme erarbeiten. Das Sozialministerium gab bislang keine Äußerung in der Sache ab, sondern ergänzte diese Hinweise lediglich dahin, es müsse auch noch andere berührte Ministerien, z. B. das Justizministerium, in die Abstimmung einbeziehen. Diese Bemühungen sind offensichtlich sehr langwierig. Bis heute liegt mir die angekündigte Stellungnahme nicht vor. Eine klare Position bezog lediglich die KDMN: sie hält – wie könnte es in Anbetracht ihres laufenden Pilotprojekts anders sein – unter Hinweis auf die beiden schon erwähnten Gutachten eine Einschaltung externer Rechenzentren für zulässig – eine Beurteilung, die ich aus den angeführten Gründen nicht teilen kann.

3. Diagnosestatistik

Die Bundespflegesatzverordnung verpflichtet mit Wirkung vom 1. Jan. 1986 die Krankenhäuser, eine anonymisierte Diagnosestatistik zu führen, um damit einen Beitrag zur Kostendämpfung im Gesundheitswesen zu leisten. In dieser Diagnosestatistik sind neben der Hauptdiagnose auch Angaben über durchgeführte Operationen, Verweildauer und Alter der Patienten zu erfassen. Die Krankenhäuser erstellen diese Statistik in der Regel auf folgende Weise: wird ein Patient entlassen oder verlegt, teilt die Station/Abteilung der Krankenhausverwaltung auf einem Vordruck Namen – oft auch noch ohne andere Identifizierungsdaten – und die Hauptdiagnose des Patienten mit; letztere gibt sie entweder mit dem dreistelligen ICD-Schlüssel oder im Klartext an. Die Krankenhausverwaltungen speichern diese Angaben unter dem Namen der Patienten in ihren automatisierten Abrechnungsdatensätzen. Darin waren bislang keine Diagnosedaten enthalten. Weil dem jetzt aber so ist, gelangen die Hauptdiagnosen der Patienten sogar in externe Rechenzentren, wenn sich die Krankenhäuser für ihre Abrechnung deren Hilfe bedienen. So ergeht es beispielsweise den Patienten der Krankenhäuser Leonberg und Sindelfingen. Eine Reihe anderer Krankenhäuser tut noch ein Übriges, weil sie eine Statistik allein mit der Hauptdiagnose nicht für aussagekräftig genug halten, erfassen sie daneben auch die – oft zahlreichen – Nebendiagnosen. Im Krankenhaus Reutlingen sah ich beispielsweise Erfassungsbogen mit sieben Nebendiagnosen.

Die Tatsache, daß nunmehr der Krankenhausverwaltung Diagnosen mitzuteilen sind, löste bei vielen Krankenhausärzten erhebliche Beunruhigung aus. Ihre Sorge ist nur zu verständlich. Denn es ist nicht einzusehen, weshalb jeder Patient mit Diagnose im Computer des Krankenhauses gespeichert wird, damit das Krankenhaus eine Statistik erstellen kann, die keine personen-

bezogenen Angaben liefern soll. Erst recht gilt dies, wenn die Krankenhäuser ihre Daten in einem externen Rechenzentrum verarbeiten und dort auch die Diagnosestatistik erstellen lassen. Das externe Rechenzentrum erfährt die Hauptdiagnose dann bloß deshalb, weil das Krankenhaus eine für die Behandlung des einzelnen Patienten völlig unerhebliche Statistik erstellen läßt. Eine Rechtsgrundlage für eine solche Durchbrechung der ärztlichen Schweigepflicht gibt es nicht: die Krankenhäuser müssen ihr derzeitiges Verfahren deshalb ändern. Leider blieb meine Aufforderung vom August 1986 an das Sozialministerium, die kommunalen Landesverbände, die Krankenhausgesellschaft Baden-Württemberg, die Datenzentrale und die Regionalen Rechenzentren, ein anderes datenschutzgerechteres Verfahren anzuwenden, bislang ohne offizielle Reaktion.

Erst recht ist es rechtswidrig, wenn die Krankenhäuser ihre EDV-Konzeption „Diagnosestatistik" dazu benutzen, auch die Nebendiagnosen zu erfassen und statistisch auszuwerten. Nebendiagnosen haben nicht nur in externen Rechenzentren nichts zu suchen; sie dürfen nicht einmal an die Krankenhausverwaltung gehen, weil diese sie – anders als die Hauptdiagnose – für Abrechnungszwecke nicht benötigt. Zu Recht erfuhr sie deshalb die Nebendiagnosen bislang nicht. So muß es auch bleiben bzw. wieder werden. Denn von einer ausdrücklichen oder stillschweigenden Einwilligung des Patienten kann hier schlechterdings nicht die Rede sein. Das heißt freilich nicht, daß der Datenschutz von vornherein verbieten würde, Nebendiagnosen statistisch zu erfassen. Notwendig wäre lediglich, ein anderes EDV-Verfahren zu wählen, das das Arztgeheimnis nicht tangiert. Nicht die Krankenhausverwaltung, sondern die einzelnen Stationen des Krankenhauses müßten die Diagnosedaten erfassen und dann zusammengefaßt ohne Namen der Patienten an die Verwaltung weitergeben. Gleichzeitig müßte das Krankenhaus sicherstellen, daß ihre Verwaltung auf die Datenspeicherungen und sonstigen Unterlagen der Stationen über die Nebendiagnosen nicht zugreifen kann. Auch zu diesem Punkt warte ich seit Monaten auf eine Antwort der für die Krankenhäuser im Lande verantwortlichen Stellen.

4. Der Doktorand und der Patient

Wenig erfreut war ein Bürger, als er eines Tages in seinem Briefkasten ein Schreiben zweier Doktoranden fand, die bei einer Universitätsklinik tätig waren, in der er sich einige Zeit zuvor wegen eines Herzleidens untersuchen ließ. Die Doktoranden verwiesen auf seine Erkrankung und boten ihm eine kostenlose Untersuchung an. Einer der Doktoranden hatte sich sogar schon mit seinem Hausarzt in Verbindung gesetzt und diesen über sein Vorhaben informiert. Die beiden Studenten wollten die Untersuchungsergebnisse für ihre Doktorarbeit auswerten. Der Bürger war mit diesem Vorgehen nicht einverstanden und bat mich um Überprüfung. Dabei stellte sich heraus, daß die beiden Doktoranden von ihren beiden Professoren zur Erstellung der Dissertation Unterlagen über Patienten erhalten hatten, die die Professoren untersucht und behandelt haben. Darunter befanden sich auch die Unterlagen des schockierten Bürgers.

Der Vorgehensweise stand zwar nicht das Landesdatenschutzgesetz, wohl aber das Arztgeheimnis entgegen. Das Landesdatenschutzgesetz greift in einem solchen Fall garnicht ein, weil es klinikinterne Vorgänge, wie z. B. die Bekanntgabe von Patientendaten durch Professoren an ihre Doktoranden, überhaupt

nicht regelt. Sein Adressat ist immer nur die „speichernde Stelle", also die einzelne Klinik. Demgegenüber nimmt das Arztgeheimnis den einzelnen Arzt persönlich in Pflicht und verbietet ihm, auch innerhalb einer Klinik Patientendaten weiterzugeben – es sei denn, die Behandlung eines Patienten erfordert dies. Daran hat sich auch die medizinische Forschung zu halten. Folglich kann eine Wissenschaftler nur mit den Daten der Patienten forschen, die er selbst ärztlich behandelt hat, nicht aber mit den Daten anderer Patienten. Eine etwas differenziertere Betrachtungsweise ist allerdings bei Universitätskliniken und -instituten am Platz. Denn diese haben neben der Krankenbehandlung auch die Aufgabe der medizinischen Forschung und Lehre. Dies ist allgemein bekannt. Begibt sich ein Patient in eine solche Klinik, muß er deshalb damit rechnen, daß die Klinik seine Unterlagen auch für medizinische Forschung nutzt und zu diesem Zweck an bei ihr arbeitende Forscher gibt. Nur wenn ein Patient dem ausdrücklich widerspricht oder auf sonstige Weise zu erkennen gibt, daß er damit nicht einverstanden ist, dürfen Universitätskliniken und -institute nicht so verfahren.

Gilt dies auch für Doktorarbeiten? Die Meinungen mögen geteilt sein, ob eine medizinische Dissertation unter der Rubrik „Forschung" einzuordnen ist. Doch seien wir großzügig und forschungsfreundlich und bejahen dies: dann darf ein in der Klinik beschäftigter Professor an seinen Doktoranden Patientenunterlagen zur Erstellung einer Dissertation weitergeben, wenn alles unter seiner Verantwortung verbleibt. Er, der Professor, und nicht der Doktorand hätte deshalb, wenn es zum Zwecke der Dissertation erforderlich wäre, den Patienten anzusprechen und um seine weitere Mitwirkung zu bitten. Eindeutig überschritten sind die Grenzen des Zulässigen, wenn der Doktorand sein Wissen aus den überlassenen Unterlagen dazu nutzt, sich eigenständig an den Patienten zu wenden und sich gar noch ohne dessen Einverständnis mit dessen Hausarzt in Verbindung setzt. Kein Patient einer Universitätsklinik muß mit einer solchen Vorgehensweise eines Doktoranden rechnen. Wer meint, er könne hier von einem stillschweigenden Einverständnis des Patienten ausgehen, überstrapaziert die Grenzen einer erlaubten Interpretation des Patientenwillens ganz erheblich.

5. Auskünfte der Pforte

Was soll die Pforte einer Klinik machen, wenn sich bei ihr jemand mündlich oder telefonisch erkundigt, ob sich ein bestimmter Patient in der Klinik aufhält, wo er liegt, ob er schon verlegt oder gar entlassen ist. Was sagt dazu der Datenschutz? Mit diesen Fragen werde ich immer wieder konfrontiert.

Die Pforte einer Klinik muß wie alle anderen Beschäftigten im Krankenhaus auch die ärztliche Schweigepflicht beachten. Sie darf deshalb nur über den konkreten Aufenthalt eines Patienten Auskünfte geben, wenn ihr dies eine Rechtsvorschrift oder einer der allgemeinen Rechtfertigungsgründe zur Durchbrechung der ärztlichen Schweigepflicht ausdrücklich erlaubt. Abgesehen von Ausnahmesituationen, z. B. Notfällen, kommt es deshalb darauf an, womit der Patient einverstanden ist und womit nicht:

- Zwar wäre es denkbar und zulässig, alle Patienten bei der Aufnahme in die Klinik ausdrücklich zur Abgabe einer entsprechenden Einwilligungserklärung aufzufordern. Von einem solchen Verfahren, das vereinzelte Krankenhäuser erwägen, kann ich nur abraten: zum einen ist es äußerst schwierig, eine solche Erklärung so abzufassen, daß sie einerseits präzise und

damit wirksam ist und anderseits der Pforte den erforderlichen Spielraum läßt. Zudem ermöglicht eine schriftliche Einwilligung immer nur Entweder-Oder-Lösungen; für Differenzierungen läßt sie keinen Raum. Und schließlich sollte man dies mit Rücksicht auf die Patienten generell nicht tun: die meisten von ihnen würden ein solches Verfahren als reichlich unnötige, lästige, bürokratische Maßnahme empfinden – sind sie doch in der Regel nicht bloß damit einverstanden, daß die Pforte Auskunft gibt, sondern erwarten es sogar.

- Die Pforte sollte deshalb immer, aber auch nur insoweit Auskunft geben, als der Patient stillschweigend eingewilligt hat. Hier liegen die Dinge so: Jedermann weiß, daß es in jedem Krankenhaus die Pforte und vielleicht noch einige andere Stellen gibt, an die sich Besucher wenden können, wenn sie einen Patienten aufsuchen oder sonst mit ihm Kontakt aufnehmen wollen; ebenso ist es, wenn jemand Blumen oder andere Geschenke abgeben läßt. Patienten, die in ein Krankenhaus kommen, müssen mit dieser Übung rechnen. Äußern sie nichts Gegenteiliges, kann das Krankenhaus davon ausgehen, daß sie diese Praxis stillschweigend akzeptieren. Wie auch sonst beim Datenschutz ist es freilich auch hier: ganz ausnahmslos geht es nicht an, die stillschweigende Einwilligung des Patienten zu unterstellen:
  - Wenn jemand etwa listenmäßig Auskunft über alle im Krankenhaus befindlichen Patienten will oder aus sonstigen Gründen erkennbar ist, daß es dem Anfragenden nicht um die übliche Kontaktaufnahme und Pflege zwischenmenschlicher Beziehungen zu einem Patienten geht, dann muß die Krankenhauspforte selbstverständlich passen. Ohne ausdrückliche Einwilligung der Patienten darf hier nichts laufen.
  - Eine Rolle muß auch spielen, um welche Art von Klinik und welche Art von Patienten es sich handelt. Denn das Schutzbedürfnis ist je nach physischer und psychischer Verfassung der Patienten recht unterschiedlich. So hätte ich Bedenken, wenn die Pforte einer psychiatrischen Klinik generell Auskunft erteilen würde. Solchen Patienten meine ich, sollte man ausdrücklich Gelegenheit geben, ihre Haltung darzulegen.
  - Ist der Patient wegen eines psychischen und physischen Zustandes überhaupt nicht mehr in der Lage, sich zu äußern, dann ist von vornherein die Annahme einer stillschweigenden Einwilligung ausgeschlossen. In diesen Fällen kann sich das Krankenhaus jedoch mit der Offenbarungsbefugnis des übergesetzlichen Notstands i.S.v. § 34 StGB helfen. Darüber hinaus darf es Auskünfte erteilen, soweit es vom mutmaßlichen Einverständnis des Patienten ausgehen kann.

