LANDTAG DES SAARLANDES
10. Wahlperiode

Drucksache 10/1403

VIERZEHNTER BERICHT

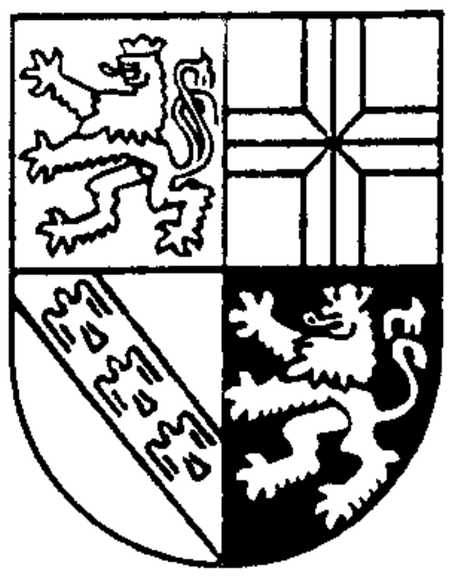
über die

Tätigkeit des Landesbeauftragten für Datenschutz gemäß § 20 Abs. 3 des Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung
(Berichtszeitraum: 1. Januar 1992 bis 31. Dezember 1992)

Ausgegeben: 03.05.93

SAARLAND

DER LANDESBEAUFTRAGTE FÜR DATENSCHUTZ



14. Tätigkeitsbericht

1992

I N H A L T S V E R Z E I C H N I S

		Seite
	Vorbemerkung	1
1.	Verfassungsschutz	4
2.	Polizei	12
2.1	Fotoausstellung zu präventiven Zwecken	12
2.2	Landeskriminalblatt	14
2.3	Notruffälle	15
2.4	Rückmeldeverfahren der Staatsanwaltschaft	16
2.5	Erkennungsdienstliche Behandlung von Asylbewerbern	19
2.6	Polizeiliches Informationssystem DIPOL	21
3.	Justiz	30
3.1	"Lauschangriff"	30
3.2	Gnadengesetz	30
3.3	Aufbewahrungsbestimmungen	33
3.4	Zahlungsabwicklung bei Auflagen zugunsten gemeinnütziger Organisationen	34
4.	Planung und Umwelt	37
4.1	Freier Zugang zu den Informationen über die Umwelt	37
4.1.1	EG-Richtlinie (90/313 EWG)	37
4.1.2	Umsetzung der EG-Richtlinie (90/313 EWG) in nationales Recht	38
4.2	Landesplanungsgesetz	43
4.3	Altstandortekataster	46
4.4	Umweltdatenerhebung durch Befragung	48

5.	Steuern und Finanzen	51
5.1	Finanzämter	51
5.1.1	Organisation und konventionelle Informationsverarbeitung	52
5.1.2	Automation und PC-Einsatz	55
5.2	Kontrollmitteilungen öffentlicher Stellen an die Steuerbehörde über gezahlte Honorare	55
6.	Gesundheit	57
6.1	Krankenpapiere auf der Straße	57
6.2	Private Schreibbüros	58
6.3	Neonatalerhebung (Bilanz)	60
6.4	Unterbringungsgesetz	61
7.	Soziales	63
7.1	Krankenversicherungskarte (Chipkarte)	63
7.2	Gesundheits-Strukturgesetz	64
7.3	SGB-Änderungsgesetz	65
7.4	Erfassung von Abrechnungsdaten der Kassenärztlichen Vereinigung (KV) durch private Stellen	68
7.5	Datenanforderungen des Versorgungsamtes	69
8.	Arbeitnehmer	74
8.1	Private Arbeitsverhältnisse	74
8.2	Öffentlicher Dienst	74
8.2.1	Entfernung von Disziplinarvorgängen aus der Personalakte	74
8.2.2	Personenbezogene Fremddaten in der Personalakte	75
8.2.3	Umsetzung der Vorschriften des Beamtenrechtsrahmengesetzes (BRRG) in Landesrecht	76
8.3	Zentrale Besoldungs- und Versorgungsstelle (ZBS)	78
8.3.1	Berechnung und Festsetzung der Bezüge	78

8.3.2	Zentrale Beihilfefestsetzungsstelle	82
8.3.3	Förmlichkeiten des Beihilfeantrags: Vorlage von Fotokopien	86
9.	Archivwesen (Bilanz)	88
10.	Epidemiologisches Krebsregister	91
10.1	Allgemeines	91
10.2	Andere gesetzlich geregelten Modelle	92
10.3	Verhältnismäßigkeit der Register-speicherung	93
10.4	Saarländisches Krebsregister (Prüfergebnisse)	94
10.4.1	Datenumfang der Registermeldungen	94
10.4.2	Sterbefallzählkarten	94
10.4.3	Dateitrennung und Anonymisierung	95
10.5	Datenanforderungen der Wissenschaft	98
11.	Automation, Neue Medien, Überwachungs-techniken	101
11.1	Fangschaltungsbeschluß des Bundes-verfassungsgerichts	101
11.2	Gefährdung des Fernmeldegeheimnisses durch unbefugtes Mithören der Funk-kommunikation	103
11.3	Telekommunikation	105
11.3.1	Interne Telekommunikationsanlagen (TK-Anlagen)	105
11.3.2	Internationaler Datenschutz	108
11.3.3	Das integrierte Verwaltungs- und Kontrollsystem der EG (InVeKos) - Kommt der gläserne Landwirt?	108
11.4	Bürokommunikation	110
11.5	Telefax	111
11.6	Auftragsdatenverarbeitung	112
12.	Die Situation der Dienststelle	116

A N L A G E N V E R Z E I C H N I S

Anlage 1: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Grundrecht auf Datenschutz vom 28. April 1992 Seite 121

Anlage 2: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuregelung des Asylverfahrens (BT-Drs. 12/2062) vom 28. April 1992 Seite 123

Anlage 3: Entschließung der Konferenz der Datenschutzbeauftragten vom 1./2. Okt. 1992 zum "Lauschangriff" Seite 126

Anlage 4: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar 1993 zur Richtlinie des Rates vom 07. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG) Seite 128

Anlage 5: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Okt. 1992 zur Chip-Karte als elektronische Krankenversicherungskarte Seite 130

Anlage 6: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung Gesundheits-Strukturgesetz 1993 (ER-Drs. 560/92) Seite 131

Anlage 7: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. März 1992 zum Arbeitnehmerdatenschutz Seite 133

Anlage 8: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen Seite 137

Anlage 9: Bericht der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und
Gemeinsame Erklärung der 14. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 29. Oktober 1992 Seite 140

Anlage 10: Dienstanweisung Nr. .. für die Übermittlung von Daten mit Hilfe von Telefax-Geräten Seite 155

A B K Ü R Z U N G S V E R Z E I C H N I S

ABl	Amtsblatt des Saarlandes
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BR-Drs.	Bundesrats-Drucksache
BRRG	Bundesrechtsrahmengesetz
Bt-Drs.	Bundestagsdrucksache
BVerfGE	Bundesverfassungsgerichtsentscheid
CR	Computer und Recht
DIPOL	DV-Infrastruktur für die Polizei
DV	Datenverarbeitung
EG	Europäische Gemeinschaft
EuGHE	Europäischer Gerichtshofsentscheid
EWG	Europäische Wirtschafts Gemeinschaft
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
G-10	Gesetz zur Beschränkung der Brief-, Post- und Fernmeldegeheimnisse
INPOL	Informationssystem der Polizei
ISDN	Integrates Services Digital Network
KABV	Kommunaler Abfallentsorgungsverband
KV	Kassenärztliche Vereinigung
LKA	Landeskriminalamt
Lt-Drucksache	Landtagsdrucksache
MfBS	Ministerium für Bildung und Sport
MdF	Ministerium der Finanzen
NJW	Neue Juristische Wochenschrift
OFD	Oberfinanzdirektion
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und der organisierten Kriminalität
PC	Personalcomputer
RSt	Ressortstellungnahme

SArchG	Saarländisches Archivgesetz
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SKHG	Saarländisches Krankenhausgesetz
SKRG	Saarländisches Krebsregistergesetz
SPolG	Saarländisches Polizeigesetz
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
TB	Tätigkeitsbericht
TK-Anlage	Telekommunikations-Anlage
Tz.	Teilziffer
UIG	Umweltinformationsgesetz
VVD StRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
ZBS	Zentrale Besoldungs- und Versorgungsstelle

S. 10

Vorbemerkung

Von grundlegender Bedeutung war im Berichtszeitraum die Verfassungsdiskussion über ein eigenständiges Grundrecht auf Datenschutz und auf Informationsfreiheit. Der gemeinsamen Verfassungskommission von Bundestag und Bundesrat, die seit dem 16. Januar 1992 aufgrund einer Empfehlung im Einigungsvertrag mit der Erarbeitung von Vorschlägen über Änderungen des Grundgesetzes beschäftigt war, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit der Entschließung vom 28. April 1992 eine Empfehlung - bei Gegenstimme von Bayern - unterbreitet (Anlage 1). Sachsen war in dieser Konferenz nicht vertreten.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 steht zweifelsfrei fest, daß das Grundrecht auf Datenschutz (Recht auf informationelle Selbstbestimmung) sich aus der in Artikel 1 des Grundgesetzes garantierten Menschenwürde und dem Grundrecht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) herleitet. Die aktuelle Verfassungsdiskussion war Anlaß für die Konferenz, sich eingehend mit der Frage auseinanderzusetzen, ob und auf welche Weise es sich empfiehlt, das Grundrecht auf Datenschutz ausdrücklich in der Verfassung zu verankern.

Für eine eigenständige Formulierung des Grundrechts auf Datenschutz spricht, daß damit für die Bürger deutlicher erkennbar wird, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte (z.B. Meinungs- und Versammlungsfreiheit). Dabei muß sichergestellt werden, daß der Datenschutzstandard, wie er durch die Rechtsprechung des Bundesverfassungsgerichts entwickelt wurde, bestätigt wird.

Daneben sollte die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung abgesichert werden.

Nach Auffassung der Konferenz sollten darüber hinaus mit einbezogen werden

- die Stärkung der Grundrechte aus Artikel 10 und 13 im Hinblick auf neue Überwachungstechniken,

- Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit),

- Instrumente zur Technikfolgenabschätzung.

Leider hat sich in der gemeinsamen Verfassungskommission von Bundestag und Bundesrat nicht die erforderliche Mehrheit für die ausdrückliche Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz gefunden.

Das Landesdatenschutzgesetz stand vor Redaktionsschluß gemeinsam mit dem Saarländischen Verfassungsschutzgesetz unmittelbar vor seiner Verabschiedung durch das Parlament. Die Bedeutung dieses Vorgangs für die Entwicklung des Datenschutzes im Saarland kann nicht hoch genug eingeschätzt werden. Seit Inkrafttreten des zur Novellierung anstehenden Saarländischen Datenschutzgesetz vom 17. Mai 1978 war - im Gegensatz zu allen anderen Bundesländern - der Verfassungsschutz der Kontrollkompetenz des Landesbeauftragten für Datenschutz entzogen. Bereits im Volkszählungsurteil vom 15. Dezember 1983 hat das Bundesverfassungsgericht festgestellt, daß " ... auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ... die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven

Schutz des Rechts auf informationelle Selbstbestimmung ..." ist (BVerfGE 65, 1, 46). Die einmalige, mit der Verfassung nicht vereinbare Sonderstellung des Verfassungsschutzes wird durch das neue Landesdatenschutzgesetz beseitigt.

Nach der Novellierung des Unterbringungsgesetzes sehe ich immer noch Regelungsbedarf für die vorsorgenden, begleitenden und nachsorgenden Hilfen für psychisch Kranke, die die Unterbringung vermeiden oder verkürzen helfen (vgl. Tz. 6.4).

Novelliert werden muß das Gesetz über das (epidemiologische) Krebsregister, um einen "schonenden Ausgleich" zwischen dem Persönlichkeitsrecht des Betroffenen Krebskranken und den im allgemeinen Interessen liegenden Informationsbedürfnissen von Statistik und Wissenschaft zu gewährleisten (vgl. Tz. 10).

Ferner ist ein Bodenschutzgesetz nicht zuletzt zur Regelung der Probleme im Zusammenhang mit den Altstandorten notwendig. Einen immer breiteren Raum nehmen die datenschutzrechtlichen Überlegungen auf dem Gebiet des Umweltschutzes und der Planung ein. Der freie Zugang zu den Informationen über die Umwelt, der durch eine EG-Richtlinie auch für den Bürger auf nationaler Ebene Wirklichkeit wurde, wirft Probleme im Hinblick auf Rechte Dritter auf, die der Gesetzgeber einer verfassungskonformen Lösung zuführen muß (vgl. Tz. 4) .

Auf Bundesebene muß der Arbeitnehmerdatenschutz in privaten Arbeitsrechtsverhältnissen geregelt werden. Hingegen hat die Personalaktenverwaltung für den öffentlichen Dienst durch bundesrechtliche Rahmenregelung einen entscheidenden Impuls erfahren. Jetzt muß jedoch die Umsetzung auf Landesebene angepackt werden (vgl. Tz. 8).

1. Verfassungsschutz

Im Berichtszeitraum wurde der Referentenentwurf eines Saarländischen Verfassungschutzgesetzes in das Anhörverfahren gebracht. In meiner Stellungnahme habe ich einige Gesichtspunkte zur Verbesserung des Datenschutzes vorgetragen, die aber nur zum geringen Teil berücksichtigt wurden.

Der Zweck des Verfassungsschutzes, nämlich Schutz der freiheitlichen demokratischen Grundordnung, Bestand und Sicherheit des Bundes und der Länder, war ausgedehnt auf die "Abwehr der diesen Schutzgütern drohenden Gefahren".

Im Interesse einer eindeutigen Aufgaben- und Befugnisverteilung zwischen Verfassungsschutz und Polizei wurde diese Formulierung auf meine Anregung hin gestrichen. Sie war zumindest mißverständlich, weil der Verfassungsschutz Vorfeldaufklärung betreibt, über keine Zwangsbefugnis verfügt und seine Beobachtung sich auch auf Gebiete ohne polizeiliche Relevanz erstreckt. Die Gefahrenabwehr hingegen obliegt der Polizei als Vollzugsorgan.

Ich habe darauf gedrungen, daß die datenschutzrechtliche Terminologie und Gesetzestechnik in den Gesetzesentwurf übernommen wird. Dem ist man insofern gefolgt, als in Anlehnung an die Datenschutzgesetze die generelle Datenerhebungs- und -verarbeitungsbefugnis als allgemeines Verbot mit Erlaubnisvorbehalt ausgestaltet und ihre zentrale Bedeutung als Befugnisnorm gesetzessystematisch untermauert wurde (§ 7 Abs. 1).

Ich hatte Gelegenheit, die von mir entwickelten "Eckwerte" für eine datenschutzgerechte Ausgestaltung des Verfassungsschutzes anläßlich des Kolloquiums am 14. Dezember 1992 im Landtag des Saarlandes darzustellen.

Das Saarland ist dem Datenschutz als Grundrecht auf "informationelle Selbstbestimmung" durch die ausdrückliche Erwähnung in seiner Verfassung besonders verpflichtet. Die Erhebung und Verarbeitung personenbezogener Daten durch den Verfassungsschutz schränkt dieses Grundrecht ein und bedarf daher einer Ermächtigung durch ein verfassungsmäßiges Gesetz, das die Grenzen zulässiger Informationsverarbeitung für den Bürger klar erkennbar festlegt.

Zwischen dem informationellen Selbstbestimmungsrecht des Einzelnen und dem Verfassungsauftrag des Verfassungsschutzes besteht ein Spannungsverhältnis. Die sich hieraus ergebenden Kollisionen müssen in der Problemlösung durch den Gesetzgeber einen "schonenden Ausgleich" erfahren. Dabei ist zu bedenken, daß der Verfassungsschutz weitgehend im geheimen arbeitet und in großem Umfang sensible Informationen über den Bürger erhebt und verarbeitet.

Die informationelle Selbstbestimmung ist - worauf das Bundesverfassungsgericht hinweist (BVerfGE 65,1, 43) - für die Funktionsbedingungen eines freiheitlich-demokratischen Gemeinwesens von elementarer Bedeutung. Die Offenheit und Freiheitlichkeit des politischen Willensbildungsprozesses ist eine wesentliche Funktion der freiheitlich-demokratischen Grundordnung, die auch der Verfassungsschutz zu gewährleisten verpflichtet ist. Dabei kommt der "Freiheit von Angst" vor den Möglichkeiten der modernen Datenverarbeitung (Denninger VVD StRL 1979/8, 26 ff) erhebliche Bedeutung zu.

Normenklarheit der gesetzlichen Ermächtigung für die Informationsverarbeitung des Verfassungsschutzes ist die notwendige Voraussetzung, die Informationsverarbeitung transparent werden zu lassen, Ängste abzubauen

und damit die demokratischen Teilhaberechte des Bürgers zu gewährleisten.

Wesentliches Element der Transparenz ist vor allem eine möglichst genaue gesetzliche Festlegung der Aufgaben und der Informationsverarbeitungsbefugnisse. Der Gesetzgeber muß die Grenzen zulässiger Informationserhebung und -verarbeitung deutlich markieren.

Diesen Anforderungen hat der überarbeitete Regierungsentwurf in vieler Hinsicht Rechnung getragen. Folgendes sei besonders hervorgehoben:

- Die personenbezogene Informationsverarbeitung wird nur zugelassen, soweit tatsächliche Anhaltspunkte für den Verdacht verfassungsfeindlicher Betätigung vorliegen (§ 7 Abs. 2 Satz 1).

- Im Extremismusbereich sind die Beobachtungsobjekte förmlich festzulegen (§ 3 Abs. 1 Satz 3). Vor dieser Festlegung dürfen Informationen grundsätzlich nur aus allgemein zugänglichen Quellen erhoben werden (§ 7 Abs. 3 Satz 1). Erst nach dieser Festlegung dürfen personenbezogene Daten in Dateien gespeichert werden (§ 10 Abs. 1).

- Das Schwergewicht der Beobachtung liegt bei den Organisationen und erst in zweiter Linie bei den Einzelpersonen (§ 5 Abs. 1 Satz 2 und Satz 3), da die für die Schutzgüter der Verfassung relevanten Gefahren vor allem von den Organisationen und Zusammenschlüssen ausgehen. Damit wird der Forderung wenigstens ansatzweise Rechnung getragen, auf die Beobachtung von Einzelpersonen nach dem Grundsatz der Verhältnismäßigkeit zu verzichten.

- Die weitere Verwendung von Personaldaten aus dem Bereich der Sicherheitsüberprüfung (§ 7 Abs. 2 Satz

2) sowie von personenbezogenen Informationen, die aus dem Einsatz eingriffsintensiver nachrichtendienstlicher Mittel herrühren (§ 8 Abs. 3 letzter Satz), ist im Interesse der Zweckbindung restriktiv geregelt.

- Der Betroffene hat einen unentgeltlichen Auskunftsanspruch, ohne daß ein besonderes Interesse darzulegen ist; die Auskunft kann nur verweigert werden, wenn das öffentliche Interesse an der Geheimhaltung oder das Geheimhaltungsinteresse Dritter überwiegt (§ 21 Abs. 2).

- Die Öffentlichkeit wird über verfassungsfeindliche Bestrebungen unterrichtet. Strukturdaten über den Verfassungsschutz - Gesamtzahl der Bediensteten sowie die Stellenübersicht des Landesamtes für Verfassungsschutz, die Gesamtzahl der in Verbunddateien des Bundes gespeicherten Personendatensätze und die Summe der für das Landesamt für Verfassungsschutz eingesetzten Haushaltsmittel - werden bekannt gegeben.

Damit entspricht der Regierungsentwurf vom 05.11.1992 (Lt-Drucksache 10/1222) einigen wesentlichen Anforderungen, die im Interesse der Offenheit und Freiheitlichkeit des politischen Willensbildungsprozesses unerläßlich sind.

Im übrigen hat der Entwurf den Zielkonflikt nicht in jeder Hinsicht bewältigen können, einerseits möglichst große Transparenz durch Konkretisierung der gesetzlichen Voraussetzungen für die Informationsverarbeitung zu erreichen, andererseits aber auch der Verfassungsschutzbehörde möglichst viel Spielraum für ihre Arbeit zu gewähren.

Die Aufgaben des Verfassungsschutzes wurden zwar durch einige Begriffsbestimmungen erläutert; dabei wurde aber auf weitere, wenig aussagekräftige Formulierungen zurückgegriffen. Dem Bürger ist kaum geholfen, wenn er etwa erfährt, daß der Verfassungsschutz Bestrebungen beobachtet, "die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden" (§ 3 Abs. 1 Nr. 3).

Das Gesetz regelt nicht abschließend, welche nachrichtendienstlichen Mittel - wie z.B. der Einsatz von V-Leuten, Observationen, Bild- und Tonaufzeichnungen - das Landesamt für Verfassungsschutz anwenden darf, sondern überläßt die Festlegung einer Dienstvorschrift (§ 8 Abs. 1).

Der Einsatz nachrichtendienstlicher Mittel ist besonders eingriffsintensiv, weil die heimliche Vorgehensweise regelmäßig mit Täuschung des Betroffenen verbunden ist und massenhaft Überschußinformationen anfallen können. Die Voraussetzungen, unter denen solche Handlungsmethoden angewendet werden dürfen, hat der Gesetzgeber selbst festzulegen (Gesetzesvorbehalt und Wesentlichkeitslehre).

Der Entwurf hat zwar den Grundsatz ausdrücklich bestätigt, daß beim Einsatz nachrichtendienstlicher Mittel keine strafbaren Handlungen begangen werden dürfen (§ 6 Abs. 1 Satz 2). Die ausnahmsweise straffreie Verwirklichung von Straftatbeständen gegen Rechtsgüter der Allgemeinheit zur Vorbereitung und Absicherung des Einsatzes nachrichtendienstlicher Mittel ist jedoch nicht in normenklarer Weise geregelt (§ 8 Abs. 1 letzter Satz). So werden Organisationsdelikte - wie die Mitgliedschaft in einer für verfassungswidrig erklärten Partei (§ 84 Abs. 2 StGB) oder deren Ersatzorganisation (§ 85 Abs. 2 StGB) - lediglich beispielhaft

aufgezählt. Der Gesetzgeber hat somit nicht eindeutig klargestellt, in welchem Umfang das Verbot strafbarer Handlungen durchbrochen werden darf.

Die Tendenz des Entwurf wird nicht verkannt, daß nachrichtendienstliche Mittel nicht gezielt gegen unverdächtige Personen eingesetzt werden können. Es ist insbesondere zu begrüßen, daß gegenüber Unbeteiligten das Beobachtungsfeld auf gewaltorientierten Extremismus und Spionage beschränkt werden soll, wenn eine solche Maßnahme "aufgrund bestimmter Tatsachen unumgänglich erscheint" (§ 8 Abs. 2 Nr. 2). Ob die Einsatzschwelle gegenüber Unverdächtigten auch dann zu beachten ist, wenn es um die Anwerbung und Überprüfung von Kontaktpersonen geht (§ 8 Abs. 2 Nr. 3) ist indessen unklar; sie sollte höher liegen, als bei der "normalen" Beobachtung ohne nachrichtendienstliche Mittel. Die "Erforderlichkeit" zur Gewinnung und Sicherung von Nachrichtenzugängen ist jedenfalls allein eine zu schwache Einsatzbremse. Auch im übrigen läßt die Regelung des Einsatzes nachrichtendienstlicher Mittel an Klarheit zu wünschen übrig, wenn auf das Gesetz zu Artikel 10 Grundgesetz verwiesen wird (§ 8 Abs. 2 Satz 2). Nach der Entwurfsbegründung sollen aufgrund dieser Vorschrift nachrichtendienstliche Mittel, die mit Telefonabhörmaßnahmen vergleichbar oder weniger eingriffsintensiv sind, bei schweren Delikten nach dem Katalog des G-10 auch gegen Unverdächtige eingesetzt werden können. Die Ungewißheit über den Umfang der zulässigen nachrichtendienstlichen Mittel wirkt sich auch hier nachteilig auf die Normenklarheit aus. Die Beschränkung des Grundrechts auf Datenschutz bedarf einer "verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für den Bürger erkennbar ergeben..." (BVerfGE 65, 1, 44). Hiermit ist es nicht vereinbar, daß der Anwendungsbereich des G-10 und damit die Voraussetzungen für den Einsatz nachrichten-

dienstlicher Mittel durch eine Dienstvorschrift konkretisiert werden.

Nicht nachvollziehbar ist, daß der Betroffene nach Ablauf von 5 Jahren seit dem Einsatz der nachrichtendienstlichen Mittel nicht mehr unterrichtet werden soll (§ 8 Abs. 3 Satz 5).

Zu beklagen ist auch der Mangel einer zentralen Vorschrift über die behördeninterne, anderweitige Verwendung personenbezogener Daten, wie sie z.B. im Bayerischen Verfassungsschutzgesetz vorgesehen ist (§ 14 Abs. 1 am Ende). Die Informationen werden für bestimmte Aufgaben des Verfassungsschutzes erhoben und dürfen nach dem Grundsatz der Zweckbindung grundsätzlich nur zu dem Erhebungszweck verwendet werden. Die Zweckdurchbrechung darf jedenfalls nicht die Regel sein und sollte im Einzelfall zumindest einer Erforderlichkeitsprüfung unterzogen werden.

Die Verfassungsgrundsätze der Zweckbindung und Verhältnismäßigkeit erfordern erst recht eine Beschränkung des wechselseitigen Datenaustausches zwischen Verfassungsschutz und anderen Behörden. Das gilt wegen der Aufgaben- und Befugnisdivergenz vor allem im Verhältnis von Polizei und Verfassungsschutz. Eine Zusammenarbeit mit anderen Behörden ist damit nicht völlig ausgeschlossen; sie bedarf jedoch eindeutiger, einschränkender Regelung über die Zulässigkeit der Zweckdurchbrechung. Vor allem die historisch gewachsene Funktionstrennung zwischen Polizei und Verfassungsschutz unterstreicht die Notwendigkeit, dem Grundsatz der Zweckbindung Rechnung zu tragen. Die Besorgnis ist nicht unbegründet, daß die aus guten Gründen eingeschränkten Erhebungsbefugnisse des Verfassungsschutzes unterlaufen werden durch allzu weit gefaßte Übermittlungspflichten anderer Stellen.

Um einer Atmosphäre des Mißtrauens vorzubeugen, ist es zu begrüßen, daß Spontanübermittlungen öffentlicher Stellen an den Verfassungsschutz nur bei tatsächlichen Anhaltspunkten für gewalttätigen Extremismus und Spionage zugelassen sind (§ 15 Abs. 1).

Im übrigen hätte das Zweckbindungsgebot beim Datentransfer an den Verfassungsschutz stärker beachtet werden müssen. Zwar dürfen die Strafverfolgungsbehörden keine Informationen, die aus Telefonabhörmaßnahmen herrühren, übermitteln (§ 8 Abs. 2 Satz 2), es sei denn, es handelt sich um schwere Delikte aus dem Staatsschutzbereich (abschließender Katalog des § 2 G-10). Eine Beschränkung bei Informationen aus anderen polizeilichen, strafprozessualen Zwangsmaßnahmen ist jedoch nicht vorgesehen. Je eingriffsintensiver die Maßnahme, umso enger sollten die Voraussetzungen der Zweckdurchbrechung sein. Das gilt vor allem für Informationen, die aus dem verdeckten Einsatz technischer Mittel herrühren (Ton-, Bildaufzeichnungen), aber auch für solche aus Beschlagnahme und Hausdurchsuchungen. Die ansonsten erkennbare Tendenz des Entwurfs hätte es nahegelegt, insoweit wenigstens den Datentransfer auf gewalttätigen Extremismus und Spionage zu beschränken.

Auch die Datenübermittlung durch den Verfassungsschutz an andere Stellen stellt einen zusätzlichen Eingriff für den Betroffenen dar, der einer normenklaren "gesetzlichen" Regelung bedarf. Dieser Anforderung genügt der Entwurf nicht (§ 17 Abs. 2 i.V.m. § 5 Abs. 4). Insbesondere ist der Begriff der "erheblichen Gefahr" nicht geeignet, den Datentransfer zur Gefahrenabwehr mit der notwendigen Bestimmtheit zu steuern. Eine Legaldefinition fehlt.

2. Polizei

2.1 Fotoausstellung zu präventiven Zwecken

Durch Hinweise aus der Nachbarschaft wurde die Polizei auf ein dreijähriges Mädchen aufmerksam, das in der völlig verwahrlosten Wohnung seiner alleinstehenden Mutter unter unmenschlichen Umständen dahinvegetierte. Der Sachverhalt führte zur Einleitung eines Strafverfahrens. Die Presse berichtete ausführlich. Im Rahmen des Ermittlungsverfahrens wurden zu Beweiszwecken von den einschreitenden Beamten Lichtbilder der Wohnung gefertigt, die Einzelheiten der Wohnungseinrichtung und deren Zustand erkennen ließen. Zweitabzüge wurden zu einer Fotodokumentation zusammengestellt und der Öffentlichkeit im Gebäude des Polizeireviers zugänglich gemacht. Personen waren nicht abgebildet.

Mit dieser Veröffentlichung beabsichtigte die Polizei die Bevölkerung für das Problem der Kindesmißhandlung zu sensibilisieren. Gewünschter Effekt war der zukünftige Schutz von Kindern.

Diese Fotoausstellung führte zu einer Petition an den Landtag des Saarlandes. Die Petentin war der Auffassung, Art und Weise der Veröffentlichung durch die Polizei und der späteren Veröffentlichung in der Presse hätten zu gravierenden Verletzungen der Grundrechte der betroffenen Mutter geführt.

Im Rahmen einer durch den Petitionsausschuß erbetenen datenschutzrechtlichen Bewertung bin ich - ebenso wie das Ministerium des Innern - zu dem Ergebnis gelangt, daß die polizeiliche Vorgehensweise einer Rechtsgrundlage entbehrte.

Wenn auch Personen nicht dargestellt und Namen nicht angegeben waren, so ist nicht auszuschließen, daß bei

zahlreichen Personen - wegen des unmittelbaren zeitlichen und räumlichen Zusammenhangs der Ausstellung mit den durch die Presse veröffentlichten Tatumständen - ein Zusatzwissen vorhanden war, das die Identifizierung der Betroffenen zuließ. Insbesondere Nachbarn konnten Kenntnisse haben, die die Zuordnung der Informationen über den Zustand der Wohnung ermöglichte.

Die Ausstellung der polizeilichen Fotodokumentation berührt den grundrechtlich geschützten Bereich der Wohnung (Art. 13 GG) und beeinträchtigt die Privat- und Intimspähre und damit die Persönlichkeitsrechte der Betroffenen (Art. 1, Art. 2 GG). Eine gesetzliche Ermächtigung, die für einen solchen Eingriff in Grundrechte notwendig ist, ist nicht ersichtlich.

Die Polizei darf auf der Grundlage des Saarländischen Polizeigesetzes personenbezogene Informationen nur zu dem Zweck übermitteln, zu dem sie diese erlangt hat. Damit ist eine eindeutige Nutzungsbeschränkung auf die Ziele der Gefahrenabwehr und Strafverfolgung gesetzlich festgelegt. Die Übermittlung an Stellen und Personen außerhalb des Polizeibereichs ist nur zu Zwecken der Gefahrenabwehr im konkreten Einzelfall zugelassen.

Die Ausstellung war weder zur Strafermittlung noch zur individuellen Vorbeugung vor weiteren Straftaten der Beschuldigten erforderlich. Zur Gefahrenabwehr im Einzelfall war sie ohnehin ungeeignet. Veröffentlichungen der Polizei, die geeignet sind, einzelne Personen zu beeinträchtigen, sind zu Zwecken der generellen Vorbeugung unzulässig. Für die Aufklärung der Bevölkerung über das kriminelle Geschehen ist die Verwendung personenbezogener Informationen nicht erforderlich und daher auch nicht zulässig.

2.2 Landeskriminalblatt

Das Kriminalpolizeiamt gibt das Landeskriminalblatt Saarland heraus. Es erscheint in unregelmäßigen Abständen und stellt ein Mittel zur Ausschreibung von polizeilich bedeutsamen Sachverhalten und Informationen dar. Es dient unter anderem der Fahndung nach Personen und Sachen, dem Erkennen von Tatzusammenhängen, der Ermittlung der Herkunft sichergestellter Gegenstände. Zur Identifikation der betroffenen Personen werden persönliche Daten mitgeteilt; häufig werden auch Fotos veröffentlicht. In einer Ausgabe wird etwa ein Mordfall geschildert mit dem Ziel, über eine detaillierte Tat- und vor allem Opferbeschreibung Hinweise für die Aufklärung zu gewinnen. Außerdem wird über eine Reihe weiterer Straftaten wie z.B. Diebstahl, Raub und Betrug berichtet, wobei die vorliegenden Erkenntnisse über die Tatverdächtigen ausführlich mitgeteilt werden. Erwähnt sei auch der Fall eines Mannes, der in fünf Fällen als Exhibitionist in Erscheinung getreten war. Er war geständig und mußte als überführt gelten. Im Landeskriminalblatt wurde er mit Namen, Geburtsdatum, Wohnanschrift, Fahrzeugkennzeichen sowie Lichtbild vorgestellt, wohl in der Absicht, mögliche weitere Taten aufzuklären. Ob konkrete Anhaltspunkte für einen derartigen Verdacht vorlagen, war nicht zu erkennen.