Diese Verfahrensweise ist auch mit dem Landesdatenschutzgesetz vereinbar. Manche bezweifeln dies zwar gelegentlich, weil das Landesdatenschutzgesetz keine stillschweigende oder mutmaßliche, sondern nur eine ausdrückliche Einwilligung kennt, die zudem noch in der Regel schriftlich abzugeben ist. Dabei wird aber übersehen, daß das Landesdatenschutzgesetz in anderer Hinsicht weitaus großzügiger als das Arztgeheimnis ist, und in § 11 Abs. 1 LDSG u. a. erlaubt, daß ein Krankenhaus Daten von Patienten auch ohne deren Einwilligung an private Personen weitergibt, wenn daran ein berechtigtes Interesse besteht und schutzwürdige Belange des Patienten nicht entgegenstehen. Diese Voraussetzungen sind immer dann erfüllt, wenn die Erteilung von Auskünften mit der ärztlichen Schweigepflicht vereinbar ist.

6. Der Gesetzgeber ist gefordert

Viele Personen und Stellen im modernen arbeitsteiligen Krankenhaus erheben und sammeln Informationen über den einzelnen Patienten. Oft sind dies Angaben sensibelster Art. Diese Informationen gehen in vielfältiger Weise innerhalb des Krankenhauses hin und her; das Krankenhaus gibt sie aber auch nach außen für unterschiedliche Zwecke weiter. Die moderne Gerätemedizin und Labortechnik und die wachsende Spezialisierung in der Medizin tun ein Übriges dazu, diesen umfangreichen Informationsaustausch zu verstärken. Dazu kommt, daß die Krankenhäuser zunehmend den Computer im medizinisch-pflegerischen Bereich einsetzen, um die Kommunikation im Krankenhaus zu verbessern. Dadurch wird sich die Informationsgewinnung und -weitergabe noch wesentlich steigern. Schon jetzt ist es für den einzelnen Patienten praktisch nicht mehr möglich zu durchschauen, was in einem großen Krankenhaus mit seinen Daten geschieht, wohin sie gelangen und wer sie für welche Zwecke nutzt. Deshalb liegt auf der Hand: Eine solche Entwicklung birgt erhebliche Risiken für das Persönlichkeitsrecht der Patienten in sich und kann zu einer Störung des Vertrauensverhältnisses zwischen Arzt und Patient führen. Aus diesem Grund ist es unerläßlich, daß der Gesetzgeber klare Vorgaben für die Datenverarbeitung im Krankenhaus macht und die notwendigen Vorkehrungen zum Schutz des Selbstbestimmungsrechts der Patienten trifft. Das derzeit geltende Recht, nämlich die allgemeinen Datenschutzgesetze und die ärztliche Schweigepflicht, können den gebotenen Schutz nicht sicherstellen:

- Die allgemeinen Datenschutzgesetze sind schon deshalb kein wirksames Regulativ, weil sie nicht regeln, welche Informationen innerhalb eines Krankenhauses für welchen Zweck hin und hergehen und genutzt werden dürfen. Die wenigen Regelungen der Datenschutzgesetze, die auch für die Krankenhäuser gelten, sind zu allgemein gehalten und tragen den Besonderheiten und speziellen Bedürfnissen des Krankenhauses nicht Rechnung. Anders gesagt: sie stellen das Krankenhaus mit seinen sensiblen Patientendaten auf eine Ebene mit einem Wirtschaftsunternehmen oder einer normalen Behörde.
- Leider zeigen aber auch die Erfahrungen, daß die ärztliche Schweigepflicht der Komplexität der Verarbeitung und Nutzung von Patientendaten im Krankenhaus nicht gerecht wird. Sie verlangt, daß ein Arzt oder anderer Mitarbeiter des Krankenhauses Patientendaten an andere Personen oder Stellen innerhalb oder außerhalb des Krankenhauses grundsätzlich nur mit Einwilligung des Patienten weitergeben darf. Bei vielen, zur Behandlung wirklich notwendigen Informationsweitergaben ist aber aus rein praktischen Gründen gar nicht möglich, die Einwilligung des Patienten einzuholen und ihn zuvor über die Bedeutung der Einwilligung aufzuklären. Gerade aber das wäre zur Garantie seines Rechts auf informationelle Selbstbestimmung eigentlich notwendig. Die Praxis schlägt deshalb zur Zeit zweierlei Wege ein, um dem Einwilligungserfordernis – allerdings nur formal – Genüge zu tun: Zum einen enthalten die Aufnahmebedingungen vieler Krankenhäuser im Kleingedruckten neben vielen anderen Hinweisen und Bedingungen auch eine sehr weit gefaßte Einwilligungserklärung. Diese Erklärung ließe, wäre sie wirksam, dem Krankenhaus praktisch freie Hand bei der Weitergabe von Patientendaten. Sie ist jedoch wegen ihrer Unbestimmtheit und wegen der mangelnden Aufklärung des Patienten über ihre Bedeutung unwirksam. Zum anderen machen die Krankenhäuser sich zunutze, daß die Einwilligung in die Durchbrechung der ärztlichen Schweigepflicht keiner be-

stimmten Form bedarf und sie deshalb der Patient auch stillschweigend durch schlüssiges Verhalten erteilen kann. Diese Rechtskonstruktion ist für einen überschaubaren Lebensbereich sicher sinnvoll und notwendig. Macht man sie aber zur Grundlage für die Informationsweitergaben sowohl im Krankenhaus als auch nach außen, dann öffnet man damit der Rechtsunsicherheit Tür und Tor. Gerade dies tut die Krankenhauspraxis im Ergebnis und kann es wegen der unzureichenden Rechtslage auch kaum anders. Die Folge davon ist: je nach Interessenlage kommen dabei die unterschiedlichsten Ergebnisse heraus. Oft genug entscheidet bei Datenweitergaben nicht etwa der – in Wirklichkeit gar nicht vorhandene – Wille des Patienten darüber, was richtig und zweckmäßig ist, sondern die Vorstellung dessen, der über die Information verfügt. Die Einwilligung des Patienten wird nicht festgestellt, sondern schlichtweg unterstellt – auch wenn der Patient von alledem gar keine Ahnung hat und mangels Information auch nicht haben kann. Wegen dieser Vorgehensweise herrscht heute schon bei vielen der Verantwortlichen für das Krankenhauswesen die Vorstellung vor, das ganze Krankenhaus sei eine Einheit; die Patientendaten dürften frei hin und her fließen und die Krankenhausverwaltung dürfe die Patientendaten aus dem medizinisch-pflegerischen Bereich beliebig für ihre Zwecke nutzen. Diese Vorstellung degradiert das Arztgeheimnis mit Hilfe des Zauberworts „stillschweigende Einwilligung" zum Krankenhausgeheimnis. Das mag zwar aus der Sicht dessen, der für einen möglichst reibungslosen, wirtschaftlichen Betrieb eines Krankenhauses zu sorgen hat, verständlich sein. Damit wird man jedoch dem besonderen Schutzbedürfnis des Patienten gerade auch im modernen technisierten Krankenhaus nicht gerecht.

Auch in der heutigen Zeit sollte man daran festhalten, daß sich ein Patient nicht einem anonymen Krankenhausapparat, sondern im Krankenhaus konkreten Menschen anvertraut. Dies muß sich auf den Umgang des Krankenhauses mit seinen Daten auswirken. So wie die Dinge inzwischen liegen, bedarf es dazu eines Machtworts des Gesetzgebers. Er muß klare Vorgaben geben, welche Patientendaten das Krankenhaus erheben und verarbeiten darf, wer darauf zugreifen kann und wer sie für welche Zwecke nutzen kann. Er muß dabei sicherstellen, daß das Arztgeheimnis nicht zum Krankenhausgeheimnis denaturiert wird. Deshalb gilt es insbesondere festzulegen,

- daß die Krankenhausverwaltung nicht unmittelbar auf die im medizinisch-pflegerischen Bereich geführten Unterlagen über den Patienten zugreifen kann,
- daß die Patientendaten tatsächlich in der ärztlichen Verantwortung bleiben und sie deshalb das Krankenhaus nicht in externen, nicht unter ärztlicher Leitung stehenden Rechenzentren verarbeiten lassen,
- für welche Zwecke die Krankenhausverwaltung welche Patientendaten erhalten darf,
- ob und unter welchen Voraussetzungen Krankenhausärzte mit Daten von Patienten, die sie nicht selbst behandelt haben, forschen und
- ob und in welchem Umfang nicht in das Behandlungsgeschehen eingeschaltete Auszubildende Kenntnis von Patientendaten erhalten können.

Schließlich gilt es auch festzulegen, welche Rechte der einzelne Patient bei der Informationsverarbeitung hat, in welchen Fällen er tatsächlich darüber entscheiden kann und muß, ob seine Daten gespeichert, verarbeitet, genutzt oder weitergegeben werden dürfen, und welche Voraussetzungen dafür gegeben sein müssen.

Leider sieht das in Baden-Württemberg für das Krankenhauswesen zuständige Sozialministerium die Sache nicht so. Sein Vorgehen beim Erlaß des soeben verabschiedeten neuen Landeskrankenhausgesetzes zeigt dies überdeutlich: Hatte es mir 1984 noch zugesagt, es werde bei der nächsten Novellierung des Krankenhausgesetzes prüfen, ob und welche Datenschutzvorschriften in das Krankenhausgesetz aufzunehmen seien, so war davon in dem Gesetzentwurf, der im Mai 1986 in die Anhörung ging, keine Rede mehr. Mein erneuter Vorschlag, doch diesen Entwurf um eine bereichsspezifische Datenschutzregelung zu ergänzen, blieb ohne Antwort. Statt dessen wurde er unverändert in den Landtag eingebracht. In der amtlichen Begründung konnte ich dann lesen, daß die Landesregierung die allgemeinen Datenschutzgesetze und die ärztliche Schweigepflicht „nach gegenwärtigem Sachstand und Diskussionsstand über den Datenschutz im Gesundheitswesen als ausreichend" ansieht. Wegen dieser absolut unbefriedigenden Reaktion machte ich von meinem Recht Gebrauch, mich unmittelbar an den Landtag zu wenden, und legte dem Parlament die Notwendigkeit einer bereichsspezifischen Datenschutzregelung im Landeskrankenhausgesetz dar. Die Oppositionsparteien griffen während der ersten Lesung diesen Hinweis auf. Die naheliegende Erwartung, nun werde die Frau Sozialministerin im Rahmen der weiteren Gesetzesberatungen wenigstens begründen, warum sie meint, das geltende Recht reiche aus, trog; auch jetzt blieb sie die Antwort schuldig. Statt dessen verteidigte sie ihre Position mit dem formalen, bis dahin nie vorgetragenen Argument, man müsse zunächst prüfen, wer überhaupt, also ob Bund oder Land für den Erlaß solcher Datenschutzvorschriften zuständig seien – ganz so, als ob dies ein völlig neues Problem wäre und als ob andere Bundesländer nicht bereits in ihre Krankenhausgesetze Datenschutzregelungen aufgenommen hätten. Zugleich quittierte sie bei der zweiten Lesung des Gesetzentwurfs mein jahrelanges Bemühen mit dem Bemerken, die Datenschutzbeauftragte sei nicht „die Hüterin der ärztlichen Schweigepflicht". Nur ein flüchtiger Blick in das Landesdatenschutzgesetz hätte ihr freilich gezeigt, daß dem schon so ist. Allerdings hat das Arztgeheimnis auch noch andere Hüter; eine Hüterin sollte die für das Krankenhauswesen zuständige Sozialministerin sein. Zu hoffen bleibt deshalb, daß der Prüfungsauftrag des Landtags, die Landesregierung möge sich des Problems der Notwendigkeit von Datenschutzvorschriften für das Krankenhaus annehmen, doch noch etwas im Lande bewegt.

7. Teil: Soziale Leistungen

Der Sozialstaat gleicht in seinem Hunger nach Informationen einem Moloch. Je mehr Bürger auf Sozialleistungen angewiesen sind, je differenzierter das Leistungssystem und die Leistungsvoraussetzungen ausgestaltet werden, desto mehr Informationen braucht er. Das durchaus berechtigte Bestreben, ungerechtfertigte Inanspruchnahmen zu verhindern, tut ein übriges dazu, daß das Datensammeln im Sozialbereich inzwischen schon immense Ausmaße angenommen hat. Um so notwendiger ist, hier ganz besonders darauf zu achten, daß die Grenzen der Erforderlichkeit nicht überschritten, die Rechtsvorschriften über die Informationsgewinnung beachtet und die Geheimhaltungsbestimmungen zum Schutz der Sozialdaten strikt eingehalten werden.

1. Essensgutscheine an Nichtseßhafte

Nichtseßhafte sind nicht immer gern gesehene Gäste. Auch findet ihre Art zu leben sicher nicht jedermanns Beifall. Dies alles rechtfertigt jedoch nicht die Art und Weise, wie das Sozialamt der Stadt Albstadt bei der Ausgabe von Lebensmittelgutscheinen an Nichtseßhafte vorging. Wer bei der Obdachlosenunterkunft einen Lebensmittelgutschein im Wert von 8,- DM beantragen wollte, mußte zunächst gegenüber dem vom Sozialamt beauftragten Polizeirevier folgende Angaben machen:

- Name und Vorname
- Geburtstag und Geburtsort
- Beruf
- Konfession
- Familienstand (ledig, verheiratet, getrennt lebend, geschieden)
- Nummer und Ausstellungsdatum des Personalausweises
- Wohnsitz
- Staatsangehörigkeit
- Ankunft am ... von
- Abgang am ... wohin.