Derartige Veröffentlichungen tangieren die schutzwürdigen Belange Betroffener in höchstem Maße. Ebenso wie der Inhalt von Ermittlungsakten darf auch der Inhalt des Landeskriminalblattes nicht Unbefugten zur Kenntnis gelangen. Nur solche öffentliche Stellen dürfen die Informationen erhalten, die im Rahmen ihrer Zuständigkeit einen Beitrag zur Aufklärung leisten können.

Das Landeskriminalblatt wurde früher an verschiedene Polizeibehörden, Einwohnermeldeämter, Jugendämter, Ordnungsämter, Zoll- und Finanzbehörden, Justizbehörden, Nachrichtendienste, verschiedene ausländische Dienststellen und Sonderpolizeibehörden versandt. Der Empfängerkreis orientierte sich an Richtlinien, die 1974 von der Arbeitsgemeinschaft der Leiter der Kriminalämter beschlossen wurden.

Das Ministerium des Innern hat mir inzwischen mitgeteilt, daß das Landeskriminalamt zukünftig das Landeskriminalblatt regelmäßig nur noch an Dienststellen der saarländischen Vollzugspolizei, das Ministerium des Innern, die Landeskriminalämter und das Bundeskriminalamt übermittelt. Damit sind beispielsweise Zollfahndungsdienst, Steuerfahndung, Staatsanwaltschaften, Postbetriebssicherungsdienst, Verfassungsschutz und Bundesnachrichtendienst aus dem Kreis der regelmäßigen Bezieher ausgeschieden. Diese deutliche Reduzierung ist zu begrüßen, auch wenn zu prüfen bleibt, ob nicht noch weitere Einschränkungen angezeigt sind, um einer unzulässigen Streuung von Informationen vorzubeugen. Problematisch ist vor allem eine regelmäßige Übermittlung an die Bereitschaftspolizei und die Polizeischule. Sie benötigen die entsprechenden Daten nur, wenn sie im Einzelfall zu entsprechenden Einsätzen herangezogen werden. Das Innenministerium als Aufsichtsbehörde benötigt solche personenbezogenen Informationen ebenfalls nicht, weil es am Vollzug nicht unmittelbar beteiligt ist.

2.3 Notruffälle

Einem Hilfesuchenden den leichten und unmittelbaren Zugang zum Rettungsdienst zu ermöglichen, ist seit langem ein Anliegen des Datenschutzes (vgl. zuletzt 13. TB Tz. 2.4). Problematisch ist, daß Anrufe häufig bei der Polizei auflaufen und diese beim Verdacht

einer strafbaren Handlung zum Einschreiten verpflichtet ist. Ich hatte deshalb bisher ohne Erfolg angeregt, nicht dem Legalitätsprinzip unterworfene Bedienstete für die Entgegennahme von Notrufen bei der Polizei einzusetzen, um so den Hilfesuchenden nicht der Gefahr strafrechtlicher Verfolgung auszusetzen.

Vor dem Hintergrund dieser Diskussion mußte es deshalb um so mehr befremden, als ich in anderem Zusammenhang in einer Ermittlungsakte den Bericht eines Polizeireviers fand, in dem festgehalten war, daß die Rettungsleitstelle von sich aus und ohne jede rechtliche Verpflichtung die Polizei von einem Fall des Verdachtes des Verstoßes gegen das Betäubungsmittelgesetz unterrichtet hatte. Gegen den Betroffenen, der wegen Konsums von Rauschgift bewußtlos in ein Krankenhaus eingeliefert wurde, wurde daraufhin ein Ermittlungsverfahren eingeleitet. Es liegt auf der Hand, daß ein solcher Vorfall nicht geeignet ist, das Vertrauen ärztlicher Hilfe bedürftiger Menschen in die Rettungseinrichtungen zu stärken.

Das Ministerium des Innern, dem ich den Sachverhalt mitgeteilt habe, hat zugesichert, es sei Vorsorge getroffen, daß ein ähnlicher Fall künftig ausgeschlossen sei. Die Bediensteten der Rettungsleitstelle seien entsprechend unterrichtet worden. Personenbezogene Informationen, die bei der Rettungsleitstelle unmittelbar eingehen, würden nicht an die Polizei weitergegeben. Deren Einschaltung erfolge ausschließlich, um eine ungehinderte Durchführung von Rettungseinsätzen sicherzustellen. Weiterhin werde die Polizei bei Verkehrsunfällen auf Wunsch der Beteiligten informiert.

2.4 Rückmeldeverfahren der Staatsanwaltschaft

Die Polizei kann personenbezogene Daten Verdächtiger, die sie aus Strafermittlungsverfahren gewonnen hat,

aufgrund einer differenzierten Prognoseentscheidung zur vorbeugenden Bekämpfung von Straftaten speichern (§ 30 Abs. 2 SPolG). Beurteilungsgrundlage sind die Erkenntnisse zum Zeitpunkt der Abgabe des Verfahrens an die Staatsanwaltschaft. Gesichtspunkte tatsächlicher oder rechtlicher Art, die sich bei der weiteren Bearbeitung oder auch erst im gerichtlichen Verfahren ergeben haben, hatten bisher keine Auswirkungen auf die weitere Speicherung, da sie bislang der Polizei regelmäßig nicht bekannt gegeben wurden. Insbesondere Verfahrenseinstellungen müssen jedoch Anlaß geben, die Fortdauer einer Speicherung in polizeilichen Dateien zu überprüfen. Deshalb habe ich schon vor Jahren gefordert, daß die Polizei durch Rückmeldungen von der Staatsanwaltschaft über den Ausgang des Strafverfahrens informiert wird (vgl. zuletzt meinen 9. TB Tz. 2.3).

Seit August 1991 wird meiner Forderung weitgehend entsprochen. Beendigungen des Verfahrens durch Einstellungen oder Freispruch werden dem Landeskriminalamt (LKA) mitgeteilt. Verkehrssachen sind allerdings ausgenommen.

Die Verfahrensweise ist durch Verfügung festgelegt. Freispruch und Verfahrenseinstellung (§ 170 Abs. 2 StPO) führen ohne weitere Prüfung zur Löschung. Im übrigen ist eine Einzelfallentscheidung zu treffen, so z.B. bei Einstellung wegen Geringfügigkeit (§ 153 StPO) und bei Einstellung mit Auflagen und Weisungen (§ 153 a StPO). Hierbei ist wiederum, wie bei der erstmaligen Speicherung, die Prognoseentscheidung ausschlaggebend, ob wegen der Art, Ausführung und Schwere der Tat und im Hinblick auf die Persönlichkeit des Betroffenen die Gefahr der Wiederholung besteht (Prognoseentscheidung nach § 30 Abs. 2 SPolG).

Im Berichtsjahr habe ich beim LKA eine Überprüfung vorgenommen; dabei hat sich gezeigt, daß die praktische Umsetzung der Anweisung verbesserungsbedürftig ist.

Das LKA erhält eine Vielzahl von Informationen, die zur Aufgabenwahrnehmung nicht benötigt werden: z.B. Mitteilungen über Ordnungswidrigkeiten und über minderschwere Delikte, die von vornherein zu Präventionszwecken nicht mehr gespeichert werden (z.B. Kaufhausdiebstähle). Gegenüber der Staatsanwaltschaft habe ich entsprechende Korrekturen gefordert, die im Rahmen der weiteren Automatisierung der Zentraldatei realisiert werden sollten.

Unvollständig bearbeitet waren die Rückmeldungen über Einstellungen mangels Tatnachweis. Die Löschungen sind in 24 von 100 überprüften Fällen nicht erfolgt. Die Fehlerquote von 24 % dürfte in Wahrheit noch größer sein. Denn ein nicht unbeträchtlicher Anteil der Straftaten wird von vornherein nicht gespeichert, weil minderschwere Fälle von vornherein garnicht mehr erfaßt werden. Ich habe gefordert, daß Löschungen entsprechend der Vorgabe in der Anweisung zukünftig vollständig und lückenlos erfolgen müssen.

In fünf Fällen der Einstellung wegen Geringfügigkeit habe ich die Löschung für notwendig gehalten. Die Polizei ist meiner Auffassung nur in einem Fall nicht gefolgt. Hierbei ging es um den Konsum von Heroin, der nach Auffassung der Polizei aus Gründen der Prävention die weitere Speicherung des Betroffenen rechtfertigt. Die Polizei will meiner Anregung folgen, im Bereich der Drogenkriminalität die Voraussetzungen der Speicherung zu präventiven Zwecken durch Verwaltungsanordnung näher zu konkretisieren. Überprüfungsbedürftig ist vor allem die Speicherungspraxis beim Gebrauch weicher Drogen (z.B. Haschisch).

Das Ministerium des Innern teilt meine Auffassung, daß bei Einstellungen wegen Geringfügigkeit in Zweifelsfällen immer eine Löschung erfolgen sollte. Die Polizei ist im übrigen meiner Anregung gefolgt, in Fällen der Einstellung wegen Geringfügigkeit oder mit Auflagen die Gründe für die Fortdauer der Speicherung zu protokollieren.

Als Stichtag für die Bereinigung im Rückmeldeverfahren wurde der 01.01.1991 angenommen. Wie bei allen zeitlichen Fixierungen dieser Art, so ergeben sich auch hier Probleme. War eine weiter zurückreichende generelle Überprüfung aus Kapazitätsgründen bisher nicht möglich, so ist es andererseits nicht hinnehmbar, daß alle gelegentlichen Mitteilungen über Vorgänge aus der Zeit vor dem Stichtag nicht bearbeitet wurden. Diese Verfahrensweise ist deshalb bedenklich, weil der Verfahrensausgang in solchen Fällen gelöscht wird und somit der Polizei Unterlagen für eine spätere, retrograde Überprüfung nicht mehr zur Verfügung stehen. Meiner Forderung, auch die Rückmeldungen mit Aktenzeichen aus den Jahren vor 1991 zukünftig zu berücksichtigen, trägt das Landeskriminalamt zwischenzeitlich Rechnung.

2.5 Erkennungsdienstliche Behandlung von Asylbewerbern

Angesichts des starken Zustroms von Asylbewerbern haben Probleme im Zusammenhang mit der Wahrnehmung des Grundrechts auf Asyl Politik und Öffentlichkeit stark beschäftigt. Unbehagen bereitete insbesondere die Tatsache, daß es zu Mißbräuchen und Fällen von unrechtmäßiger Inanspruchnahme von Sozialleistungen gekommen ist. Zweifellos hat im Rahmen des Asylverfahrens deshalb die Kenntnis der Identität von Asylbewerbern erhebliche Bedeutung. Sie muß im Zweifelsfall auch mit erkennungsdienstlichen Mitteln geklärt werden, damit der mehrfa-

chen Inanspruchnahme von Sozialhilfe vorgebeugt werden kann.

Nach dem bis zum 30. Juni 1992 geltenden Recht waren Lichtbilder und Fingerabdrucke bei Asylsuchenden nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt war. Das zum 1. Juli 1992 in Kraft getretene Asylverfahrensgesetz sieht nunmehr vor, daß von sämtlichen Asylbewerbern - bis auf wenige Ausnahmen - Lichtbilder und Fingerabdrucke zu fertigen sind (§ 16 Abs. 1). Die Datenschutzbeauftragten des Bundes und der Länder haben hierin einen Verstoß gegen den Verfassungsgrundsatz der Verhältnismäßigkeit gesehen (Entschließung vom 28.04.1992, Anlage 2)

Eine lückenlose, erkennungsdienstliche Behandlung ließe sich allenfalls dann rechtfertigen, wenn feststünde, daß die Identität eines hohen Anteils von Asylbewerbern zweifelhaft ist. Hierfür fehlt jedoch bisher der Nachweis. Die amtliche Begründung zum Gesetzentwurf beruft sich lediglich auf Feststellungen in den Niederlanden, daß 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Empirische Untersuchungen anderer Art lagen zum Zeitpunkt der Verabschiedung im Bundestag nicht vor und sind bisher auch nicht bekannt geworden. Gegen Mitglieder einer ganzen Personengruppe ohne jeden Ansatz einer Differenzierung erkennungsdienstliche Maßnahmen zu ergreifen, die nach bisherigem Recht gegen Straftatverdächtige oder bei Vorliegen einer im Einzelfall konkret festzustellenden Gefahr zulässig sind, ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Im übrigen sind auch weniger eingriffsintensive Maßnahmen, die inzwischen ergriffen werden, durchaus geeignet, dem Mißbrauch etwa bei der Inanspruchnahme von Sozialleistungen vorzubeugen; so z.B. die Unterbringung in Sammelunterkünften und die Gewährung von Sozialhilfen in Form von Sachleistungen, die Auszahlung

von Barbeträgen durch die Gemeinden nur noch am selben Tag und die immer mehr in Gang kommende Beschleunigung der Verfahren.

Aber auch die Regelungen über die im einzelnen zur Feststellung der Identität zu treffenden Maßnahmen, verstoßen gegen das Übermaßverbot. Statt des Abdrucks von einem Finger dürfen nunmehr Abdrücke von allen zehn Fingern genommen werden (§ 16 Abs. 1 Satz 2 Gesetz zur Neuregelung des Asylverfahrens), obwohl zur Identitätsfeststellung der Einfingerabdruck ausreicht. Damit wird die Tendenz des Gesetzes unterstrichen, die Asylbewerber wie Straftäter zu behandeln, denn Zehnfingerabdrücke werden vor allem für den Spurenvergleich benötigt.

Das Problem bleibt auf dem Prüfstand. Greifen die neuerdings in die Wege geleiteten Maßnahmen, wird man sich darüber unterhalten müssen, ob die uneingeschränkte, erkennungsdienstliche Behandlung der genannten Gruppen der Asylbewerber noch beibehalten werden muß.

2.6 Polizeiliches Informationssystem DIPOL

Das neue Informationssystem DIPOL - ich berichtete bereits in meinem 11. Tätigkeitsbericht für das Jahr 1989 (Tz. 3.2) - soll die informationstechnische Infrastruktur der Polizei auf eine neue Grundlage stellen. Die bisherigen Formen konventioneller Informationsverarbeitung und der interne, polizeiliche Meldedienst sollen weitgehend durch ein System ersetzt werden, das die Vorgangsbearbeitung und -verwaltung und die Informationsvermittlung zwischen den Dienststellen integriert. Dieses Telekommunikationssystem, das wesentliche Elemente der sog. Bürokommunikation enthält, basiert auf der Verknüpfung von automatisierter Datenverarbeitung und Fernmeldetechnik. Rechnerleistungen werden mit einem ISDN-fähigen Fernsprechsondernetz für

die Polizei verbunden. Die Ermittlungsakte als Grundlage der Strafverfolgung bleibt jedoch erhalten; nach Abgabe an die Staatsanwaltschaft bleibt die Polizei jedoch weitgehend auf den eigenen, automatisierten Datenbestand angewiesen.

Auf der Grundlage des Hauptuntersuchungsberichts hatte ich bereits am 10. Januar 1991 Gelegenheit, dem Ausschuß für Innere Verwaltung über DIPOL und die damit verbundenen Gefährdungen aus datenschutzrechtlicher Sicht vorzutragen. Die besonderen Risiken liegen darin begründet, daß alle in den Polizeidienststellen anfallenden Informationen aufgrund etwa von Ereignissen, Hinweisen, Mitteilungen, Ersuchen, Anzeigen im Computer dokumentiert werden und etwa damit der Bürger nicht nur als Beschuldigter, sondern auch als Opfer, Geschädigter, Anzeiger, Hinweisgeber, Zeuge, Auskunftsperson, Finder mehr als bisher für die Polizei abrufbar und recherchierbar werden kann. Jede Berührung mit der Polizei hinterläßt ihre elektronischen Spuren.

Nicht zu unterschätzen ist vor allem die fernmeldetechnische Komponente, die den Informationstransport im Interesse eines effektiven, polizeilichen Meldedienstes beschleunigt und die Anbindung lokaler Polizeidienststellen an zentrale und externe Datenbanken - insbesondere an das bundesweite INPOL-System - ermöglicht. Der Qualitätssprung liegt aber nicht nur begründet in der Möglichkeit einer schnellen, landesweiten Zusammenführung von Polizeiinformationen, sondern auch in der gezielten Abrufmöglichkeit von auf lokaler und auf zentraler, regionaler Ebene gespeicherten Daten, die bei konventioneller Datenhaltung in dieser komfortablen Weise nicht verfügbar wären.

DIPOL - ein flexibles Informationssystem, das den jeweils aktuellen praktischen Bedürfnissen leicht angepaßt werden kann - eröffnet mit konventionellen

Mitteln nicht erreichbare Verknüpfungs- und Auswertungsmöglichkeiten. Die elektronischen Spuren, die der Einzelne im System hinterläßt - darüber besteht Einigkeit mit der Polizei - dürfen indessen nur in dem durch Gesetz vorgegebenen Umfang genutzt werden. Rechtsgüterschutz durch die Polizei (Gefahrenabwehr, Verbrechensbekämpfung) einerseits und Persönlichkeitsrecht des Bürgers andererseits, der schließlich nicht nur als Verdächtiger, Beschuldigter im Polizeicomputer registriert wird, müssen als gleichrangige Verfassungspositionen zum Ausgleich gebracht werden. Auf der Grundlage des Saarländischen Polizeigesetzes, das in verfassungskonformer Weise anzuwenden ist, muß eine praktische Konkordanz hergestellt werden, die beide Positionen optimal zur Geltung kommen läßt.

Eindeutige Schranken ergeben sich aus dem Saarländischen Polizeigesetz. Zur vorbeugenden Bekämpfung von Straftaten dürfen Informationen aus Strafermittlungsverfahren nach einer sorgfältigten Prognoseentscheidung gespeichert werden (§ 30 Abs. 2 SPolG). Im übrigen schreibt das Gesetz eine strenge Zweckbindung vor (§ 30 Abs. 1 Satz 2 und 3 SPolG). Dies gilt vor allem für die Informationen zum Nachweis des Eingangs, der Bearbeitung, des Ausgangs und des Verbleibs von Vorgängen, die als Daten der sogenannten Vorgangsverwaltung ausschließlich nur zu diesem Zweck und keinesfalls zur Prävention genutzt werden dürfen (§ 31 SPolG).

Die Vorgangsverwaltung ist bisher nicht abschließend definiert. Darunter fallen nach bisheriger Auffassung vor allem Informationen, die konventionell in Tagebüchern, Tätigkeitsbüchern, Ordnungsbüchern, Indices zum Nachweis von Vorkommnissen geführt werden. Ihre Verwertbarkeit für polizeiliche und Strafverfolgungszwecke wird in dem Maße steigen, als sie elektronisch auf Knopfdruck unter den verschiedensten Selektionskriterien zur Verfügung stehen. Soweit dies zum Wieder-

auffinden des Vorgangs genutzt wird, ist dagegen zwar nichts einzuwenden. Wird der Bürger jedoch in jeder Rolle, in der mit der Polizei in Berührung gekommen ist - etwa als Finder, Zeuge, Auskunftsperson, Anzeiger, Opfer, Geschädigter - für Zwecke der Vorbeugung herangezogen, ist dies ein vom Gesetz nicht gebilligter Verstoß gegen die Zweckbindung (§ 31 Satz 2 SPolG). Wo aber die Grenze des Zulässigen und Unzulässigen genau verläuft, ist aus dem Gesetz nicht zu erkennen und belastet daher jede Diskussion über die Behandlung der Vorgangsverwaltung in DIPOL.

Einer unverhältnismäßigen Beeinträchtigung der Betroffenen ist jedenfalls vorzubeugen. Deshalb habe ich vor allem gefordert:

- Die technische Konzeption von DIPOL darf nicht dazu führen, daß den bestehenden, zentralen, polizeilichen Datenbeständen weitere hinzugefügt werden, die alle auf lokaler Ebene vorhandenen Informationen allen Polizeidienststellen zur Verfügung stellen. Eine überdimensionale, landesweite Vorgangsdatei (zentraler Index) habe ich von vornherein abgelehnt.

- Die Zweckbindung der Daten muß - auch in den örtlichen Polizeidienststellen - gewährleistet sein. Es bedarf eines Systems von Datensicherungsmaßnahmen und Zugriffsregelungen, die die Informationsnutzung entsprechend steuern.

Für richtungweisend halte ich die Reaktion des Ministers des Innern auf meinen 11. Tätigkeitsbericht in seiner Presseerklärung vom 12. Februar 1990. Seine Auffassung hat er wie folgt umrissen:

> "Unverdächtige Bürger dürfen nicht gespeichert werden; auch das DIPOL-System erweitert die heute zulässige Speicherung nicht, ..."

und weiter:

"So müßten selbstverständlich die Zugriffsregelungen, die im Saarländischen Polizeigesetz festgeschriebenen Grundsätze der Zweckbindung verwirklichen. Informationen, die nicht der Strafermittlung und Gefahrenabwehr unmittelbar dienen, dürfen nur für die Zwecke des jeweiligen Vorgangs genutzt werden. Die polizeiliche Vorgangsverwaltung durch DIPOL müsse präzise festgelegt werden, und es bedürfe eines abgestuften Systems von Datensicherungsmaßnahmen und Zugriffsregelungen, das die Nutzung der Informationen und Kommunikationsmöglichkeiten in DIPOL steuert."

Meine Gespräche mit der Arbeitsgruppe DIPOL haben zu folgenden Ergebnissen geführt:

- Ein zentraler, auskunftsfähiger Index aller auf örtlicher Dienststellenebene geführten Vorgänge wird nicht eingerichtet. Lediglich zu technischen Zwecken der Datensteuerung können aus örtlichen Dienststellen Informationen über in Bearbeitung befindliche Vorgänge zentral auflaufen, die aber nicht auskunftsfähig sind und deshalb nicht genutzt werden können. Neben den INPOL-Anwendungen werden auf Landesebene in DIPOL lediglich die zentrale Falldatei geklärter (Landesaktennachweis) und ungeklärter Fälle (Landesfalldatei) geführt. Es wird sichergestellt, daß die zu präventiven Zwecken zulässige Speicherung nur im Einzelfall auf der Grundlage der gesetzlich vorgesehenen Prognoseentscheidung erfolgt. Die Richtigkeit der Entscheidung des Sachbearbeiters wird durch einen zentralen Dienst überprüft.

- Eine automatische Durchschleusung von personenbezogenen Vorgängen in den Kriminalaktennachweis des Bun-

des findet nicht statt, sondern erfolgt nur aufgrund einer Einzelfallentscheidung des zentralen Dienstes.

- Das "Lagebild" und die polizeiliche Kriminalstatistik werden nur aufgrund von nicht identifizierbaren Daten erstellt.

- Die zentralen Dienste haben keinen Zugriff auf örtliche Bestände.

- Ermittlungsergebnisse aufgrund besonderer polizeilicher Befugnisse (§ 26 Abs. 2, § 27, § 28, § 29, § 30 Abs. 3 SPolG) werden zu präventiven Zwecken in DIPOL nicht gespeichert. Damit steht fest, daß Kontaktpersonen im Vorfeld konkreter Gefahren in diesem System nicht erfaßt werden.

- Der Zugriff auf die in laufenden Ermittlungen anfallenden Informationen - hierbei handelt es sich um die große Masse der der Polizei zur Verfügung stehenden Daten - ist beschränkt auf:

  * den zuständigen Sachbearbeiter, bei seiner Abwesenheit auf seinen zuständigen Vertreter und

  * die Angehörigen der Leitungsebene.

Das Problem der Vorgangsverwaltung und die Sicherung der Zweckbindung versuchte man, in pragmatischer Weise zu lösen. Nach Abschluß des Verfahrens - in der Mehrzahl der Fälle handelt es sich um Ermittlungsverfahren, die nach vier Wochen abgeschlossen und an die Staatsanwaltschaft abgegeben werden - sind die Vorgänge dem Zugriff des Sachbearbeiters entzogen. Zugleich sollen nur noch Personendaten von Beschuldigten und in ungeklärten Fällen von Geschädigten in der Vorgangsverwaltung geführt werden; die Textdokumente werden gelöscht. Finder, Anzeiger, Zeugen, Auskunftspersonen

werden nach Abschluß des Vorgangs nicht mehr recherchierbar vorgehalten.

Nach Abschluß des Vorgangs stehen die nicht mehr in Bearbeitung befindlichen Vorgänge (Vorgangsverwaltungsdaten) nur der Leitungsebene zur Verfügung. Die Speicherfristen reichen allerdings - bezogen auf den Zeitpunkt der Erfassung im System - von vier Monaten für Mitteilungen, Meldungen, Feststellungen, Ersuchen bis zu fünf Jahren für Strafanzeigen. Wie die Zugriffsrechte im einzelnen ausgestaltet sind, ist jedoch noch offen.

Die Vorgangsverwaltungsdaten können nur standardisiert ausgewertet werden.

Diese an sich positiv zu bewertenden Ansätze können nicht darüber hinwegtäuschen, daß der pragmatische Lösungsansatz für die Behandlung von Vorgangsverwaltungsdaten letztlich nicht befriedigen kann:

- Die Leitungsebene umfaßt einen relativ großen Personenkreis, der im Vertretungsfall bis auf eine relativ niedrige Funktionsebene (Dienstgruppenleiter) hinab reichen kann.

- Hinzu kommt noch, daß die Selektionsmöglichkeiten und Recherchen so gestaltet sind, daß nicht etwa nur - entsprechend der vorgegebenen Zweckbindung - das Wiederauffinden des "jeweiligen Vorgangs", sondern auch die Nutzung zur vorbeugenden Verbrechensbekämpfung technisch möglich bleibt. An dieser Stelle werden die Grenzen der pragmatischen Auffassung von dem Begriff der Vorgangsverwaltung sichtbar. Das System und die Organisation kann keine weiteren Möglichkeiten der Beschränkung und Steuerung anbieten. Jede noch so genaue differenzierende und einschränkende Selektionsweise führt immer zu einem

ambivalenten Erfolg, der im Trefferfall zum gesuchten Vorgang führt, aber auch eine Nutzung zu präventiven Zwecken nicht ausschließt. Somit ist der Mangel einer rechtlich eindeutig abgegrenzten Begriffsdefinition der Vorgangsverwaltung mit organisatorisch-technischen Mitteln nicht auszugleichen.

Manches ist erreicht, manches ist auch noch in der Diskussion.

Die inzwischen vorliegende dv-technische Feinkonzeption läßt erkennen, daß die technische Grundausstattung von DIPOL eine außerordentlich hohe Flexibilität der Anwendung zur Folge hat. Deshalb kommt der ständigen internen Revision ebenso wie der Kontrolle durch den Landesbeauftragten für Datenschutz erhebliche Bedeutung zu. Die datenschutzrechtlichen Vorgaben für die Anwendung müssen daher - sozusagen als "Grundgesetz" für die Verfahrensrealisierung - nicht nur in Anwenderhandbüchern, sondern im Interesse einer eventuellen datenschutzgerechten Fortschreibung des Systems in allgemeinen, nachprüfbaren Anweisungen festgeschrieben werden.

Im Interesse der Transparenz polizeilicher Informationsverarbeitung in DIPOL halte ich eine - wenn auch nur stichprobenartige Protokollierung der Anwenderaktivitäten für geboten, um eine interne Revision und externe Prüfung durch das Datenschutzkontrollorgan zu ermöglichen.

Es wäre nunmehr eine Analyse auf der Grundlage des dv-technischen Feinkonzepts geboten, die die Risiken im Hinblick auf die einzusetzende Hardware und die zu entwickelnde Software untersucht. Beispielsweise sind die Maßstäbe für die technischen Anforderungen an die Systemsicherheit einschließlich der Systemzugänge, an

die Netzkomponenten einschließlich Übermittlungswege und Übertragungsprotokolle kritisch zu prüfen.

Die Projektentwicklung hat inzwischen ein Stadium erreicht, das ich mit der mir zur Verfügung stehenden Personalausstattung nicht mehr weiter sachgerecht begleiten kann. War es bisher schon nur unter Zurückstellung anderer dringender Kontrollen möglich, die umfangreichen und vorwiegend verwaltungsorganisatorischen Untersuchungen zu verfolgen und in zahlreichen Besprechungen und Stellungnahmen zu kommentieren sowie unter Datenschutzgesichtspunkten Anregungen zu geben, ist mit der Vorlage des technischen Feinkonzeptes der Mangel eines ausgebildeten Informatikers endgültig nicht mehr zu kompensieren (zur Frage der Personalausstattung unten Tz. 12). Angesichts des Entwicklungsstandes des Projekts und mit Rücksicht auf die Tatsache, daß ein Informatiker - so er denn nunmehr zur Verfügung stände - nicht mehr in der Lage wäre, den Informationsrückstand aufzuholen, ist der Zeitpunkt für eine weitere angemessene Beteiligung und Begleitung von DIPOL durch meine Dienststelle versäumt.

3. Justiz

3.1 "Lauschangriff"

Das Anwachsen der organisierten Kriminalität erfordert zweifellos angemessene staatliche Maßnahmen zum Schutze der Bürger. Ohne daß aber Erfahrungen mit dem Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) vom 15. Juli 1992 gesammelt und ausgewertet worden sind, ist der Ruf laut geworden, durch eine weitere Gesetzesnovelle den sog. "großen Lauschangriff" zuzulassen.
Der Polizei soll in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen ermöglicht werden. Aus datenschutzrechtlicher Sicht muß dieser Absicht widersprochen werden. Die Wohnung stellt ein privates Refugium dar. Dem Bürger muß ein persönlicher Bereich bleiben, der insbesondere heimlicher obrigkeitlicher Ausforschung entzogen ist. Auch im Strafprozeßrecht darf es eine Wahrheitserforschung um jeden Preis nicht geben, zumal im Rahmen eines Ermittlungsverfahrens auch unverdächtige oder unschuldige Bürger betroffen sein können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu am 1./2. Oktober 1992 eine Entschließung verabschiedet (Anlage 3).

3.2 Gnadengesetz

Das Begnadigungsrecht hat eine lange Tradition. Es verleiht im wesentlichen die Befugnis, bestimmte Rechtsfolgen wie etwa strafgerichtliche Verurteilungen, Bußgelder oder Disziplinarmaßnahmen zu erlassen oder zu mildern, wenn Rechtsmittel nicht mehr eingelegt werden können. Um das Gnadenwesen auf eine sichere rechtliche Grundlage zu stellen und dem gewandelten Gnadenbegriff Rechnung zu tragen, hat das Ministerium

der Justiz den Entwurf eines Saarländischen Gnadengesetzes vorgelegt.

Das Verfahren zur Ausübung des Begnadigungsrechts weist Besonderheiten auf. Dem Betroffenen steht weder ein Rechtsanspruch auf Begnadigung noch ein Rechtsbehelf gegen eine ablehnende Entscheidung zur Verfügung. Das Verfahren ist geprägt durch Vertraulichkeit und eingeschränkte Transparenz hinsichtlich des Verfahrensganges und der Entscheidungsgründe. Bei der Vorbereitung einer Gnadenentscheidung werden personenbezogene Daten, die als sensibel einzustufen sind, in beträchtlichem Umfange verarbeitet. Der Eingriff in das informationelle Selbstbestimmungsrecht bedarf demnach normenklarer, am Grundsatz der Verhältnismäßigkeit orientierter gesetzlicher Regelungen. Meine Anregungen zum Gesetzentwurf zielten vor allem auf mehr Durchschaubarkeit und Rechtssicherheit für den Betroffenen ab. Im einzelnen:

- Ein Gnadengesuch kann vom Betroffenen eingereicht, aber auch von Amts wegen eingeleitet werden, ohne daß dem Betroffenen dies bekannt wird. Das Gnadenverfahren sollte jedoch nicht gleichsam hinter seinem Rücken und im geheimen durchgeführt werden; er kann nicht als bloßes Objekt staatlichen Handelns angesehen werden. Die Einleitung des Verfahrens muß dem Betroffenen zur Kenntnis gebracht werden; seine Einwilligung sollte in Betracht gezogen werden. Nach der vorgesehenen Regelung würde der Betroffene von der Gnadenentscheidung nichts erfahren, wenn er nicht selber das Gesuch gestellt hat. Er sollte jedoch stets über den Ausgang des Verfahrens informiert werden.

- Es ist vorgesehen, daß die Ermittlungen auf nachgeordnete Behörden übertragen werden können. Dies führt zwangsläufig zu einer Streuung von Informa-

tionen. Angesichts der räumlichen Ausdehnung des Saarlandes und der daraus resultierenden Verwaltungsstruktur ist eine Delegation nicht erforderlich. Die notwendigen Informationen können auch im Wege eines Auskunftsersuchens beschafft werden.

- Der Entwurf bestimmt ferner, daß personenbezogene Daten insoweit verarbeitet werden dürfen, als dies für den Erfolg der Ermittlungen oder der Überwachung unerläßlich ist. Die Festschreibung des Erforderlichkeitsprinzips ist zu begrüßen. Es bleibt jedoch völlig offen, was Ziel und Zweck der Ermittlungen sein soll. Es fehlen Kriterien für die Behörden, an denen sie ihre Entscheidung zu orientieren hat. So wird nicht geregelt, ob für eine Begnadigung eines zu Haft Verurteilten lediglich dessen Verhalten in der Strafvollzugsanstalt von Bedeutung ist oder ob etwa ein mehr oder weniger umfassendes Bild seiner Persönlichkeit erstellt werden muß. Ich halte deshalb die Festlegung materieller Gesichtspunkte für unverzichtbar.

- Der Entwurf gesteht nur ein begrenztes Akteneinsichtsrecht zu. Dieses kann nicht durch den Betroffenen selber, sondern nur durch einen zur Vertretung in Rechtssachen Befugten - also in erster Linie durch einen Rechtsanwalt - ausgeübt werden. Die generelle Verweigerung der persönlichen Akteneinsicht ist nicht gerechtfertigt. Der Betroffene sollte aus eigener Anschauung die Gesichtspunkte zur Kenntnis nehmen können, die die Entscheidung tragen werden. Nicht wenige Betroffene werden in der Lage sein ohne Rechtsbeistand den Akteninhalt zu würdigen. Zum anderen dürfte gerade einem Gefangenen aus finanziellen Gründen die Beauftragung eines Rechtsanwalts Schwierigkeiten bereiten. Im übrigen blieben die Erkenntnisse, die ein Anwalt aus der Akteneinsicht gewinnt, dem Betroffenen vorenthalten.

sicht gewinnen würde, dem Betroffenen ohnehin nicht verborgen.

- Mit Genugtuung habe ich zur Kenntnis genommen, daß nach diesem Gesetzentwurf auch das Gnadenwesen in den Geltungsbereich des Saarländischen Datenschutzgesetzes einbezogen werden soll. Dies habe ich bereits in meinen Stellungnahmen zum Entwurf des Saarländischen Datenschutzgesetzes nicht zuletzt mit Rücksicht auf die Kontrollkompetenz des Landesbeauftragten für Datenschutz gefordert.

3.3 Aufbewahrungsbestimmungen

Die Dauer der Aufbewahrung von Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden richtet sich nach bundeseinheitlichen Aufbewahrungsbestimmungen. Die Fristen betragen zwischen fünf und dreißig Jahren. Bei den Aufbewahrungsbestimmungen handelt es sich um Verwaltungsvorschriften, nicht um Rechtsnormen. Besondere Bedeutung gewinnen diese Regelungen vor dem Hintergrund, daß zunehmend im Bereich der Justiz automatische Datenverarbeitungssysteme eingeführt werden. Auch die Aufbewahrung von Akten greift in das informationelle Selbstbestimmungsrecht der in den Vorgängen erfaßten Personen ein. Einschränkungen dieses Grundrechts sind nur im überwiegenden Allgemeininteresse und aufgrund einer verfassungsgemäßen, gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entspricht, zulässig. Ich habe deshalb gegenüber dem Ministerium der Justiz die Auffassung vertreten, daß Aufbewahrungsbestimmungen auf eine gesetzliche Grundlage zu stellen sind.
Unabhängig von der Frage der Normenqualität sind jedoch die Aufbewahrungsbestimmungen auch inhaltlich nach Maßgabe des Volkszählungsurteils zu überarbeiten.

Wegen der Sensibilität der Daten ist dabei besonderes Augenmerk auf die Strafverfahrensakten zu richten. Wenn auch zum jetzigen Zeitpunkt eine abschließende Bewertung nicht vorgenommen werden kann, habe ich einige besonders problematische Punkte angesprochen.
Es ist fraglich, ob der Beginn der Aufbewahrungsfrist an die Weglegung der Akten zu knüpfen ist. Dies ist der spätestmöglichste Zeitpunkt im Verfahren. Es sollte geprüft werden, ob nicht auf den Tatzeitpunkt oder den Eingang bei der Staatsanwaltschaft abgestellt werden kann.
Außerdem muß diskutiert werden, ob nicht der Ausgang des Verfahrens einen stärkeren Einfluß auf die Aufbewahrungsfrist haben soll. So hat es in bestimmten Fällen keine Auswirkungen, ob der Angeklagte zu einer erheblichen Geldstrafe verurteilt oder freigesprochen worden ist.

Das Ministerium der Justiz hat mir mitgeteilt, daß es mit den anderen Landesjustizverwaltungen Verbindung mit dem Ziel einer gemeinsamen Erörterung aufgenommen habe. Eine Stellungnahme in der Sache stand zum Zeitpunkt des Redaktionsschlusses noch aus.

3.4 Zahlungsabwicklungen bei Auflagen zugunsten gemeinnütziger Organisationen

Strafverfahren enden nicht stets damit, daß der Täter zu Geld- oder Freiheitsstrafe verurteilt oder ein Strafbefehl erlassen wird. Bei geringer Schuld kann dem Betroffenen eine Geldzahlung auferlegt und das Verfahren vorläufig eingestellt werden (§ 153 a StPO, § 56 b Abs. 2 Nr. 2 StGB).

Besonders häufig wird die Zahlung eines Geldbetrages zugunsten einer gemeinnützigen Einrichtung auferlegt. Bei der Abwicklung ergeben sich datenschutzrechtliche Probleme, da der entsprechenden Organisation Daten der

Betroffenen zur Kenntnis gelangen. Damit wird auch bekannt, daß ein Ermittlungsverfahren stattgefunden und der Betroffene sich strafbar gemacht hat.

Im Saarland stellt sich die Praxis bei der Zahlungsabwicklung folgendermaßen dar: Überwiegend erhält der Betroffene vorgefertigte Überweisungsträger. Ihm wird zur Pflicht gemacht, den quittierten Einzahlungsbeleg zu den Akten zu reichen. Zum Teil wird auch so verfahren, daß bei der Einrichtung nachgefragt oder diese von vornherein über die Zahlungsauflage informiert und die Erfüllung im Benehmen mit dieser überwacht wird.

Die Praxis genügt datenschutzrechtlichen Anforderungen nicht. Unabhängig davon, ob sich der Betroffene unter dem Druck der Situation selbst gegenüber dem Zahlungsempfänger offenbart oder diesem Informationen über den Betroffenen durch die Justiz übermittelt werden, bestehen erhebliche Zweifel, ob sich die mit der Zahlung verbundene Übermittlung personenbezogener Daten auf einer zureichenden Rechtsgrundlage vollzieht.

Daß die gemeinnützige Organisation Kenntnis von persönlichen Verhältnissen des Betroffenen erlangt, muß nach heutigem Grundrechtsverständnis als zusätzliche Sanktion von nicht geringem Gewicht angesehen werden, die über das eigentliche vom Gesetzgeber verfolgte Ziel hinausgeht, dem Betroffenen ein finanzielles Opfer aufzuerlegen. Der Zahlungsauflage wohnt nicht gleichzeitig eine Prangerfunktion inne. Sie hat keinen Strafcharakter und soll die Resozialisierung des Betroffenen erleichtern, die aber gerade durch die Offenlegung der Tatsache verhindert werden kann, daß gegen den Betroffenen ermittelt wurde und daß wenigstens "zureichende tatsächliche Anhaltspunkte" für eine Straftat vorlagen. Der in dieser Offenbarung liegende Eingriff in das Grundrecht auf informationelle Selbstbestimmung kann nicht auf die geltenden Bestimmungen (§

153 a StPO, § 56 b StGB) gestützt werden, da es insoweit an der nötigen Normenklarheit fehlt. Mag im Falle der Erbringung gemeinnütziger Leistungen - etwa Arbeit in einem Tierheim oder Krankenhaus - die Offenlegung persönlicher Verhältnisse unausweichlich mit dem Vollzug verbunden sein. Ein zwingender Bestandteil der Geldzahlung ist die Offenbarung persönlicher Verhältnisse jedenfalls nicht, so daß diese zusätzliche Belastung des Betroffenen jedenfalls einer ausdrücklichen gesetzlichen Regelung bedarf, die derzeit nicht vorliegt.

Auch die Zustimmung des Betroffenen (§ 153 a StPO) kann wegen der in der Datenübermittlung liegenden zusätzlichen Belastung die Offenbarung gegenüber dem Zahlungsempfänger nicht rechtfertigen. Der Betroffene befindet sich in einem faktischen Zwang, weil er im Falle seiner Verweigerung mit seiner Strafe und ggf. Eintragung in das Strafregister rechnen muß.

Aus meiner Sicht entspricht die sogenannte "Gerichtskassenlösung" den Anforderungen des Datenschutzes. Danach würde der Pflichtige den Betrag an die Gerichtskasse überweisen oder einzahlen, die ihn dann im Einzelfall oder in regelmäßigen Abständen anonymisiert an die begünstigten Organisationen weiterleitet.

Eine Verbesserung gegenüber dem jetzigen Stand könnte auch schon erzielt werden, wenn die Zahlungsabwicklung ohne Angabe des Namens erfolgen könnte. In Betracht käme ein Durchschreibeverfahren, bei dem der Name auf dem für den Empfänger bestimmten Überweisungsträger nicht erscheint. Die Überwachung des Zahlungseinganges könnte durch Code-Wort oder Schlüsselzahl und anonymisierte Listen gewährleistet werden.

Bei Redaktionsschluß war die Diskussion mit dem Ministerium der Justiz noch nicht abgeschlossen.

4. Planung und Umwelt

4.1 Freier Zugang zu den Informationen über die Umwelt

4.1.1 EG-Richtlinie (90/313 EWG)

Mit seiner Richtlinie vom 7. Juni 1990 hat der Rat der Europäischen Gemeinschaft die Mitgliedstaaten verpflichtet, allen natürlichen und juristischen Personen - ohne Nacheis eines Interesses - Informationen über die Umwelt zur Verfügung zu stellen (ABl. der EG L 158 vom 23.06.1990). Die Ausnahmeregelung des Artikels 3 Abs. 2 läßt zwar zu, den Zugang zu derartigen Informationen abzulehnen, wenn u.a. "Geschäfts- und Betriebsgeheimnisse" oder die "Vertraulichkeit personenbezogener Daten und/oder Akten" berührt werden. Insgesamt wird jedoch der Grundsatz der Informationsfreiheit - jedenfalls für Behördeninformationen über die Umwelt - wesentlich gestärkt. Damit wird auch ein wesentlicher Beitrag zu einem Grundanliegen des Datenschutzes geleistet, das Verwaltungshandeln transparenter werden zu lassen. Mit der Ausgestaltung zu einem Jedermann-Recht, das nicht an dem nur individuellen Rechtsschutz anknüpft, wird eine aus dem Demokratieprinzip herzuleitende Öffentlichkeit und Kommunikation auf dem Umweltsektor verwirklicht.

Das Recht auf Informationsfreiheit steht allerdings in einem Spannungsverhältnis zum Grundrecht auf "informationelle Selbstbestimmung". Der Bürger hat auch einen Anspruch auf Schutz seiner personenbezogenen Daten, die mit Informationen über den Zustand der Umwelt verbunden sein können. Informationsfreiheit und Datenschutz bilden dabei jedoch keinen unauflösbaren Gegensatz; beide Positionen müssen aber zugleich optimal zur Geltung kommen. Zu diesem Prinzip der "praktischen Konkordanz" haben sich die Datenschutzbeauftragten des

Bundes und der Länder in ihrer Entschließung vom 16./17.02.1993 ausdrücklich bekannt (Anlage 4).

4.1.2 Umsetzung der EG-Richtlinie (90/313 EWG) in nationales Recht

Die Mitgliedstaaten sind ihrer Verpflichtung nach Art. 9 Abs. 1 der EG-Richtlinie, spätestens bis zum 31. Dezember 1992 Rechts- und Verwaltungsvorschriften zu ihrer innerstaatlichen Umsetzung zu erlassen, nicht nachgekommen. Ein Referentenentwurf des Bundes liegt zwar vor; er ist jedoch bislang nicht in das Gesetzgebungsverfahren eingebracht worden. Das Bundesumweltministerium ist der Auffassung, daß wesentliche Teile der EG-Richtlinie unmittelbar gelten. Einige Bundesländer - so das Saarland (Erlaß vom 07.06.1990) - haben zur Ausführung Verwaltungsanordnungen getroffen. Ich hielte allerdings eine Vorgehensweise für problematisch, die auf eine gesetzliche, innerstaatliche Ermächtigung verzichtet.

Nach Art. 189 EWG- Vertrag ist eine Richtlinie im Gegensatz zur Verordnung grundsätzlich als zweistufiger Rechtsakt konzipiert; die Mitgliedstaaten haben selbst die Umsetzung in nationales Recht zu vollziehen. Nur in Ausnahmefällen ist eine unmittelbare Wirkung von EG-Richtlinien möglich und in der Rechtsprechung des Europäischen Gerichtshofs anerkannt (EuGHE 1982, 53 ff.). Voraussetzung ist jedoch, daß die Vorschrift so "perfekt regelungsintensiv ausgestaltet ist, daß die Umsetzung ... sich mehr oder weniger in einem Abschreiben des Richtlinieninhaltes erschöpfen müßte" (Oppermann, Europarecht, München 1991, Rdnr. 466). Von einer "unbedingten und hinreichend genauen" Ausformulierung kann jedoch jedenfalls hinsichtlich der Einschränkungen des Informationszuganges mit Rücksicht auf das informationelle Selbstbestimmungsrecht keine Rede sein (Art. 3 Abs. 2 EG-Richtlinie). Wie das

Spannungsverhältnis zwischen dem Anspruch auf Informationsfreiheit und dem Grundrecht auf Datenschutz aufgelöst werden soll, ist nicht ersichtlich, wenn die Richtlinie den Mitgliedstaaten etwa lediglich die Möglichkeit einräumt, den Informationszugang abzulehnen, wenn

> "die Vertraulichkeit personenbezogener und/oder Akten"

berührt ist (Art. 3 Abs. 2, 5. Anstrich). Nicht einmal die insoweit notwendige Güter- und Interessenabwägung folgt aus einer solchen Formulierung, so daß unter Zugrundelegung lediglich der EG-Richtlinie weit über den normalen Auslegungsbedarf hinausgehende wesentliche Grundlagen für eine Rechtsanwendung fehlen. Ein Eingriff in das informationelle Selbstbestimmungsrecht ist jedoch nur im überwiegenden Allgemeininteresse und auf der Grundlage eines Gesetzes zulässig, das den Anforderungen der Normenklarheit genügt (Art. 2 Saarl. Verfassung; BVerfGE 65, 1, 43). Verwaltungsvorschriften zur Umsetzung der EG-Richtlinie reichen jedenfalls nicht aus. Der Zustand kann allenfalls übergangsweise hingenommen werden. Die Konferenz der Datenschutzbeauftragten hält es deshalb für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes zügig zum Abschluß zu bringen (Anlage 4).

Entgegen § 18 Abs. 1 SDSG ist der Landesbeauftragte für Datenschutz vor Inkrafttreten des Erlasses zur Umsetzung der EG-Richtlinien im Saarland nicht beteiligt worden. Abgesehen von der mangelnden Rechtsnormqualität ergab die nachträgliche Überprüfung jedoch, daß den Anforderungen des freien Informationszuganges und des Datenschutzes jedenfalls in folgenden Punkten Rechnung getragen wurde:

- Jedermann hat Anspruch auf freien Zugang zu den bei einer Behörde vorhandenen Informationen über die Umwelt. Des Nachweises eines besonderen Informationsinteresses bedarf es nicht.

- Der Anspruch auf Informationszugang ist grundsätzlich ausgeschlossen oder beschränkt, soweit personenbezogene Daten oder Betriebs- oder Geschäftsgeheimnisse offenbart werden. Die Offenbarung ist im Einzelfall zulässig, wenn keine schutzwürdigen Belange der Betroffenen entgegenstehen; die öffentlichen und privaten Interessen sind gegeneinander abzuwägen. Hierbei zu beachtende Gesichtspunkte werden konkret genannt.

- Werden personenbezogene Daten offenbart, sind die Rechte der Betroffenen -- vor allem ihre Verfahrensrechte - zu berücksichtigen; die Betroffenen sind vor der Offenbarung anzuhören.

- Informationen, die von Privaten freiwillig - ohne gesetzliche Verpflichtung - geliefert werden, dürfen nur mit deren Zustimmung zugänglich gemacht werden. Niemand soll öffentlicher Anfeindung ausgesetzt werden, der im Interesse des Umweltschutzes unter Hintansetzung seiner eigenen Interessen, womöglich mit nachteiligen Folgen für ihn selbst, Informationen den Behörden übermittelt.

Mängel mußte ich in folgender Hinsicht feststellen:

- Der Informationszugang ist während des "laufenden verwaltungsbehördlichen Verfahrens" generell oder dann ausgeschlossen, wenn die "Vertraulichkeit der Beratung von Behörden" beeinträchtigt werden kann. Die Möglichkeit einer Beeinträchtigung allein sollte dem Anspruch nicht entgegenstehen. Im übrigen sollte der Ausschluß wegen öffentlicher Belange

zugunsten einer Güter- und Interessenabwägung aufgelöst werden. Eine völlige Verweigerung sollte nur zugelassen werden, wenn die öffentlichen Belange überwiegen. Dies gilt auch für "verwaltungsinterne Mitteilungen"; der Innenbereich der Behörde sollte nach einheitlichen Grundsätzen behandelt werden.

- Andererseits ist der Erlaß zu großzügig, wenn es um Informationen aus "noch nicht abgeschlossenen Schriftstücken" oder um "nicht aufbereitete Daten" handelt. Teilinformationen oder solche, die gerade bearbeitet werden, geben ein unzutreffendes Bild. Zur Vorbereitung von Umweltverträglichkeitsprüfungen, zur Erstellung von Raumordnungs- und Altlastenkataster werden - zunehmend edv-gestützt - Datensammlungen geführt, die wegen der Raum-, Produkt-, Projekt- oder Verhaltensbezogenheit personenbezogene Daten enthalten (Taeger CR 1991, 681 ff.). Die Risiken werden zukünftig in eklatanter Weise zutage treten, wenn die geplanten automatisierten Umweltinformationssysteme vorhanden sein werden. Die Gefahr von Fehleinschätzungen aufgrund übermittelter Daten aus solchen Sammlungen werden dann noch zunehmen, so daß auch der Vorbehalt eines Haftungsausschlusses nicht befriedigen kann. Die Behörden können sich auf diese Weise nicht aus der Verantwortung für die von ihr vorgehaltenen und übermittelten Informationen stehlen. Es muß klargestellt werden, daß die weitergegebenen Informationen an sich richtig und in ihrem tatsächlichen Wahrheitsgehalt abgesichert sind. Nicht aufbereitete Informationen dürfen jedenfalls nicht übermittelt werden.

- Besonders gravierend ist der Mangel einer grundsätzlichen Festlegung, daß kein Informationsanspruch auf personenbezogene Daten besteht, wenn anonymisierte Daten - etwa Strukturdaten über den Zustand von Luft, Wasser, Boden, Klima - das Informations-

interesse abdecken. Informationen sind deshalb grundsätzlich in anonymisierter Form zu geben.

- Mit der aus dem Demokratieprinzip herzuleitenden Öffentlichkeit und Kommunikation im Umweltsektor ist die Belastung des Auskunftsbegehrenden mit dem Kostenrisiko im Fall der Ablehnung des Anspruchs nicht vereinbar. Gerade die Auseinandersetzung mit dem informationellen Selbstbestimmungsrecht Dritter, das komplizierte Abwägungsentscheidungen zur Folge haben kann, erschwert zu Recht den Informationszugang; zusätzliche Hürden unter Kostengesichtspunkten sollten nicht aufgebaut werden.

- Unklar war, was "unter Betriebsgeheimnisse oder Geschäftsgeheimnisse" zu verstehen ist, so daß Unsicherheiten über den Umfang des Informationszugangs auftreten müssen. Damit im Zusammenhang stehen Urheberrechte und andere dem geistigen Eigentum gleichkommende Rechte, die in vermögensrechtlicher Hinsicht der verfassungsrechtlichen Eigentumsschutzgarantie unterliegen. Diese Rechte bedürfen - wie auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstrichen hat - einer verfahrensrechtlichen Absicherung. Ein bloßes Anhörrecht dürfte insoweit nicht ausreichen. Besteht Unklarheit darüber, ob Daten als Betriebs- oder Geschäftsgeheimnisse anzusehen sind und kann hierüber eine Einigung mit dem Unternehmen nicht erzielt werden, ist über den Informationszugang in einem rechtsmittelfähigen Bescheid zu entscheiden; die Herausgabe der Daten ist bis zur Klärung dieser Frage (Bestandskraft des Bescheides) zurückzustellen. Den betroffenen Unternehmen sollte jedenfalls die Möglichkeit zu einer offensiven Informationspolitik gegeben werden. In diesem Zusammenhang ist an das Genehigungsverfahren nach dem Immissionsschutzgesetz zu erinnern, das die Veröffentlichung

von Einzelangaben untersagt, wenn aus ihnen Rückschlüsse auf Betriebs- oder Geschäftsgeheimnisse gezogen werden können (§ 27 Abs. 3).

Die mit dem freien Zugang zu Umweltinformationen verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht bedürfen einer gesetzlichen Ermächtigung (Art. 2 Saarländische Verfassung). Deshalb ist die alsbaldige Verabschiedung des Umweltinformationsgesetzes geboten. Da das Inkrafttreten gesetzlicher Normen nicht abzusehen ist und die Möglichkeiten des Landes, auf eine Beschleunigung des Gesetzgebungsverfahrens hinzuwirken, gering sind, habe ich eine Nachbesserung des Erlasses im Interesse einer übergangsweisen verfassungskonformen Regelung gefordert.

4.2 Landesplanungsgesetz

Zum Gesetzentwurf, mit dem hinfort die Landesplanung auf eine neue Grundlage gestellt werden soll, habe ich Stellung genommen. Die Landesentwicklungspläne, die die Ziele der Landesplanung und der Raumordnung festlegen, können auch für einzelne "raumbedeutsame Planungen und Maßnahmen" (§ 6 Abs. 1 Satz 2) verbindlich sein. Auf meine Anregung hin stellt der Entwurf klar, daß die "textliche und zeichnerische Darstellung der Landesentwicklungspläne" sowie die Erläuterungsberichte keine personenbezogene Daten enthalten dürfen. Ferner wurde auf eine Darstellung der "altindustriellen Standorte" verzichtet, weil hiermit Feststellungen für mehr oder weniger bestimmte Gebiete und Grundstücke verbunden sind, die die Eigentümer belasten, ohne daß die Voraussetzungen einer solchen Bewertung bisher geregelt sind. Somit sind zwar die Ergebnisse der Landesplanung allgemeinverbindlich, ohne daß jedoch allein aufgrund der Darstellung im Landesentwicklungsplan unmittelbar auf Personen zurückgeschlossen werden könnte. Dies ist deshalb wichtig, weil zur

Erstellung eines Landesentwicklungsplanes - insbesondere im Rahmen der Raumordnungsverfahren - personenbezogene Informationen erhoben und verarbeitet werden müssen, um eine verläßliche Grundlage für die Landesplanung zu gewinnen. Diese Informationen werden jedoch durch die Darstellung im Landesentwicklungsplan jedenfalls nicht personenbezogen offengelegt.

Gerade im Raumordnungsverfahren können personenbezogene Daten anfallen. In diesem Zusammenhang sind Umweltverträglichkeitsprüfungen durchzuführen, deren Ergebnisse regelmäßig bestimmten Grundstücken zugeordnet werden können; daraus können sich - etwa bei kontaminationsverdächtigen Flächen - Auswirkungen für die Grundstückseigentümer ergeben. Ich habe keinen Zweifel daran gelassen, daß als Grundlage für die Landesplanung ein Bodenschutz- und Altlastengesetz unerläßlich ist, um sicherzustellen, daß die Informationsgewinnung in verfassungskonformer Weise durchgeführt wird.

Ich habe Vorschläge unterbreitet, die bereits im Rahmen der Landesplanung, insbesondere im Raumordnungsverfahren, die verfahrensrechtlichen Voraussetzungen der Datenerhebung und -verarbeitung liefern sollten. Der Entwurf beschränkt sich indessen auf die Festschreibung der "Erforderlichkeit zur Aufgabenwahrnehmung" (§ 17 Abs. 1), bietet also zur Steuerung der Informationserhebung und -verarbeitung nicht mehr an als im Saarländischen Datenschutzgesetz geregelt ist. Der Normgehalt des Saarländischen Datenschutzgesetzes vermag jedoch den bereichsspezifischen Anforderungen der Landesplanung und der Raumordnungsverfahren nicht gerecht zu werden. Auch die Vorschrift zur Übermittlung personenbezogener Informationen ist nicht befriedigend (§ 17 Abs. 2). Der Entwurf schreibt die Geheimhaltung von Auskünften Privater im Raumordnungsverfahren vor (§ 15 Abs. 2 letzter Satz). Hieraus und aus der Tatsache, daß die Landesentwicklungspläne selbst

keine personenbezogenen Informationen enthalten, muß im Interesse der schutzwürdigen Belange der Betroffenen der Schluß gezogen werden, daß öffentliche Behörden und Stellen personenbezogene Daten nicht erhalten dürfen. Zumindest wäre eine restriktivere Regelung für den Datentransfer an öffentliche Stellen geboten gewesen, um der verfassungsrechtlich begründeten Zweckbindung Rechnung zu tragen.

Ein Regelungsdefizit ist auch im Hinblick auf das Raumordnungskataster festzustellen (§ 16). Ich hatte gefordert, daß der Inhalt des Raumordnungskatasters, in das Behörden und öffentliche Planungsträger Einsicht nehmen können, im Gesetz oder aufgrund einer Ermächtigung im Gesetz durch Rechtsverordnung im einzelnen festzulegen ist. In einer Besprechung ist sogar angeklungen, daß in Ergänzung zum Raumordnungskataster eine automatisierte Datenhaltung vorgesehen ist. Zweck und inhaltlicher Umfang des Katasters und der automatisierten Datei hätten möglichst konkret durch Gesetz oder aufgrund des Gesetzes bestimmt werden müssen.

Positiv bewerte ich die Regelung für das Raumordnungsverfahren, daß die Unternehmen zur Preisgabe von Geschäfts- und Betriebsgeheimnissen nur verpflichtet sind, soweit dies für das Verfahren unerläßlich ist. Das Unternehmen ist darauf hinzuweisen. Informationen dieser Art dürfen nicht weitergegeben oder veröffentlicht werden (§ 13 Abs. 5).

Die Diskussion um die EG-Richtlinie über den freien Zugang zu Umweltinformationen und deren Umsetzung in die Praxis haben gezeigt, daß dem Persönlichkeitsrecht durch verfahrensrechtliche Regelungen im Interesse der schutzwürdigen Belange der Betroffenen Rechnung getragen werden muß. Insbesondere das Raumordnungsverfahren genügt den Anforderungen nicht.

4.3 Altstandortekataster

Über das im Rahmen eines Forschungsprojekts erstellte Verzeichnis kontaminationsverdächtiger Flächen des Stadtverbandes Saarbrücken berichtete ich bereits in meinem 12. Tätigkeitsbericht (Tz. 9.2). Datenschutzrelevant sind derartige Verzeichnisse und Kataster, weil sie grundstücksbezogen sind und deshalb regelmäßig mit nicht unverhältnismäßig hohem Aufwand den Eigentümern zugeordnet werden können. Bei den erfaßten Flächen besteht ein mehr oder weniger begründeter Kontaminationsverdacht, der aber wegen der noch ausstehenden Bewertung unsicher bleibt und demnach auch das Ausmaß einer eventuellen Nutzungsbeschränkung der betroffenen Grundstücke nicht endgültig eingeschätzt werden kann. Hierin liegt eine nicht unerhebliche Beeinträchtigung der betroffenen Eigentümer, weil der Umfang der Wertminderung der Grundstücke endgültig nicht bemessen werden kann. Ich habe das Ministerium für Umwelt seit 1990 immer wieder darauf hingewiesen, daß der auch nur übergangsweise, eingeschränkte Betrieb eines solchen Katasters ohne normenklare, bereichsspezifische gesetzliche Grundlage voraussetzt, daß eine solche überhaupt in absehbarer Zeit angestrebt wird. Der Entwurf eines Bodenschutzgesetzes, in dem auch die Voraussetzungen eines Bodenbelastungskatasters im einzelnen geregelt werden soll, wurde bereits 1991 erarbeitet. Ein Referentenentwurf soll inzwischen vorliegen, der bisher aber noch nicht in das Gesetzgebungsverfahren eingebracht wurde. Wie aus der Ressortstellungnahme zu entnehmen ist, sieht der Entwurf ausschließlich eine zentrale Datenerfassung und Katasterführung beim Landesamt für Umweltschutz vor und verzichtet im Hinblick auf den "datenschutzrechtlich überaus sensiblen Bereich" bewußt auf eine dezentrale Lösung. Für das Verzeichnis kontaminationsverdächtiger Flächen des Stadtverbandes Saarbrücken sehe ich deshalb keine Rechtsgrundlage mehr. Konsequenterweise

müßte der Datenbestand vernichtet oder in das Zentralregister überführt werden.

Zwischenzeitlich führte das Landesamt für Umweltschutz Erhebungen über Altstandorte im Saarland durch; die Erfassung im Saarpfalzkreis, im Stadtverband, in den Landkreisen Saarlouis, Merzig-Wadern und St. Wendel soll im Jahre 1992 bereits abgeschlossen sein; für den Landkreis Neunkirchen wurden in diesem Zeitraum die Erhebungsarbeiten vergeben. Mit der Erhebung sind private Firmen beauftragt. Diese Vorgänge weisen darauf hin, daß das Verzeichnis des Stadtverbandes Saarbrücken für die Zwecke des zentralen Katasters offensichtlich nicht genutzt werden soll. Um so mehr ist nunmehr eine Entscheidung im Hinblick auf den dezentralen kommunalen Datenbestand erforderlich.

Die neuerlichen Erhebungen geben aber auch in anderer Hinsicht Anlaß zu Bedenken. Bislang war die übergangsweise Führung bereits bestehender Kataster und Datensammlungen von Altablagerungen bis zum Inkrafttreten gesetzlicher Regelung diskutiert worden. Inzwischen wurden trotz mangelnder Rechtsgrundlagen neue Datenbestände über kontaminierte oder möglicherweise altlastenverdächtige Grundstücke angelegt. Trotz der Dringlichkeit, das Altlastenproblem aufzuarbeiten, ist ein solches Vorgehen angesichts des Zeitablaufs, seit dem die Rechtsgrundlagenproblematik mit dem Umweltministerium diskutiert wird, im Hinblick auf die Gefahr der Beeinträchtigung von Rechten Dritter bedenklich.

Der Mangel einer Rechtsgrundlage hat regelmäßig zur Folge, daß die Maßnahme als verfassungswidrig "aufzuheben" ist. Das würde bedeuten, daß die Datensammlung zu vernichten wäre. Eine Regelungslücke hat das Bundesverfassungsgericht unter bestimmten Voraussetzungen ausnahmsweise hingenommen, um dem Gesetzgeber eine Übergangsfrist einzuräumen (BVerfGE 41, 251, 267). Bis zur

Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber reduzieren sich die Befugnisse der Behörden und Gerichte auf das, was im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Betriebes unerläßlich ist. Somit konnten die Grundsätze des "Übergangsbonus" allenfalls für bereits bestehende Kataster zur Anwendung kommen. Die Anlegung neuer Datenbestände, Verzeichnisse und Kataster, die in verfassungsrechtlich geschützte Rechtspositionen - hier das Eigentum - eingreifen, begegnet allergrößten Bedenken. Es ist keine Zeit zu versäumen. Die Datensammlung der Altstandorte bedarf einer gesetzlichen Regelung.

4.4 Umweltdatenerhebung durch Befragung

Der Kommunale Abfallentsorgungsverband (KABV) hat eine privatrechtlich organisierte Ingenieurgemeinschaft mit einem umfangreichen Untersuchungsprogramm über Geruchsbelästigungen der Bevölkerung im Umfeld einer Mülldeponie beauftragt.