Alle diese Angaben trug das beauftragte Polizeirevier in den Gutscheinvordruck ein und händigte ihn dem Antragsteller aus. Wollte er diesen Gutschein einlösen, blieb ihm nichts anderes übrig, als alle die eingetragenen Informationen dem Lebensmittelgeschäft zur Kenntnis zu geben.

Ein solches Vorgehen steht in evidentem Widerspruch zu § 60 SGB I. Wer eine Sozialhilfeleistung beantragt, muß danach nur die Angaben machen, die zur Entscheidung über seinen Antrag notwendig sind. An diese Vorgabe hielt sich das Sozialamt in keiner Weise: warum beispielsweise der Nichtseßhafte zur Entscheidung über die Gewährung eines Gutscheins in Höhe von 8,- DM u. a. sogar seine Konfessionszugehörigkeit angeben mußte, ist schlechterdings unerfindlich. Gegen die Regeln des Datenschutzes verstieß die Praxis des Sozialamts aber auch, weil sie die Nichtseßhaften faktisch zwang, den Mitarbeitern der Lebensmittelgeschäfte die ganze Palette ihrer persönlichen Angaben bekanntzugeben; § 35 SGB I steht dem entgegen. Weil er das Sozialamt verpflichtet, alle ihm bekanntgewordenen Angaben über die persönlichen und sächlichen Verhältnisse von Hilfeempfängern als Sozialgeheimnis zu wahren, muß das Sozialamt auch alles unterlassen, was die Sozialhilfeempfänger zwingt, Informationen über sich weiterzugeben, die das Sozialamt selbst nicht weitergeben dürfte.

Nachdem ich das Sozialamt der Stadt Albstadt um Äußerung zu seiner Verfahrensweise gebeten hatte, geschah lange Zeit nichts. Dann – sieben Monate später – teilte mir die Stadt Albstadt schließlich mit, die Obdachlosenunterkunft sei seit Monaten wegen Umbauarbeiten geschlossen. Der von mir kritisierte Vordruck werde nach ihrer Wiedereröffnung abgeändert; man wolle dann keine datenschutzrechtlich bedenklichen Fragen mehr stellen.

2. Nachbar hört mit

Mehr Datenschutz in den Schalterräumen der Banken und Sparkassen forderte die CDU-Fraktion in einer parlamentarischen Initiative (LT-Drs. 9/3001). Sie hält es zu Recht für untragbar, daß Bankkunden ihre Geschäfte oft nicht abwickeln können, ohne daß andere Kunden das Gespräch mitbekommen. Die gleiche Situation findet sich leider auch bei einer ganzen Reihe von Sozialämtern im Lande. Wiederholt beklagten sich zum Beispiel Bür-

ger, daß sie beim Sozialamt der Stadt Stuttgart gezwungen gewesen seien, die für die Begründung eines Sozialhilfeantrags notwendigen Angaben zu machen, obwohl im gleichen Raum noch ein weiterer Antragsteller anwesend war. Beide Antragsteller hätten dann hören können, womit der andere seinen Antrag begründete. Es sei eine Zumutung, wenn man auf diese Weise genötigt sei, seine Lebensverhältnisse Dritten mitzuteilen.

Ich halte diese Klage für berechtigt. Die Sozialämter sind nach § 35 SGB I verpflichtet, solche Situationen zu vermeiden. Die dort festgelegte Pflicht zur Wahrung des Sozialgeheimnisses verbietet nicht nur eine unbefugte Offenbarung durch die Sozialämter, sondern verlangt auch, daß sie Vorkehrungen zum Schutz der Sozialdaten treffen, um auf diese Weise eine ungewollte Kenntnisnahme durch Dritte zu unterbinden. Demgegenüber kann nicht, wie dies leider immer wieder geschieht, geltend gemacht werden, die räumlichen Verhältnisse ließen ein anderes Vorgehen nicht zu. Wenn diese Verhältnisse tatsächlich so sind, dann müssen sie eben geändert werden. Die Erfüllung des Anspruchs auf Wahrung des Sozialgeheimnisses darf man jedenfalls nicht von solchen Überlegungen abhängig machen. Die Stadt Stuttgart will sich, wie sie mir auf meine Anfrage vom Mai 1986 vor wenigen Tagen mitteilte, jetzt wenigstens darum bemühen.

3. Das Bürgermeisteramt als Anlaufstelle

Bei einer ganzen Reihe von Sozialleistungen ist das Bürgermeisteramt auch dann Anlaufstelle, wenn es selbst nicht über die Leistungen entscheidet. So nimmt das Bürgermeisteramt in seiner Eigenschaft als Ortsbehörde für die Arbeiter- und Angestelltenversicherung Rentenanträge entgegen; Wohngeldanträge sind bei ihm einzureichen; Sozialhilfeanträge und Anträge auf Erziehungsgeld kann man dort abgeben. Deshalb stellt sich immer wieder die Frage, was das Bürgermeisteramt mit solchen Anträgen und den dazugehörigen Nachweisen tun darf. Muß es sich darauf beschränken, diese an die zuständigen Behörden weiterzuleiten, oder darf es Mehrfertigungen der Anträge und Kopien der beigefügten Nachweise (z. B. Steuerbescheide, ärztliche Bescheinigungen, Zeugnisse o. ä.) herstellen und bei sich aufbewahren? Letzteres ist weit verbreitet; als Grund geben die Bürgermeisterämter an, nur so bei späteren Beschwerden und Rückfragen die eigene Vorgehensweise nachvollziehen zu können. Darüber hinaus sei die Aufbewahrung der Unterlagen hilfreich, falls sich der Antragsteller später von ihnen beraten lassen will und läge deshalb in dessen Interesse.

Datenschutzrechtlich bewerte ich dieses Vorgehen wie folgt: Wenn ein Bürgermeisteramt solche Anträge entgegennimmt, dann wird es damit als Sozialleistungsträger tätig und muß folglich die Bestimmungen zum Schutz des Sozialgeheimnisses beachten. Seine Anlaufstelle darf deshalb die Informationen aus den Antragsunterlagen grundsätzlich nicht an andere Stellen innerhalb und außerhalb des Bürgermeisteramts weitergeben – es sei denn, die §§ 67 bis 77 SGB X erlauben dies ausnahmsweise. Insbesondere wäre rechtswidrig, Antragsunterlagen in die Einwohnerakten aufzunehmen, die noch manche Bürgermeisterämter über die Kontakte jedes ihrer Einwohner mit seiner Gemeinde führen. Wegen des Sozialgeheimnisses muß das Bürgermeisteramt Vorkehrungen zum Schutz gegen eine unbefugte Nutzung und Weitergabe der in den Antragsunterlagen gemachten Angaben treffen. Es darf deshalb nur die Unterlagen bei sich

aufbewahren, die zur Erfüllung seiner Aufgaben als Anlaufstelle für Sozialleistungsanträge erforderlich sind. Festzuhalten ist deshalb in aller Regel bloß, daß und wann ein bestimmter Bürger einen bestimmten Antrag auf eine bestimmte Sozialleistung gestellt, welche Nachweise er dazu vorgelegt und welche Unterlagen das Bürgermeisteramt an den Sozialleistungsträger weitergeleitet hat. Mit Hilfe dieser Angaben kann das Bürgermeisteramt jederzeit die Aktivitäten, für die es bei der Entgegennahme und Weitergabe von Anträgen verantwortlich ist, rekonstruieren. Dagegen sehe ich keine Notwendigkeit, daß es darüber hinaus noch Antragsunterlagen aufbewahrt. Das Argument, eine etwaige spätere Beratung des Bürgers erfordere dies, sticht nicht. Denn beim Einreichen des Antrags ist vielfach völlig ungewiß, ob dieser Bürger später nochmals zur Beratung erscheint und ob es dann nötig ist, auf Unterlagen zurückzugreifen. Im Ergebnis liefe das Vorhalten von Photokopien der Antragsunterlagen auf eine reine Vorratsdatensammlung hinaus, die der Datenschutz gerade nicht will. Natürlich mag es Fälle geben, in denen wegen der besonderen Lebensumstände eine andere Verfahrensweise auch im Interesse des Bürgers liegen kann. In solchen Ausnahmefällen besteht die Möglichkeit, die Einwilligung des Bürgers zur Aufbewahrung der Photokopien des Antrags einzuholen. Das sollte das Bürgermeisteramt aber wirklich nur dann tun, wenn ein solches Bedürfnis tatsächlich erkennbar besteht. Wenn dem so ist, dann muß es auch Vorkehrungen treffen, daß die Anlaufstelle die aufbewahrten Unterlagen nicht auch für andere als Beratungsaufgaben verwendet.

4. Das Erziehungsgeld

Die Landeskreditbank Baden-Württemberg scheint zunehmend zur Allzweckwaffe der Landesregierung zu werden. Mit Wirkung vom 1. Jan. 1986 übertrug sie ihr die Entscheidung über die Gewährung von Bundes- und Landeserziehungsgeld. Wer meint – und was liegt näher, weil doch die Zielrichtung beider Leistungen dieselbe ist und der Antragsteller im wesentlichen die gleichen Angaben machen und Nachweise beibringen muß –, der Datenschutz sei bei beiden Verfahren derselbe, irrt sehr. Für das Verfahren „Bundeserziehungsgeld" gelten die strengen Vorschriften des Sozialgesetzbuchs, weil die Landeskreditbank insoweit Sozialleistungsträger ist. Für das Verfahren „Landeserziehungsgeld" gilt dagegen nur das Landesdatenschutzgesetz, weil das Landeserziehungsgeld allein aufgrund der Verwaltungsvorschrift des Sozialministeriums zum Landeserziehungsgeld vom April 1986 als freiwillige Leistung des Landes Baden-Württemberg gewährt wird. Diese unterschiedliche Rechtslage hat folgende unbefriedigenden Konsequenzen:

- Wer Bundeserziehungsgeld beantragt, muß der Landeskreditbank nur im Rahmen von § 60 SGB I Angaben machen und Einwilligungserklärungen abgeben. Die Landeskreditbank kann deshalb nicht, wie sie es in ihrem ersten Antragsvordruck vorsah, das Erziehungsgeld unter der Bedingung gewähren, daß der Antragsteller in die Weitergabe seiner Daten für statistische Zwecke an das Ministerium für Jugend, Familie und Gesundheit in Bonn und an das Sozialministerium in Stuttgart einwilligt. Darüber hinaus muß die Landeskreditbank im Verfahren „Bundeserziehungsgeld" das Sozialgeheimnis (§ 35 SGB I) beachten. Infolgedessen darf sie Angaben, die sie dabei erfährt, nicht für andere ihrer Aufgaben – etwa im Bereich der Wohnbauförderung – nutzen.
- Wer im Anschluß an das Bundeserziehungsgeld noch 12 Monate lang Landeserziehungsgeld beziehen möchte, ist dage-

gen viel schlechter dran: das Landesdatenschutzgesetz schützt die Angaben, die er dafür der Landeskreditbank machen muß, nur, soweit sie in Dateien, also in Karteien oder im Computer gespeichert sind; das ist längst nicht bei allen der Fall. Zudem darf die Landeskreditbank diese Angaben nach § 10 LDSG immer schon dann an andere Behörden, z. B. Landratsämter, weitergeben, wenn diese erklären, sie benötigten diese Informationen zur Erfüllung ihrer Aufgaben, also z. B. für Zwecke der Wohngeldberechnung. Ein weiterer Nachteil war, daß die Antragsteller nach der Verwaltungsvorschrift des Sozialministeriums anfangs ihre Anträge durchweg bei den Bürgermeisterämtern einreichen mußten. Dadurch liefen sie schon dort Gefahr, daß ihre Antragsunterlagen für andere Zwecke genutzt wurden. Denn es gibt keine Rechtsvorschrift, die den Bürgermeisterämtern verbietet, ihnen aus Anträgen auf Gewährung von Landeserziehungsgeld bekannt gewordene Umstände für ganz andere ihrer Aufgaben, z. B. für die Festsetzung der Feuerwehrabgabe oder Sozialhilfe zu verwenden.

Das Sozialministerium blieb auf meinen Hinweis auf diese äußerst unbefriedigende Rechtslage nicht untätig: zum einen sorgte es dafür, daß Anträge auf Landeserziehungsgeld auch direkt an die Landeskreditbank gehen können. Zum anderen forderte es die Bürgermeisterämter und Landeskreditbank auf, im Verfahren „Landeserziehungsgeld" die Vorschriften zum Schutz des Sozialgeheimnisses entsprechend anzuwenden. Soweit recht und gut, bloß bleibt der Nachteil: die Aufforderung ist für die Adressaten in keiner Weise verbindlich; es gibt kein irgendwie geartetes Weisungsrecht des Sozialministeriums gegenüber den Bürgermeisterämtern und der Landeskreditbank. Infolgedessen hängt es allein von deren Bereitschaft ab, ob sie im Verfahren „Landeserziehungsgeld" die strengeren Datenschutzvorschriften des Sozialgesetzbuches beachten und sich nicht bloß an die Minimalregeln des Landesdatenschutzgesetzes halten. Ich meine: es genügt nicht, daß der Datenschutz in einem so sensiblen Bereich wie der Gewährung von Landeserziehungsgeld – die Antragsteller müssen dabei beispielsweise ihre Familienverhältnisse angeben und ihren Einkommensteuerbescheid vorlegen – allein vom Goodwill der Behörden abhängt. Die äußerst unbefriedigende Rechtslage sollte vielmehr Anlaß sein, das Landeserziehungsgeld und alle sonstigen, nicht unter das Sozialgesetzbuch fallenden sozialen Leistungen des Landes und der Kommunen durch Landesrecht den Regeln über den Schutz des Sozialgeheimnisses zu unterstellen. Eine Antwort des Sozialministeriums auf diesen Vorschlag steht noch aus.