Der KABV hat aus seinem Datenbestand der Mülltonnenbesitzer Adressen von Bürgern eines etwa 220 Haushalte umfassenden Ortsteils einer Gemeinde dem Ingenieurbüro zur Durchführung einer Befragung als Grundlage für ein Gutachten zur Verfügung gestellt. Dem persönlichen Anschreiben des Büros an die Bürger war ein Fragebogen beigefügt, um eine repräsentative Gruppe von Einwohnern zu gewinnen, die bereit war, entweder Geruchsmessungen oder auch Tagebücher über Geruchsbelästigungen zu führen. Dazu wurde ein Fragebogen mitversandt, der eine Fülle personenbezogener Daten enthielt, auf deren freiwillige Angabe nicht in unmißverständlicher Weise hingewiesen wurde. Gefragt wurde u.a. nach Familienstand, Alter, Anzahl der Kinder, Beruf, Freizeitaktivitäten. Die Abfrage dieser Informationen sollte

eine repräsentative Auswahl der zur Mitwirkung bereiten Anlieger der Mülldeponie ermöglichen.

Den Fall habe ich auf die Beschwerde mehrerer Einwohner hin eingehend überprüft. Es hat sich gezeigt, daß der Fragebogen personenbezogene Angaben enthielt, die für den Zweck der Untersuchung nicht benötigt wurden. Zur Rückantwort war ein als Drucksache ausgewiesener - mithin nicht zu verschließender - Briefumschlag vorgesehen.
Auf meine Veranlassung hin wurde die Aktion auf der Grundlage der zunächst verwendeten Formulare gestoppt. Die Adressenlisten des KABV und die Fragebögen wurden auf meiner Dienststelle vernichtet. Seitens der Ingenieurgemeinschaft wurde zugesagt, daß man sich mit einer Postwurfsendung begnüge. Der Rücklauf sollte selbstverständlich in einem geschlossenen Schreiben erfolgen.
Im Fragebogen waren folgende Schwachpunkte auszuräumen:

- Auf die Freiwilligkeit der Teilnahme an der Befragung sollte in unzweideutiger und optisch hervorgehobener Form hingewiesen werden.

- Eine förmliche Einwilligungserklärung mit Unterschrift des/der Befragten als Rechtsgrundlage für die Informationserhebung und Verarbeitung war erforderlich.

- Der Umfang der Erhebung war auf das für die Untersuchung erforderliche Maß zu reduzieren.

- Zweck der Untersuchung und die Vorgehensweise bei der Informationserhebung und -verarbeitung waren in einem Begleitpapier und im Fragebogen näher zu beschreiben. Insbesondere war der Bürger auf folgendes hinzuweisen:

* keine Übermittlung personenbezogener Daten an Dritte

* keine automatisierte Verarbeitung

* sofortige Löschung personenbezogener Daten, wenn sie für die Zwecke der Untersuchung nicht mehr benötigt werden.

Der mir zuletzt vorgelegte Fragebogen hat diesen Forderungen Rechnung getragen.

Festzuhalten ist allerdings, daß der KABV als Auftraggeber und damit als die nach § 5 SDSG verantwortliche öffentliche Stelle für die Auftragsdatenverarbeitung die Beachtung datenschutzrechtlicher Bestimmungen durch das Privatunternehmen nicht von vornherein sichergestellt hatte. Es war überdies nicht zulässig, daß der KABV die Anschriften der Bürger dem Privatunternehmer zur Verfügung gestellt hat, weil die Kontaktaufnahme mit den zu befragenden per Postwurfsendung erfolgen konnte und deshalb Adressen nicht benötigt wurden.

5. Steuern und Finanzen

5.1 Finanzämter

Im Berichtszeitraum hat sich ein Untersuchungsausschuß des Landtages mit Fragen des Steuervollzugs im Saarland beschäftigt. Einem Pressebericht habe ich entnommen, daß die Steuerakten eines freiberuflich Tätigen einer Fraktion im Landtag "zugespielt" worden waren. Aus dieser Formulierung konnte geschlossen werden, daß dem Steuergeheimnis unterliegende Unterlagen, die der Untersuchungsausschuß nicht angefordert hatte, unbefugten Dritten offenbart worden waren. Der Minister der Finanzen hat deshalb Strafanzeige wegen Verdachts des Bruchs des Steuergeheimnisses gestellt.

Bereits in meinem 12. Tätigkeitsbericht (Tz. 9.3) habe ich über die mangelhafte Aufbewahrung von Steuerakten in einem Finanzamt berichtet. Steuerunterlagen waren in nicht verschließbaren Holzschränken außerhalb der Diensträume, auf Fluren aufbewahrt.

Beide Vorgänge gaben mir Veranlassung, das Problem der Datensicherung in den Finanzbehörden aufzugreifen. Anläßlich der umfassenden Prüfung eines Finanzamtes wurden Kontrollen in allen Geschäftsbereichen dieser Behörde durchgeführt: Geschäftsstelle, Finanzkasse, Kraftfahrzeugsteuer, Vollstreckung, Arbeitnehmer, Arbeitgeber, Prämien, Rechtsbehelfe, Veranlagung und Bewertung. Gegenstand der Prüfung waren die innerbehördliche Organisation und neben konventioneller insbesondere die automatisierte Datenverarbeitung. Sie hatte folgendes Ergebnis:

5.1.1 Organisation und konventionelle Informationsverarbeitung

- Im betreffenden Finanzamt ist eine Schließanlage installiert. Jeder Bedienstete verfügt über einen Schlüssel, den er stets mit sich führen kann. Bei Abwesenheit sind so die Diensträume leicht verschlossen zu halten. Dies ist eine empfehlenswerte Maßnahme, um den Zugang Unbefugter zu den Diensträumen zu verhindern.

- Die Bediensteten sind angewiesen, sämtliches Papier getrennt von anderem Abfall im Büro zu sammeln. Dieses wird vom Reinigungsdienst in Plastiksäcken zusammengetragen und im Keller abgestellt, wo es vom Hausmeister in einer Zerkleinerungsanlage zerschnitten und anschließend verpreßt wird. Beim Prüfbesuch fanden sich in einer Toilette sowie im Keller Säcke gefüllt mit Papierabfall, die leicht zugänglich waren.
Auf einem Tisch im Keller lagen Altakten, die von einer Aussonderungsaktion übrig geblieben waren.
Ich habe gefordert, daß bei der Aufbewahrung und Entsorgung von Papierabfall und ausgesonderten Altakten in entsprechenden Anweisungen die besonderen Anforderungen an die Vernichtung von personenbezogenem Material stärker zum Ausdruck kommen müssen, um so die Einhaltung des Steuergeheimnisses auch in dieser Verarbeitungsphase zu gewährleisten.
Auf die Richtlinie des Ministeriums des Innern zur Vernichtung von Schriftgut und sonstigen Datenträgern vom 09.01.1989 habe ich besonders hingewiesen.

- In einem zentralen Archiv werden alle Akten, die in den Sachgebieten nicht mehr stets vorgehalten werden müssen, abgelegt. Jeder Bedienstete hat ohne weiteres Zugang zu diesem Archiv und Zugriff auf die dort vorhandenen Akten. Damit ist nicht gewähr-

leistet, daß jeder nur im Rahmen seiner Zuständigkeit Kenntnis vom Akteninhalt nehmen kann. Ich habe gefordert, unbefugte Zugriffe durch technisch-organisatorische Maßnahmen auszuschließen, wie etwa die Bestellung eines Archivverwalters oder nach Sachbereichen getrennte Aufbewahrung der jeweiligen Akten mit Zugang nur für die zuständigen Bediensteten.

- Da das Finanzamt über keinen Botendienst verfügt, werden die Vorgänge über die Poststelle verteilt. Dafür stehen offene Fächer für die einzelnen Sachbereiche zur Verfügung. Diese holen dort ihre Sachen ab und sortieren Vorgänge für andere Stellen im Hause ein. Die Poststelle ist mit zwei Bediensteten besetzt, von denen einer zum Zeitpunkt des Besuchs anwesend war.
  Hier habe ich gefordert, daß auch bei der Poststelle sichergestellt sein muß, daß Bedienstete nur auf die Vorgänge zugreifen können, die in ihren Zuständigkeitsbereich fallen. Es ist deshalb wenigstens dafür Sorge zu tragen, daß der Zugang zur Poststelle nur dann möglich ist, wenn die Poststelle besetzt ist, um eine Überwachung des Zugriffs auf die nach Zuständigkeitsbereichen geordneten Postfächer zu gewährleisten.

- Die Aufbewahrung von Steuerakten hat nicht in allen Bereichen den Anforderungen entsprochen (Verschluß der Schränke außerhalb der Dienstzeit; Aufbewahrung von Akten in Schränken außerhalb der Diensträume).
  In verschiedenen Bereichen mußte ich feststellen, daß die in der Finanzverwaltung geltenden Aufbewahrungsbestimmungen nicht beachtet wurden.

Unabhängig von der Querschnittsprüfung in einem Finanzamt habe ich das Ministerium der Finanzen um Stellungnahme zu den allgemeinen, organisatorischen Maßnahmen

hinsichtlich der konventionellen Datenverarbeitung, insbesondere in Akten, gebeten.

Die Geschäftsordnung für die Finanzämter sieht bereits jetzt vor, daß die Akten durch geeignete Maßnahmen - insbesondere außerhalb der Dienststunden - vor einer Einsichtnahme durch Unbefugte zu schützen sind. Mein Vorstoß hatte zur Folge, daß die Oberfinanzdirektion zur Konkretisierung dieser Regelung eine Verfügung an die saarländischen Finanzämter erließ. Damit sollte auch eine einheitliche Verfahrensweise sichergestellt werden. Es wurde angeordnet, daß die Diensträume beim Verlassen zu verschließen und die Schlüssel mitzunehmen sind. Steuerakten und sonstige Unterlagen sind in verschließbaren Schränken aufzubewahren, die außerhalb der Dienststunden unter Verschluß zu halten sind. Auf den Fluren dürfen nur noch Metallschränke verwandt werden, die stets verschlossen zu halten sind. Auch Altakten müssen sicher untergebracht und gegen unbefugten Zugriff gesichert werden. Altakten, die nicht archiviert werden, müssen im Reißwolf zerkleinert und in Ballen gepreßt werden. Dies gilt in gleicher Weise für Vorentwürfe von Schreiben.

Die konkretisierende Anweisung habe ich grundsätzlich begrüßt. Ich habe jedoch bei der Vorschrift über die Vernichtung aussonderungsfähiger Altakten und des Tagesanfalls von Abfallpapier Regelungen entsprechend der Richtlinie des Ministeriums des Innern vom 09.01.1989 (GMBl S. 2) zur Vernichtung von Schriftgut und sonstigen Datenträgern vermißt. Insbesondere sind Bestimmungen hinsichtlich der Schnitzelgröße, der Entsorgung von sonstigen Materialien wie Einmalkohlepapier, Farbbändern, Mikrofiches notwendig. Ferner ist zu prüfen, ob die Entsorgung durch Dritte mit Rücksicht auf das Steuergeheimnis in Betracht kommt und welche Maßnahmen der Datensicherung gegebenenfalls zu treffen sind.

Von besonderer Bedeutung sind die Regelungen der Geschäftsordnung der Finanzämter über die Aktenweitergabe (§ 27 Abs. 10). Werden danach Akten und Vorgänge außerhalb der regelmäßigen Bearbeitung ausgegeben, ist der Empfänger zu vermerken und die Rückgabe zu überwachen. Der Regelungsinhalt ist allerdings zu allgemein und lediglich beispielhaft. Anläßlich der Prüfung vor Ort konnte nicht geklärt werden, ob weitere konkretisierende Anordnungen bestehen. Solche präzisierenden, zusätzlichen Anweisungen halte ich für notwendig. Auf diese Weise ließe sich die Chance deutlich verbessern, die Verantwortlichen im Falle der Verletzung des Steuergeheimnisses nachträglich festzustellen.

5.1.2 Automation und PC-Einsatz

Die Datensicherung im automatisierten Bereich des Finanzamtes ist zu verbessern. Insbesondere folgende Maßnahmen sind geboten:

- Einsatz von Datensicherungs-Software auf PC's
- konsequente Vergabe von Benutzerkennung und Paßwörtern
- Beschränkung der Direktzugriffe auf den im jeweiligen Sachgebiet erforderlichen Datenumfang.

5.2 Kontrollmitteilungen öffentlicher Stellen an die Steuerbehörden über gezahlte Honorare

Insbesondere öffentliche Stellen übermittelten einer lang andauernden Praxis entsprechend den Finanzbehörden Informationen über die Auszahlung von Geldbeträgen, die nicht einem direkten Steuerabzug unterliegen. Dazu gehören z.B. Zahlungen aus dem Landeshaushalt an Unterrichtende und Vortragende im Nebenberuf oder an

Bauunternehmungen für Leistungen bei der Errichtung öffentlicher Bauten oder der Instandsetzung von Straßen. Bereits 1989 hatte ich das Finanzministerium auf die Rechtswidrigkeit dieser Verfahrensweise hingewiesen, weil eine entsprechende Rechtsgrundlage fehlt (11. TB Tz. 11.1). Solche Kontrollmitteilungen können zwar unter den im Gesetz genannten Voraussetzungen durch Rechtsverordnung zugelassen werden (§ 93 a AO), die jedoch bisher nicht erlassen worden ist. Erst auf meine erneute Intervention hat das Finanzministerium Mitte 1992 die öffentlichen Stellen des Landes angewiesen, von der Praxis der Übersendung von Kontrollmitteilungen Abstand zu nehmen. Andere Bundesländer hatten rechtsstaatlichen Überlegungen bereits früher Vorrang eingeräumt - so z.B. der Hessische Finanzminister mit Erlaß vom 2. November 1989 - und hatten entsprechende Anweisungen an die Landesbehörden erteilt.

6. Gesundheit

6.1 Krankenpapiere auf der Straße

Der ordnungsgemäße Umgang mit Krankenunterlagen läßt noch immer zu wünschen übrig.

Nachdem ich im vergangenen Jahr über den Fund von Mikrofilmen am Straßenrand berichten mußte (13. TB, Tz. 5.1.3), waren es jetzt Krankenakten, die Schüler auf der Straße entdeckt haben. Meine Nachforschungen ergaben, daß ein Krankenhaus ein Privatunternehmen mit dem Transport und der Vernichtung älterer Krankenunterlagen (Krankenblätter, Fieberkurven, OP-Berichte, Gutachten usw.) beauftragt hatte und daß auf dem Weg zur Vernichtung mehrere Säcke mit derartigen Akten vom Lastkraftwagen heruntergefallen waren.

Das Saarländische Krankenhausgesetz (§ 29 Abs. 6) erlaubt eine Verarbeitung von Patientendaten - dazu gehört auch die Vernichtung der Datenträger - durch private Dritte nur, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der Datenverarbeitung hierdurch kostengünstiger besorgt werden können. Das Krankenhaus konnte den Nachweis nicht führen, daß diese Voraussetzungen geprüft wurden.

Für die Beauftragung der Firma bestand lediglich eine mündliche Absprache. Es ist jedoch unerläßlich, in einem Vertrag schriftlich die beiderseitigen Pflichten im einzelnen festzulegen; insbesondere, welche konkreten, technischen und organisatorischen Maßnahmen der Datensicherung zu treffen sind, um das Patientengeheimnis zu wahren (vgl. § 29 Abs. 6 SKHG).

Das Krankenhaus wird künftig die Aktenvernichtung in eigener Regie durchführen.

S. 67

6.2 Private Schreibbüros

Wegen Personalengpässen haben Krankenhäuser - darunter das Landeskrankenhaus Merzig - aber auch niedergelassene Ärzte Schreibarbeiten von privaten Büros erledigen lassen. Tonbänder mit diktierten Arztberichten werden an ein Schreibbüro gegeben, das die Texte im PC erfaßt, Entwürfe zur Korrektur vorlegt und danach die endgültige Version der Schreiben dem Krankenhaus übergibt.

Die Beauftragung einer privaten Firma mit dem Schreiben von diktierten Arztberichten halte ich für äußerst problematisch. Man muß sich vor Augen halten, daß hier sensible medizinische Daten aus dem Vertrauensverhältnis Arzt/Patient an außenstehende Dritte weitergegeben werden, ohne daß der Patient davon Kenntnis hat. In den, für den weiterbehandelnden Arzt bestimmten Arztberichten des Krankenhauses wird regelmäßig dargestellt, in welcher Zeit der Patient stationär behandelt, welche Diagnosen und Befunde festgestellt, welche Therapie mit welchem Ergebnis vorgenommen wurde und welche weitere Behandlung empfohlen wird. Welcher Stellenwert der Gesetzgeber dem Schutz der Patientendaten eingeräumt hat, läßt sich daraus entnehmen, daß er in § 203 Strafgesetzbuch die unbefugte Offenbarung durch den Arzt unter Strafe gestellt hat. Erst in jüngster Zeit ist das Arztgeheimnis durch zwei richtungsweisende Urteile des Bundesgerichtshofes erheblich aufgewertet worden. So hat der Bundesgerichtshof mit Urteil vom 10.07.1991 (NJW 1991, S. 2955) festgestellt, daß die Abtretung einer ärztlichen Honorarforderung an eine gewerbliche Verrechnungsstelle und die damit verbundene Übergabe der Patientenunterlagen gegen die ärztliche Schweigepflicht verstoße. Ebenfalls einen Verstoß gegen die ärztliche Schweigepflicht hat der Bundesgerichtshof angenommen in dem Verkauf einer Praxis mit Patientenkarteikarten ohne

Beteiligung der betroffenen Patienten (BGH, Urteil vom 11.12.1991, NJW 1992, S. 737).

Im Hinblick auf diese neuere Rechtsentwicklung sollte von der grundsätzlich den Krankenhäusern durch § 29 Abs. 6 des Saarländischen Krankenhausgesetzes eingeräumten Möglichkeit, Patientendaten außerhalb des Krankenhauses im Auftrag verarbeiten lassen, wenn überhaupt, dann nur äußerst zurückhaltend Gebrauch gemacht werden. In der Erledigung von Schreibarbeiten durch externe Büros sehe ich vielfältige Gefahren für die Wahrung des Patientengeheimnisses. Es muß sichergestellt sein und ständig kontrolliert werden, daß die Briefe zeitnah gelöscht, Entwürfe sachgerecht vernichtet und Unbefugte keinen Zugang zu den Daten nehmen können. Diese Probleme stellen sich insbesondere dann, wenn solche Schreibbüros als Nebenbeschäftigung in der Privatwohnung betrieben werden. Eine Schwachstelle ist auch der Transport. Meine Erfahrungen aus der Vergangenheit bestätigen, daß es hier immer wieder zu Pannen kommt, indem z.B. Datenträger auf dem Transport verloren gehen.

Wenn dennoch die Vergabe von Schreibarbeiten in Betracht gezogen wird, ist durch strikte organisatorisch-technische Maßnahmen eine Verletzung des Patientengeheimnisses auszuschließen. Dazu gehören etwa ein Verbot der Heimarbeit, ein sicherer Transport der Datenträger von der Klinik zu dem Schreibbüro, eine Unterwerfung des Schreibbüros unter meine Kontrolle und Sicherungsmaßnahmen im PC-Bereich. Die einzelnen Punkte müssen in einem Vertrag zwischen Klinik und Schreibbüro im einzelnen schriftlich vereinbart werden.

In einem Schreiben an die saarländische Ärztekammer, das in deren Informationsdienst veröffentlicht wurde, habe ich auf die Rechtslage bei niedergelassenen Ärzte aufmerksam gemacht. Dabei habe ich darauf hingewiesen,

6.2 Private Schreibbüros

Wegen Personalengpässen haben Krankenhäuser - darunter das Landeskrankenhaus Merzig - aber auch niedergelassene Ärzte Schreibarbeiten von privaten Büros erledigen lassen. Tonbänder mit diktierten Arztberichten werden an ein Schreibbüro gegeben, das die Texte im PC erfaßt, Entwürfe zur Korrektur vorlegt und danach die endgültige Version der Schreiben dem Krankenhaus übergibt.

Die Beauftragung einer privaten Firma mit dem Schreiben von diktierter Arztberichten halte ich für äußerst problematisch. Man muß sich vor Augen halten, daß hier sensible medizinische Daten aus dem Vertrauensverhältnis Arzt/Patient an außenstehende Dritte weitergegeben werden, ohne daß der Patient davon Kenntnis hat. In den, für den weiterbehandelnden Arzt bestimmten Arztberichten des Krankenhauses wird regelmäßig dargestellt, in welcher Zeit der Patient stationär behandelt, welche Diagnosen und Befunde festgestellt, welche Therapie mit welchem Ergebnis vorgenommen wurde und welche weitere Behandlung empfohlen wird. Welcher Stellenwert der Gesetzgeber dem Schutz der Patientendaten eingeräumt hat, läßt sich daraus entnehmen, daß er in § 203 Strafgesetzbuch die unbefugte Offenbarung durch den Arzt unter Strafe gestellt hat. Erst in jüngster Zeit ist das Arztgeheimnis durch zwei richtungsweisende Urteile des Bundesgerichtshofes erheblich aufgewertet worden. So hat der Bundesgerichtshof mit Urteil vom 10.07.1991 (NJW 1991, S. 2955) festgestellt, daß die Abtretung einer ärztlichen Honorarforderung an eine gewerbliche Verrechnungsstelle und die damit verbundene Übergabe der Patientenunterlagen gegen die ärztliche Schweigepflicht verstoße. Ebenfalls einen Verstoß gegen die ärztliche Schweigepflicht hat der Bundesgerichtshof angenommen in dem Verkauf einer Praxis mit Patientenkarteikarten ohne

daß die externe Schreibkraft nicht mit dem in der Arztpraxis tätigen Personal gleichgestellt werden kann. Die externe Kraft ist der Aufsicht des Arztes praktisch völlig entzogen. Die Weisungsbefugnis und die Aufsichtsmöglichkeiten des Arztes hat der Bundesgerichtshof jedoch als Kriterium dafür angesehen, ob eine befugte oder unbefugte Offenbarung von Patientengeheimnissen vorliegt. Auch mit Einwilligung des Patienten sollte von der Vergabe von Schreibarbeiten in Heimarbeit abgesehen werden. Die Gefahr, daß dabei Patientendaten auch dritten Personen zur Kenntnis gelangen, ist zu groß. Angesichts der immer wieder zu registrierenden Pannen bei der Auftragsdatenverarbeitung muß ernsthaft darüber nachgedacht werden, inwieweit derart sensible Daten den unmittelbaren ärztlichen Verantwortungsbereich verlassen sollten. Das gilt angesichts der großen Datenmengen insbesondere für die Krankenhäuser, für die der Saarländische Gesetzgeber über die Gesetzgebungskompetenz verfügt.

6.3 Neonatalerhebung (Bilanz)

In meinem 13. Tätigkeitsbericht (Tz. 5.3) habe ich über die sogenannte "Neonatalerhebung" berichtet, die die Ärztekammer des Saarlandes zusammen mit der Kassenärztlichen Vereinigung des Saarlandes seit dem 1. Januar 1991 durchführt. Ziel der Neonatalerhebung ist die Qualitätsverbesserung in der medizinischen Versorgung Neugeborener.

Um Reidentifizierungen auszuschließen, hatte ich kritisiert, daß auf den für die Dokumentationsstelle bei der Kassenärztlichen Vereinigung Trier bestimmten Erhebungsbogen die ersten drei Stellen der Postleitzahl aufgetragen werden. Gerügt habe ich desweiteren die mangelnde Beteiligung der Eltern des Neugeborenen bei der Übersendung des Erhebungsbogens an die einweisende Geburtsklinik und an den nachbehandelnden Arzt.

Im Berichtszeitraum hat sich die Ärztekammer des Saarlandes zu meinen datenschutzrechtlichen Bedenken geäußert. Nicht durchsetzen konnte ich mich mit meiner Forderung, auf die Erhebung der Postleitzahl in dreistelliger Form zu verzichten. Zu dieser Frage wird in einer Entschließung der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder vom 08.09.1985 zu Unrecht auf eine Zustimmung der Datenschutzkontrollorgane verwiesen, die sich in dieser Form bisher nicht geäußert haben. Regionale Auswertungen machten die dreistellige Erhebung der Postleitzahl erforderlich. Zwar sei der Datenbestand bisher regional noch nicht ausgewertet worden. Dies hänge allerdings damit zusammen, daß aussagekräftige, regionalbezogene Ergebnisse erst nach Zusammenfassung von acht bis zwölf Jahrgängen zu erwarten seien. Ich werde die Angelegenheit unter diesem Gesichtspunkt weiter beobachten.

Übereinstimmung konnte erzielt werden in der Frage der Beteiligung der Eltern bei der Weitergabe der Erhebungsbögen. Die Ärztekammer hat die an der Neonatalerhebung teilnehmenden Ärzte in einem Rundschreiben ausdrücklich darauf hingewiesen, daß die Weitergabe der Formulare an die Geburtsklinik und den nachbehandelnden Arzt der Zustimmung der Eltern bedürfe.

6.4 Unterbringungsgesetz

Das Gesetz zur Unterbringung psychisch Kranker ist novelliert worden (Gesetz vom 11. November 1992, Amtsblatt S. 350). Ich bin nicht beteiligt worden. Abgesehen von einigen begrüßenswerten Klarstellungen hinsichtlich der Voraussetzungen der Unterbringung ist zu beklagen, daß die vorsorgenden, begleitenden und nachsorgenden Hilfen, die die Unterbringung vermeiden oder verkürzen helfen sollen (Subsidiärität der Unterbrin-

gung § 2) im einzelnen nicht geregelt werden und demzufolge die schon seit 1981 wiederholt festgestellte Unsicherheit über die Voraussetzungen der Erhebung und Verarbeitung der Daten psychisch Kranker im Vorfeld einer Unterbringung nicht beseitigt ist (3. TB Tz. 7.2 S. 165; 7. TB Vorbemerkung S. 2; 10. TB Vorbemerkung S. 1; 12. TB Tz. 6.3.1 S. 62. Ich bleibe bei meiner Forderung, daß insoweit ein Gesetz über die Hilfen und Schutzmaßnahmen psychisch Kranker im Interesse der Vorsorge für diesen Personenkreis auch aus datenschutzrechtlichen Erwägungen notwendig bleibt. Die in der Vergangenheit geschilderten Fälle haben insbesondere gezeigt, daß die Voraussetzungen der Informationserhebung und -verarbeitung von Personen dringend einer gesetzlichen Regelung bedürfen, bei denen vorab nicht mit ausreichender Sicherheit das Vorliegen einer psychischen Erkrankung festgestellt werden kann. Oft werden Angehörige oder Nachbarn bei der Verwaltungsbehörde vorstellig, um eine bestimmte Person "unterbringen zu lassen". Wenn erkennbar ist, daß der geschilderte Sachverhalt für eine Unterbringung nicht ausreicht, stellt sich die Frage, wie mit den Informationen umzugehen ist. Es handelt sich hierbei nicht mehr nur um eine polizeirechtliche Problematik, sondern auch um eine Frage der Gesundheitsvorsorge, die einer näheren Regelung bedarf.

7. Soziales

7.1 Krankenversicherungskarte (Chipkarte)

Der herkömmliche Krankenschein soll durch eine Krankenversichertenkarte abgelöst werden. Dies sieht das Gesundheitsreformgesetz 1989 vor. Presseberichten ist zu entnehmen, daß die ersten Krankenversicherungskarten demnächst in verschiedenen Regionen Deutschlands ausgegeben werden sollen. Die Karte darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden. Bei einem Arzt- oder Zahnarztbesuch legt künftig der Versicherte anstelle des Krankenscheines seine Krankenversichertenkarte vor. Mit einem Lesegerät in der Arztpraxis werden die Daten von der Karte auf die Belege wie etwa Abrechnungsscheine oder Rezepte übertragen. Auf der Karte dürfen ausschließlich folgende Angaben gespeichert werden: Bezeichnung der ausstellenden Krankenkasse, Name sowie Geburtsdatum und Anschrift des Versicherten und dessen Versichertenstatus, Gültigkeitsdatum sowie die Krankenversichertennummer. Die Krankenversichertenkarte soll auf der Grundlage der Chiptechnik gestaltet werden. Wegen des großen Speichervolumens der Chipkarte besteht die Gefahr, daß auf dieser Karte mehr Gesundheitsdaten des Versicherten gespeichert werden, als es das Gesetz zuläßt. Überlegungen in dieser Richtung sind in der Vergangenheit bekannt geworden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung am 1./2. Oktober 1992 eindeutig festgestellt, daß eine Speicherung auf einer Chipkarte auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß (vgl. Anlage 5).

7.2 Gesundheits-Strukturgesetz

Am 01.01.1993 ist das Gesundheits-Strukturgesetz in Kraft getreten. Ziel des Gesetzes ist die Kostenbegrenzung in der gesetzlichen Krankenversicherung. Neben den verschiedenen Maßnahmen, die zu Einsparungen führen sollen, sind auch die Datenverarbeitungsbefugnisse der am System der gesetzlichen Krankenversicherung Beteiligten erweitert worden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in ihrer Sitzung am 1./2. Oktober 1992 mit dem Gesundheits-Strukturgesetz befaßt und in einer Entschließung (vgl. Anlage 6) auf die Gefahren für die Persönlichkeitsrechte der Versicherten hingewiesen.
Nachbesserungen an dem Gesetzentwurf im Detail konnten zwar erreicht werden. An der grundlegenden Problematik der fortschreitenden, automatisierten Speicherung von Versichertendaten bei den Kassenärztlichen Vereinigungen und Krankenkassen hat sich jedoch nichts geändert.

Nach der neuen Rechtslage sind die Kassenärzte verpflichtet, den Kassenärztlichen Vereinigungen auf den Abrechnungsscheinen die Diagnosen mitzuteilen. Mit der Problematik der Angabe der Diagnosen auf den Krankenscheinen habe ich mich bereits in meinem 12. Tätigkeitsbericht, Tz. 7.1, kritisch auseinandergesetzt. Der Gesetzgeber hat indessen die bisher aufgrund des Gesetzeswortlauts bestehenden Unsicherheiten beseitigt und sich dafür entschieden, daß die Diagnosen zu Abrechnungszwecken an die Kassenärztliche Vereinigung übermittelt werden dürfen (§ 295 Abs. 1 Nr. 2 SGB V). Klargestellt ist inzwischen, daß zur Abrechnung ärztlicher Leistungen die Diagnosen versichertenbezogen keinesfalls an die Krankenkassen übermittelt werden dürfen (§ 295 Abs. 2 SGB V). Hierin sehe ich einen

entscheidenden Fortschritt im Interesse des betroffenen Patienten.

Der Katalog der den Krankenkassen von den Krankenhäusern zu übermittelnden personenbezogenen Angaben wurde allerdings gegenüber der geltenden Rechtslage erheblich erweitert. Zweifel an der Erforderlichkeit sämtlicher Angaben sind angebracht, wenn den Krankenkassenverbänden und den Leistungserbringern gleichzeitig das Recht eingeräumt wird, den Umfang der zu übermittelnden Angaben vertraglich einzuschränken (§ 303 Abs. 1 SGB V). Das Gesetz legt einen Maximalkatalog fest, anstatt sich auf die Daten zu beschränken, die für die Abrechnung der Krankenhauskosten unbedingt erforderlich sind. Dies hat auch die Konferenz der Datenschutzbeauftragten gerügt.

Im Ergebnis ist festzuhalten, daß die Befugnisse der Kassenärztlichen Vereinigungen und der Krankenkassen Versichertendaten automatisiert vorzuhalten und zu verarbeiten, in großem Umfang erweitert wurden, ohne daß die Vorschriften über die Zweckbindung und ihre Durchbrechung gleichermaßen differenziert und ausreichend konkret ausgestaltet worden wären. Fraglich ist insbesondere, ob die Wirtschaftlichkeitsprüfungen mit Hilfe der Automation sich in einem Ausmaß optimieren lassen, daß das mit der fortschreitenden Automation verbundene Anwachsen des Gefährdungspotentials angemessen erscheint. Eine kritische Prüfung der Verwaltungspraxis wird in Zukunft um so dringlicher.

7.3 SGB-Änderungsgesetz

Die Verarbeitung von Sozialdaten durch die Sozialleistungsträger ist - außer in den bereichsspezifischen Vorschriften - im Ersten Buch und im Zehnten Buch des Sozialgesetzbuches geregelt. Im Berichtszeitraum hat das Bundesministerium für Arbeit und Sozialordnung den

Entwurf für ein Zweites Gesetz zur Änderung des Sozialgesetzbuches vorgelegt. Durch das Gesetz soll der Schutz der Sozialdaten unter Berücksichtigung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 weiterentwickelt werden. Im Mittelpunkt der 1981 in Kraft getretenen Bestimmungen stand der Schutz der Sozialdaten vor unbefugten Übermittlungen. Neu geregelt werden sollen die Bestimmungen über die Datenerhebung, die Sperrung von Daten, die Rechte des Betroffenen, den automatisierten Abruf und die Gefährdungshaftung.

Ich habe zu dem Gesetzentwurf detailliert Stellung genommen. Neben einer Fülle von Detailfragen, die ich aufgegriffen habe, halte ich folgende Mängel des Entwurfs für besonders gravierend:

Ein wichtiger datenschutzrechtlicher Grundsatz lautet, daß personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind. Von diesem Ansatz geht auch der Gesetzentwurf aus; die Ausnahmefälle der Erhebung beim Betroffenen sind jedoch so weitgehend, daß der Vorgang der Datenerhebung beim Betroffenen dadurch praktisch zur Bedeutungslosigkeit degradiert wird.

Der Entwurf läßt ebenso wie die noch geltende Fassung einen großzügigen Datenaustausch aller Sozialleistungsträger untereinander zu, der lediglich durch die Aufgabenerfüllung nach dem Sozialgesetzbuch und das Erforderlichkeitsprinzip begrenzt ist. Ohne nennenswert hohe gesetzliche Schranken überwinden zu müssen, sollen die Sozialleistungsträger von Sozialdatenbeständen profitieren, die in den verschiedensten Bereichen - Kranken-, Renten-, Unfall-, Arbeitslosenversicherung, Sozialhilfe, Ausbildungsförderung - vorgehalten werden; hinzu kommt noch, daß der Entwurf die Einrichtung des automatisierten Direktabrufs grundsätzlich bereichsübergreifend - wenn auch erst nach einer Güter-

abwägung - ermöglicht. Der Entwurf berücksichtigt mit dieser Regelung die Verfassungsgrundsätze der Zweckbindung und Verhältnismäßigkeit nicht ausreichend. Die Voraussetzungen der Zweckdurchbrechung sollten bereichsspezifisch entsprechend dem konkreten Datenbedarf in den einzelnen Sozialleistungsbereichen geregelt werden. Zumindest ist ein konkreter Katalog der Voraussetzungen für die Zweckdurchbrechungen zu entwickeln.

Angesichts des Gefährdungspotentials, das mit der Einrichtung des automatisierten Direktabrufs verbunden ist, sollten solche Verfahren nur aufgrund einer Rechtsverordnung im Einzelfall zugelassen werden.

Kritisiert habe ich die Vorschriften über die Datenschutzkontrolle; der Entwurf sieht eine Beschränkung insofern vor, als die Kontrolle der Informationsverarbeitung in Akten nur noch möglich sein soll, wenn der Betroffene in einer Beschwerde hinreichende Anhaltspunkte dafür darlegt, daß er in seinen Rechten verletzt worden ist, oder dem Datenschutzbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen (§ 24 Abs. 1 Satz 2 BDSG). Dies hätte zur Folge, daß der Landesbeauftragte keine Routine- und Querschnittsprüfungen hinsichtlich Akten durchführen darf. Gerade in dem sensiblen Sozialleistungsbereich würde damit ein geringeres Kontrollniveau erreicht, als dies bei sonstigen öffentlichen Stellen im Saarland der Fall ist.

Schließlich habe ich gefordert, daß das Recht auf Einsicht in die Unterlagen der Sozialleistungsträger erweitert wird (§ 25 SGB X). Ein früherer Sozialhilfeempfänger hat sich bei mir darüber beschwert, daß das Sozialamt es abgelehnt hat, die Kopie einer in den Verwaltungsakten enthaltenen amtsärztlichen Stellungnahme auszuhändigen. Er benötigte dieses Untersuchungs-

ergebnis zur Beurteilung seiner Arbeitseinsatzmöglichkeiten im Rahmen von Vermittlungsbemühungen des Arbeitsamtes. Nach der Rechtslage hätte dem Betroffenen die Kopie nicht ausgehändigt werden müssen, weil ihm ein Anspruch nach Abschluß seines Sozialhilfeverfahrens nicht zusteht. Es ist mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar, wenn nach der derzeitigen Rechtslage das Akteneinsichtsrecht nur im Rahmen eines laufenden Verfahrens gewährt werden muß.

7.4 Erfassung von Abrechnungsdaten der Kassenärztlichen Vereinigung (KV) durch private Stellen

Die Kassenärztliche Vereinigung Saarland hat mich darüber informiert, daß sie beabsichtige, eine private Firma mit der Erfassung von Abrechnungsdaten aus Behandlungsscheinen zu beauftragen. Wegen personeller Engpässe habe sie sich zu diesem Schritt entschließen müssen.

Ich habe gegenüber der Kassenärztlichen Vereinigung und dem zuständigen Ministerium deutlich gemacht, daß ich eine solche Auftragsdatenverarbeitung für unzulässig halte. Einer Privatfirma werden im Zusammenhang mit der Datenerfassung so sensible Informationen wie Diagnosen und Behandlungsmaßnahmen einzelner betroffener Patienten zur Kenntnis gegeben. Es handelt sich um Sozialdaten, die Offenbarungsbeschränkungen des Sozialgesetzbuches unterliegen (§ 69 Abs. 1 Nr. 2 i.V.m. § 76 SGB X). Nach diesen Bestimmungen dürfen die Stellen, die den Sozialdatenschutz zu beachten haben, Daten, die ihnen von einem Arzt zugänglich gemacht worden sind, nur unter den Voraussetzungen weitergeben, unter denen der Arzt selbst offenbarungsbefugt wäre. Eine Befugnis des Arztes zur Weitergabe von Patientendaten an eine private Stelle zu Abrechnungszwecken ist nicht ersichtlich. Eine Offenbarungsbefug-

nis ergibt sich weder aus gesetzlichen Vorschriften, noch kann eine solche aus einer Einwilligung der Versicherten hergeleitet werden. Der Annahme einer stillschweigenden Einwilligung steht entgegen, daß den Versicherten die Weitergabe der Behandlungsscheine an eine Privatfirma nicht bekannt ist. Eine mutmaßliche Einwilligung scheidet aus, weil diese voraussetzt, daß der Betroffene erkennbar kein Interesse an der Wahrung des Geheimnisses hat.

Der Bundesgerichtshof hat im Hinblick auf eine vergleichbare Interessenlage unterstrichen, daß die Bekanntgabe von Abrechnungsdaten an gewerbliche Verrechnungsstellen ohne Einwilligung des Patienten den Straftatbestand des § 203 StGB erfüllt (NJW 1991, 2955).

Mit Rücksicht auf die Rechtslage habe ich der Kassenärztlichen Vereinigung von einer Beauftragung der privaten Firma abgeraten. Den Einwand der Kassenärztlichen Vereinigung und des Ministeriums, die zeitnahe Durchführung der Abrechnung zwinge zu der Maßnahme, kann ich nicht gelten lassen. Der Kassenärztlichen Vereinigung kann der Vorwurf nicht erspart bleiben, keine rechtzeitigen Vorkehrungen getroffen zu haben, damit der Engpaß in der technisch-organisatorischen Durchführung vermieden wird.

Zu meinem Bedauern hat die Kassenärztliche Vereinigung den Auftrag trotz meiner Bedenken erteilt. Erreicht habe ich aber immerhin, daß sich die zuständigen Stellen der Problematik bewußt geworden sind. Die Einstellung weiterer Mitarbeiter bei der Kassenärztlichen Vereinigung ist geplant.

7.5 Datenanforderungen des Versorgungsamtes

Bereits in meinem 12. Tätigkeitsbericht (Tz. 7.4) habe ich mich mit der Behandlung medizinischer Unterlagen

beim Versorgungsamt befaßt. Auch im Berichtszeitraum war der Umgang des Versorgungsamtes mit medizinischen Informationen Gegenstand intensiver Erörterungen mit der Behörde. Es kann nicht verwundern, daß es im Bereich des Versorgungsamtes eine Vielzahl datenschutzrechtlicher Probleme gibt, da bei allen Entscheidungen des Versorgungsamtes sensible medizinische Informationen eine große Rolle spielen. Die Antragsteller selbst geben dem Versorgungsamt umfassend Auskunft über ihre gesundheitlichen Verhältnisse, um etwa bei Anträgen nach dem Schwerbehindertengesetz einen möglichst hohen Grad der Behinderung zu erreichen. Trotz dieses Umstandes muß sichergestellt sein, daß die Selbstbestimmung des Patienten ernst genommen wird, daß dem Versorgungsamt nur die Informationen zur Verfügung gestellt werden, die zur Aufgabenerfüllung erforderlich sind und daß eine sinnvolle Aufgabenverteilung zwischen dem ärztlichen Dienst und dem Verwaltungsbereich des Versorgungsamtes stattfindet.

Als positives Ergebnis meiner Bemühungen um eine Verbesserung des Datenschutzes im Versorgungsamt kann ich feststellen, daß aufgrund einer Anordnung des Versorgungsamtes bei Bearbeitung von Schwerbehindertenanträgen grundsätzlich nicht mehr die gesamten Krankenpapiere von den Krankenhäusern angefordert werden dürfen. Sollte im Einzelfall doch einmal die Einsichtnahme in die Krankenpapiere erforderlich sein, wurde folgendes Verfahren angeordnet:

- Der ärztliche Dienst fordert die Krankenpapiere an mit der gleichzeitigen Aufforderung an die Krankenanstalt, die Postsendung deutlich als "Arztsache" zu kennzeichnen.

- Die entsprechenden Sendungen werden von der Posteingangsstelle des Versorgungsamtes ungeöffnet an den ärztlichen Dienst weitergeleitet.

- Der ärztliche Dienst wertet die Krankenpapiere aus und nimmt die Auswertung zu den Akten.

- Damit die Auswertung später nachvollzogen werden kann (z.B. im Widerspruchsverfahren), sind die für die Auswertung bedeutsamen Unterlagen zu kopieren.

- Die Unterlagen sind in einem verschlossenen und versiegelten Umschlag als "Arztsache" gekennzeichnet bei den Schwerbehindertenakten aufzubewahren.

Auch wenn es gegenüber der früheren Praxis einen Fortschritt bedeutet, daß nunmehr nicht mehr die gesamten Krankenpapiere bei den Krankenhäusern angefordert werden, bin ich mit der jetzigen Handhabung, statt dessen die Entlassungsberichte anzufordern, immer noch nicht zufrieden. Ich bin der Meinung, daß es ausreicht, wenn das Versorgungsamt vom Krankenhaus die Beantwortung bestimmter Fragen verlangt. Nur so kann verhindert werden, daß das Versorgungsamt in den Besitz von Informationen gelangt, die es für seine Aufgabenerfüllung nicht benötigt. Die Entlassungsberichte sind für den nachbehandelnden Arzt bestimmt und deshalb bezüglich des Datenumfangs an dieser Zweckbestimmung orientiert. Die Gefahr liegt nahe, daß der Entlassungsbericht Informationen enthält, die für den nachbehandelnden Arzt wichtig, für das Versorgungsamt jedoch ohne Relevanz sind.

Bei einem Prüfbesuch im Versorgungsamt bin ich auf ein weiteres Problem aufmerksam geworden. Der Antragsteller hat das Recht, seinen Antrag auf bestimmte Leiden zu beschränken. Dadurch soll dem Betroffenen die Möglichkeit eingeräumt werden, sozialdiskriminierende Krankheiten - wie z.B. Alkoholismus oder psychiatrische Leiden - dem Versorgungsamt nicht zu offenbaren. Es fragt sich jedoch, was dieses Recht wert ist, wenn

durch die Datenanforderung des Versorgungsamtes bei den behandelnden Ärzten und Krankenhäusern die Gefahr besteht, daß diese Krankheiten dem Versorgungsamt dennoch bekannt werden, weil ein umfassender Arztbericht angefordert wird. Um den Antragsteller gegen die unerwünschte Offenbarung von bestimmten Krankenheitsbildern abzusichern, muß nicht nur das Antragsformular die Möglichkeit eröffnen, den Antrag auf bestimmte Krankheitsbilder zu beschränken. Auch die Anforderung gegenüber dem behandelnden Arzt oder Krankenhaus muß in einem solchen Fall deutlich erkennen lassen, daß in dem Befundbericht nur auf solche Krankheiten eingegangen werden darf, die der Antragsteller in seinem Antrag ausdrücklich genannt hat. Als weiteres Mittel zur Verhinderung der Übermittlung unzulässiger Überschußinformationen sind Berichte stets nur von dem die Verantwortung jeweils im konkreten Fall tragenden Krankenhaus oder Arzt anzufordern. Bisher ist es so, daß das Versorgungsamt Facharztberichte und Krankenhausentlassungsberichte bei dem Hausarzt anfordert, wenn dieser im Besitz dieser Unterlagen ist. Auf diese Weise kann die Zweckbindung der für die Nach- oder Mitbehandlung übermittelten Krankheitsdaten leicht unterlaufen werden.

Keine Annäherung der Standpunkte kann ich verzeichnen, was das Verfahren der Kriegsopferversorgung nach dem Bundesversorgungsgesetz betrifft. Das Versorgungsamt beharrt bisher darauf, daß hier stets die Anforderung der gesamten Krankenpapiere bei Krankenhausbehandlung erforderlich sei. Nach meiner Einschätzung dagegen müßte es möglich sein, die Fragen an das Krankenhaus so zu formulieren, daß eine Beurteilung möglich ist, ob die Gesundheitsstörung auf ein schädigendes Ereignis im Sinne des Bundesversorgungsgesetzes zurückzuführen ist. Sollte im Einzelfall doch einmal die Anforderung der gesamten Krankenpapiere erforderlich sein, so müssen diese Krankenpapiere so behandelt werden,

wie es die Anordnung für die Durchführung des Schwerbehindertengesetzes vorsieht.

Ich bin mit dem Versorgungsamt weiterhin im Gespräch.

8. Arbeitnehmer

8.1 Private Arbeitsverhältnisse

Die Datenschutzbeauftragten des Bundes und der Länder haben aus Anlaß des Volkszählungsurteils bereits 1984 spezielle gesetzliche Regelungen zum Arbeitnehmerdatenschutz gefordert. Die Notwendigkeit eines solchen, nicht auf den öffentlichen Bereich beschränkten Gesetzes ist - wie den Antworten der Bundesregierung auf parlamentarische Anfragen zu entnehmen ist - unbestritten. Die Konferenz der Datenschutzbeauftragten hat in ihrer Entschließung vom 23./24.03.1992 die wesentlichen Anforderungen für eine Gesetzesregelung dargestellt (Anlage 7). Dem Mangel einer umfassenden und präzisen, bereichsspezifischen Regelung muß abgeholfen werden.

8.2 Öffentlicher Dienst

8.2.1 Entfernung von Disziplinarvorgängen aus der Personalakte

Ein Polizeibeamter hat bei der Einsicht in seine Personalakte festgestellt, daß diese auch eine Beiakte über einen mehrere Jahre zurückliegenden Verwaltungsrechtsstreit enthält. Dem Rechtsstreit lag die Versagung einer Genehmigung zur Ausübung einer Nebentätigkeit als Fahrlehrer zugrunde. Dabei waren auch Ermittlungsergebnisse aus einem Disziplinarverfahren beigezogen worden. Die Beiakte enthielt u.a. zahlreiche Fotokopien aus der Disziplinarakte. Zwar wurde die eigentliche Disziplinarakte entsprechend den Vorschriften der Saarländischen Disziplinarordnung nach Ablauf der Tilgungsfrist vernichtet, die Beiakte verblieb jedoch in der Personalakte.

Ich habe mich beim Ministerium des Innern dafür eingesetzt, daß auch diese Beiakte aus der Personalakte entfernt wird. Mit der Aufbewahrung von Vorgängen aus dem Disziplinarverfahren innerhalb der Personalakte wird die Tilgungsvorschrift des § 111 Saarländische Disziplinarordnung unterlaufen. Diese Vorschrift geht von der Vorstellung aus, daß nach Tilgung der Disziplinarmaßnahme der Beamte wieder unbelastet und die Personalakte makellos sein soll, so daß ihm die verfristeten Verfehlungen nicht mehr vorgehalten werden können.

Das Ministerium hat "wegen der Besonderheit des vorliegenden Falles und weil das Verwaltungsgericht keine Entscheidung in der Sache getroffen hat", die Entfernung des Vorganges aus der Personalakte veranlaßt. Indessen sind die Disziplinarvorgänge, auf welche Weise sie auch immer in die Personalakte gelangen, nach Ablauf der für die Disziplinarverfahren geltenden Tilgungsvorschriften zu vernichten.

8.2.2 Personenbezogene Fremddaten in der Personalakte

Bei der Überprüfung der Personalakte eines Polizeibeamten habe ich festgestellt, daß darin eine Liste aller Beförderungen im Polizeibereich zu einem bestimmten Termin ebenso abgeheftet war, wie Teilnehmerlisten von Fortbildungsmaßnahmen und von Ausbildungen an der Schußwaffe.

In die Personalakte gehören nur Unterlagen, die den Beamten selbst betreffen, nicht dagegen Daten anderer Bediensteter. Da der Beamte ein uneingeschränktes Einsichtsrecht in seine Personalakte hat, werden durch seine Einsichtnahme personenbezogene Daten der Kollegen unbefugt offenbart. Ebenso werden bei der Akteneinsicht durch andere Stellen, z.B. mit Einwilligung des Beamten bei Stellenbewerbungen, Personaldaten Dritter unzulässigerweise preisgegeben.

Das Ministerium des Innern hat erklärt, künftig keine kompletten Namenslisten mehr in der Personalakte eines jeden Beteiligten aufzunehmen. Außerdem sollen die Listen aus den vorhandenen Personalakten entfernt werden. Ich erwarte, daß die Aktenbereinigung nicht nur am "gezogenen Fall", sondern systematisch in einem überschaubaren Zeitraum erfolgt.

In einem anderen Fall hat ein Beamter des Ministeriums für Umwelt gegen seine Regelbeurteilung geklagt. In diesem Verfahren ist ihm ein vom Zweitbeurteiler verfaßter Vermerk zur Kenntnis gegeben worden, in dem nicht nur zu seiner Beurteilung, sondern auch zu der eines Kollegen Stellung genommen wurde. Die Zusammenfassung zweier Beurteilungen in einem Vermerk hatte nachteilige Folgen. Die auch in den Beurteilungsrichtlinien des Ministeriums vorgeschriebene Vertraulichkeit hätte im vorliegenden Falle ohne weiteres gewährleistet werden können, wenn der Zweitbeurteiler in zwei getrennten Vermerken die jeweilige Beurteilung abgegeben hätte. Das Ministerium hat mir gegenüber die Vorgehensweise bedauert und zugesichert, "entsprechende Vorkehrungen zu treffen, um solche Unzulänglichkeiten zu vermeiden".

8.2.3 Umsetzung der Vorschriften des Beamtenrechtsrahmengesetzes (BRRG) in Landesrecht

Mit dem 9. Gesetz zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 sind datenschutzrechtlich bedeutsame Vorschriften des Personalaktenrechts in das Beamtenrechtsrahmengesetz eingefügt worden. Die Datenschutzbeauftragten des Bundes und der Länder haben im Laufe des Gesetzgebungsverfahrens wesentliche Verbesserungen des ursprünglichen Entwurfs erreicht (vgl. meinen 11. TB, Tz. 10.1). Das Ergebnis kann sich sehen lassen. Erstmals wird gesetzlich festgelegt, welche

Unterlagen in die Personalakte gehören. Der in der Vergangenheit immer wieder betonte Grundsatz der Vollständigkeit der Personalakte, die ein lückenloses Bild über die persönlichen und dienstlichen Verhältnisse des Beamten vermitteln soll, wird aufgegeben. Künftig dürfen nur noch Unterlagen in die Personalakte aufgenommen werden, die mit dem Dienstverhältnis des Beamten in einem unmittelbaren und inneren Zusammenhang stehen. Der Dienstherr darf personenbezogene Daten über Bewerber und Beamte nur erheben, soweit dies zur Erfüllung der im Gesetz genannten Zwecke erforderlich ist. Klargestellt wird, daß nur diejenigen Beschäftigten Zugang zur Personalakte haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Die gelegentlich vorkommende Vorlage von Personalakten an den Fachvorgesetzten ist somit unzulässig.

Hervorzuheben ist auch die Vorschrift des § 56 a BRRG, mit der eine bessere Abschottung der Beihilfefestsetzung von der Personalsachbearbeitung erreicht werden soll. Beihilfeunterlagen sind getrennt von Personalakten aufzubewahren. Die Beihilfe soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben. Bei der Umsetzung in saarländisches Recht sollte die Abschottung zur Pflicht gemacht werden. Verwaltungen, die dies nicht leisten können, muß Gelegenheit gegeben werden, die Beihilfebearbeitung an eine externe öffentliche Stelle zu übertragen (vgl. meinen 13. TB, Tz. 7.2).

Es stellt sich nunmehr die Frage, auf welche Weise die bundesrechtlichen Regelungen im Saarland umgesetzt werden. In anderen Bundesländern (z.B. Hamburg, Rheinland-Pfalz) werden Novellierungen des Landesbeamtengesetzes vorbereitet. Meine Anfrage bei dem federführen-

den Ministerium des Innern wurde bisher noch nicht beantwortet. Ich gehe davon aus, daß die auf Bundesebene erreichten datenschutzrechtlichen Fortschritte in das Saarländische Beamtengesetz übernommen werden und, soweit es um die Ausfüllung von Rahmenrecht geht, datenschutz- und arbeitnehmerfreundliche Fortschritte erzielt werden können. Neben der oben bereits erwähnten Abschottung der Beihilfesachbearbeitung sollte z.B. die Datenübermittlung zwischen Dienstbehörde und Amtsarzt geregelt sowie die Tilgungsvorschrift des Personalaktenrechts den kürzeren Fristen der Saarländischen Disziplinarordnung angepaßt werden.

8.3 Zentrale Besoldungs- und Versorgungsstelle (ZBS)

8.3.1 Berechnung und Festsetzung der Bezüge

Die Bezüge der Landesbediensteten, der Versorgungsempfänger sowie der Mitglieder der Landesregierung werden seit Jahren nicht mehr von den einzelnen Ressorts berechnet und festgesetzt. Sie haben diese Aufgaben der bei der Oberfinanzdirektion gebildeten ZBS übertragen. Der Umfang der Aufgabenübertragung ist unterschiedlich. Während etwa das Ministerium des Innern sich z.B. die Festsetzung des Besoldungsdienstalters und der ruhegehaltsfähigen Dienstzeit vorbehalten hat, haben andere Ressorts dies der ZBS übertragen.

Bei einer Kontrolle der ZBS habe ich mich vor allem von dem Gedanken leiten lassen, daß nur soviel Personen der Zugriff auf die Personaldaten eingeräumt sein soll, als es für die Aufgabenwahrnehmung unbedingt notwendig ist. Dabei wurden u.a. folgende Mängel festgestellt:

- Vorlage von Personalakten
  Bei Einstellungen, Versetzungen in den Ruhestand oder auch für die Festlegung des Versorgungsausgleichs im Ehescheidungsverfahren ist die ZBS auf zahlreiche Informationen über den Bediensteten angewiesen, etwa um das Besoldungsdienstalter oder die ruhegehaltsfähige Dienstzeit zu berechnen. In solchen Fällen übersenden die Ressorts der Einfachheit halber der ZBS die gesamte Personalakte. Bei der Prüfung habe ich mich davon überzeugen können, wie umfangreich solche Akten oft sind und welche Informationen sich z.B. bei der Ruhestandsversetzung nach einer jahrzehntelangen Dienstzeit angesammelt haben. Bewerbungsunterlagen, Zeugnisse, Strafregisterauszüge, Dienstversäumnisblätter, Beurteilungen sind darin ebenso zu finden, wie ärztliche Gutachten und alte Beihilfevorgänge. Diese Unterlagen werden vollständig durchgesehen, um die benötigten Daten herauszusuchen.

  Ich halte diese Verfahrensweise für unzulässig; die Personalakte enthält Informationen, deren Kenntnis für die ZBS zur Aufgabenerfüllung überwiegend nicht benötigt werden. Es reicht aus, wenn die personalaktenführende Dienststelle ihre Akten selbst auswertet und der ZBS die für die jeweilige Personalmaßnahme benötigten Daten übermittelt. Um zu gewährleisten, daß die Dienststellen die Daten in dem erforderlichen Umfange mitteilen, sollte die ZBS - wie dies in der Gemeinsamen Anordnung aus dem Jahre 1978 vorgesehen ist - für die jeweiligen Zwecke Vordrucke zur Verfügung stellen. Keine Bedenken bestehen, wenn die ZBS die den Anspruch begründenden Unterlagen, z.B. Bescheid, Urkunde, erhält.

  Die ZBS teilt zwar im wesentlichen meine Auffassung; sie will jedoch in Einzelfällen nicht auf die Anforderung der Personalakte verzichten. Ich halte

diese Forderung nicht für gerechtfertigt. Auch in schwierigen und unklaren Fällen können durch konkrete Nachfragen bei der personalaktenführenden Stelle die relevanten Fakten ermittelt werden.

- Direktauskunftsverfahren (Datenbankanwendung)
  Die ZDV-Saar, auf deren Rechner die Personalabrechnungsverfahren ablaufen, stellt der ZBS monatlich aktualisierte Daten aus den Bezügedateien in einer Datenbank zur Verfügung. Auswertungen aus der Datenbank werden sowohl für die ZBS selbst als auch auf Anforderung der einzelnen Ressorts vorgenommen.

Die Staatskanzlei hat regelmäßig in Form einer Personalliste Angaben über Bezüge, Familienstand, Anzahl der Kinder aller Landesbediensteten erhalten. Die Staatskanzlei rechtfertigt diese Datenanforderung damit, daß angesichts der extremen Haushaltsnotlage die Kenntnis der Bruttobezüge Voraussetzung einer zutreffenden Einschätzung möglicher Einsparpotentiale im Bereich der Personalkosten sei. Auf diese Weise werde das Besoldungs- und Tarifsystem transparent und kostenbezogen durchschaubar. Ich halte dieses Argument nicht für stichhaltig. Es ist nicht einzusehen, aus welchen Gründen die Staatskanzlei für ihre Planungsvorhaben personenbezogene Angaben benötigt. Auswertungen für die Ressorts dürfen - soweit nicht aggregierte, anonymisierte Daten ausreichen - nur den Personalbestand des jeweiligen Ressorts betreffen und nur die Daten enthalten, die zur Aufgabenerfüllung der anfordernden Stelle unerläßlich sind. Die der Staatskanzlei übermittelten Listen wurden mittlerweile vernichtet.

Die beliebige Auswertbarkeit des sowohl hinsichtlich der Vielzahl der Datenarten als auch hinsichtlich der Zahl der Betroffenen umfangreichen Daten-

bestandes ist problematisch. Die Sensibilität der Daten steht außer Frage; immerhin werden neben den Bezügebeträgen u.a. auch Angaben über Familienstand, Name und Alter der Kinder, Ehegatte im öffentlichen Dienst, Dienst- und Beschäftigungszeit, Besteuerungsmerkmale gespeichert. Es steht nicht von vornherein fest, welche Auswertungen für welche Zwecke mit welchem Inhalt für welche Empfänger vorgenommen werden. Zudem ist eine nachträgliche, vollständige Kontrolle über Art und Umfang der einzelnen Auswertungen nicht möglich.

Bei der automatisierten Verarbeitung von Personaldaten ist der Grundsatz der Transparenz der Datenverarbeitung zu beachten. Die Auswertungen der Datenbank sind auf Standardfälle zu beschränken; sie sind ihrer Art nach und mit dem Katalog der maximal darin aufzunehmenden Datenarten festzulegen und zu dokumentieren. Soweit über diese Standardauswertungen hinaus im Einzelfall für ein Ressort Auswertungen vorgenommen werden müssen, bedarf deren Ausführung der Beteiligung des jeweils zuständigen Personalrates.

Dem Transparenzerfordernis trägt das Beamtenrechtsrahmengesetz bereits Rechnung (§ 56 f). Danach sind in automatisierten Personalverwaltungsverfahren die Verarbeitungs- und Nutzungsformen festzulegen, zu dokumentieren und einschließlich des jeweiligen Verwendungszwecks sowie der regelmäßigen Empfänger allgemein bekannt zu geben.

Bei der "Einführung und Anwendung" automatisierter Verarbeitung von Personaldaten hat der Personalrat ein Mitbestimmungsrecht, soweit es sich nicht nur um die bloße Berechnung und Zahlbarmachung der Bezüge handelt (§ 84 Saarländisches Personalvertretungsgesetz). Die Datenbankanwendung unterliegt

deshalb - zumindest soweit Auswertungen für die Ressorts vorgenommen werden - der Mitbestimmung der Personalvertretung. Eine förmliche Beteiligung der Personalvertretung konnte nicht nachgewiesen werden. Die Personalvertretung ist nur dann im Stande mitzubestimmen, wenn Art und Umfang der Datenauswertungen festgelegt und damit übersehbar ist.

Mängel waren auch hinsichtlich der Datensicherung festzustellen. Die Zugriffsberechtigung auf die Datenbank ist auf zwei Mitarbeiter zu beschränken. Das Verfahren der Paßwortvergabe ist zu verbessern.

- PC-Einsatz
  Bei der ZBS sind mehrere PC eingesetzt; darunter auch ein Gerät für Anwendungen mit personenbezogenen Daten. Diese Anwendungen waren weder nach § 18 SDSG freigegeben noch waren ausreichende Maßnahmen zur Datensicherung getroffen. Das Ministerium der Finanzen hat am 26.08.1992 einen Leitfaden für die Erstellung von Dienstanweisungen für den PC-Einsatz in der Landesverwaltung herausgegeben. Die dort vorgesehenen Sicherheitsmaßnahmen, die Zuständigkeiten (insbesondere Funktionstrennung zwischen Programmierung, Systemverwaltung und Anwendung) und die zugelassenen Nutzungen sollten auch bei der ZBS festgeschrieben werden.

8.3.2 Zentrale Beihilfefestsetzungsstelle

Die Beihilfefestsetzung wurde 1989 für die gesamte Landesverwaltung der Zentralen Besoldungs- und Versorgungsstelle (ZBS) übertragen. Die Zentralisierung hat aus der Sicht des Datenschutzes den Vorzug, daß die Beihilfe von der Personalsachbearbeitung getrennt ist. Dadurch wird dem Gebot der Zweckbindung Rechnung getragen, daß keine medizinischen Daten aus der Beihilfe bei Personalentscheidungen verwendet werden. Die orga-

nisatorische und personelle Trennung ist bei der ZBS wegen ihrer Einbindung in die OFD nicht konsequent eingehalten; an den in meinem 12. TB (Tz. 8.1.1) beschriebenen, möglichen Konfliktsituationen hat sich seither nichts geändert.

Die Zentrale Beihilfefestsetzungsstelle wurde erstmals seit ihrer Bildung datenschutzrechtlich überprüft. Dabei hat sich herausgestellt, daß im automatisierten Beihilfeabrechnungssystem BABSY von seiner Konzeption her regelmäßig keine Krankheitsbezeichnungen gespeichert werden. Ebensowenig werden die einzelnen ärztlichen Leistungen sowie die Art der Heil- und Hilfsmittel erfaßt. Der Bearbeiter kann zwar Gebührenziffern von Einzelleistungen am Bildschirm eingeben, um den höchstzulässigen Gebührensatz festzustellen. Dieses lediglich zur Rechenunterstützung der Sachbearbeiter dienende Programm führt jedoch nicht zu einer Speicherung von Einzelleistungen oder Krankheitsbezeichnungen.
Unter Datenschutzgesichtspunkten problematisch ist dagegen die Speicherung bestimmter Beihilfedaten in Sondermasken zur Überwachung der Abrechnung, weil diese zum Teil Rückschlüsse auf bestimmte Erkrankungen zulassen. Problematisch ist vor allem die Speicherung psychotherapeutischer Behandlungen, weil daraus das Vorliegen einer seelischen Erkrankung erkennbar ist. Die Speicherung dieser Informationen stellt für den Betroffenen einen schwerwiegenden Eingriff in sein Persönlichkeitsrecht dar. Die Zugriffsrechte müssen beschränkt und die Speicherungsdauer muß verkürzt werden. Eine über die Einzelbearbeitung hinausgehende Selektion dieser Fälle ist derzeit programmtechnisch nicht realisiert und muß auch für die Zukunft ausgeschlossen werden.

Die organisatorisch-technischen Maßnahmen der Datensicherung müssen verbessert werden:

- Zugriffsbefugnisse:
  Zugriffsbefugnisse - vor allem der sogenannten "Springer" ohne festes Arbeitsgebiet, die im Bedarfsfall eingesetzt werden - müssen im tatsächlichen jeweiligen sachlichen Zuständigkeitsbereich entsprechend vergeben werden. Es geht nicht an, daß Sachbearbeiter auf alle gespeicherten Beihilfedaten zugreifen können. Das Argument, das die Vergabe von Paßwörtern einen zu großen Arbeitsaufwand verursache, kann man nicht gelten lassen. Wenn der Einsatz von vier Springern beibehalten wird, muß der dadurch entstehende Aufwand für die Vergabe der Zugriffsrechte in Kauf genommen werden. Entsprechende Zugriffssicherungen werden z.B. im Bereich des Versorgungsamtes bei dem Verfahren nach dem Schwerbehindertengesetz beachtet.