5. Amtshilfe durch Krankenkassen

Wer wäre nicht überrascht und peinlich berührt, wenn er erfahren müßte, daß ein unbekannter Gläubiger bei seinem Arbeitgeber sein Gehalt pfänden ließ. Genau dies widerfuhr einem Bürger, weil ein Mitarbeiter der Allgemeinen Ortskrankenkasse Heidelberg die Bestimmungen zum Schutz des Sozialgeheimnisses nicht beachtet hat. Geschehen war folgendes: die Landesoberkasse Karlsruhe unternahm bei der Heidelberger Ortskrankenkasse einen Pfändungsversuch gegen einen Schuldner und stellte ihr deshalb eine Pfändungsverfügung zu. Der Sachbearbeiter dieser Ortskrankenkasse übersah bei der Bearbeitung der Pfändungsverfügung, daß seiner Krankenkasse niemand mit exakt dem Namen und der Anschrift gemeldet war, wie sie in der Pfändungsverfügung angegeben waren. Er nahm vielmehr an, daß der von der Landesoberkasse gesuchte Schuldner identisch

ist mit einem seiner Krankenkasse unter einer anderen Anschrift gemeldeten Bürger gleichen Namens, dessen Schreibweise zudem geringfügig abwich. Anstatt die Landesoberkasse darüber zu informieren, daß der Ortskrankenkasse niemand mit dem in der Pfändungsverfügung genannten Namen und der darin genannten Anschrift gemeldet ist, teilte er ihr mit, für den in der Pfändungsverfügung bezeichneten Schuldner würde dessen Arbeitgeber, die Firma X., Beiträge zur Renten- und Arbeitslosenversicherung entrichten. Dies wiederum war für die Landesoberkasse Anlaß, die Gehaltspfändung mit dem eingangs erwähnten Ergebnis vorzunehmen.

Das Vorgehen der Allgemeinen Ortskrankenkasse war aus zwei Gründen fehlerhaft: zum einen hätte selbstverständlich die Personenverwechslung nicht passieren dürfen; zum anderen hätte sie den Arbeitgeber des vermeintlichen Schuldners und noch weniger die Tatsache, daß dieser Beiträge zur Renten- und Arbeitslosenversicherung entrichtet, mitteilen dürfen. Diese Mitteilung wäre selbst dann rechtswidrig gewesen, wenn die Ortskrankenkasse die Personen nicht verwechselt hätte, sondern der Vollstreckungsschuldner tatsächlich bei ihr gemeldet gewesen wäre. Denn auch in einem solchen Falle ist sie nach § 69 Abs. 1 Nr. 1 SGB X nur befugt, die sog. Drittschuldnererklärung im Sinne von § 840 der Zivilprozeßordnung oder § 316 der Abgabenordnung abzugeben. Dagegen ist ihr nicht gestattet, den Arbeitgeber zu benennen, weil eine Offenbarungsbefugnis dafür fehlt. Eine solche läßt sich weder aus § 69 Abs. 1 Nr. 1 SGB X herleiten, weil die Ortskrankenkasse mit einer solchen Auskunft keine ihr obliegende gesetzliche Pflicht erfüllt, noch aus § 68 Abs. 1 SGB X, weil dessen Voraussetzungen für die Leistung von Amtshilfe nicht gegeben waren: es lag kein ausdrücklich gestelltes Amtshilfeersuchen der Landesoberkasse vor; auch kann man in der Pfändungsverfügung nicht schon das Ersuchen der Landesoberkasse an die Ortskrankenkasse sehen, ihr im Falle der Erfolglosigkeit der Pfändung im Wege der Amtshilfe den Arbeitgeber des Schuldners mitzuteilen. Erst recht nicht läßt sich auf § 68 Abs. 1 SGB X eine Mitteilung stützen, daß der Arbeitgeber Beiträge zur Renten- und Arbeitslosenversicherung bezahlt. Denn danach darf eine Ortskrankenkasse solche Informationen niemals weitergeben.

Die Allgemeine Ortskrankenkasse bezeichnete den Vorfall als bedauerlichen Einzelfall und nahm ihn inzwischen zum Anlaß, ihre Mitarbeiter auf die Rechtslage hinzuweisen, um so eine Wiederholung auszuschließen.

6. Das Jugendamt und der Regreß

Übernimmt ein Jugendamt die Kosten einer Familienpflegestelle, so kann es zur Deckung seiner Kosten etwaige Unterhaltsansprüche des Kindes auf sich überleiten und diese selbst gegen den Unterhaltspflichtigen geltend machen. Dazu braucht es freilich Informationen über die Einkommensverhältnisse des Unterhaltspflichtigen. Unter welchen Voraussetzungen es diese bei Krankenkassen und Rentenversicherungsträgern einholen kann, ist eine in der Praxis viel diskutierte Rechtsfrage. Ich beurteile sie so: das Jugendamt kann sich nicht nach Belieben an diese Stellen wenden. Denn bei seiner Anfrage wegen der geplanten Überleitung eines Unterhaltsanspruchs muß es unausweichlich Tatsachen über die persönlichen und sächlichen Verhältnisse des Kindes und des Unterhaltspflichtigen bekanntgeben, die unter den Schutz des Sozialgeheimnisses fallen. Solche Tatsachen darf es nach § 69 Abs. 1 Nr. 1 SGB X nur offenbaren, soweit dies zur Erfüllung seiner Aufgaben nach dem Sozialgesetz-

buch erforderlich ist. Nicht zweifelhaft kann sein, daß es sich bei der Überleitung von Unterhaltsansprüchen um eine solche Aufgabe handelt: denn das Jugendwohlfahrtsgesetz (JWG) gilt als besonderer Teil des Sozialgesetzbuchs; damit gehört zu den Aufgaben des Jugendamts nach dem Sozialgesetzbuch auch die Aufgabe, Unterhaltspflichtige nach Maßgabe des § 82 JWG in Anspruch zu nehmen. Schwierigkeiten bereitet dagegen immer wieder, ob eine solche Anfrage des Jugendamts bei Krankenkassen oder Rentenversicherungsträger tatsächlich notwendig ist. Hier gilt zu bedenken, daß das Jugendamt die erforderlichen Informationen auch beim Unterhaltspflichtigen selbst anfordern kann: § 1605 BGB verpflichtet diesen, Auskünfte über seine Einkommens- und Vermögensverhältnisse zu geben und Nachweise darüber vorzulegen. Folglich muß sich das Jugendamt zunächst einmal an den Unterhaltspflichtigen wenden. Dabei muß es ihn – in entsprechender Anwendung des § 74 SGB X – auch darauf hinweisen, daß es sich im Falle seiner Untätigkeit die erforderlichen Auskünfte von Dritten beschaffen darf. Erst wenn dies nichts fruchtete, erlaubt der Grundsatz der Verhältnismäßigkeit dem Jugendamt, bei Krankenkasse oder Rentenversicherungsträger anzufragen und dem Unterhaltspflichtigen die darin liegende zusätzliche Belastung seiner Rechtssphäre zuzumuten. Ist all dies beachtet, sind auch die ersuchten Krankenkassen und Rentenversicherungsträger befugt, die ja ebenfalls das Sozialgeheimnis zu beachten haben, dem Jugendamt die erbetenen Auskünfte zu erteilen.

7. Die Auskunftspflicht des Arbeitgebers

Sozialämter benötigen in vielen Fällen Informationen über die Einkommensverhältnisse von Hilfesuchenden oder Hilfeempfängern, Unterhalts- oder Kostenersatzpflichtigen. Sie haben zwei Möglichkeiten, an diese Informationen zu kommen: entweder wenden sie sich an den, um dessen Einkommensverhältnisse es geht, oder dessen Arbeitgeber. Der Arbeitgeber freilich ist gegenüber dem Sozialamt nicht unbeschränkt auskunftspflichtig; er muß nach § 116 Abs. 2 des Bundessozialhilfegesetzes (BSHG) dem Sozialamt nur Angaben über die Art und Dauer der Beschäftigung sowie die Arbeitsstelle und den Arbeitsverdienst des Mitarbeiters, um dessen Einkommensverhältnisse es geht, machen, soweit dies die Durchführung des Bundessozialhilfegesetzes erfordert. Diese Rechtslage müssen die Sozialämter beachten, wenn sie Auskunftsersuchen an Arbeitgeber richten. In der Praxis sieht es leider häufig anders aus: aus einer Anfrage des Finanzministeriums beispielsweise weiß ich, daß die Sozialämter unter Berufung auf § 116 Abs. 2 BSHG oft auch Dinge erfragen, über die der Arbeitgeber nicht Auskunft geben muß. So finden sich in ihren Vordrucken, mit denen sie die Auskünfte einholen, auch Fragen nach der Krankenkasse, dem Namen der Kinder, nach Lohnpfändungen oder Abtretungen und nach dem Grund des Ausscheidens, sofern der Mitarbeiter bereits ausgeschieden ist. All diese Angaben führt § 116 Abs. 2 BSHG nicht auf; eine Auskunftspflicht des Arbeitgebers besteht deshalb insoweit nicht. Ungenügend berücksichtigen die Sozialämter leider auch, daß der Arbeitgeber Fragen nach dem Arbeitsverdienst nur beantworten muß, soweit das Sozialamt diese tatsächlich zur Durchführung des Bundessozialhilfegesetzes kennen muß. Gerade daran fehlt es aber in der Regel, weil nach § 76 BSHG nur das Nettoeinkommen relevant ist. Aus diesem Grunde genügt es, wenn das Sozialamt Brutto- und Nettobezüge, die Art der dabei berücksichtigten Abzüge und der Sonderzahlungen (z. B. Weihnachts- und Urlaubsgeld) vom Arbeitgeber er-

fährt. Genaue Zahlenangaben – etwa darüber, wie hoch die Lohnsteuer, die Kirchenlohnsteuer oder der Arbeitnehmeranteil an der Sozialversicherung ist – benötigt das Sozialamt dagegen zur Erfüllung seiner Aufgaben nicht. Diese Rechtsauffassung teilte ich dem Finanzministerium mit, das sich wegen der aufgetretenen Schwierigkeiten zwischen Landesamt für Besoldung und Versorgung auf der einen und den Sozialämtern auf der anderen Seite seit längerem mit diesem Problem befaßt. Es ließ mich inzwischen wissen, daß die kommunalen Landesverbände nunmehr beabsichtigen, den Sozialhilfeträgern die Verwendung eines Vordrucks zu empfehlen, der sich auf die notwendigen Angaben beschränkt.

8. Reha-Entlaßberichte

In der Vergangenheit erreichten mich immer wieder Eingaben von Mitarbeitern von Suchtkliniken und anderen Krankenhäusern, die Suchtkranke oder andere in ihrer Erwerbsfähigkeit wegen Krankheit oder körperlicher, geistiger oder seelischer Behinderung gefährdete oder geminderte Personen zum Zwecke ihrer Rehabilitation behandeln. Die Mitarbeiter klagten über das Verlangen der Versicherungsanstalten, die behandelnde Klinik solle die Entlaßberichte nach Beendigung der Kur auch den gesetzlichen Krankenkassen der Patienten zusenden. Auf diese Weise würden die Krankenkassen ohne Notwendigkeit die sehr detaillierten Angaben im Entlaßbericht über die gesundheitlichen und sozialen Verhältnisse der Patienten, den Verlauf ihrer stationären Behandlung, die dabei angewandten therapeutischen Verfahren, ihr Verhalten während dieser Zeit und den Behandlungserfolg enthalten. Diese Klagen über die bundesweit geübte Praxis der Versicherungsanstalten sind berechtigt:

Da der Arzt der Rehabilitationseinrichtung den Entlaßbericht im Auftrag der Versicherungsanstalt erstellt, unterliegen die darin gemachten Angaben dem Schutz des Sozialgeheimnisses. Sie dürften deshalb nur dann automatisch an die Krankenkassen der Versicherten gehen, wenn diese in jedem Einzelfall alle im Entlaßbericht enthaltenen Informationen benötigen würden. Das läßt sich aber sicherlich nicht in dieser Allgemeinheit sagen. Denn weder die Pflicht der Krankenkasse, den Versicherten zu beraten, noch ihre Pflicht, aufgrund von § 5 Abs. 2 des Rehabilitationsangleichungsgesetzes mit den anderen am Rehabilitationsverfahren beteiligten Trägern eng zusammenzuarbeiten, berechtigt zu einem so umfassenden automatischen Austausch höchst sensibler Informationen. So sehen es inzwischen auch die Versicherungsanstalten. Im Mai 1986 entschloß sich die Landesversicherungsanstalt Baden und später dann auch die Landesversicherungsanstalt Württemberg dazu, ihre bisherige Praxis aufzugeben. Den vollständigen Entlaßbericht erhält eine Krankenkasse nunmehr nur noch, wenn sie im Einzelfall nachweist, alle Daten daraus zu benötigen. In der Regel wird jetzt nur noch eine Zusammenfassung des Entlaßberichts weitergegeben, aus der im wesentlichen die Dauer der stationären Behandlung, die Diagnosen, das Behandlungsergebnis und die Vorschläge für weitere Maßnahmen zu ersehen sind. Wer auch diese Informationsweitergabe verhindern will, kann ihr nach § 76 Abs. 2 SGB X widersprechen. Auf dieses Widerspruchsrecht weisen die Landesversicherungsanstalten Baden und Württemberg ihre Versicherten hin, wenn sie den Krankenhausaufenthalt beantragen. Erfolgte ein Widerspruch, kann dies freilich für sie nachteilig sein – denn sie laufen Gefahr negativ beschieden zu werden, wenn die Krankenkasse Angaben aus dem Entlaßbericht braucht, um über eine beantragte Leistung zu entscheiden.