- Datenlöschung
  Die Daten der 12 letzten Beihilfeanträge werden - unabhängig davon, wie lange sie zurückliegen - gespeichert. Jeder Folgeantrag verursacht die Löschung der ältesten Antragsdaten. Beihilfedaten eines Beihilfeberechtigten, der 12 Anträge im Jahr stellt, bleiben demnach - sofern keine "Sondermaske" in Betracht kommt - nur ein Jahr gespeichert, Daten desjenigen, der nur einen Antrag jährlich vorlegt, dagegen 12 Jahre. Die in den bereits oben beschriebenen "Sondermasken" gespeicherten Daten wurden seit dem erstmaligen Einsatz des Verfahrens nicht gelöscht.
  Die Daten dürfen nur solange gespeichert bleiben, wie sie zur Aufgabenerfüllung erforderlich sind. Nach § 17 Abs. 3 Beihilfeverordnung wird die Beihilfe nur gewährt, wenn der Beihilfeberechtigte sie innerhalb eines Jahres nach Entstehen der Aufwendungen, spätestens jedoch ein Jahr nach der ersten Ausstellung der Rechnung beantragt hat. Maßgebend

für den Löschungszeitpunkt kann demnach nicht die Anzahl der Anträge, sondern nur der Ablauf einer Frist sein. Die Löschung darf sich nicht an der Speicherkapazität orientieren, sondern daran, wie lange die Daten für die Beihilfebearbeitung benötigt werden. Der 1989 im Rahmen des Freigabeverfahrens vorgelegte Entwurf eines Löschungskonzepts ging von dem richtigen Ansatz aus, indem er programmgesteuert die Sperrung und Löschung nach Ablauf bestimmter, von der Fallkonstellation abhängiger Fristen vorgesehen hat. Allerdings waren die in dem Konzept vorgesehenen Fristen sehr lange bemessen, weil alle theoretisch nur denkbaren Verzögerungen (z.B. Verjährungsfrist für Arztforderung) mit jeweils maximal kalkuliertem Zeitablauf berücksichtigt waren. Dadurch ergeben sich Speicherungszeiträume von bis zu 8 Jahren. Eine Fristverkürzung erscheint möglich, aber auch geboten.
Unerläßlich ist wegen der besonderen Sensibilität eine Löschung der Daten bei psychotherapeutischer Behandlung, wenn die Maßnahme abgeschlossen ist, d.h. alle bewilligten Sitzungen abgerechnet sind. Es ist zumutbar, sofern eine neue Rechnung vorgelegt wird, anhand der Beihilfeakte zu kontrollieren, ob eine Doppeleinreichung vorliegt.

Seit der Einrichtung der Zentralen Beihilfefestsetzungsstelle wurden keine Beihilfevorgänge ausgesondert und vernichtet. Die damals von den einzelnen Landesbehörden übernommenen Akten enthalten zum Teil jahrzehntealte Vorgänge, unter anderem auch Einzelbelege mit medizinischem Inhalt. Eine Aussonderung wurde von der ZBS zwischenzeitlich zwar zugesagt, der Termin jedoch offengehalten.

Eine besondere Behandlung der Beihilfeanträge von Mitarbeitern der Festsetzungsstelle ist nicht vorgesehen. Zur Zeit ist - mehr zufällig mit Rücksicht auf

die Buchstabenaufteilung - lediglich gewährleistet, daß kein Sachbearbeiter in eigenen Beihilfeangelegenheiten tätig wird. Mit dem Beihilfeantrag werden der Dienststelle Informationen über die Erkrankungen des Antragstellers und dessen Angehörigen offenbart (Diagnose auf Arztrechnungen, Art der verordneten Medikamente). Wie Eingaben zeigen, ist das Problem im Bereich der Beihilfestelle wiederholt aufgetreten. Kollegen und möglicherweise auch der Vorgesetzte erhalten Kenntnis von der gesundheitlichen Situation, z.B. von psychiatrischen Behandlungen. Bei gesetzlichen Krankenkassen schreibt das Sozialgesetzbuch V (§ 284 Abs. 4) vor, daß Personen, die kassenintern Personalentscheidungen treffen oder daran mitwirken können, keinen Zugang zu den Versicherungs- und Leistungsdaten der Beschäftigten einschließlich der Daten ihrer mitversicherten Angehörigen haben dürfen. Um Risiken einer unbefugten Nutzung der Beihilfedaten zu verringern, habe ich vorgeschlagen, die Bearbeitung der Beihilfe für die Mitarbeiter einem bestimmten Sachbearbeiter zu übertragen, der das Vertrauen der Kollegen genießt. Darüber hinaus sollte der Arbeitsablauf so gestaltet werden, daß Vorgesetzte und (außer dem Prüfer) weitere Mitarbeiter keine Einzelbelege einsehen können.

Bisher war die ZBS nicht davon zu überzeugen, daß die Beihilfedaten der Mitarbeiter des besonderen Schutzes bedürfen.

8.3.3 Förmlichkeiten des Beihilfeantrags: Vorlage von Fotokopien

Beihilfefähige Aufwendungen sind durch Vorlage der Belege nachzuweisen. Dabei genügen Rechnungsduplikate; die Originalbelege werden der Krankenversicherung zur Erstattung der Restkosten eingereicht.

Ein Beihilfeberechtigter hatte sich in einer Eingabe darüber beklagt, daß von der Apotheke gefertigte und beglaubigte Fotokopien von Arzneimittelrezepten bei der Beihilfe nicht anerkannt werden. Die Übereinstimmung der Kopie mit dem Original mußte durch eine Behörde oder die Krankenversicherung beglaubigt werden. Wenn der Antragsteller nicht den Weg zur Versicherung auf sich nehmen wollte, legte er die Belege dem ein Dienstsiegel führenden Kollegen oder Vorgesetzten zur Beglaubigung der Kopie vor. Dieser konnte unschwer aus der Art der verordneten Medikamente oder aus der Facharztbezeichnung Rückschlüsse auf die Erkrankungen des Beamten oder dessen Angehörigen ziehen. Um solche Beeinträchtigungen der Persönlichkeitsrechte der Betroffenen zu vermeiden, habe ich beim federführenden Ministerium des Innern angeregt, auch die Anerkennung der von Apotheken gefertigten Kopien zuzulassen. Das Ministerium des Innern hat in einer eingehenden Stellungnahme dieses Ansinnen zurückgewiesen und andere Alternativen aufgezeigt. Die Ablehnung gipfelte in der Aussage, daß dann, wenn der Antragsteller selbst entscheide, statt der Originalbelege (bevor sie der Krankenversicherung vorgelegt werden) beglaubigte Abschriften einzureichen, seine Persönlichkeitsrechte nicht verletzt seien.

Ich habe daraufhin den Petenten darüber informiert, daß ich mit meinen Argumenten leider nicht durchgedrungen bin. Später habe ich durch Zufall erfahren, daß mittlerweile das Ministerium des Innern die Ausführungsvorschriften zur Beihilfeverordnung geändert und darin ausdrücklich (nicht beglaubigte) Fotokopien als Nachweis der Aufwendungen anerkannt hat. Offensichtlich sollte verhindert werden, daß diese Verfahrensänderung als Konzession an den Datenschutz verstanden wird.

9. Archivwesen (Bilanz)

Am 1. Januar 1993 ist das Saarländische Archivgesetz (SArchG) in Kraft getreten. Bereits in meinem 4. Tätigkeitsbericht für das Jahr 1982, Tz. 8, habe ich auf die Notwendigkeit eines Archivgesetzes hingewiesen. Trotz meiner wiederholten Forderungen nach Erlaß eines Archivgesetzes in den Folgejahren hat es 10 Jahre bis zur Verabschiedung des Gesetzes gedauert.

Ein Archivgesetz ist notwendig, weil in den Archiven des Landes, der Gemeinden und Gemeindeverbände und sonstiger öffentlicher Stellen eine Vielzahl personenbezogener Daten vorgehalten wird. Archivgesetze sind geeignet, die Rechte und Pflichten der Archive, der datenliefernden Verwaltungsstellen, der Benutzer und der Betroffenen festzulegen und gegeneinander abzugrenzen.

Das Archivgesetz definiert, was unter "Archivgut" und "Archivierung" zu verstehen ist. Es legt Schutzrechte für die Betroffenen fest, deren personenbezogene Daten in einem Archiv gespeichert sind. Unzulässig gespeicherte personenbezogene Daten sind zu löschen, unrichtige Daten sind entsprechend zu kennzeichnen. Den Betroffenen steht grundsätzlich ein Auskunftsrecht zu, auf Antrag kann auch Akteneinsicht gewährt werden, soweit schutzwürdige Interessen Dritter nicht berührt werden. Meiner Forderung, dem Betroffenen einen Anspruch auf Akteneinsicht einzuräumen, hat der Gesetzgeber nicht entsprochen. Nicht entsprochen wurde auch meinem Vorschlag, eine Bestimmung aufzunehmen, wonach der Betroffene darauf hinzuweisen ist, daß er sich an den Landesbeauftragten für den Datenschutz wenden kann, wenn Auskunft oder Akteneinsicht nicht gewährt werden. In Fällen der Auskunftsverweigerung hat sich die Beteiligung des Landesbeauftragten für Datenschutz in der Vergangenheit bewährt. Nach dem Entwurf sollten

das Recht auf Auskunft und Akteneinsicht auch den Erben des Betroffenen zustehen. Ich habe erreicht, daß die Wahrnehmung dieser Schutzrechte auf die nächsten Angehörigen, nämlich die Ehegatten, die Kinder und die Eltern beschränkt worden sind.

Einen weiteren Schwerpunkt des Gesetzes bilden die Vorschriften über das Verfahren der Aussonderung und Anbietung der Verwaltungsunterlagen an das Landesarchiv. So dürfen die nach den Bestimmungen des Strafgesetzbuches geschützten Unterlagen der Gesundheitsbehörden und der Beratungsstellen nur in anonymisierter Form angeboten werden. Auf meine Anregung hin wurde in das Archivgesetz die Bestimmung aufgenommen, daß Unterlagen spätestens 30 Jahre nach ihrer Entstehung auszusondern und anzubieten sind und das Archiv nach Ablauf eines halben Jahres über die Übernahme zu entscheiden hat. Eine längere Aufbewahrung ist nur zulässig, wenn diese gesetzlich zugelassen oder ausnahmsweise für die Wahrnehmung dienstlicher Aufgaben erforderlich ist. Die Abgabe an das Landesarchiv kann jedenfalls nicht auf unabsehbare Zeit verzögert werden.

Nicht aufgegriffen wurde mein Vorschlag, daß umfangreiche Sammlungen von Unterlagen und gespeicherte maschinenlesbare Informationen nicht vollständig, sondern nur in einer Auswahl übernommen werden dürfen. Ich bin der Auffassung, daß eine vollständige Übernahme ganzer Verwaltungsbereiche dem Grundsatz der Verhältnismäßigkeit widerspricht. Für Archivzwecke ist eine gezielte Auswahl ausreichend.

Zentrale Bedeutung kommt den Vorschriften über die Nutzung personenbezogenen Archivgutes durch Dritte zu. Das Archivgesetz gestattet die Nutzung zu amtlichen, wissenschaftlichen oder publizistischen Zwecken sowie zur Wahrnehmung berechtigter persönlicher Belange. Die

Nutzungsrechte Dritter werden durch Schutzfristen eingeschränkt. So darf personenbezogenes Archivgut erst 30 Jahre nach dem Tod des Betroffenen genutzt werden. Wenn der Todestag nicht feststellbar ist, endet die Schutzfrist 110 Jahre nach der Geburt des Betroffenen. Für wissenschaftliche Forschungen können die Schutzfristen im Einzelfall verkürzt werden. Eine Verkürzung ist zulässig, wenn die Betroffenen eingewilligt haben, oder wenn die Benutzung für die Durchführung eines bestimmten Forschungsvorhabens erforderlich ist und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt. Im Gesetzgebungsverfahren habe ich die Auffassung vertreten, daß die Voraussetzungen der Verkürzung der Schutzfristen für Forschungsvorhaben zu großzügig formuliert sind.

Das Gesetz entspricht nur in einigen Punkten nicht meinen Vorstellungen. Es ist zu begrüßen, daß in einem wichtigen Bereich der Umgang mit personenbezogenen Daten gesetzlich geregelt wurde.

10. Epidemiologisches Krebsregister

Im Berichtszeitraum hat das saarländische Krebsregister sein 25jähriges Bestehen gefeiert. Aus diesem Anlaß wurde ein wissenschaftliches Symposium veranstaltet, bei dem auch die Anforderungen des Datenschutzes an Krebsregister diskutiert wurden. Das Jubiläum war auch für mich Anlaß, meine Überlegungen zu diesem Thema zusammenfassend darzustellen.

10.1 Allgemeines

Das Saarland hat als erstes Bundesland 1979 ein Krebsregistergesetz verabschiedet. Zu diesem Zeitpunkt war die Datenschutzdiskussion noch in den Anfängen. Deshalb können Defizite in der gesetzlichen Regelung nicht verwundern.

Ausgangspunkt aller Überlegungen ist der rechtsstaatliche Ansatz, der auch in der saarländischen Verfassung (Art. 2) verankert ist. Der Eingriff in das informationelle Selbstbestimmungsrecht als Grundrecht durch Erhebung und Verarbeitung personenbezogener Daten darf, wenn nicht der Betroffene verbindlich eingewilligt hat, nur im überwiegenden Allgemeininteresse aufgrund eines förmlichen Gesetzes erfolgen (Art. 2 GG). Es unterliegt keinem Zweifel, daß gerade die Erhebung und Verarbeitung personenbezogener, medizinischer Daten von Krebskranken als Eingriff in die durch das Grundgesetz verbürgten Persönlichkeitsrechte einer detaillierten, bereichsspezifischen, gesetzlichen Grundlage bedürfen. Krankheitsdaten gehören zu dem intimsten Bereich der persönlichen Geheimsphäre.

Selbst wenn der betroffene Patient in voller Kenntnis der Verwendungszusammenhänge seiner Daten in die Übermittlung an das Krebsregister eingewilligt hat, sind gesetzliche Regelungen notwendig, um die organisato-

risch-technischen Vorkehrungen festzulegen, die den Schutz der Persönlichkeitsrechte der Betroffenen gewährleisten (BVerfGE 65, 1 ff., 44).

Aus der verfassungsrechtlichen Verpflichtung des Gesetzgebers, für jede Einschränkung des Selbstbestimmungsrechts durch Informationsverarbeitung eine gesetzliche Grundlage zu schaffen, folgt, daß sich die gesetzlichen Regelungen nicht auf den Schutz vor Mißbrauch der Daten allein beschränken. Gegenstand des Datenschutzes ist der rechtmäßige Umgang mit personenbezogenen Daten und nicht nur - wie man in den Diskussionen um das Krebsregister immer wieder hört - die Verhinderung vorwerfbaren Verhaltens (vgl. § 1 Abs. 1 BDSG). Der betroffene Patient ist eben nicht nur ein reines Objekt der Informationsverarbeitung, auch wenn es um Forschung oder statistische Aufbereitung im Interesse der Wissenschaft geht.

10.2 Andere gesetzlich geregelten Modelle

Das saarländische Melderechtsmodell unterscheidet sich in einem wesentlichen Punkt von den anderen gesetzlich geregelten Modellen in der BRD.

Im Gegensatz zu dem nordrhein-westfälischen und hamburgischen Krebsregistergesetz ermächtigt das saarländische Gesetz über das Krebsregister (SKRG) vom 17. Januar 1979 (Amtsbl. S. 105) den behandelnden Arzt ohne Einwilligung des Betroffenen, personenbeziehbare Einzelheiten der Krebserkrankung seiner Patienten an die beim Statistischen Landesamt des Saarlandes eingerichtete Registerstelle zu melden.

Im Gegensatz zum Sächsischen Entwurf eines Krebsregistergesetzes sind die Ärzte im Saarland zu einer Meldung berechtigt, jedoch nicht verpflichtet; die Meldung erfolgt von seiten der Ärzte freiwillig. Der

betroffene Krebskranke ist jedoch nicht beteiligt; er muß jedenfalls von dieser seiner Meldung zum Register nichts erfahren. Diese Art einer förmlichen Erhebung und Übersendung an das Statistische Landesamt als öffentlicher Stelle - ohne Kenntnis des Betroffenen - kommt einer zwangsweisen Datenverarbeitung gleich. Ist die Aufklärung des einzelnen Betroffenen - aus welchen Gründen auch immer - nicht möglich, bedarf es um so mehr einer gesetzlichen Ermächtigung, die den Umfang des Eingriffes genau festlegt.

Normenklarheit der gesetzlichen Eingriffsermächtigung ist ein wesentliches Instrument der Transparenz. Patienten haben sich darüber beklagt, daß sie keine Auskunft darüber erhalten, was über sie gespeichert ist, was mit ihren Daten geschieht. Das sind Ängste, die ernstzunehmen wir verpflichtet sind. Auch deshalb hat das Gesetz den genauen Umfang der Datenerhebung und die Verarbeitungsprozeduren präzise festzulegen, damit der Bürger wenigstens erkennen kann, welche Datenarten zu seiner Person erhoben wurden und wie mit seinen Daten umgegangen wird.

10.3 Verhältnismäßigkeit der Registerspeicherung

Ein weiteres wesentliches Element einer Krebsregisterregelung ist der Verfassungsgesichtspunkt der Verhältnismäßigkeit. Es ist ein schonender Ausgleich zwischen dem Eingriff in das Persönlichkeitsrecht des betroffenen Patienten und den im Allgemeininteresse liegenden Informationsbedürfnissen von Statistik und Wissenschaft zu finden, der beide Positionen optimal zur Geltung kommen läßt. Da auf die Einwilligung als der milderen Form der Datenerhebung verzichtet wurde, ist ein besonders schonender Umgang mit den Krankheitsdaten auch intern in der Registerstelle geboten. Es geht eben nicht nur um den Schutz vor Mißbrauch, sondern um den rechtmäßigen, d.h. verfassungsmäßigen Umgang mit

den Daten des Krebspatienten. Es ist das jeweils mildeste Mittel für den Verarbeitungsprozeß zu wählen.

10.4 Saarländisches Krebsregister (Prüfergebnisse)

Bei einer Überprüfung des saarländischen Krebsregisters haben sich im wesentlichen folgende Kritikpunkte ergeben:

10.4.1 Datenumfang der Registermeldungen

Die Ärzte melden Daten in größerem Umfang zum Register, als im Gesetz vorgesehen. Weder für die "Straße" als Teil der Wohnadresse noch für das vollständige Geburtsdatum besteht eine gesetzliche Ermächtigung (lediglich Alter und Wohnort sind im Gesetz ausdrücklich erwähnt). Ein abschließender Katalog der Erhebungsmerkmale ist durch Gesetz festzulegen. Wenn die genannten Angaben für die Zwecke des Registers erforderlich sind, und daran habe ich keinen Zweifel, ist das Gesetz insoweit zu ergänzen.

10.4.2 Sterbefallzählkarten

Die Sterbefallzählkarten aus der "Statistik der Bevölkerungsbewegung und der Fortschreibung des Bevölkerungsstandes" sowie die Todesbescheinigungen, die die genannte Zählkarte ersetzen können, werden zum Abgleich mit dem Krebsregister zur Feststellung und Registrierung neuer Fälle sowie zur Ergänzung des Sterbedatums und der Todesursache bereits bekannter Fälle genutzt. Bei neuen Fällen von Krebserkrankungen fordert das Krebsregister den die Todesbescheinigung ausstellenden Arzt auf, zur Ergänzung der medizinischen Angaben eine Krebsregistermeldung abzugeben.

Daten aus der Bevölkerungsstatistik können nicht ohne weiteres für eine Aufforderung an den Arzt genutzt

werden, der aus welchen Gründen auch immer bisher nicht zu einer Meldung bereit war. Personenbezogene Daten, die für einen ganz anderen Zweck erhoben wurden, dürfen ohne gesetzliche Ermächtigung nicht zur Informationsbeschaffung für das Krebsregister verwendet werden. Hinzu kommt noch, daß der Arzt, der bisher eine Meldung nicht abgegeben hat, in eine Art faktischen Zwang gerät, seine Meldung abzugeben.

10.4.3 Dateitrennung und Anonymisierung

Die Registerstelle hat nach dem Saarländischen Krebsregistergesetz die Daten zu anonymisieren (§ 5 Satz 1 SKRG). Deshalb gebietet das Gesetz Dateitrennung. Die identifizierenden Daten und die medizinischen Angaben sind gesondert zu speichern. Die Dateien dürfen nur zusammengeführt werden, wenn es für statistische Zwecke erforderlich ist (§ 5 Satz 3); das bedeutet, eine Deanonymisierung ist auch innerhalb des Registers nur für statistische Zwecke zugelassen. Wie die Anonymität durch Absonderung der Identifikatoren im einzelnen herzustellen ist, legt das Gesetz nicht mit der gebotenen Klarheit fest. Daß eine Reidentifikation zu statistischen Auswertungen ausdrücklich zugelassen wird, macht aber auch deutlich, daß die Anforderungen an die Anonymität nicht zu niedrig angesetzt werden dürfen. Es geht jedenfalls nicht an, daß die Dateitrennung so gestaltet wird, daß eine statistische Auswertung auch ohne Zusammenführung der beiden Dateien jederzeit und zu jedem Zweck möglich ist. Sonst wäre die Dateitrennung sinnlos und könnte entfallen. Gerade dies wäre aber mit dem Gesetz und dem Prinzip der Verhältnismäßigkeit nicht vereinbar.

Die Dateitrennung, wie sie derzeit praktiziert wird, dürfte ihren Zweck nicht erfüllen. Als Identifikatoren kommen insbesondere in Betracht: Namen, Adresse, Geburtsdatum und Sterbedatum. Tatsächlich sind von die-

sen Merkmalen in der Datei der medizinischen Daten Wohnort, Geburtsdatum und Sterbedatum gespeichert, lediglich Namen und Straße sind in die Datei der Identifikatoren übernommen. Der Umfang der abgesonderten, identifizierenden Daten ist so minimal gehalten, daß eine Zusammenführung der Dateien für Zwecke der statistischen Auswertung bislang nicht notwendig geworden war. So die Aussage der Bediensteten der Registerstelle, die durch die Tatsache erhärtet wird, daß Protokolle für die Tatsache und den Grund der Zusammenführung - wie es das Gesetz in einem solchen Fall vorsieht - nicht vorgelegt wurden (§ 5 Satz 4 SKRG). Dem Buchstaben des Gesetzes wird zwar formell durch den Aufbau zweier Dateien Rechnung getragen. Wird eine Deanonymisierung durch Zusammenführung der Dateien aber überhaupt nicht notwendig, ist die tatsächlich verwirklichte Anonymität außerordentlich gering. Bei den kleinräumigen Verhältnissen im Saarland können aufgrund von Wohnort, Beruf und Sterbedatum mit Hilfe der Sterbeanzeigen in der Saarbrücker Zeitung ohne größeren Aufwand die Daten auf natürliche Personen zugeordnet werden. Der Verfahrenspraktikabilität wird der Vorrang vor einer ausreichenden Anonymität gegeben.

Die - wie auch immer ausgestaltete - Anonymität steht und fällt mit der Effizienz der Zugriffsregelung für die beiden Dateien, da jedenfalls über die Ordnungsnummer eine vollständige Reidentifizierung innerhalb des Krebsregisters möglich ist. Die Überprüfung hat ergeben, daß gerade die Zugriffsregelung erhebliche Mängel aufzeigt.

Im Krebsregister waren zum Zeitpunkt der Prüfung sechs Bedienstete beschäftigt. Außer der Leiterin und einer weiteren Kraft war allen Bediensteten der Zugriff zugleich auf die Identifikatoren und die medizinischen Daten eingeräumt. Die Dateitrennung durch entsprechen-

de Zugriffsregelung sicherzustellen, wird erst recht unterlaufen, wenn zusätzliche Schwierigkeiten durch Personalausfälle auftreten.

Die seit einiger Zeit angemahnte Dienstanweisung, die vor allem eine Funktionstrennung zwischen Anwender, Nutzung und Systemverwaltung sicherstellen und die Zugriffe regeln soll, ist bisher nicht vorgelegt worden. Beide Dateien werden auf einem einzigen Personalcomputer geführt. Der Paßwortschutz kann nach unseren Feststellungen unterlaufen werden, weil eine spezielle Sicherungssoftware zum Zeitpunkt der Prüfung nicht eingesetzt war.

Der Mangel einer genauen gesetzlichen Festlegung, wie die Anonymität herzustellen ist, nutzt die Registerstelle einseitig für eine Speicherorganisation, die einen möglichst komfortablen Ablauf der Auswertung ermöglicht. Die Dateitrennung war außerdem - jedenfalls zum Zeitpunkt der Prüfung - infolge gravierender Mängel in der Datensicherung nicht gewährleistet.

Die Defizite sind grundsätzlicher Art. Das Konzept des Saarländischen Krebsregistergesetzes ist insgesamt in Frage gestellt. Insbesondere muß gefragt werden, ob ein schonender Ausgleich durch Dateitrennung überhaupt erreicht werden kann, wenn der Registerstelle die alleinige Verfügungsmacht eingeräumt ist, die Anonymisierung und Reidentifikation zu organisieren. Ich greife eine These von Luhmann auf, daß Behörden ebenso wie alle sozialen Systeme für die Versuchung anfällig sind, Ziele unter Umgehung lästiger Vorschriften zu erreichen (Funktionen und Folgen formaler Organisation, Berlin 1964, S. 153 ff., 183, 270 f, 204 ff.). Unter den Bedingungen der Automation muß dies noch mehr gelten, wenn Betreiber und Benutzer der Automation identisch sind. Das Prüfergebnis spricht unter

Datenschutzgesichtspunkten gegen die Geeignetheit saarländischer Modelle.

10.5 Datenanforderungen der Wissenschaft

Aus dem Krebsregister dürfen Daten nur in anonymisierter Form übermittelt werden (§ 6 Satz 1 SKRG). Dieses derzeit geltende, strikte, gesetzliche Übermittlungsverbot gilt auch für die Datenanforderungen der Wissenschaft. Fall-, Kontroll- und Kohortenstudien, für die personenbezogene Daten aus dem Krebsregister benötigt werden, können derzeit trotz ihres unbestreitbaren Nutzens nicht durchgeführt werden.

Dieses für den Fortschritt der Wissenschaft bedauerliche Ergebnis muß korrigiert werden. Zwar ist aus der im Grundgesetz verbürgten Wissenschaftsfreiheit (Artikel 5 Abs. 3 GG) kein unmittelbarer Informationsanspruch herzuleiten (BVerfGE NJW 1986, 1241). Der Staat hat jedoch im Interesse der Wissenschaft wenigstens wissenschaftsfreundliche Bedingungen herzustellen. Das Grundrecht auf Leben (Artikel 2 Abs. 2 Satz 1 GG) begründet zwar nach überwiegender Meinung ebenfalls kein einklagbares Teilhaberrecht. Jedoch trifft den Staat aufgrund des Sozialstaatsgebots (Artikel 20 Abs. 1, Artikel 28 Abs. 1 GG) die Pflicht, eine möglichst optimale medizinische Versorgung aufrecht zu erhalten und auszubauen (vgl. v. Münch, Grundgesetz Kommentar Artikel 2, Rdnr. 51 a; Hesse, Handbuch des Verfassungsrechts, Herausgeber, Benda, Maihofer, Vogel, Seite 97 f). Der Staat hat für die notwendigen Einrichtungen der Daseinsvorsorge und die notwendigen gesetzlichen Ermächtigungen und die notwendigen Rahmenbedingungen zum Schutz des Persönlichkeitsrechts zu sorgen. Dazu muß das saarländische Krebsregister unter entsprechender Modifikation des Übermittlungsverbots novelliert werden. Dies fordere ich seit 1986 vergebens.

Es versteht sich von selbst, daß auch hier die Anforderungen der Verhältnismäßigkeit beachtet werden müssen. In Betracht zu ziehen ist unter anderem ein Genehmigungsverfahren unter Beteiligung sachverständiger Dritter (Ethik-Kommission, Ärztekammer), die die Erforderlichkeit der Datenanforderung im Hinblick auf ein bestimmtes Forschungsprojekt zu beurteilen hat. Je dichter das Netz verfahrensmäßiger Regelungen geknüpft ist, desto eher sind dem Betroffenen Eingriffe zuzumuten.

Ich habe nichts gegen die Auffassung des zuständigen Ministeriums einzuwenden, daß die Nutzung personenbezogener Krebsregisterdaten für besondere Forschungsvorhaben von der Zustimmung des Erkrankten abhängig zu machen ist. Diese Vorstellungen, die ich als grundsätzliche, konzeptionelle Aussage aus der Sicht des Datenschutzes nur positiv bewerten kann, können jedoch in die Praxis nur umgesetzt werden, wenn das gesetzliche Übermittlungsverbot aufgehoben ist. Niedrige Verarbeitungsschranken innerhalb des Registers haben den Gesetzgeber veranlaßt, die Abschottung nach außen um so strikter festzulegen. Deshalb rütteln die Versuche, die Datenübermittlung an externe Stellen zu lockern, an der Grundkonzeption des saarländischen Krebsregisters.

Verwahren muß ich mich gegen Vorwürfe, der Datenschutz verhindere die wissenschaftliche Forschung. Auf anderen Feldern der Verarbeitung von Krankheitsdaten habe ich dazu beigetragen, daß unter Abwägung aller verfassungsrechtlich relevanten Positionen praktikable, gesetzliche Regelungen gefunden wurden (so z.B. im Saarländischen Krankenhausgesetz zur Nutzung von Krankheitsdaten für wissenschaftliche Zwecke und für die Einrichtung klinischer, behandlungsbezogener Krankheitsregister). Die Informationserhebung und -verarbeitung für Zwecke des Krebsregisters steht unter dem

Gesetzesvorbehalt. Die Mitwirkung des Gesetzgebers ist unerläßlich. Versäumnisse der Gesetzgebung können dem Datenschutz nicht angelastet werden.

Als Ergebnis ist festzuhalten, daß die Rechtsgrundlage für die Datenerhebung und -verarbeitung im Epidemiologischen Krebsregister des Saarlandes unzulänglich ist. Das Saarländische Krebsregistergesetz muß fortgeschrieben werden.

11. Automation, Neue Medien, Überwachungstechniken

11.1 Fangschaltungsbeschluß des Bundesverfassungsgerichts

Das Bundesverfassungsgericht hat mit seinem Beschluß vom 25.03.1992 (NJW S. 1875) eine grundlegende Entscheidung zum Schutzbereich von Artikel 10 Abs. 1 GG getroffen. Die bisher in der Literatur vertretene Meinung kann nicht mehr aufrecht erhalten werden, das Fernmeldegeheimnis unterliege einer "betriebsbedingten", technischen oder organisatorischen, "immanenten" Schranke, die etwa die Mißbrauchsabwehr durch Fangschaltungen und Zähleinrichtungen ohne ausdrückliche gesetzliche Ermächtigung erlaube. Durch solche technischen Einrichtungen werden die Rufnummern der Anrufer bei bestimmten Anschlüssen registriert, um den Urheber von Belästigungen und Bedrohungen ausfindig zu machen. Damit hat das Bundesverfassungsgericht wieder einmal deutlich gemacht, daß der Gesetzgeber die wesentlichen Entscheidungen über die Verarbeitung personenbezogener Daten selbst treffen muß und diese nicht delegieren kann. Für die Erfassung von Gesprächsdaten mittels Fangschaltung und Zahlenvergleichseinrichtungen ist derzeit - so das Gericht - keine ausreichende gesetzliche Grundlage gegeben.

Zugleich unterstreicht das Gericht für den Bereich der Telekommunikation, daß das Fernmeldegeheimnis nicht nur die Kommunikationsinhalte, sondern auch den Kommunikationsvorgang, und damit auch die Nebendaten über Art, Zeitpunkt und Teilnehmer der Kommunikation schützt. Jegliche Registrierung solcher Daten bedarf somit einer verfassungskonformen, gesetzlichen Grundlage. Damit sind die in meinem letzten Tätigkeitsbericht (13. TB Tz. 3) angesprochenen Probleme im Zusammenhang mit den 1991 in Kraft getretenen Telekommunikationsverordnungen erneut auf dem Prüfstand. Denn die diesen

Rechtsverordnungen zugrundeliegende, gesetzliche Ermächtigung genügt nicht den Anforderungen.