Alles in allem: Die Änderung der bisherigen Praxis ist aus der Sicht des Datenschutzes zwar eine Verbesserung. Nach wie vor bleibt freilich die Frage, ob es nicht auch Fälle gibt, in denen die Krankenkassen nicht einmal eine Kurzfassung des Entlaßberichts benötigen.

8. Teil: Das Rathaus – ein Umschlagplatz von Daten

1. Computer auf dem Rathaus

Auch die 1111 Städte und Gemeinden des Landes wissen die Vorteile der modernen Datenverarbeitungstechnik zu nützen. Die allermeisten von ihnen nehmen dafür die Dienste eines kommunalen Rechenzentrums in Anspruch und lassen dort die Daten ihrer Einwohner und Mitarbeiter verarbeiten. Einige Städte und Gemeinden gingen einen anderen Weg und beschafften eigene Computer. Sie glaubten, auf diese Weise Kosten zu sparen, flexibler zu sein und schneller auf ihre Daten zugreifen zu können. Bei zwei von etwa 20 Gemeinden, die das EDV-System des gleichen Computerherstellers verwenden und damit Personendaten aus dem Einwohner-, Personal- und Abgabewesen verarbeiten, führte ich Kontrollbesuche durch. Was ich in Lenzkirch und Pfalzgrafenweiler vorfand, war alles andere als erfreulich, ja in Pfalzgrafenweiler so bedenklich, daß ich einen weiteren Einsatz des EDV-Systems in dieser Form in Frage stellen mußte. Beim Kontrollbesuch zeigte sich nämlich, daß sich diese Gemeinde nicht darauf verlassen kann, was der Computer anzeigt oder ausdruckt. So enthielt ein Ausdruck Angaben über den Familienstand, die Staatsangehörigkeit, die Religionszugehörigkeit, das Geschlecht, das Wahlrecht und die Wehrüberwachung, obwohl – glaubt man der Bildschirmanzeige – diese Angaben über diese Person überhaupt nicht gespeichert sind. Bei einer anderen Person, bei der eigentlich nur einige wenige Daten gespeichert sein durften, druckte der Computer weitere Daten anderer Einwohner als deren Daten aus. Ähnliche Diskrepanzen zeigten sich in einer Reihe anderer Fälle. Offensichtlich waren Personendaten verfälscht und vermischt. Ebenso führten z. B. die Programme bei der Eingabe von Todesfällen nicht die im Meldegesetz vorgeschriebenen Löschungen aus. Diese und zahlreiche weitere Fehlfunktionen des EDV-Systems sind nur durch schwerwiegende Fehler im Aufbau des Systems zu erklären. Sie legen den Schluß nahe, daß nicht nur der Inhalt der einzelnen Datenfelder fehlerhaft ist, sondern sogar die technische Struktur insgesamt Lücken aufweist.

Zu diesen schweren Sicherheitsmängeln trugen zu einem guten Teil Fehler und Versäumnisse der Gemeinde bei:

- Sie nahm es hin, daß der Computerhersteller wichtige Informationen über die Datenverarbeitungsprogramme zurückhielt, so daß sie keinen Einblick darüber erhalten konnte, wie die Verarbeitung der Daten durch das EDV-System tatsächlich erfolgte. Sie zog die notwendigen Konsequenzen auch dann nicht, als ihre Mängelrügen beim Hersteller keine oder nur unzureichende Reaktionen zur Fehlerbehebung bewirkten. Die Gemeinde wurde damit ihrer Verantwortung für eine gesetzmäßige Datenverarbeitung nicht gerecht.
- Sie setzte neue oder überarbeitete EDV-Programme, die ihr der Hersteller übergab, ohne ausreichende Vorbereitungs-

maßnahmen ein. Sie versäumte vor allem, neue Programme mit besonderen Testdaten zu testen, die neben Standardfällen auch extreme, korrekte und fehlerhafte sowie auf früher festgestellte Programmfehler hin ausgerichtete Testfälle enthalten. Sie setzte neue Programme vielmehr sofort mit aktuellen Einwohnerdaten ein, obwohl sie wissen mußte, daß bei neuen oder geänderten Programmen häufig Fehler und Fehlfunktionen auftreten können, die zu einer unzulässigen Veränderung oder gar zum Verlust von Einwohnerdaten führen können.

- Jeder Benutzer des EDV-Systems konnte jederzeit durch einfachen Druck auf die sog. Break-Taste versehentlich oder absichtlich laufende Datenverarbeitungsvorgänge beliebig unterbrechen und Eingriffe in Dateien und Programme vornehmen. Sie beschwor damit die Gefahr herauf, daß gespeicherte Daten verfälscht, die Integrität der Dateien verletzt oder die Datenverarbeitungsvorgänge gestört werden. Derartige Manipulationen darf ein EDV-System nicht ermöglichen.
- Jeder Benutzer des EDV-Systems konnte durch eine verhältnismäßig einfache Manipulation die für ihn geltende Zugriffsbeschränkung umgehen und sich den Zugriff auf das ganze System mit allen Verarbeitungsmöglichkeiten beschaffen. Eine automatisierte Eingabekontrolle, die eine nachträgliche Feststellung ermöglichte, welche personenbezogenen Daten zu welcher Zeit von wem eingegeben wurden, leistete das System nicht.

Dies waren aber nur die gravierendsten Mängel. Beanstanden mußte ich auch Mängel oder Unzulänglichkeiten bei der Protokollierung von Datenverarbeitungsvorgängen, der Dokumentation des Verfahrens, der Sicherung der Programme und Daten gegen Verluste und der räumlichen Unterbringung des Computers. Ähnliche Fehler und Versäumnisse traf ich, wenn auch in geringerem Ausmaß, in Lenzkirch an. Wie die ersten Reaktionen der beiden Gemeinden zeigen, wird es noch einiger Anstrengungen bedürfen und wird noch mancher bei der Entscheidung für den eigenen Computer nicht einkalkulierte Aufwand notwendig werden, bis sie eine ordnungsgemäße Verarbeitung ihrer Einwohnerdaten sichergestellt haben.

2. Die Schwarzfahrerdateien

Wer öffentliche Verkehrsmittel benutzt, muß, solange der Traum vom Nulltarif noch nicht wahr geworden ist, im Besitz eines gültigen Fahrausweises sein und diesen bei Fahrausweiskontrollen auf Verlangen vorzeigen. Was aber geschieht, wenn ein Fahrgast bei einer solchen Kontrolle keinen gültigen Fahrausweis vorweisen kann? Welche Daten halten die Kontrolleure in solchen Fällen fest und was macht der Verkehrsbetrieb mit diesen Daten? Um dies zu klären, überprüften wir die Verkehrsbetriebe der Städte Baden-Baden, Esslingen a.N., Heilbronn, Karlsruhe, Konstanz und Pforzheim. Diese Verkehrsbetriebe unterliegen anders als die privatrechtlich organisierten kommunalen Verkehrsbetriebe meiner Kontrolle, weil sie von der Stadt als sog. Eigenbetriebe geführt werden.

2.1 Wie befragen die Kontrolleure die Fahrgäste?

Fordert eine öffentliche Stelle, die das Landesdatenschutzgesetz zu beachten hat, einen Bürger auf, Angaben über sich zu machen, dann muß sie ihn zuvor darüber informieren, ob er zur Antwort verpflichtet ist oder nicht und welche Konsequenzen es hat, wenn er der Aufforderung nicht nach-

kommt. Kurzum, der Bürger muß über seine Rechte informiert werden. Dieser Verpflichtung aus § 9 Abs. 2 LDSG trugen bisher die Verkehrsbetriebe, wenn überhaupt, nur sehr unvollkommen oder fehlerhaft Rechnung. Ihre Reaktion auf meine Kritik an dieser Praxis war positiv. Sie werden künftig die Fahrgäste über die Rechtslage informieren und dabei berücksichtigen, daß ihre Fahrgäste weder gesetzlich noch vertraglich verpflichtet sind, einem Fahrscheinkontrolleur die Personalien anzugeben.

2.2 Was Verkehrsbetriebe über Personen ohne gültigen Fahrausweis speichern

Stellen die Kontrolleure bei ihren Fahrausweiskontrollen fest, daß ein Fahrgast keinen gültigen Fahrausweis bei sich führt, fertigen sie eine Beanstandungsmeldung an. Diese Meldungen enthalten neben den üblichen Identifizierungsdaten (Name, Anschrift und Geburtstag) meist auch Angaben über die Art des Ausweises, mit der sich der Fahrgast bei der Kontrolle ausgewiesen hat und die Nummer dieses Ausweises. Bei Minderjährigen nehmen die Kontrolleure auch Name und Anschrift der Erziehungsberechtigten auf. Die Kontrolleure in Heilbronn tragen bei Schülern die Schule und die Klasse ein; in Konstanz geschieht dies nur dann, wenn der Schüler bei der Kontrolle keinen Schülerausweis zeigen konnte. Schließlich vermerken die Kontrolleure in Karlsruhe in ihrer Meldung auch Angaben zum Verhalten des Fahrgastes, z. B. ob er bei der Kontrolle „einsichtig" oder „uneinsichtig" war oder gar „handgreiflich" wurde. Die Verkehrsbetriebe bewahren die Beanstandungsmeldungen meist in Karteiform auf. Karlsruhe speichert die von den Kontrolleuren erhobenen Angaben seit 1. Mai 1986 auch noch im Computer. Pro Jahr beanstanden dieVerkehrsbetriebe in Baden-Baden ca. 1500 - 2000 Fahrgäste bei einer Gesamtfahrgastzahl von ca. 8 Millionen, in Esslingen ca. 2500 Fahrgäste bei einer Gesamtfahrgastzahl von ca. 14 Millionen, in Heilbronn ca. 1000 Fahrgäste bei einer Gesamtfahrgastzahl von 14 Millionen, in Karlsruhe ca. 20 000 Fahrgäste bei einer Gesamtfahrgastzahl von ca. 53 Millionen, in Konstanz ca. 2400 Fahrgäste bei einer Gesamtfahrgastzahl von ca. 8 Millionen und in Pforzheim ca. 1700 Fahrgäste bei einer Gesamtfahrgastzahl von 15 Millionen.

Beanstandet werden nicht nur echte Schwarzfahrer - also Personen, die auch nicht nachträglich einen gültigen Fahrausweis vorlegen können und von denen die Verkehrsbetriebe deshalb ein erhöhtes Beförderungsentgelt verlangen. Beanstandet werden auch die sog. Graufahrer. Das sind Personen, die zwar Inhaber eines gültigen Fahrausweises sind, bei der Kontrolle aber diesen Ausweis nicht bei sich führten. Legt ein solcher Fahrgast den Verkehrsbetrieben innerhalb einer Woche nach einer Beanstandung einen am Beanstandungstag gültigen Fahrausweis vor, so verlangen die meisten der Verkehrsbetriebe lediglich ein reduziertes erhöhtes Beförderungsentgelt. Insgesamt betreffen etwa ein Drittel bis die Hälfte der festgestellten Beanstandungen solche Graufahrer.

Zu dieser Datenspeicherung ist folgendes zu sagen: Die Verkehrsbetriebe dürfen personenbezogene Daten von Fahrgästen gem. § 9 Abs. 1 LDSG speichern, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Da sie selbstverständlich dafür zu sorgen haben, daß das ihnen zustehende Beför-

derungsentgelt auch tatsächlich eingeht, sind sie berechtigt, Daten all der Fahrgäste zu speichern, die sie bei Fahrausweiskontrollen ohne gültigen Fahrausweis angetroffen haben. Dabei müssen sie sich jedoch auf das Erforderliche beschränken. Erforderlich sind die Daten, die der Verkehrsbetrieb kennen muß, damit er mit Aussicht auf Erfolg seine zivilrechtlichen Ansprüche durchsetzen und zur Sicherung der Zahlungsmoral gegebenenfalls auch Anzeige wegen Beförderungserschleichung erstatten kann. Zu weit geht es deshalb, wenn nicht nur die Ausweisart, sondern auch die Ausweisnummer gespeichert wird. Das gleiche gilt für die Speicherung der Schule und der Klasse eines Schülers, wenn er seine Identität durch einen Ausweis nachgewiesen hat. Nicht gerechtfertigt ist schließlich auch, wenn ein Verkehrsbetrieb Angaben wie „einsichtig" oder „uneinsichtig" speichert. Diese Angaben sind zur Erfüllung der Aufgaben des Verkehrsbetriebs nicht notwendig. Die Verkehrsbetriebe teilten mir inzwischen mit, daß sie diese Rechtslage in Zukunft beachten werden.

2.3 Wie lange bleibt ein Schwarz- oder Graufahrer gespeichert?

Bei meinen Kontrollen stellte ich in dieser Frage große Unsicherheiten fest. Ein Teil der Verkehrsbetriebe hatte nicht geregelt, wann die gespeicherten Daten zu sperren und zu löschen sind. Bei einem anderen Teil existierten zwar solche Regeln; die Speicherdauer war aber in aller Regel viel zu lang bemessen. Häufig differenzierten sie bei der Speicherdauer auch nicht zwischen Schwarz- und Graufahrern.