Der Bundesminister für Post und Telekommunikation hat bereits eine Arbeitsgruppe eingerichtet, die die geforderten verfassungsgemäßen Rechtsgrundlagen erarbeiten soll. Es ist beabsichtigt, zusätzliche Vorschriften im Postverfassungsgesetz und im Fernmeldeanlagengesetz einzuführen, die nicht nur eine pauschale "Verordnungsermächtigung" enthalten sollen. Man kann gespannt sein, ob mit Ablauf dieser Legislaturperiode die notwendigen gesetzlichen Voraussetzungen geschaffen sein werden und die in der Entschließung der Datenschutzbeauftragten des Bundes und der Länder am 08.03.1991 formulierten datenschutzrechtlichen Mindesterfordernisse erfüllt sind (vgl. 13. TB Tz. 8 und Anlage 3). Diese Forderungen kann man wie folgt zusammenfassen:

- Die Verbindungsdaten sind nach Ende der Verbindung grundsätzlich zu löschen; für die Erstellung von Einzelentgeltnachweisen sollten die Zielrufnummern um die letzten vier Ziffern gekürzt werden.

- Die Erstellung von "Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

- Bei der Rufnummernanzeige müssen Anrufer und Angerufener die Möglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall "auf Knopfdruck" zu unterdrücken.

Mit dem Verhältnismäßigkeitsgrundsatz nicht vereinbar ist die Regelung des § 12 Fernmeldeanlagengesetz, wonach praktisch in jeder beliebigen strafgerichtlichen Ermittlung auf gespeicherte Verbindungsdaten zurückgegriffen werden darf.

11.2 Gefährdung des Fernmeldegeheimnisses durch unbefugtes Mithören der Funkkommunikation

Der Bundesminister für Post und Telekommunikation hat im Zuge der Liberalisierung des Rundfunkgerätemarktes durch Amtsblattverfügung die Herstellung und den Vertrieb von Runkfunkempfängern erlaubt, die das Abhören von kritischen Funkfrequenzbereichen ermöglichen. Der Funkverkehr von Behörden und Organisationen mit Sicherheitsaufgaben, insbesondere Polizei, Feuerwehr, Rettungsdienst, Katastrophenschutz, aber auch die Benutzung von schnurlosen Telefonen, Autotelefonen (C-Netz), Betriebsfunknetzen kann hinfort mit allgemein zugänglichen Rundfunkgeräten abgehört werden. Damit wachsen die Risiken für die Vertraulichkeit des nichtöffentlich gesprochenen Wortes und für das Recht auf ungestörte Kommunikation. Es ist nicht auszuschließen, daß durch Abhören des Polizeifunkes Namen und Adressen und sonstige polizeiliche Erkenntnisse über Personen bekannt werden. Dies gilt für einfache Verkehrsunfälle genauso wie für Kapitalverbrechen. Hochsensible medizinische Daten werden im Funkverkehr des Rettungsdienstes Unbefugten zugänglich. Zur Erzielung von Wettbewerbsvorteilen wächst das Interesse, solche sensiblen Frequenzen etwa im Bereich von Betriebsfunknetzen abzuhören.

Die Risiken sind umso größer, als Zweifel bestehen, ob der Empfang solcher Sendungen, die nicht für die Allgemeinheit bestimmt sind, untersagt und strafbar ist. Gemäß Beschluß des Bundesverfassungsgerichts genügt die Strafvorschrift des § 15 Fernmeldeanlagengesetz nicht den verfassungsrechtlichen Bestimmtheitsanforderungen (NJW 1989, 1663).

Aufgrund dieser Sachlage habe ich gefordert, daß zum Schutz des Fernmeldegeheimnisses eine Bestandsaufnahme

und Risikoanalye erforderlich ist. Dabei muß geprüft werden, für welche Funkanlagen jedenfalls mittelfristig zusätzliche Schutzmaßnahmen, in der Regel in Gestalt einer kryptografischen Verschlüsselung des Funkverkehrs geboten ist. Ferner sind Dienstvorschriften oder Arbeitsanweisungen mit dem Ziel zu überprüfen, daß die Übermittlung sensibler Sachverhalte im Funkwege möglichst unterbleibt oder so erfolgt, daß die Identifikation Betroffener möglichst erschwert wird. Alle Nutzer von Funkgeräten sollten umgehend auf die stark erhöhte Möglichkeit unbefugten Mithörens hingewiesen und zu entsprechendem Verhalten angehalten werden.

Nach Auffassung des Ministeriums des Innern gibt es derzeit noch keine ausgereiften technischen Möglichkeiten, dem unbefugten Abhören entgegenzuwirken, da weder praktikable Verschlüsselungs- noch genügend schutzbietende Verschleierungseinrichtungen verfügbar sind. Das Fernmeldegeheimnis soll durch Einhaltung einer besonderen Funkdisziplin gewahrt werden. Eine Lösung dieses Problemes sei erst nach Einführung neuer digitaler Funknetze möglich; dies sei jedoch erst ab dem Jahr 2000 zu erwarten.

Eine derartig lange Übergangszeit ist aus Datenschutzgesichtspunkten nicht akzeptabel. Ich halte es für unerläßlich, daß die bereits vorhandenen technischen Möglichkeiten (Verschleierungseinrichtungen), die das Abhören zwar nicht unmöglich machen, es jedoch erschweren, konsequent benutzt werden. Für besonders sensible, überschaubare Teilbereiche (z.B. Staatsschutz, Sondereinsatzkommandos) ist eine Ausstattung mit Geräten erforderlich, die den Funkverkehr verschlüsseln. Im übrigen ist der Funkverkehr mit personenbezogenen Daten auf das unbedingt notwendige Minimum zu reduzieren. Besteht eine Auswahl zwischen mehreren möglichen Verbindungen wie Telefon, Funk, Telefax, Telex, ist

grundsätzlich die für den Betroffenen am wenigsten belastende Verbindung zu wählen.

In der öffentlichen Verwaltung ist die Neubeschaffung von Autotelefonen, die bisher nicht im abhörsicheren D-Netz betrieben werden, im Interesse des Telefongeheimnisses unbedingt erforderlich. Aber auch die Bürger sowie die Unternehmen müssen auf die Gefahr hingewiesen werden. So kann nicht ausgeschlossen werden, daß im privaten Bereich Schnurlostelefone von Nachbarn oder Professionellen, z.B. durch Detekteien, abgehört werden. Auch im Bereich von Unternehmen (Geschäftsgeheimnisse) und der freien Berufe (z.B. Gespräch eines Anwaltes mit einem Mandanten oder eines Arztes mit einem Patienten) ist die Gefährdung des Fernmeldegeheimnisses nicht zu verkennen.

11.3 Telekommunikation

11.3.1 Interne Telekommunikationsanlagen (TK-Anlagen)

Die Überprüfung der TK-Anlage eines Ministeriums hat ergeben, daß den Risiken für das nichtöffentlich gesprochene Wort durch technische Vorkehrungen etwa der Hersteller nicht immer ausreichend vorgebeugt wird (12. TB Tz. 9.1; RSt S. 24). Vielfach kann gerade nur dem Erfordernis der Transparenz dadurch Rechnung getragen werden, daß die Betroffenen auf die bestehenden Risiken hingewiesen werden. So sind die Anwender der Funktion "Lauthören", die das unbemerkte Mithören eines Telefonats durch im Raum Anwesende ermöglicht, durch Rundschreiben darauf hingewiesen worden, daß der Gesprächspartner über die Aktivierung in Kenntnis zu setzen ist. Ferner sind die Bediensteten der Telefonzentrale angewiesen worden, sich nur in Ausnahmefällen in ein Gespräch einzuschalten. Andere Funktionen sind in der vorhandenen Anlage oft nicht änderbar (z.B. Unterdrückung der Rufnummernanzeige durch den Anrufer

bei Beratungsstellen). Wiederum andere Funktionen (z.B. Fangschaltung zur Registrierung von Verbindungsdaten mit der Möglichkeit gesonderter Auswertung) sind zwar gesperrt, die Schutzmechanismen, die ihre Aktivierung verhindern, sind jedoch nicht ausreichend entwickelt.

Angesichts des Ranges des geschützten Rechtsguts dürfte es nicht ausreichen, sich lediglich auf die bestehenden Vorschriften zu berufen, die eine Nutzung verbieten (RSt a.a.O.). Der Ausbau technisch-organisatorischer Maßnahmen der Datensicherung muß verbessert werden. Der Hersteller darf bei der Systemverwaltung nicht beteiligt bleiben (MdF RSt a.a.O.: eine völlige Ablösung ist zur Zeit nicht möglich), um Einflüsse Dritter auf die Handhabung dieser sensiblen Einrichtung vollständig auszuschalten. Dementsprechend wird im Bereich des Ministeriums für Bildung und Sport die Systemverwaltung durch eigene Bedienstete wahrgenommen (MfBS, RSt a.a.O.).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 1./2. Oktober 1992 (Anlage 8) darauf hingewiesen, daß der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes beim Einsatz von digitalen Telekommunikationsanlagen auch im Arbeitsverhältnis gewahrt werden muß. In diesem Bereich fehlen weitgehend verbindliche Vorgaben für die technische Ausgestaltung und den Umfang der zulässigen Datenverarbeitung.

Ich habe wiederholt das Ministerium der Finanzen aufgefordert, in der Landesverwaltung Regelungen für den Einsatz digitaler Nebenstellenanlagen zu treffen. Vor allem sind bisher keine Konsequenzen gezogen worden, wie den bei der Prüfung der Telefonnebenstellenanlage eines Ministeriums (vgl. 12. TB Tz. 9.1) zu Tage getre-

denen Mängeln bei der künftigen Beschaffung und Installation von Anlagen begegnet werden kann. Das Bundesverfassungsgericht hat betont, daß der Gesetzgeber mehr als früher organisatorische und verfahrensrechtliche Regelungen zu treffen hat, welche der Gefahr der Verletzung des Persönlichkeitsrechts entgegenwirken (BVerfGE 65,1 ff, 44). Wenigstens durch Verwaltungsanweisungen sollte im Interesse eines vorbeugenden Rechtsschutzes dieser Notwendigkeit Rechnung getragen werden. Folgende Regelungen halte ich für notwendig:

- Für die Beschaffung ist festzulegen, welche Leistungsmerkmale installiert werden dürfen, welche technischen Anforderungen erfüllt sein müssen (z.B. Unterdrückung der Rufnummernanzeige, Signalton beim Lauthören, automatische Ansage bei Rufumleitung, Datensicherungseinrichtungen wie Paßwortschutz und Protokollierung des Systemzustandes).

- Für die Betreiber ist vorzuschreiben, wie z.B. das Freigabeverfahren nach § 18 SDSG durchzuführen ist; daß ein eigener Systemverwalter zu bestellen ist; welche konkreten Maßnahmen der Datensicherung erfüllt sein müssen (insbesondere Zugang zur Anlage, Zugriff auf die im Gebühren-PC gespeicherten Daten), welche Kontrollen durchzuführen sind.

- Sind bestimmte Schutzmechanismen nicht installiert, sind die Benutzer anzuweisen, wie bei einzelnen Leistungsmerkmalen zu verfahren ist (z.B. Information des Anrufers bei Anrufumleitung, so daß dieser die Möglichkeit hat, die Verbindung abzubrechen; Unterrichtung des Gesprächsteilnehmers, wenn Einrichtungen zum Freisprechen, Lauthören oder Konferenzbetrieb eingeschaltet werden und kein automatischer Signalton erfolgt).

Das Ministerium hat wegen der Schwierigkeit, konkrete Mindestanforderungen zu entwickeln, den Erlaß allgemeiner Regelungen abgelehnt.

11.3.2 Internationaler Datenschutz

Die Arbeitsgruppe Telekommunikation und Medien der internationalen Datenschutzkonferenz hat sich in einem Bericht mit Problemen des Fernmeldegeheimnisses befaßt und dabei die Situation in den europäischen Ländern zu den Ausnahmeregelungen dargestellt, unter denen staatliche Stellen Telefongespräche abhören dürfen. Außerdem wird auf die Risiken der Satellitenkommunikation hingewiesen, die sowohl nationale als auch EG-Gesetzgebung umgehen kann. Satelliten werden zunehmend für Zwecke der Navigation und Standortbestimmung nicht nur von Schiffen, sondern auch von Lastwagen und sogar Einzelpersonen genutzt. Mit Hilfe der satellitengestützten Fernmeßtechnik kann nicht nur die Temperatur in einem Kühlwagen kontrolliert und angepaßt, sondern auch der Fahrer einer verstärkten Überwachung unterworfen werden.

Der Bericht sowie die gemeinsame Erklärung der 14. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 29.10.1992 sind in Anlage 9 abgedruckt.

11.3.3 Das integrierte Verwaltungs- und Kontrollsystem der EG (InVeKos) - Kommt der gläserne Landwirt?

Im Rahmen der tiefgreifenden strukturellen Umstellung im System der Landwirtschaftsförderung der EG sollen u.a. auch die Verfahren zur Antragstellung und -bearbeitung sowie zur Kontrolle der Angaben neu gestaltet werden. Die Überwachung mit Hilfe der Satellitentechnik ist ein wesentlicher, integraler Bestandteil des Konzepts. Der Rest der EG hat am 27.11.1992 als Rechts-

grundlage die Verordnung Nr. 3509/92 (ABl der EG L 355/1 vom 5.12.1992) erlassen.

In jedem Bundesland soll eine Datenbank nach einheitlichen Kriterien eingerichtet werden, in der alle Landwirte erfaßt werden, die an bestimmten Förderungsmaßnahmen teilnehmen. Die Flächen der betroffenen Landwirte, ihre geographische Lage, die Flächennutzungsarten sowie Daten zur wirtschaftlichen Situation der Betriebe sollen erfaßt werden. Förderungsrelevante Informationen - teilweise auch zur sozialen Lage des betroffenen Landwirts (Angaben zu Familienangehörigen, zum Familienstand, zum Einkommen) - sollen gespeichert werden. Die Grundstücke sollen nach einheitlichen Kriterien so bezeichnet werden, daß eine Kontrolle der angegebenen Nutzungsarten durch einen Vergleich mit Satellitenaufnahmen möglich wird.

Da im Bereich der EWG wohl kaum ein Landwirt ohne Beteiligung an irgendeiner Förderungsmaßnahme existieren kann, ist die Erfassung fast aller Landwirte in der landwirtschaftlichen Betriebsdatenbank unausweichlich. Das integrierte Verwaltungs- und Kontrollsystem ist also nichts anderes als eine lückenlose Erfassung der Landwirte zum Zwecke der Kontrolle im Bereich landwirtschaftlicher Förderungsmaßnahmen.

Ich habe das Ministerium für Wirtschaft gebeten, mich über den Sachstand zu unterrichten. Insbesondere habe ich um Mitteilung gebeten, welche datenschutzrechtlichen Vorkehrungen das Land vorgeschlagen hat.

Zwar muß von vornherein eingeräumt werden, daß hinreichende Kontrollen zur Wahrung des Gleichheitssatzes erforderlich sind (vgl. zum Bereich der Besteuerung Bundesverfassungsgericht NJW 91, 2129, 2131). Andererseits darf eventueller Mißbrauch staatlicher Leistungen nicht dazu führen, daß die rechtsstaatlichen Grund-

sätze der Verhältnismäßigkeit völlig vernachlässigt werden. Die Einschränkung des informationellen Selbstbestimmungsrechts darf nicht weitergehen, als es zum Schutz öffentlicher Interessen unerläßlich ist. Der einzelne darf nicht nur Objekt der staatlichen Maßnahmen sein. Nur in begründeten Fällen sollten Überwachungsmaßnahmen durchgeführt werden dürfen, nicht für ganze Bevölkerungsgruppen darf ausnahmslos das Mißtrauen zum Grundsatz werden.

Es ist zu bedauern, daß EG-Rechtsetzungsakte häufig an nationalen Institutionen vorbei wirksam werden. Eine grundsätzliche datenschutzrechtliche Erörterung der genannten Aspekte vor Erlaß der EG-Verordnung wäre dringend geboten gewesen. "Der gläserne Landwirt" sollte im Ergebnis nicht akzeptiert werden.

11.4 Bürokommunikation

Die Gefahren der Bürokommunikation habe ich bereits in meinem 11. Tätigkeitsbericht (Tz. 2) dargestellt. Ich habe stets gefordert, daß die datenschutzrechtlichen Aspekte als integrierender Bestandteil von vornherein gleichrangig mit allen anderen technischen und organisatorischen Problemen in die Untersuchungen für ein Bürokommunikationskonzept einbezogen werden müssen. Dies ist umso dringlicher, da - wie dem Protokoll des Ausschusses für Informationstechnologie und Kommunikation vom 12.01.1993 zu entnehmen ist - für einige Geschäftsbereiche schon umfassende Untersuchungen und Rahmenplanungen vorliegen und verbindliche Richtungsentscheidungen getroffen wurden (z.B. für UMIKOM beim Ministerium für Umwelt, für MIKOS beim Ministerium für Bildung und Sport, für SOJUS, SIJUS beim Ministerium der Justiz).

Im Auftrag der Haushaltsstrukturkommission hatte das Ministerium der Finanzen bis Ende 1992 einen Stufen-

plan zur Entwicklung der Bürokommunikation in der Landesverwaltung vorzulegen. Meine bereits dargelegte Forderung wurde zunächst nur zum Teil berücksichtigt. Bei den flankierenden Maßnahmen wurde lediglich die Abstimmung mit dem Landesbeauftragten für Datenschutz sowie ein Hinweis auf die Erforderlichkeit der Erstellung von Dienstanweisungen übernommen. Erst aufgrund weiterer Intervention meinerseits hat mir das Ministerium der Finanzen nunmehr mitgeteilt, daß im Zuge der Fortschreibung des Bürokommunikationskonzepts die folgende, von mir vorgeschlagene Formulierung aufgenommen werden soll: "Der Datenschutzaspekt ist integrierender Bestandteil der Entwicklung; die Verträglichkeit mit dem Persönlichkeitsrecht ist von Anfang an durch geeignete Maßnahmen zu gewährleisten."

Bis zu welchem Zeitpunkt diese Fortschreibung allerdings erfolgen soll, ist mir nicht bekannt.

11.5 Telefax

Nicht nur in der Privatwirtschaft, sondern auch in der öffentlichen Verwaltung verzeichnen Telefax-Geräte einen starken Zuwachs. So waren allein im Bereich der Landesverwaltung Ende 1992 ca. 250 Geräte installiert. Hinzu kommt noch eine unbekannte Zahl bei sonstigen öffentlichen Stellen, wie z.B. Körperschaften, Anstalten und den Gemeinden.

Folge ist, daß in der Verwaltung immer mehr Schreiben per Telefax versendet werden. Da davon auch verstärkt solche mit personenbezogenen Daten betroffen sind, sah ich die Notwendigkeit, auf die damit verbundenen Gefahren für den Datenschutz hinzuweisen.

Anders als Briefe kommen Schreiben über Telefax unverschlossen beim Empfänger an, so daß jeder, der vor der Entnahme durch den befugten Empfänger an das Gerät

gelangt, solches Schreibgut lesen oder gar entwenden kann.

Hinzu kann durch falsche Anwahl - ohne daß der Absender es merkt - ein Telefax leicht einem Empfänger zugesandt werden, für den es nicht bestimmt war.

Risiken entstehen auch dadurch, daß moderne Telefax-Geräte Anwahlspeicher mit Kurzrufnummern besitzen und zudem eine bedienerlose Übermittlung (z.B. zeitversetzt) zulassen.

Deshalb dürfen personenbezogene Daten per Telefax nur übermittelt werden, wenn durch technische und organisatorische Maßnahmen gewährleistet ist, daß das Schreiben nicht einer unbefugten Person zugänglich wird. Dies gilt erst recht für die einer besonderen Geheimhaltungspflicht unterliegenden Personal-, Sozial-, Arzt- oder Steuerdaten. Vorkehrungen sind insbesondere zu treffen zur Überprüfung der Anschlußkennung, damit der richtige Adressat angewählt wird und zur Sicherstellung des Empfangs durch den Befugten bei Eingängen innerhalb und vor allem außerhalb der Dienstzeit.

In einer mit dem Ministerium für Umwelt erarbeiteten Dienstanweisung für die Übermittlung von Daten mit Hilfe von Telefax-Geräten wurden meine datenschutzrechtlichen Aspekte weitgehend berücksichtigt. Ich habe diese Anweisung allen Ressorts, dem Saarländischen Städte- und Gemeindetag sowie dem Landkreistag zur Einführung empfohlen. Die Dienstanweisung ist als Anlage 10 abgedruckt.

11.6 Auftragsdatenverarbeitung

Im Rahmen der Erstellung eines Gesamtkonzeptes zur Fortentwicklung der Informationstechnik in der Landesverwaltung hat das Ministerium für Finanzen die Daten-

erfassung der öffentlichen Stellen zum Gegenstand von Wirtschaftlichkeitsbetrachtungen gemacht. Die Erfassungskosten privater Dienstleistungsunternehmen liegen oft unter den vergleichbaren Kosten der öffentlichen Stellen. Aufgrund der Haushaltssituation des Saarlandes sollten alle Ressort deshalb prüfen, ob und gegebenenfalls welche Erfassungsarbeiten kostengünstiger an private Unternehmen weitergegeben werden können. Neben den wirtschaftlichen sind jedoch auch die datenschutzrechtlichen Aspekte einer solchen Auftragsdatenverarbeitung zu beachten. Zuerst ist deshalb die rechtliche Zulässigkeit einer Auftragsdatenverarbeitung im konkreten Fall zu prüfen. Für eine Reihe von Fallbeispielen habe ich gegenüber den Ressorts folgende Auffassung vertreten:

Besonders sensible personenbezogene Daten sollten zur Auftragsdatenverarbeitung grundsätzlich nur an öffentliche Stellen vergeben werden, es sei denn, die Beauftragung privater Stellen ist auf gesetzlicher Grundlage erlaubt. Als besonders sensibel sind insbesondere Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen sowie Steuerdaten anzusehen.

Eine Auftragsdatenverarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, ist nur zulässig, wenn im Einzelfall eine Befugnis zur Offenbarung vorliegt.

Da für Daten, die dem Arztgeheimnis unterliegen, keine gesetzliche Vorschrift die Durchbrechung der Schweigepflicht erlaubt, bedarf es einer ausdrücklichen Entbindung von der Schweigepflicht durch den Betroffenen. Aus Gründen der Beweissicherung ist Schriftlichkeit der Einwilligung geboten. Auf die Rechtsprechung des Bundesgerichtshofs zur Abrechnung durch gewerbliche Verrechnungsstellen wird verwiesen (NJW 1991, 2955).

Krankenhäuser dürfen Patientendaten durch andere Stellen verarbeiten lassen, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der Datenverarbeitung hierdurch kostengünstiger besorgt werden können (vgl. oben Tz. 6.1 und 6.2). Mit Rücksicht auf die Sensibilität der Krankheitsdaten empfehle ich - ungeachtet der Rechtslage und mit Rücksicht auf die bisherigen Erfahrungen - von einer Auftragsdatenverarbeitung ohne Einwilligung des Betroffenen abzusehen. Der Patient sollte die Risiken kennen. Der Petent wird nicht nachvollziehen können, daß Krankenhäuser seine Krankheitsdaten sehr viel großzügiger durch andere Stellen verarbeiten lassen dürfen, als dies im Sozialbereich zulässig ist.

Daten, die dem Sozialgeheimnis unterliegen, dürfen durch nichtöffentliche Stellen nur bei Unvermeidbarkeit im Hinblick auf den Betriebsablauf und erheblichen Kostenvorteilen im Auftrag verarbeitet werden (§ 80 Abs. 5 SGB X). Für Daten der Sozialleistungsträger, die dem Arztgeheimnis unterliegen (vgl. oben Tz. 7.4), ist hingegen eine ausdrückliche Einwilligung des Betroffenen erforderlich (§ 76 Abs. 1 SGB X).

Daten, die dem Statistikgeheimnis unterliegen, dürfen durch Dritte im Auftrag verarbeitet werden, wenn die Vorschriften zum Schutz personenbezogener Daten und der statistischen Geheimhaltung eingehalten werden. Die Kenntnisnahme von Hilfsmerkmalen durch den Auftragnehmer muß dabei ausgeschlossen sein.

Neben diesen rechtlichen Voraussetzungen für die Zulässigkeit einer Auftragsdatenverarbeitung müssen auch strenge Anforderungen an die technisch-organisatorischen Datensicherungsmaßnahmen gestellt werden:

Der Auftragnehmer muß sorgfältig unter besonderer Berücksichtigung der Eignung und der getroffenen technischen und organisatorischen Datenschutzmaßnahmen ausgewählt werden.

Der Schutz beim Auftragnehmer muß gleichwertig mit dem der auftraggebenden Behörde sein.

Der Auftraggeber hat die Datenschutzmaßnahmen beim Auftragnehmer zu überwachen.

Die Verarbeitung oder Nutzung der Daten durch den Auftragnehmer darf nur im Rahmen der Weisungen des Auftraggebers erfolgen. Der schriftliche Auftrag sollte deshalb Regelungen enthalten über:

- Art und Gegenstand der vom Auftraggeber erwarteten DV-Tätigkeit;
- die zum Einsatz kommenden DV-Programme;
- die technischen und organisatorischen Maßnahmen der Datensicherung;
- etwaige Unterauftragsverhältnisse;
- Weisungsgebundenheit gegenüber dem Auftraggeber;
- Vertragsstrafen und das Recht auf Kündigung, wenn Datenschutzvorschriften verletzt werden;
- Unterwerfung unter die Kontrolle des Landesbeauftragten für Datenschutz.

12. Die Situation der Dienststelle

Die Aufgaben des Landesbeauftragten für Datenschutz sind vielfältig. Neben der Beratung in Fragen der Gesetzgebung auf Bundes- und Landesebene, die häufig umfangreiche Stellungnahmen erfordert, liegt das Hauptgewicht bei den Kontrollen aller öffentlichen Stellen des Landes und derjenigen, die seiner Aufsicht unterstehen. Zu letzteren gehören neben den Gemeinden und Landkreisen, alle nachgeordneten Landesdienststellen, aber auch sonstige Körperschaften des öffentlichen Rechts. Neuerdings ist der vielschichtige Bereich des Verfassungsschutzes hinzugekommen. Einen großen Raum nimmt aber auch die Beratung des Bürgers und der öffentlichen Stellen in allen Fragen des Datenschutzes ein. Als Aufsichtsbehörde für den privaten Bereich hat die Dienststelle seit der Novellierung des Bundesdatenschutzgesetzes erweiterte Kompetenzen wahrzunehmen.

Für die Wahrnehmung dieser meiner Funktionen als Landesbeauftragter für Datenschutz und als Aufsichtsbehörde für den privaten Bereich sind im höheren Dienst derzeit zwei Beamte in meiner Dienststelle tätig. Angesichts der Fülle und der Komplexität der Aufgaben genügt die Personalausstattung nicht mehr den Anforderungen. Zum Vergleich sei darauf verwiesen, daß der Bremische Datenschutzbeauftragte allein sechs Bedienstete des höheren Dienstes beschäftigt. Der Verwaltungsaufwand dürfte im Saarland sogar noch höher zu veranschlagen sein. Das Statistische Jahrbuch weist für das Saarland Ende 1990 einen Bevölkerungsstand von 1.073.000 und für Bremen zum gleichen Zeitpunkt von 682.000 Einwohner aus. Hinzu kommt noch die größere Flächenausdehnung des Saarlandes, die eine vielgestaltige, eher dezentrale Organisationsstruktur mit allein 52 Gemeinden zur Folge hat; in Bremen konzentriert sich die Verwaltung auf zwei Stadtgemeinden.

Die Fortentwicklung der Automation hat in den letzten Jahren einen stürmischen Verlauf genommen. Umfangreiche Systeme werden etwa in der Universität, im Landeskrankenhaus, bei der Zentralen Datenverarbeitung Saar, bei der Landesversicherungsanstalt, bei der Allgemeinen Ortskrankenkasse, bei den Städten und Gemeinden und in vielen anderen Bereichen unterhalten. Über die komplexen Probleme der Bürokommunikation und das DIPOL-System im Bereich der Polizei habe ich bereits berichtet. Angesichts der Bedeutung der Automation und der Gefahren, die sich hieraus für das Grundrecht der informationellen Selbstbestimmung ergeben, ist es nicht länger vertretbar, daß mir kein ausgebildeter Informatiker zur Verfügung steht. Ein solcher Mangel wird dem Stellenwert nicht gerecht, den Artikel 2 der Saarländischen Verfassung dem Datenschutz einräumt. Bereits mit Anlaufen des sehr umfangreichen DIPOL-Projektes Mitte des Jahres 1989 habe ich mit Schreiben vom 11.07.1989 das Innenministerium darum gebeten, auf eine entsprechende Stellenplanänderung hinzuwirken. Seither wurde in den Haushaltsverhandlungen mit dem Minister der Finanzen vergebens versucht, den Stellenplan entsprechend auszugestalten. Auch ein Schreiben an den Präsidenten des Landtages und die Fraktionsvorsitzenden vom 29.10.1990 hatte keinen Erfolg. Mit Schreiben vom 05.08.1991 habe ich das Innenministerium eindringlich darauf hingewiesen, daß die unter technischen Gesichtspunkten zu führende Erörterung der bislang vorliegenden Ergebnisse der Detailkonzeption von DIPOL die Zuweisung eines qualifizierten Informatikers erfordern. Ich habe ferner darauf aufmerksam gemacht, daß meine Beteiligung an dem Projekt sich auf die rein juristische Beurteilung beschränken muß und ich für die datenschutzgerechte, praktische Umsetzung keine Verantwortung übernehmen kann. Ich habe zugleich darauf hingewiesen, da angesichts des Entwicklungsstandes von DIPOL und mit Rücksicht darauf, daß die Ausschreibung einer Stelle sowie die sorgfältige Aus-

wahl von Bewerbern und die Einführung eines Technikers in das Datenschutzrecht viel Zeit in Anspruch nimmt, ich die Gefahr sehe, eine zeitgerechte Beurteilung von DIPOL nicht mehr garantieren zu können. In der Zwischenzeit ist die Dringlichkeit des Personalbedarfs vor allem im technischen Bereich nicht geringer geworden.

Aber auch im übrigen sind Mängel in der Personalausstattung vor allem in der Personalplanung zu beklagen.

Die hohe Personalfluktuation - Beamte des höheren Dienstes werden schon nach drei Jahren, in dem vergangenen Jahr bereits nach zwei Jahren ausgewechselt - hat die Kontinuität in der Aufgabenwahrnehmung - vor allem aber die Vertretung im Falle meiner Abwesenheit - bisher nicht gewährleisten können.

Mein Einfluß auf die Auswahl des Personals ist äußerst gering. Nach dem Saarländischen Datenschutzgesetz ist in Personalfragen lediglich das "Benehmen" mit mir herzustellen (§ 19 Abs. 4 SDSG); d.h. es besteht lediglich ein Anhörrecht. In allen anderen Bundesländern ist bei der Stellenbesetzung die Zustimmung des Datenschutzbeauftragten erforderlich. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder war anläßlich ihrer Sitzung vom 16./17. Februar 1993 übereinstimmend der Auffassung,

> "daß zur Sicherstellung der verfassungsrechtlich gebotenen Unabhängigkeit der Datenschutzbeauftragten stets ihr Einvernehmen bei Stellenbesetzungen in ihren Dienststellen herzustellen ist."

Das bedeutet, daß meine Zustimmung bei der Personalauswahl notwendig ist und der Gesetzgeber dies durch eine entsprechende Regelung im Saarländischen Datenschutzgesetz sicherstellen sollte.

Meine Arbeit war im Berichtszeitraum dadurch beeinträchtigt, daß einem mir zugewiesenen Beamten des höheren Dienstes zusätzlich die Aufgabe eines Arbeitsgemeinschaftsleiters für Gerichtsreferendare übertragen wurde. Zu dieser Personalverfügung wurde ich nicht einmal gehört. Vor allem aber hat das Innenministerium völlig ignoriert, daß der Beamte durch die Arbeitsgemeinschaftsleitung, die seine Arbeitskraft erheblich in Anspruch nahm, gleichzeitig der Weisungsbefugnis des Innenministeriums und der des Landesbeauftragten unterstand. Es ist jedoch gesetzlich festgeschrieben, daß die dem Landesbeauftragten für Datenschutz zugewiesenen Bediensteten nur an seine Weisung gebunden sind (§ 19 Abs. 4 SDSG). Ich habe in erheblichem Umfang auf mein eigenes Weisungsrecht verzichtet, um den Beamten nicht in eine Konfliktlage zu bringen. Mit meiner durch Gesetz festgeschriebenen Unabhängigkeit ist eine solche Situation jedoch unvereinbar.

Neuerdings sollte mir ein weiterer Beamter des höheren Dienstes zugewiesen werden; dies ist auch im Hinblick auf die neue Aufgabe im Bereich des Verfassungsschutzes dringend geboten. Wie das Ministerium des Innern jedoch meine Beteiligung in Personalfragen einschätzt, wird auch in diesem Fall deutlich. Obwohl die Organisationsverfügung im Zusammenhang mit der Neugestaltung des Organisations- und Geschäftsverteilungsplanes im Innenministerium diesen Beamten eindeutig meiner Dienststelle zuordnet, ist diese Verfügung, ohne daß ich hierüber überhaupt nur verständigt worden wäre, bislang nicht vollzogen worden. Der Beamte wurde an eine andere Stelle des Innenressorts zur Dienstleistung abgeordnet.