Diese Praxis ist mit § 13 Abs. 2 und 3 LDSG nicht vereinbar. Nach dieser Bestimmung sind die Verkehrsbetriebe verpflichtet, personenbezogene Daten zu löschen, zumindest aber zu sperren, wenn ihre Kenntnis zur rechtmäßigen Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Dies hat für die Datenspeicherung der Verkehrsbetriebe folgende Konsequenzen:

- Schwarzfahrer

  Die Verkehrsbetriebe dürfen die Daten der Schwarzfahrer so lange vorhalten, als ihr Zahlungsanspruch noch nicht erfüllt oder verjährt und eine strafrechtliche Verfolgung noch möglich ist. Da Beförderungserschleichung gem. § 265 a StGB in aller Regel 3 Jahre nach der Begehung verjährt, entfällt spätestens nach 3 Jahren - gerechnet ab dem Tag der Schwarzfahrt – die Erforderlichkeit der Datenspeicherung. Da es nach neuerlichen Untersuchungen sehr unwahrscheinlich ist, daß jemand eine erneute Schwarzfahrt unternimmt, wenn seit der ersten bereits ein Zeitraum von 2 Jahren verstrichen ist, empfahl ich den Verkehrsbetrieben, die Speicherung im Regelfall auf einen Zeitraum von 2 Jahren zu beschränken.

- Graufahrer

  Da Graufahrer den Straftatbestand des § 265 a StGB nicht erfüllen, ist eine Datenspeicherung zu dem Zweck, eine Strafverfolgung zu ermöglichen, von vornherein ausgeschlossen. In diesen Fällen ist die Kenntnis der Daten entgegen der Auffassung des Innenministeriums als Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich nur solange erforderlich, bis das Beförderungsentgelt beglichen oder die Forderung verjährt ist.

- Kinder unter 14 Jahren
  Kinder unter 14 Jahren sind gem. § 19 StGB nicht strafmündig. Deshalb scheidet auch hier eine Datenspeicherung mit dem Zweck, eine Strafverfolgung zu ermöglichen, aus. Auch in diesen Fällen ist deshalb eine Datenspeicherung nur erlaubt, bis der Anspruch auf das Beförderungsentgelt erfüllt oder aber die Forderung verjährt ist.

Um dieser Rechtslage gerecht zu werden, forderte ich die Verkehrsbetriebe auf,
- ihren Datenbestand umgehend zu bereinigen;
- den Datenbestand über Schwarzfahrer in regelmäßigen Abständen von maximal 3 Monaten daraufhin zu überprüfen, bei welchen Daten die zulässige Speicherungsdauer abgelaufen ist;
- die gespeicherten Daten über Graufahrer und Kinder unter 14 Jahren umgehend zu löschen, wenn das Beförderungsentgelt bezahlt ist, und durch geeignete organisatorische Maßnahmen sicherzustellen, daß die Buchungsbelege über Zahlungen von Schwarz- und Graufahrern, die nach § 147 der Abgabenordnung aus steuerrechtlichen Gründen 6 Jahre aufzubewahren sind, nicht als Ersatz-Schwarz- oder Graufahrerdatei genutzt werden.

Die Verkehrsbetriebe schlossen sich meinen Bewertungen an: sie werden in Zukunft die Schwarzfahrerdaten nur noch zwei Jahre, und wenn in diesem Zeitraum eine erneute Schwarzfahrt erfolgt, drei Jahre vorhalten. Alle – mit Ausnahme der Verkehrsbetriebe Karlsruhe, mit denen insoweit noch keine Einigung möglich war – löschen die gespeicherten Daten über Graufahrer, sobald diese den Besitz einer am Beanstandungstag gültigen, auf sie lautenden Zeitkarte nachgewiesen und gegebenenfalls das für solche Fälle vorgesehene Beförderungsentgelt bezahlt haben. Das bedeutet: in aller Regel werden diese Daten nach ca. 1 Woche gelöscht. Die Verkehrsbetriebe sicherten mir darüber hinaus auch zu, ihren gesamten Datenbestand in Abständen von maximal 3 Monaten darauf durchzusehen, welche Daten zu löschen sind. Außerdem haben sie auch umgehend die bereits vorhandenen Datenbestände überprüft und die nicht mehr benötigten Daten gelöscht.

3. Das kommunale Archiv und die zeitgeschichtliche Forschung

Zunehmend wollen interessierte Kreise die Zeit des Nationalsozialismus auch auf lokaler Ebene erforschen und aufarbeiten. So wichtig und begrüßenswert solche Aktivitäten auch sind, so stellen sie doch die kommunalen Archive oft vor schwierige Situationen. In welchem Umfang müssen sie bei der Herausgabe von Unterlagen darauf Rücksicht nehmen, daß ein Teil der darin erwähnten Personen noch lebt oder zumindest noch nahe Angehörige vorhanden sind? So lautet die Gretchenfrage, die die kommunalen Archive immer wieder beantworten müssen. Exemplarisch zeigte sich diese Problematik bei zwei Fällen, mit denen sich eine Kreisstadt auseinanderzusetzen hatte. Zum einen wollte sie meinen Rat, ob sie an „interessierte Kreise" im Jahr 1946 auf Anordnung der französischen Besatzungsmacht erstellte Listen herausgeben könne, in die alle während des Zweiten Weltkriegs dauernd oder vorübergehend in Kommandos, Lagern oder einzeln in der Stadt untergebrachten Ausländer eingetragen waren. Neben Name, Geburtstag, Anschrift des Lagers oder der Wohnung, sowie der Zeit des Aufenthalts waren aus

der Liste auch die jeweiligen Arbeitgeber zu ersehen. Zum anderen stellte sich die Frage, unter welchen Voraussetzungen die Stadt archivierte „Berichte über die Besprechungen und Entschließungen des Antifaschistischen Vertrauensrats der Stadt" einem Bürger, der sich wiederholt schon mit zeitgeschichtlichen Themen befaßt hatte, für Forschungszwecke zur Verfügung stellen darf oder muß. Der antifaschistische Vertrauensrat war unmittelbar nach Kriegsende gebildet worden und beanspruchte für sich Beratungs- und Kontrollbefugnisse gegenüber den einzelnen Behördenleitern.

In beiden Fällen hilft ein Blick in das Landesdatenschutzgesetz nicht weiter, da dieses Gesetz auf solche Unterlagen keine Anwendung findet. Auch existiert bis jetzt noch keine andere Rechtsvorschrift, die näher regelt, unter welchen Voraussetzungen das Städtische Archiv Dritten Unterlagen zur Verfügung stellen kann oder muß. Insbesondere hat die Stadt keine Satzung über die Benutzung ihres Archivs erlassen. Folglich steht es im pflichtgemäßen Ermessen der Stadt, ob sie Dritten Archivunterlagen zur Verfügung stellen will. Bei dieser Entscheidung ist sie allerdings nicht völlig frei. Sie muß insbesondere das durch Art. 2 Abs. 1 und Art. 1 GG geschützte allgemeine Persönlichkeitsrecht der Personen beachten, über die in den Unterlagen Informationen enthalten sind. Die Stadt muß also im Einzelfall das mögliche Interesse dieser Personen an einer Geheimhaltung gegen das Interesse derjenigen, die in die Unterlagen Einblick nehmen wollen, abwägen. Dabei kommt es u. a. darauf an, ob die Betroffenen noch leben, wann die Unterlagen entstanden sind, ob sich in den Unterlagen Informationen befinden, die sich auf den privaten Bereich der genannten Personen beziehen oder ob es in den Unterlagen um dienstliche und damit von vornherein stärker in die Öffentlichkeit wirkende Betätigungen von Inhabern öffentlicher Ämter geht. Schließlich ist sicherlich auch noch von Bedeutung, in welcher Weise die Unterlagen ausgewertet werden sollen, ob eine Veröffentlichung von personenbezogenen Informationen vorgesehen ist, ob auch sichergestellt ist, daß die Unterlagen tatsächlich nur für Zwecke der zeitgeschichtlichen Forschung verwendet werden.

Aufgrund einer Abwägung all dieser Interessen sieht die Landesregierung im Entwurf eines Landesarchivgesetzes (LT-Drs. 9/3345) folgende Fristen vor: Für „normale" Unterlagen soll eine Sperrfrist von 30 Jahren gelten. Für Unterlagen, die besonderen Geheimhaltungsvorschriften, z. B. dem Steuergeheimnis oder Sozialgeheimnis, unterliegen, ist eine Sperrfrist von 60 Jahren nach Entstehung der Unterlagen vorgesehen. Dagegen soll Archivgut, das sich seiner Zweckbestimmung nach auf eine natürliche Person bezieht, z. B. Personalakten, Strafakten, grundsätzlich erst 30 Jahre nach deren Tod oder, wenn dieser Zeitpunkt nicht feststellbar ist, 120 Jahre nach der Geburt genutzt werden dürfen. Unter bestimmten, im Gesetzentwurf näher festgelegten Voraussetzungen ist eine Verkürzung oder Verlängerung dieser Sperrfristen möglich:

- Danach wäre es sehr wohl zulässig, die Berichte über die Besprechungen und Entschließungen des antifaschistischen Vertrauensrats einem Forscher für ein konkretes zeitgeschichtliches Forschungsvorhaben zur Verfügung zu stellen, da die für solche Unterlagen vorgesehene Sperrfrist von 30 Jahren schon seit über 10 Jahren abgelaufen ist. Gründe, die eine Verlängerung dieser Sperrfrist notwendig machen würden, sind nicht ersichtlich. Dabei gilt es zu berücksichtigen, daß der Vertrauensrat Verwaltungstätigkeit ausgeübt hat, und Angaben über solche Aktivitäten weniger schutzwürdig sind

als Angaben, die Bürger als Privatleute für Zwecke der Verwaltung zur Verfügung stellen mußten.

- Anders liegt die Situation bei der Ausländerliste. Hier handelt es sich in der Terminologie des Gesetzentwurfs um Archivgut, das sich „nach seiner Zweckbestimmung auf eine natürliche Person bezieht" und bei dem die Sperrfrist demzufolge erst 120 Jahre nach der Geburt der jüngsten auf der Liste genannten Person endet. In solchen Fällen kommt eine frühere Nutzung nur dann in Frage, wenn die Nutzung zu wissenschaftlichen Zwecken unerläßlich ist und die schutzwürdigen Belange der Betroffenen durch Anonymisierung oder auf andere Weise angemessen berücksichtigt werden. Danach aber ist eine Herausgabe an „interessierte Kreise" für nicht näher festgelegte Zwecke nicht möglich. Vielmehr wäre nötig, zunächst exakt aufzuklären, wer die Unterlagen zu welchem konkreten Verwendungszweck in welcher Weise nutzen will.

Die Archive sind selbstverständlich nicht verpflichtet, sich an dieser Interessenabwägung des Gesetzentwurfs zu orientieren; sie können auch ganz anders entscheiden. Fälle, wie der geschilderte, sollten jedoch für den Landtag Anlaß sein, das Landesarchivgesetz so bald wie möglich zu verabschieden, damit auch in diesem Bereich mehr Rechtssicherheit einkehrt.

4. Das Finanzamt als Datenlieferant

Das Vertrauen der Bürger in das Steuergeheimnis ist groß. Das zeigen mir immer wieder Eingaben von Bürgern, die daran Anstoß nehmen, daß ihr Finanzamt ihrer Gemeinde oder ihrer Kammer Angaben über ihr Einkommen oder über ihren Umsatz mitgeteilt hat. Diesen Bürgern muß ich zunächst sagen, daß die Finanzämter nach § 31 der Abgabenordnung sehr wohl berechtigt sind, anderen Körperschaften des öffentlichen Rechts Besteuerungsgrundlagen mitzuteilen, die diese zur Festsetzung ihrer Abgaben benötigen. Das Steuergeheimnis ist insoweit durch eine ausdrückliche gesetzliche Vorschrift durchbrochen. Die Klagen der Büger sind jedoch gleichwohl nicht immer unberechtigt:

- Die Stadt Calw ließ sich vom Finanzamt das Jahreseinkommen aller abgabepflichtigen Bürger mitteilen, um ihre nach dem Einkommen gestaffelte Feuerwehrabgabe erheben zu können. Zuvor hatte sie nicht versucht, die nötigen Angaben von den abgabepflichtigen Bürgern selbst zu erhalten – ein Verfahren, das viele andere Gemeinden so oder ähnlich, sei es bei der Feuerwehrabgabe oder der Fremdenverkehrsabgabe, praktizieren. So darf es freilich nicht laufen: nach der Abgabenordnung, die auch für die Erhebung von Kommunalabgaben gilt, ist jede Gemeinde gehalten, sich zunächst an den Abgabepflichtigen zu wenden, wenn sie die Bemessungsgrundlage für eine Abgabe ermitteln will. Andere Personen und Stellen darf sie erst und nur dann um Auskunft bitten, wenn sie den Sachverhalt nicht mit Hilfe des Abgabepflichtigen aufklären kann. So bestimmt es § 93 Abs. 1 Satz 3 der Abgabenordnung ausdrücklich. Diese Regelung hätte auch die Stadt Calw beachten müssen. Denn es gab keine Anhaltspunkte, sie könne den Sachverhalt nicht mit Hilfe der Abgabepflichtigen aufklären. Die Stadt hätte deshalb nicht davon absehen dürfen, zunächst die abgabepflichtigen Bürger um die erforderlichen Auskünfte zu bitten. Allein der Umstand, daß der Weg über das Finanzamt für die Stadtverwaltung der einfachere war, berechtigte sie noch lange nicht dazu, die abgabepflichtigen Bürger zu umgehen.

- Das Finanzamt Calw, das die Bitte der Stadt um Auskunft über die Jahreseinkommen der Feuerwehrabgabepflichtigen wegen seiner angespannten Personallage in Bedrängnis brachte, verfiel auf folgenden Ausweg: Es „lieh" sich einfach von der anfragenden Stadt Calw einige Bedienstete aus, funktionierte diese für kurze Zeit zu Finanzamtsbeauftragten um und wies ihnen die Aufgabe zu, die von der Stadt gewünschten Angaben anhand ihrer Steuerakten zusammenzustellen. Auf diese Weise erhielten die städtischen Bediensteten auch Kenntnis solcher steuerlichen Verhältnisse der Abgabepflichtigen, die die Stadt für die Veranlagung zur Feuerwehrabgabe nicht zu kennen brauchte. Darin liegt ein Verstoß gegen das Steuergeheimnis, den ich nach § 18 LDSG beanstandete. Obwohl das Finanzministerium schon im Jahr 1984 die Finanzämter angewiesen hatte, den Gemeinden keine Akteneinsicht zu gewähren, wollte es in dem Verfahren des Finanzamts Calw keinen Rechtsverstoß sehen. Es zog sich auf das formale Argument zurück, das Finanzamt habe ja nicht der Stadt Akteneinsicht gewährt, sondern seine eigenen Aufgaben durch Personen erledigen lassen, die keine Amtsträger der Steuerverwaltung waren. Die Finanzämter würden ja auch Studenten oder Praktikanten beschäftigen. Immerhin sah das Finanzministerium, daß die Bürger für ein solch trickreiches Ausleihverfahren kein Verständnis haben dürften. Ob deshalb oder aus anderen Gründen: das Finanzministerium wies immerhin die Finanzämter an, künftig keine Bediensteten von Gemeinden mehr einzusetzen, wenn es darum geht, eben diesen Gemeinden Auskünfte für die Erhebung der Feuerwehrabgabe zu erteilen.
- Richtig machen wollte es die Landesapothekerkammer, als sie für die Festsetzung der Mitgliedsbeiträge die dazu notwendige Bemessungsgrundlage, nämlich den Jahresumsatz, ermittelte. Sie forderte zunächst die Beitragspflichtigen auf, die erforderlichen Angaben zu machen. Blieb diese Aufforderung erfolglos, bat die Kammer das jeweilige Finanzamt, ihr den Jahresumsatz mitzuteilen. Einige der angegangenen Finanzämter gaben der Kammer die erbetene Auskunft anstandslos, andere dagegen lehnten ab. Was die Kammer nicht bedacht hatte: Auf ihr Beitragsverfahren findet nicht die Abgabenordnung, sondern eine spezielle Vorschrift im Kammergesetz Anwendung. Danach hat die Kammer den Jahresumsatz zu schätzen, wenn eines ihrer Mitglieder keine Angaben zum Jahresumsatz macht oder Gründe für die Annahme vorliegen, daß die Angaben falsch sind. Nicht erlaubt das Kammergesetz einer Kammer, Auskünfte bei Dritten, z. B. beim Finanzamt, einzuholen.

5. Forschungsvorhaben „Gemeinderäte"

Die Forschung nimmt sich auch des Gemeinderats an: Das Freiburger Institut für Kommunalpolitik Baden-Württemberg e.V. führt eine Untersuchung über Gemeinderäte in Baden-Württemberg durch, die Aufschlüsse über Zusammensetzung, Struktur und Funktionsweise kommunaler Parlamente geben soll. Dazu versandte es im Sommer 1986 an ca. 2800 Gemeinderäte im Land einen Fragebogen, der insgesamt 63 Fragen zu den sozialen und beruflichen Verhältnissen und zur kommunalpolitischen Betätigung der einzelnen Mandatsträger enthielt.

Das Institut informierte mich ausführlich über sein Vorhaben. Es hob dabei – wie auch schon zuvor gegenüber den Gemeinderäten und dem Innenministerium – besonders hervor, die Erhebung erfolge anonym, da die Fragebogen ohne Namensnen-

nung auszufüllen seien. Freilich ist das Gegenteil der Fall: Anhand der Ordnungsnummer jedes Fragebogens läßt sich mühelos die Gemeinde des befragten Gemeinderats feststellen. Schon dessen Angaben über Alter, Geschlecht, Beruf und Listenzugehörigkeit lassen mit Sicherheit in vielen Fällen eine Identifizierung zu; denn diese Angaben sind auch in den noch zugänglichen öffentlichen Bekanntmachungen der Wahlvorschläge vor der letzten Gemeinderatswahl enthalten. Darüber hinaus sieht der Fragebogen zahlreiche weitere Angaben vor, die zur Identifizierung des Befragten beitragen können: So wird z. B. nach der Dauer der Mitgliedschaft im Gemeinderat, nach Parteiämtern, nach Mitgliedschaft und Funktionen in Vereinen und Verbänden gefragt, ebenso nach zusätzlichen Ämtern und Funktionen in der Gemeindeverwaltung, z. B. als Stellvertreter des Bürgermeisters oder Ortsvorsteher, und nach zusätzlichen Mandaten im Kreistag, im Landtag oder im Bundestag. Angeben sollen die Gemeinderäte ferner weitere persönliche Umstände wie etwa Familienstand, Zahl der Kinder und Dauer der Ansässigkeit in der Gemeinde. Wer alles dies weiß, kann in der Regel feststellen, um welchen Gemeinderat es sich im Einzelfall handelt. Denn das erforderliche Zusatzwissen, das zusammen mit diesen Angaben eine Identifizierung ermöglicht, ist gerade bei Gemeinderäten häufig allgemein zugänglich, da sich ihr Wirken zu einem großen Teil in der Öffentlichkeit abspielt und auf Öffentlichkeitswirkung angelegt ist. Als Informationsquellen kommen außer den Bekanntmachungen der Wahlvorschläge vor allem Zeitungen, Einwohnerbücher, Telefonbücher und Branchenverzeichnisse in Betracht. Mit einem Wort: in nicht wenigen Fällen läßt sich trotz des Verzichts auf die Nennung des Namens ohne Schwierigkeit ermitteln, welcher Gemeinderat den Fragebogen ausgefüllt hat. Die Befragung ist also nicht anonym. Das Institut mußte deshalb besondere Vorkehrungen zum Schutz dieser Daten treffen. Da es als eingetragener Verein nicht meiner Kontrolle, sondern der Aufsicht des Innenministeriums unterliegt, verwies ich es wegen dieser Einzelheiten dorthin. Meine Kontrollbefugnis berührt das Forschungsvorhaben aus anderem Grund: Das Institut will die ausgefüllten Fragebogen in einem Universitätsrechenzentrum, also bei einer öffentlichen Stelle, auswerten lassen. Ich muß deshalb darauf achten, daß das Rechenzentrum bei der Verarbeitung der Forschungsdaten den Anforderungen des § 8 LDSG entspricht. Das Institut hat es bei seinem Forschungsvorhaben folglich mit zwei Kontrollinstanzen zu tun. Es läuft damit Gefahr, sich mit zwei Instanzen auseinandersetzen zu müssen und hat dabei nicht einmal die Gewähr, daß beide den gleichen Maßstab anlegen: Ein Zustand, der einmal mehr zeigt, wie unbefriedigend die Aufsplitterung der Datenschutzkontrolle in Baden-Württemberg ist.

9. Teil: Sorgen der Bürger

Wie jedes Jahr wandten sich auch 1986 viele Bürger des Landes mit der Bitte um Abhilfe an mich. Wer ihre Briefe liest, sich am Telefon ihre Sorgen anhört oder persönlich mit ihnen spricht, ist immer wieder aufs neue erstaunt, wo überall der Datenschutz zum Tragen kommt und mit welchem Gespür sich die Bürger oftmals damit auseinandersetzen. Mir liegt fern, hier und jetzt die ganze Palette der Bürgersorgen auszubreiten. Doch sollen einige exemplarische Fälle aufzeigen, wo den Bürger der Schuh drückt:

- Personenkennzeichen auf Lohnsteuerkarten?

  Selbst die Lohnsteuerkarten, die uns das Bürgermeisteramt vor Jahresbeginn zusendet, beinhalten Datenschutzprobleme. Das konnte ich mir zunächst nicht so recht vorstellen; doch ein aufmerksamer Bürger belehrte mich eines anderen. Die Gemeinden drucken anstelle des Geburtsdatums auf jeder Lohnsteuerkarte das melderechtliche Ordnungsmerkmal des Einwohners aus, das aus dem Geburtsdatum des Einwohners und vier oder sechs weiteren Ziffern besteht. Das ist nicht rechtens: weder sehen die steuerrechtlichen Bestimmungen den Eintrag des Ordnungsmerkmals auf der Lohnsteuerkarte vor noch läßt das Meldegesetz einen Ausdruck auf ihr zu. Es verbietet dem Einwohnermeldeamt vielmehr ausdrücklich, das Ordnungsmerkmal an Private weiterzugeben; öffentliche Stellen dürfen es nur erhalten, soweit sie es zur Erfüllung ihrer Aufgaben benötigen. Ferner untersagt das Meldegesetz jedermann, beim Bürger sein Ordnungsmerkmal zu erfragen. Diese Regelung unterlaufen die Gemeinden mit dem Ausdruck des Ordnungsmerkmals auf der Lohnsteuerkarte: denn Arbeitnehmer sind verpflichtet, die Lohnsteuerkarte ihrem Arbeitgeber vorzulegen; für die Mehrzahl der Arbeitnehmer gilt gegenüber dem Finanzamt zumindest faktisch das Gleiche. Diese Bewertung teilte ich dem Finanzministerium mit, dessen Weisungen die Gemeinden bei der Ausstellung der Lohnsteuerkarten unterstehen, und bat, der Ausdruck des Ordnungsmerkmals auf den Lohnsteuerkarten künftig zu unterbinden. Das Finanzministerium antwortete mir nur lapidar, dazu sei es nicht bereit. Es berief sich dabei wieder einmal auf Absprachen der obersten Finanzbehörden des Bundes und der Länder aus dem Jahre 1980, die damals in dem Ausdruck des Ordnungsmerkmals keine Probleme gesehen hatten. Auch wies es darauf hin, es könne keine schutzwürdigen Interessen des Bürgers an der Geheimhaltung des Ordnungsmerkmals sehen. Mit dieser Argumentation verkennt das Ministerium, daß der Gesetzgeber und nicht die Verwaltung über die Geheimhaltungsbedürftigkeit einer Angabe zu entscheiden hat, und daß er sich 1983 im Meldegesetz für die Geheimhaltungsbedürftigkeit des Ordnungsmerkmals entschied. Er wollte auf diese Weise nämlich verhindern, daß sich das Ordnungsmerkmal zu einem allgemeinen, auch von anderen Behörden benutzten Personenkennzeichen entwickelt. Diese Entscheidung hat auch das Finanzministerium zu respektieren. Ich hoffe deshalb, daß es bereit ist, seine Auffassung zu überdenken.

- Wahlwerbung mit EDV

  Die Adressen von Jungwählern oder Seniorenwählern sind in Wahlkampfzeiten begehrt. Nach dem Meldegesetz dürfen die Einwohnermeldeämter den Parteien für Zwecke der Wahlwerbung 6 Monate vor einer Wahl die Namen und Anschriften von wahlberechtigten Einwohnern bestimmter Altersgruppen mitteilen. Sie tun dies im allgemeinen in der Form von ausgedruckten Listen oder auch Adreßaufklebern. Der technische Fortschritt macht aber auch hier nicht Halt: eine Partei bat eine Gemeinde, ihr für die bevorstehende Bundestagswahl die Adressen von Erstwählern auf einem Magnetband, also in maschinell lesbarer Form, zu überlassen. Das Meldegesetz verbietet eine Adressenübermittlung in dieser Form nicht. Eine Gemeinde ist jedoch andererseits auch nicht verpflichtet, die erbetene Auskunft gerade in dieser Form zu erteilen; es liegt vielmehr grundsätzlich in ihrem pflichtgemäßen Ermessen, in welcher Form sie die Adressen herausgibt. Sie muß dabei die besonderen Risiken in Rechnung stellen, die mit einer Herausgabe maschinell lesbarer Datenträger verbunden sind, und deshalb besonders prüfen, ob und wie sie diese Risiken ausschalten kann. Einer Gemeinde, die mich um Rat fragte, nannte ich eine Reihe möglicher Auflagen, durch

die sie die Risiken eines Mißbrauchs mindern kann. Auf jeden Fall sollte die Gemeinde von der Partei verlangen, daß sie die Daten unter sicherem Verschluß hält, Dritten nicht zugänglich macht, von eigenen Datenbeständen getrennt hält, nach Gebrauch unverzüglich löscht oder an die Gemeinde zurückgibt und keine Kopien anfertigt. Die Gemeinde sollte die Partei ferner darauf hinweisen, daß die Daten nur für Zwecke der Werbung in Zusammenhang mit einer bestimmten Wahl übermittelt werden und deshalb nicht für andere Zwecke verwertet werden dürfen. Gemeinde und Partei müssen ferner bedenken, daß die auf maschinell lesbaren Datenträgern gespeicherten Daten der Wahlberechtigten eine Datei im Sinne des Datenschutzrechts darstellen mit der Folge, daß die Partei „speichernde" Stelle wird und folglich Verpflichtungen aus dem Bundesdatenschutzgesetz Rechnung tragen muß.

- Bürgerbegehren und Wahlgeheimnis

  Oftmals gehen die kommunalpolitischen Wogen wegen eines Bürgerbegehrens gegen ein von der Stadtverwaltung beschlossenes Vorhaben hoch. Als es in Rastatt zu einem Bürgerbegehren wegen des umstrittenen Baus einer Stadthalle kam, gab es freilich noch aus anderen Gründen Wirbel. Der Oberbürgermeister hatte die Unterschriftslisten für das Bürgerbegehren dazu genutzt, die Unterzeichner des Begehrens persönlich anzuschreiben und sie unter Hinweis auf ihre Unterstützung des Bürgerbegehrens zu einer Bürgerversammlung einzuladen. Zahlreiche Bürger und die Presse wollten daraufhin von mir wissen, ob die Stadt den Datenschutz beachtet hat. Ich mußte ihnen sagen, daß der Oberbürgermeister so nicht hätte verfahren dürfen. Solche Unterschriftslisten unterliegen auch dem Wahlgeheimnis; nach der Kommunalwahlordnung dürfen sie nur zur Feststellung der Zulässigkeit des Bürgerbegehrens, zur Durchführung eines Rechtsmittelverfahrens oder zur Aufklärung des Verdachts einer Wahlstraftat genutzt werden; darum aber ging es hier nicht. Befremdlich war die Reaktion des Oberbürgermeisters: er wollte seinen Fehler lange nicht eingestehen und attackierte mich deshalb heftig. Schließlich wollte er mir sogar das Recht absprechen, meine Auffassung kundzutun, wenn mich Bürger oder Presse danach fragen. Er gab erst Ruhe, als das Innenministerium, die oberste Rechtsaufsichtsbehörde, gesprochen hatte und in der Sache zum gleichen Ergebnis gekommen war wie ich.

- Publizität am falschen Platz

  Die Einwohnermeldeämter dürfen bestimmte Daten ihrer Einwohner auch ohne deren Einwilligung in Einwohnerbüchern veröffentlichen. So sieht es das Meldegesetz vor. Bekanntgeben dürfen sie auch die Daten von Alters- und Ehejubilaren. Die Veröffentlichungen müssen jedoch unterbleiben, soweit die Einwohner oder Jubilare widersprechen. Auf dieses Widerspruchsrecht müssen die Einwohnermeldeämter die Bürger nicht nur beim Zuzug, sondern regelmäßig jedes Jahr durch öffentliche Bekanntmachung hinweisen. Obwohl die Regelung schon seit 1980 gilt, zeigen mir Anfragen und Hinweise von Bürgern immer wieder, daß die Einwohnermeldeämter damit auch heute noch ihre Probleme haben:

  - So veröffentlichte eine Stadt in Zusammenarbeit mit einem Verlag ein Einwohnerbuch, in dem alle volljährigen Einwohner aufgeführt waren, ohne daß die Stadt sie zuvor öffentlich auf ihr Widerspruchsrecht hingewiesen hatte. Diese gesetzliche Pflicht übersah die Meldebehörde schlichtweg.
  - Eine große Kreisstadt veröffentlichte jahrelang die Namen und Anschriften der Altersjubilare in der örtlichen Presse, ohne zuvor die Jubilare auf ihr Widerspruchsrecht öffentlich hin-

gewiesen zu haben. Nur wer direkt bei der Stadt deshalb nachfragte, wurde belehrt. Erstmals im August 1986 erfolgte ein öffentlicher Hinweis; zu danken ist dies einer couragierten Bürgerin, die ich über die Rechtslage informiert hatte und die dann bei der Stadt darauf bestand, man möge ihr eine öffentliche Bekanntmachung vorlegen. Allerdings war diese Bekanntmachung vom August 1986 fehlerhaft und informierte die Bürger nur unzureichend über ihre Rechte.

- Eine andere Stadt veröffentlichte auch den Geburtsnamen von Altersjubilaren, obwohl das Meldegesetz entgegen einer früher weit verbreiteten Praxis nur noch die Veröffentlichung aktueller Familien- und Vornamen zuläßt.

Dies ist nur eine kleine Auswahl aus den Anfragen bei meinem Amt. Sie zeigen zweierlei: Zum einen werden sich immer mehr Bürger ihrer Rechte bewußt und machen davon auch Gebrauch. Zum andern aber sind nicht wenige Einwohnermeldeämter nach über sechs Jahren seit Inkrafttreten dieser Regelung immer noch nicht in der Lage, die Bestimmungen über die Veröffentlichung von Einwohnerdaten zu beachten – ein Phänomen, das zu denken gibt.

- Rentnerausweis

  Wer soziale Leistungen in Anspruch nehmen will, muß in aller Regel nachweisen, daß er zu dem begünstigten Personenkreis gehört. Oft genug muß er dabei aber bloß deshalb mehr als notwendig über sich offenbaren, weil die Nachweise noch weitere Informationen über ihn enthalten. So ärgerte sich ein Rentner, daß er bei einer Schloßbesichtigung dem kontrollierenden Pförtner seinen Rentenausweis vorlegen mußte, aus dem auch die Höhe seiner monatlichen Rente zu ersehen war. Er meinte zu Recht, daß es doch möglich sein müsse, den Rentnern für solche Fälle „neutrale" Rentnerausweise zur Verfügung zu stellen. Ich konnte dem Bürger mitteilen, daß die Rentenversicherungsträger dies schon seit einiger Zeit tun. Sie und auch die Bürgermeisterämter stellen auf Antrag solche neutralen Ausweise aus.

- Der neugierige Sportlehrer

  Große Verwunderung löste der Fragebogen eines Sportlehrers bei Eltern von Fünftkläßlern eines Gymnasiums aus. Den Pädagogen interessierte nicht nur Name, Klasse, Schule, Geburtsdatum und Adreßdaten der Schüler, sondern u. a. auch der Geburtsort, ihre Religionszugehörigkeit, Zahl, Alter, der Beruf bzw. Schulklasse ihrer Geschwister. Außerdem wollte er wissen, welche Musikinstrumente die Schüler spielen, welche Hobbys sie haben und welchen Beruf die Eltern ausüben. Zu Recht waren die Eltern der Meinung, daß der Sportlehrer mit diesen Fragen weit mehr wissen wollte als er zur Wahrnehmung seiner Aufgaben benötigt. Bei aller Anerkennung der pädagogischen Verantwortung, die ein Lehrer für seine Schüler hat, sehe ich keinen vernünftigen Grund, weshalb ein Sportlehrer etwa den Geburtsort, die Religionszugehörigkeit, die musikalische Betätigung, die Hobbys der Schüler und vor allem die Angaben über ihre Geschwister und den Beruf der Eltern wissen muß. Für ein solches Verlangen gibt es keine Rechtsgrundlage. Ich teilte deshalb den Eltern mit, daß sie solche Fragen nicht beantworten müssen.

- Der Kampf um die Schüleradressen

  Besonderen Einfallsreichtum legen Banken und Sparkassen an den Tag, wenn sie die Namen und Anschriften von Schülern erfahren wollen. Nachdem das Kultusministerium die von mir schon 1982 kritisierte Praxis der Schulen unterbunden hat, den Banken und Sparkassen Schüleradressen Zug um Zug gegen Spenden für Schullandheimaufenthalte zu liefern, wenden sich

nunmehr einzelne Kreditinstitute direkt an die Klassensprecher. Diese sollen Namen und Anschriften der Mitschülerinnen und Mitschüler liefern; ihre Bemühungen werden mit einem bereitgelegten Geschenk honoriert – so heißt es jedenfalls in einem Schreiben einer Bank an den Klassensprecher einer 9. Hauptschulklasse. Mit einem solchen Verfahren unterlaufen die Kreditinstitute praktisch die Bestimmung des § 11 LDSG; diese erlaubt nämlich eine Weitergabe gespeicherter Schüleradressen durch die Schulen an Kreditinstitute für Werbezwecke nicht. Zu Recht versagte deshalb der Rektor der Hauptschule dieser nicht nur aus der Sicht des Datenschutzes fragwürdigen Aktion seine Mitwirkung. Er will zudem seine Bedenken gegen diese Praxis anderen Schulleitern und Lehrern, Eltern und Schülern mitteilen und vor allem im Gespräch mit den Kreditinstituten versuchen, diese von solchen Praktiken abzubringen. In der Tat: ein engagiertes Eintreten für den Datenschutz, das Schule machen sollte.

- Vom Auto, das es nicht gibt, aber falsch parkt

  Wie man einen Strafzettel wegen Falschparkens für ein überhaupt nicht existierendes Auto bekommen kann, berichtete mir eine darob verblüffte Bürgerin. Ein Gemeindevollzugsbeamter einer Stadt entdeckte ein falsch parkendes Auto und schrieb dessen Kennzeichen auf. Dabei unterlief ihm allerdings ein Fehler: er notierte nämlich ein Kennzeichen, das bislang überhaupt noch nicht vergeben war. Um das fällige Verwarnungsgeld geltend zu machen, fragte die Bußgeldstelle fernmündlich beim Landratsamt, bei dem das falsch geparkte Auto gemeldet sein sollte, nach dessen Halter. Dort passierte nun ebenfalls ein Fehler. Bei der Eingabe des Kennzeichens in den Computer vertippte sich der Bedienstete: statt XX - X 980 gab er XX - X 870 ein. Das aber war das Kennzeichen des Autos unserer verblüfften Bürgerin. Den Irrtum bemerkten weder das Landratsamt noch die Stadt, obgleich das falsch geparkte Auto ein Volkswagen, das Auto unserer Bürgerin eine andere Marke war. So kam es denn, daß sie ein Verwarnungsgeld für ein nicht existierendes Fahrzeug zahlen sollte. Hier zeigte sich einmal mehr, daß telefonische Auskünfte ein erhöhtes Fehlerrisiko mit sich bringen, und daß deshalb dabei besondere Vorsicht am Platze ist.

- Dienst ist Dienst

  Informationen, die ein Mitarbeiter einer Behörde während seiner Arbeit erfährt, darf er nur für seine Arbeit und nicht für private Zwecke nutzen. Leider beachten gelegentlich Bedienstete diesen selbstverständlichen Grundsatz nicht. So fragte der Lohnbuchhalter einer Universität eines Tages einen Kollegen, weshalb er eigentlich die vermögenswirksamen Leistungen des Arbeitgebers nicht voll in Anspruch nehme. Er empfahl ihm, deshalb einen Bausparvertrag abzuschließen – und zwar der einfachheithalber gleich bei ihm. Denn unser Lohnbuchhalter war nicht nur Lohnbuchhalter, sondern nebenbei auch Vertreter einer Bausparkasse. Dieser Vorfall hatte für den Lohnbuchhalter Konsequenzen: die Universität versetzte ihn auf einen anderen Arbeitsplatz, an dem er keinen Zugriff mehr auf Daten seiner Kollegen hat. Völlig zu Recht; denn es ist keine Frage: ein Mitarbeiter im öffentlichen Dienst, der das ihm beruflich anvertraute Wissen über seine Kollegen für eigene Zwecke verwendet, verstößt damit gegen die Regeln des Datenschutzes.

Ausblick

Datenschutz ja, aber ... ist heutzutage oft zu hören. Der Politiker sagt es in seinen Reden ebenso wie der Beamte, der für seine Entscheidungen Informationen benötigt, oder der Bürger, der sich für die Vermögensverhältnisse seines Schuldners interessiert. Hinter dieser Ausdrucksweise steckt die Vorstellung, der Datenschutz wolle im Grunde jede Informationsweitergabe verhindern. Ein solch „absoluter" Datenschutz ist in Wirklichkeit ein Phantom, gegen das sich zwar trefflich polemisieren läßt, das jedoch mit dem eigentlichen Anliegen des Datenschutzes nichts gemein hat. Man könnte folglich rasch zur Tagesordnung übergehen, würde diese irrige Vorstellung nicht in so vielen Köpfen stecken und deren Einstellung zum Datenschutz negativ prägen. Deshalb sei auch hier und jetzt gesagt: Beim Datenschutz geht es nicht darum, das Sammeln und Weitergeben von Informationen von vornherein zu verhindern. Sein primäres Zeil ist sicherzustellen, daß jeder von uns selbst darüber bestimmen kann, was andere über ihn wissen sollen und wozu sie dieses Wissen benutzen dürfen. Die Sicherung des Selbstbestimmungsrechts ist also das Entscheidende. Selbstverständlich unterliegt dieses Selbstbestimmungsrecht auch Beschränkungen, weil wir in der Gesellschaft leben, auf sie angewiesen sind und umgekehrt ihr gegenüber Pflichten haben. Nur: nach unserer Verfassung muß der Gesetzgeber und niemand anderes über diese Einschränkungen entscheiden. Er kann diese Aufgabe auch nicht durch vage Generalklauseln auf Regierung oder Verwaltung delegieren, sondern muß sich selbst klar werden, ob ein überwiegendes Allgemeininteresse den Eingriff in das Selbstbestimmungsrecht tatsächlich gebietet. Sich dabei auf das Unumgängliche zu beschränken, fällt im Zeitalter der Informationsgesellschaft besonders schwer. Denn ihre überall eingesetzten Techniken sind darauf angelegt, möglichst viele Informationen möglichst schnell zu erfassen, auszuwerten und anderen zur Verfügung zu stellen. Wer gleichwohl das Selbstbestimmungsrecht sichern will, muß deshalb gerade hier Schranken aufbauen und den freien Informationsfluß unterbrechen. Daß diese verfassungsrechtliche Notwendigkeit so viele Emotionen wie hier im Lande wekken kann, erstaunt mich immer wieder. Eigentlich sollte es doch möglich sein, darüber sachlich zu diskutieren. Darum jedenfalls haben sich meine Mitarbeiter, denen ich wiederum für ihren Einsatz sehr herzlich danke, und ich auch 1986 bemüht.