Dem Landesbeauftragten für Datenschutz sind gemäß § 19 Abs. 4 SDSG das zur Erfüllung seiner Aufgaben erforderliche Personal zur Verfügung zu stellen. Ich vermag

meinen Pflichten nicht mehr zeitgerecht und in dem gebotenen Umfang nachzukommen.

Anlage 1

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

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

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

Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG

den nachfolgenden Text zur Beratung:

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

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

- Stärkung der Grundrechte aus Art. 10 und 13 im Hinblick auf neue Überwachungstechniken
- Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)
- Instrumente zur Technikfolgenabschätzung.

Anlage 2

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuregelung des Asylverfahrens (BT-Drs. 12/2062) vom 28. April 1992

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

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

Zu 1.:
Nach dem geltenden Recht sind Lichtbilder und Fingerabdrucke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern - bis auf wenige Ausnahmen - Lichtbilder und Fingerabdrucke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar:
Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder - gleichgültig ob Deutscher oder Ausländer - muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die

Identität eines hohen Anteils der Asylbewerber - also nicht bloß diejenige einzelner oder bestimmter Gruppen - zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2.:

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

- Fingerabdrucke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sog. Kurzsatzverformelung der Fingerabdrucke aus. Gerade aber dabei soll es nicht bleiben: Mit der bevorstehenden Einführung von AFIS - einem neuen automatisierten Fingerabdruckverfahren - sollen künftig auch die Fingerabdrucke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrucke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche

Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte - über das Trennungsgebot des § 16 Abs. 4 hinaus - die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

- Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrucke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht - wie es der Gesetzentwurf aber vorsieht - praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.

- Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrucke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

Anlage 3

Entschließung
der Konferenz der Datenschutzbeauftragten
vom 1./2. Okt. 1992
zum "Lauschangriff"

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

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein "Innenraum" verbleiben, in dem er "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung - insbesondere heimlicher - entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbeson-

dere nicht das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf.

   Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z.B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

Anlage 4

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 16./17. Februar 1993
zur
Richtlinie des Rates vom 07. Juni 1990 über den freien Zugang zu Informationen über die Umwelt
(30/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaft die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgegebenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährleistung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgestzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grund-

sätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

Anlage 5

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 1./2. Okt. 1992
zur
Chip-Karte als elektronische Krankenversicherungskarte

Der LfD Hamburg trägt vor, daß es immer wieder Anfragen gibt, welche Daten auf der elektronischen Krankenversicherungskarte gespeichert werden dürfen. Im Hinblick darauf faßt die Konferenz folgenden

Beschluß:
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt wegen der wachsenden Automatisierung bei allen Institutionen des Gesundheitswesens und der Erweiterung des Anteils maschinenlesbarer Datenträger fest, daß eine Speicherung auf einer Chip-Karte als elektronische Krankenversicherungskarte auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß und nicht auf Gesundheitsdaten ausgedehnt werden darf. Eine technische Sicherung dieser Beschränkung ist zu gewährleisten.

Anlage 6

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

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

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.

- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präzisier als bisher vorgesehen geregelt werden.

- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie - auch zur Abrechnung - im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.

- Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

S. 143

Anlage 6

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

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

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.

- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präzisier als bisher vorgesehen geregelt werden.

automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

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

II. Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.

2. Der Arbeitgeber darf Daten des Arbeitnehmers - auch durch Befragen des Arbeitnehmers oder Bewerbers - nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetz-

lich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.

3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z.B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.

4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.

5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm - soweit erforderlich - nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.

7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen.

Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.

8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.

9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.

10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschn. I Abs. 4) eingewilligt hat.

Anlage 8

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

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

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

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

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

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.

- Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z.B. bei Feuerwehr und Rettungsdiensten).

- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.

- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.

- Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erfordelich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.

- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

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

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

Anlage 9

Bericht der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation

und

Gemeinsame Erklärung der 14. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 29. Oktober 1992

B e r i c h t

Fernmeldegeheimnis

1.

Jeder Bürger, der ein Telefon benutzt, hat grundsätzlich die legitime Erwartung, daß sein Telefongespräch von niemandem, insbesondere von keiner staatlichen Stelle, abgehört wird.

Der Grundsatz der Vertraulichkeit von Telefongesprächen ist deshalb in den Verfassungen verschiedener Länder wie z.B. Österreichs, Deutschlands, Griechenlands, der Niederlande, Portugals und Spaniens verankert. Darüber hinaus garantiert die Europäische Menschenrechtskonvention das Recht jedes Einzelnen auf Achtung seiner Privatsphäre, seines Familienlebens, seiner Wohnung und seiner Korrespondenz. Dieser Artikel der Europäischen Menschenrechtskonvention ist vom Europäischen Menschenrechtsgerichtshof so ausgelegt worden, daß er auch das Fernmeldegeheimnis umfaßt.

In vielen Ländern ist das Abhören von Telefongesprächen sogar ein Straftatbestand. Die bloße Behauptung, daß Telefone illegal abgehört worden seien, kann auch weitreichende politische Konsequenzen haben. So mußte kürzlich ein Minister der Republik Irland aufgrund derartiger Vorwürfe zurücktreten, um nur ein Beispiel zu geben.

Andererseits ist in den meisten Ländern anerkannt, daß es unter besonderen Voraussetzungen Ausnahmen vom Fernmeldegeheimnis geben muß. In Belgien, dem einzigen Land, in dem es bisher ein absolutes Verbot des Abhörens von Telefongesprächen gibt, bereitet die Regierung einen Gesetzentwurf für entsprechende Ausnahmen vor.

Die Statistik zeigt, daß Telefongespräche für Zwecke der Strafverfolgung im Jahre 1990 in 2449 Fällen in Deutschland und in 2031 Fällen in den Niederlanden abgehört wurden (Quelle: Bundesministerium für Post und Telekommunikation; Niederländisches Justizministerium).

Nach Art. 8 Abs. 2 der Europäischen Menschenrechtskonvention ist der "Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts" (auf Achtung des Post- und Fernmeldegeheimnisses) "nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist". Dieser Katalog von Ausnahmen, die der nationale Gesetzgeber vorsehen kann, ist sehr

weitreichend, und einige europäische Länder haben restriktivere Vorschriften erlassen, die das Abhören von Telefongesprächen erlauben (vgl. auch Ziffer 2.4 des Entwurfs einer Empfehlung für den Schutz von personenbezogenen Daten im Bereich der Telekommunikationsdienste, mit besonderem Bezug zu Telefondiensten, angenommen vom Ausschuß für rechtliche Zusammenarbeit des Europarats, Juni 1992).

Die Arbeitsgruppe hat die neueren Entwicklungen der Gesetzgebung in den einzelnen Ländern untersucht und dabei festgestellt, daß trotz einiger Zweifel hinsichtlich der Effektivität des Telefonabhörens als Mittel im Kampf gegen die "organisierte Kriminalität" dennoch eine wachsende Tendenz zu beobachten ist, die Unverletzlichkeit des Fernmeldegeheimnisses mit zusätzlichen Ausnahmen zu versehen. In Deutschland trat in diesem Jahr ein neues Gesetz in Kraft, das eine Verwaltungsbehörde ermächtigt, Telefongespräche abzuhören, um illegale Waffenexporte zu verhindern (sogar bevor Straftaten begangen werden). In vielen Ländern kann das Telefonabhören in Strafverfahren angeordnet werden, die spezielle schwere Straftaten wie Drogenhandel, Mord und terroristische Verbrechen betreffen.

Allerdings wird das Abhören von Telefongesprächen neuerdings von Politikern auch als effektive Waffe im Kampf gegen Korruption und organisierte Kriminalität angesehen (Australien, Deutschland). Es ist bisher nicht gelungen, diese Kategorien von Straftatbeständen präzise zu beschreiben. Deshalb birgt jede Gesetzgebung, die mit derart ungenauen Tatbeständen arbeitet, die Gefahr, daß die Telefongespräche unverdächtiger Personen abhört werden.

In Österreich wird andererseits über einen Gesetzentwurf diskutiert, der sogar den Geheimdienst verpflich-

tet, eine richterliche Anordnung zu beantragen, bevor Telefongespräche rechtmäßig abgehört werden dürfen.

Die Notwendigkeit einer Rechtsgrundlage für jeden staatlichen Eingriff in das Fernmeldegeheimnis hat der Europäische Menschenrechtsgerichtshof sehr strikt ausgelegt. In seiner neueren Rechtsprechung betont der Gerichtshof, daß Abhören und andere Formen der Registrierung von Telefongesprächen einen schwerwiegenden Eingriff in das Privatleben und die Kommunikation darstellen und deshalb auf einer Rechtsvorschrift beruhen müssen, die besonders präzise formuliert ist. Der Gerichtshof hebt hervor, daß es entscheidend ist, klare, detaillierte Vorschriften in diesem Bereich zu haben, insbesondere weil die verfügbare Technologie sich ständig weiterentwickelt (Fall Kruslin, 7/1989/167/223, Ziffer 33). Aus diesem Grund (Mangel an Präzision) wurde festgestellt, daß die Vorschriften des französischen Rechts über das Abhören von Telefongesprächen, gegen die Europäische Menschenrechtskonvention verstießen. Zwischenzeitlich ist Frankreich dem Beispiel des Vereinigten Königreichs gefolgt und hat ein neues Abhörgesetz verabschiedet, um den Anforderungen des Europäischen Menschenrechtsgerichtshofs zu entsprechen.

Das deutsche Bundesverfassungsgericht hat vor kurzem entschieden, daß eine präzise Rechtsgrundlage notwendig ist, um Fangschaltungen vorzunehmen, auch wenn der Inhalt der belästigenden Anrufe nicht aufgezeichnet wird.

Man kann drei Verfahrensstadien unterscheiden, wenn staatliche Stellen Telefone überwachen wollen:

- die Entscheidung, Telefongespräche abzuhören;
- die Durchführung dieser Entscheidung und

- die Kontrolle dieser Überwachungsmaßnahme, nachdem sie beendet worden ist.

Die Entscheidung, Telefongespräche abzuhören, kann getroffen werden von einer Verwaltungsbehörde (im Vereinigten Königreich), von einem Untersuchungsrichter (in den meisten Ländern) oder von einer Verwaltungsbehörde bzw. einem Gericht, je nachdem zu welchem Zweck abgehört werden soll (Deutschland). Beauftragte für den Datenschutz und den Schutz der Privatsphäre sind an diesen Entscheidungen nicht beteiligt und haben keine Kompetenz, sie zu überwachen. Dies bezieht sich ebenso auf die Durchführung der Anordnung, Telefongespräche abzuhören.

Sobald allerdings die Abhörmaßnahme beendet worden ist, gibt es gute Gründe dafür, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die Befugnis erhalten, die Nutzung der Daten zu kontrollieren, die aus der Abhörmaßnahme stammen. In einigen Ländern wächst die Erkenntnis, daß Beauftragte für den Datenschutz und den Schutz der Privatsphäre eine wichtige Rolle in diesem Bereich zu spielen haben, obwohl sie bisher noch keine derartige Kompetenz haben mögen.

In den Niederlanden wird das Recht möglicherweise in naher Zukunft in der Weise geändert, daß die Ergebnisse einer Abhörmaßnahme in den Akten der Nachrichtendienste dokumentiert werden. Sobald dies geschieht, würden diese Akten der Kontrollkompetenz der Registratiekamer unterliegen.

In Deutschland kann der Bundesbeauftragte für den Datenschutz nicht in ein gerichtes Verfahren eingreifen, das zu einer Abhöranordnung führt. Aber der Bundesminister für Post und Telekommunikation hat anerkannt, daß der Bundesbeauftragte für den Datenschutz

zu kontrollieren hat, ob die Deutsche Bundespost TELEKOM die Abhöranordnung korrekt durchführt, welche Art personenbezogene Daten bei Durchführung der richterlichen Anordnung erhoben werden und für welchen Zweck sie genutzt werden. Es ist entscheidend, daß die Ergebnisse einer Abhörmaßnahme nur für den Zweck benutzt werden, für den die Daten ursprünglich erhoben wurden.

In mehreren Ländern wird das Recht geändert, um die Überwachung von Nachrichten zu ermöglichen, die mit anderen Telekommunikationsmitteln (Telefax, Telex, Datenübertragung etc.) übermittelt werden. Zum Teil wird diese Gesetzgebung sich auch auf private Netzbetreiber und Diensteanbieter erstrecken und sie zur Zusammenarbeit mit der Polizei verpflichten.

Man muß sich vergegenwärtigen, daß die Überwachung von Telekommunikationsverbindungen, insbesondere das Abhören von Telefongesprächen, kein gewöhnliches Überwachungsmittel ist, das automatisch gegen jeden eingesetzt werden kann, der bestimmte Verbrechen begeht oder die nationale Sicherheit bedroht. Es ist im Gegenteil in den meisten Ländern eine Ermittlungsmethode für Ausnahmesituationen und unterliegt zusätzlichen Bedingungen. In einer Reihe von Ländern kann die Überwachung von Telefongesprächen nur angeordnet werden, wenn jemand einer Straftat verdächtigt wird, zu deren Aufklärung die Abhörmaßnahme beitragen kann, und nur dann, wenn herkömmliche Ermittlungsmethoden unpraktikabel oder erfolglos sind.

Es ist entscheidend, daß die Person, deren Telefongespräche abgehört worden sind, von der verantwortlichen Behörde über die Abhörmaßnahme informiert wird, sobald dies möglich ist, ohne den Zweck der Ermittlungen zu gefährden.

Nur dann ist der Einzelne in der Lage, die Abhörmaßnahme durch einen Richter oder ein anderes unabhängiges Organ überprüfen zu lassen. Die Benachrichtigung des Betroffenen ist bisher allerdings nur in wenigen nationalen Rechtssystemen vorgesehen.

3.

Das Recht des Bürgers, das Telefon zu benutzen, ohne registriert und beobachtet zu werden, schützt ihn nicht nur gegen die Aufzeichnung der Gesprächsinhalte, sondern auch gegen die Nutzung der technischen Daten, die vom Telekommunikationsnetz für andere als Abrechnungszwecke erzeugt werden (Verbindungsdaten wie Zeit, Dauer des Gesprächs und Rufnummer des Angerufenen). Allerdings gibt es von diesem Grundsatz noch weiterreichende Ausnahmen als vom Prinzip der Vertraulichkeit des Gesprächsinhalts. In Belgien und Deutschland können Verbindungsdaten aufgrund einer strafgerichtlichen Anordnung in jedem Strafverfahren genutzt werden, während das Abhören von Telefongesprächen im eigentlichen Sinn in vielen Ländern nur bei bestimmten Katalogstraftaten zulässig ist.

Auch in dieser Beziehung lassen sich in den verschiedenen Rechtssystemen unterschiedliche Tendenzen feststellen. In Australien hat der Attorney-General vor kurzem vorgeschlagen, den Begriff der Kommunikationsüberwachung neu zu definieren, so daß er das Mithören oder Aufzeichnen von Informationen umfaßt, die eine Person einer anderen über ein Telekommunikationssystem übermittelt, ohne das beide Gesprächsteilnehmer davon wissen; die Registrierung von Verbindungsdaten sollte nicht mehr unter diesen Begriff fallen. Diesen Vorschlag hat der australische Beauftragte für den Schutz der Privatsphäre scharf kritisiert. Nach seiner Auffassung sollten Verbindungsdaten und Inhaltsdaten, die über ein Telefonnetz übermittelt werden, in der glei-

chen Weise geschützt werden. Aufgrund neuerer technischer Entwicklungen (insbesondere der Einrichtung von digitalen Telekommunikationsnetzen) werden Verbindungsdaten systematisch von den Netzbetreibern gespeichert und sind deshalb für eine gewisse Zeit auch für andere Zwecke wie Strafverfahren verfügbar. Es gibt keinen Grund für ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Verbindungsdaten andererseits. Der Grundsatz der Vertraulichkeit von Telefongesprächen schützt sowohl deren Inhalt als auch deren nähere Umstände (Zeit, Dauer und die an ihnen beteiligten Personen).

Aus demselben Grund hat die deutsche Konferenz der Datenschutzbeauftragten den Bundestag aufgefordert, die alte Vorschrift aufzuheben, die die Nutzung von Verbindungsdaten für jedes Strafverfahren zuläßt. Wendet man diese Vorschrift auf digitale Netze an, so ist sie mit dem verfassungsrechtlich geschützten Fernmeldegeheimnis nicht mehr vereinbar.

4.

Da die Gesetzgebung über die Telekommunikationsüberwachung gegenwärtig in vielen Ländern, die in der Arbeitsgruppe vertreten sind, geändert wird, kann dieser Bericht nur ein Zwischenbericht sein. Es ist notwendig, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die technische und rechtliche Entwicklung in diesem Bereich genau beobachten, um die Privatsphäre des Einzelnen gegen exzessive Überwachung zu schützen.

Satellitenkommunikation

Vor mehr als sechs Jahren verabschiedete die VII. Internationale Konferenz der Datenschutzbeauftragten in Luxemburg eine Entschließung über Datenschutz und

Neue Medien, in der sie betonte, daß der "Einsatz von Satelliten zur Kommunikation" ... "Im Hinblick auf die Datenintegrität und den Schutz vor unbefugtem Abhören ebenfalls Risiken" schafft.

Seitdem scheinen diese Risiken fast vergessen, obwohl es geradezu eine Revolution am Himmel gegeben hat, was die Kapazität der Satelliten angeht. Der Kapazitätszuwachs der europäischen Satelliten von 1989 bis 1993 wird bei 215% liegen (vgl. EG-Kommission, Grünbuch zur Satellitenkommunikation, Tabelle 5. S. 57).

Satelliten können für eine Reihe von Zwecken eingesetzt werden, deren wichtigste die Verteilung von Fernsehprogrammen und die Telekommunikation sind. Es gibt andere Einsatzmöglichkeiten wie etwa die weltweite

- Positionsbestimmung und das Flottenmanagement,
- Fernmessen und Fernwirken,
- Fernerkundung.

1. Telekommunikation

Ein Satellitensystem besteht in der Regel aus mindestens zwei Erdfunkstationen und dem Raumsegment. Informationen werden von einer leistungsstarken Erdfunkstation zum Satelliten gefunkt ("Uplink", Aufwärtsstrecke; ein fester Punkt - zu - Punkt-Dienst). Sie werden dann über Transponder im Satelliten zurück zu einer anderen Erdfunkstation oder mehrere Erdfunkstationen übermittelt ("Downlink", Abwärtsstrecke). Bei der Abwärtsstrecke sind verschiedene Dienstformen vorstellbar, wie z.B. ein fester (Punkt - zu - Punkt Telekommunikations-) Dienst, ein Fernsehverteil-(Punkt - zu - Mehrfachpunkt-) Dienst, ein mobiler Dienst, bei dem Informationen zu beweglichen Empfangsstationen wie etwa Lastwagen mit kleinen Dachantennen gefunkt wer-

den. Moderne Satelliten tragen bis zu 16 Transponder und jeder Transponder kann bis zu zwei Fernsehkanälen oder 1700 Telefonsprachkanäle übertragen.

In Europa werden nur 2 - 3% der internationalen Telefongespräche über Satellit abgewickelt, während Satelliten eine weit größere Rolle bei transatlantischer und internkontinentaler Telekommunikation spielen, wo sie fast 60% des Verkehrsaufkommens übernehmen. Satellitengestützte Kommunikationsnetze sind von großer Bedeutung für den Aufbau der Telefoninfrastruktur in Ost- und Zentraleuropa. Die Entwicklung von billigen Antennen mit einem Durchmesser von weniger als einem Meter, insbesondere VSATs (Very Small Apperture Terminals, auch Mikrostationen genannt) die schon in den Vereinigten Staaten weit verbreitet sind, erleichtert neue Punkt - zu Mehrfachpunkt-Dienste. Die Unterscheidung zwischen Individual- und Massenkommunikation verschwimmt immer mehr. Mikrostationen können reine Empfangs- oder interaktive Empfangs- und Sendeterminals sein. Diese technische Entwicklung führt zur Entstehung von weltweiten mobilen "Overlay"-Telekommunikationsnetzen. Sie werden terrestrische Mobilfunknetze, die in dicht besiedelten Gebieten bestehen, ergänzen, allerdings nicht ersetzen. Satellitenkommunikation wird besondere Bedeutung in großen, dünn besiedelten Ländern wie Australien, Kanada und Rußland haben.

Das Raumsegment eines Satellitensystems steht im Eigentum einer internationalen Organisation wie z.B. INTELSAT (International Telekommunications Satellite Organisation), EUTELSAT, INMARSAT (International Maritime Satellite Organisation), American Mobile Satellite Corporation (USA), TELESAT MOBILE (Kanada) oder AUSSAT (Australien). Dabei handelt es sich um kommerzielle Organisationen auf der Grundlage von zwischenstaatlichen Verträgen, die selbst allerdings keine

Völkerrechtssubjekte sind. Alle Unterzeichnerstaaten haben einen gewissen Kapitalanteil an der Organisation. Die Satellitenorganisationen verkaufen Kapazitäten im Raumsegment entweder selbst oder durch Dienstanbieter.

Neue Dienste vor allem für geschlossene Benutzergruppen umfassen:

a) INTELSAT Business Service (IBS), der Sprachübermittlung, Fax, Telex, Datenübertragung, elektronische Post und Videokonferenzen integriert,

b) INTELNET-Dienste, die auf Datenverteilung und Datensammlung beschränkt sind,

c) nationales oder weltweites satellitengestütztes Paging.

Geostationäre Telekommunikationssatelliten (also Satelliten, die sich in einer gleichzeitigen Umlaufbahn zur Erdoberfläche bewegen), die gegenwärtig in Betrieb sind, reflektieren lediglich die Daten, die zu ihnen heraufgefunkt werden, auf einer anderen Frequenz hinunter zu einer anderen Erdfunkstation.

Eine neue Satellitengeneration könnte allerdings durchaus auf andere Weise arbeiten:

Nicht-geostationäre Satelliten können Informationen von einem Punkt der Erdumlaufbahn zu einem anderen transportieren, was die Speicherung von Daten im Raumsegment über eine längere Zeit erforderlich machen würde, als für das bloße Reflektieren der Daten erforderlich ist. Ein deutscher Forschungssatellit, der gegenwärtig Wissenschaftlern in der Arktis dient, funktioniert auf diese Weise (wie ein Postbote).

Sobald Daten im Raumsegment verarbeitet werden, wachsen die klassischen Risiken für die informationelle Selbstbestimmung, die mit jeder Verarbeitung von personenbezogenen Daten verbunden sind. Die EG-Kommission hat erkannt, daß satellitengestützte Kommunikation sowohl nationale wie auch EG-Gesetzgebung umgehen kann. Allerdings hat die Kommission bisher kein überzeugendes Konzept entwickelt, wie diesen Risiken zu begegnen ist.

2.

Positionsbestimmung und Flottenmanagement

Satelliten werden zunehmend für Zwecke der Navigation nicht nur von Schiffen (die das INMARSAT-System nutzen), sondern auch von Lastwagen und sogar Einzelpersonen genutzt.

EUTELTRACS ist ein europäisches satellitengestütztes System für die mobile Landkommunikation zum Management von LKW-Flotten. Die Position eines Fahrers und seine Bewegungen mit dem LKW können von einer Zentralstelle zu jeder Zeit überprüft werden. Dies spart für das Unternehmen Zeit und Geld und könnte auch zur Vermeidung von Verkehrsstauungen beitragen, wenn die Zentralstelle den Fahrern alternative Routen vorschlagen kann, die weniger überfüllt sind.

Das Global-Positioning-System (GPS- globales Positionsbestimmungssystem) wurde vom Pentagon entwickelt und erfolgreich im Golfkrieg getestet. Es beruht auf gegenwärtig 16 Satelliten (Ende 1993 werden es 21 sein), von denen jeder die genaue Zeit und Position aussendet, die von jedem, der mit einem GPS-Empfänger ausgerüstet ist, empfangen werden kann. Der Empfänger wiederum berechnet seine genaue Position im Verhältnis zum Satelliten. Dieses System erlaubt z.B. einer Reederei,

den Standort jedes ihrer Schiffe weltweit zu ermitteln und dann Informationen an das Schiff über INMARSAT zu übermitteln. Piloten und in naher Zukunft auch Fahrer können das System zusammen mit digitalen Landkarten benutzen, um ihren Weg in unbekannter Umgebung zu finden.

Gleichzeitig ist es offensichtlich, daß mit einem solchen System ein elektronisches Bewegungsprofil des Einzelnen ohne dessen Einwilligung erzeugt werden kann.

3.

Fernmessen und Fernwirken

Satellitengestützte Netze können auch genutzt werden, um Pipelines, Eisenbahnlinien, Stromleitungen und Ölquellen zu überwachen. Mit Hilfe der Fernmeßtechnik kann sogar die Temperatur in einem Kühlwagen kontrolliert und angepaßt werden. Zugleich würde dies auch eine verstärkte Überwachung der Arbeitnehmer bedeuten.

4.

Fernerkundung

Fernerkundung ist eine ältere (ursprünglich militärische) Einsatzform von Satelliten, durch die Bodenschätze, Wolkenbildungen (für die Wettervorhersage) Umweltverschmutzung und sogar die Routen von Zugvögeln vom Himmel aus beobachtet werden können.

Im Jahre 1991 startete die European Space Agency (ESA) einen modernen Satelliten (ERS-I), um Umweltveränderungen zu erkunden. Dieser Satellit verfügt über ein Radarsystem (SAR-Synthetic Aperture-Radar), das in der Lage ist, sogar nachts oder durch eine geschlossene

Wolkendecke Fotografien der Erdoberfläche zu machen. Dieser Satellit speichert bestimmte Daten, bis er eine Position erreicht, von der aus er sie zu der nächsten Erdfunkstation abstrahlen kann.

Fernerkundungssatelliten, die von den alliierten Streitkräften im Golfkrieg eingesetzt wurden, waren in der Lage, Objekte (z.B. Panzer) zu erkennen, die zwischen 1 und 5 Metern Kantenlänge hatte. Es ist sehr wahrscheinlich, daß Satellitentechnologie, die von den Militärs entwickelt wurde, mit einer gewissen zeitlichen Verzögerung auch für den zivilen Einsatz verfügbar sein wird.

Die EG-Kommission plant, über Satellit zu kontrollieren, ob Landwirte eine geringere Menge einer bestimmten Getreideart anbauen, als die, für die sie Gemeinschaftszuschüsse erhalten. Die Technik wird bald verfügbar sein, z.B. mit Hilfe eines Satelliten die Schlagzeilen einer Zeitung zu lesen, die jemand an einer Bushaltestelle liest.

5.

Die unbestrittenen Vorteile der Satellitentechnologie werden begleitet von offensichtlichen Risiken für die Privatsphäre, sobald der Einzelne ins Blickfeld des Satelliten gerät. Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre sollten sich deshalb für internationale Abkommen einsetzen, die regeln

- in welchem Ausmaß personenbezogene Daten im Weltall verarbeitet werden dürfen,
- wer der verantwortliche Datenverarbeiter ist, wenn personenbezogene Daten im Raumsegment gespeichert werden, und wer für die Datensicherheit verantwortlich ist,

- daß besondere technische Maßnahmen ergriffen werden müssen, z.B. sollten Verschlüsselungstechniken (die bereits im militärischen Bereich angewandt werden) für die zivile Nutzung ohne zusätzliche Kosten angeboten werden.

Der internationale Normungsprozeß für weltweite Mobilkommunikation über Satellit berücksichtigt den Datenschutz noch immer nicht hinreichend.

G e m e i n s a m e E r k l ä r u n g

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre, die sich zu ihrer XIV. Internationalen Konferenz in Sydney getroffen haben,

- begrüßen den Bericht der Arbeitsgruppe Telekommunikation und Medien,
- heben die Bedeutung der beschriebenen Probleme im Bereich des Fernmeldegeheimnisses und der Satellitenkommunikation hervor und
- stimmen darin überein, daß die technische und rechtliche Entwicklung im Bereich des Fernmeldegeheimnisses sorgfältig beobachtet werden muß, um die Privatsphäre des Einzelnen vor exzessiver Überwachung zu schützen.

Anlage 10

Dienstanweisung Nr.
für die Übermittlung von Daten mit Hilfe von Telefax-Geräten

Der Landesbeauftragte für Datenschutz hat darauf hingewiesen, daß in der Verwaltungspraxis sehr oft Schriftstücke mit Telefax-Geräten versendet werden. Damit personenbezogene Daten bei der Übermittlung mit Hilfe von Telefax-Geräten geschützt sind und eine Beeinträchtigung schutzwürdiger Belange von natürlichen Personen verhindert wird, wird die folgende Anordnung erlassen:

Geltungsbereich

Diese Dienstanweisung gilt für alle Bediensteten des ..... die personenbezogene Daten mit Hilfe von Telefax-Geräten übermitteln bzw. übermittelt bekommen.

Allgemeine Hinweise im Umgang mit Telefax-Geräten

Die Telefax-Geräte dürfen nur in ausreichend gesicherten Räumen untergebracht werden.

Eine Telefaxsendung darf nicht unbeobachtet ankommen und nicht von Unbefugten entnommen oder eingesehen werden.

Die Bediensteten, die ein Telefax-Gerät bedienen und somit Kenntnis vom Inhalt eines Telefax erhalten, unterliegen dem Fernmeldegeheimnis.

Die Daten von Sende- und Empfangsprotokollen unterliegen ebenfalls dem Fernmeldegeheimnis. Aus diesem Grund sind alle Sende- und Empfangsprotokolle (Journale),

die durch das Telefax-Gerät erzeugt werden, sorgfältig und sicher aufzubewahren. Die Einsichtnahme der Protokolle durch Unbefugte ist nicht zulässig.

Jeder Sendung ist ein Vorblatt beizufügen, welches den Absender, die Telefax- und Telefonnummer (für evtl. Rückrufe) sowie die Gesamtanzahl der gesendeten Seiten ausweist. Das Sendeprotokoll ist dem Vorgang beizufügen.

Bei Ausfall der Netzstromversorgung besteht die Gefahr, daß - sofern vorhanden - Ziel- und Gruppenwahlnummern gelöscht oder unrichtig werden. Deshalb ist von Zeit zu Zeit, in jedem Fall bei bekannt gewordenem Netzausfall, der Speicherinhalt zu prüfen.

Telefax-Ausgänge

Die Übermittlung von Schriftstücken mit personenbezogenen Daten hat grundsätzlich in einem verschlossenen Brief zu erfolgen.

Wenn es sich um eilbedürftige Angelegenheiten handelt, sind ausnahmsweise Schriftstücke mit personenbezogenen Daten mit dem Telefax-Gerät zu übermitteln.

Schriftstücke mit personenbezogenen Daten, insbesondere im Personal-, Sozial- oder ärztlichen Bereich, dürfen allerdings auch im Fall der Eilbedürftigkeit nur mit Telefax-Geräten übermittelt werden, wenn beim Empfänger durch technische und organisatorische Maßnahmen gewährleistet ist, daß diese dort nicht in den Besitz einer unbefugten Person gelangen können.

Sind diese Voraussetzungen beim Empfänger nicht sichergestellt, so ist eine Übermittlung personenbezogener Daten per Telefax nur noch in den Fällen zulässig, in denen zuvor mit dem Adressaten verabredet wurde, daß

dieser am Telefax-Gerät steht, wenn die vertrauliche Telefax-Sendung ausgedruckt wird.

Vor der Absendung des Telefax muß sich der Bedienstete des Gerätes über die Richtigkeit der Anschlußnummer Gewißheit verschaffen. Hierdurch soll ausgeschlossen werden, daß ein anderer als der gewünschte Anschluß erreicht wird. Deshalb ist bei jeder Sendung stets die Rücksendung der Kennung des angewählten Gerätes abzuwarten und zu überprüfen. Bei fehlender Übereinstimmung ist die Sendung sofort abzubrechen.

Des weiteren ist sicherzustellen, daß ein Telefax nicht außerhalb der Dienstzeit beim Empfänger ankommt und dadurch gegebenenfalls Unbefugten zur Kenntnis gelangt. Von der Möglichkeit der zeitversetzten Sendung ist deshalb nur ausnahmsweise in begründeten Fällen Gebrauch zu machen. Es ist allerdings vorab mit dem Empfänger abzuklären, daß keine unbefugte Person an das Telefax-Gerät gelangen kann.

Telefax-Eingänge

Schriftstücke mit personenbezogenen Daten, die per Telefax-Gerät an ..... übermittelt werden, sind im Eilfall dem Adressaten selbst - nicht über eine dritte Person - auszuhändigen. Ansonsten sind die Schriftstücke in einem verschlossenen Briefumschlag mit entsprechendem Sichtvermerk (z.B. vertraulicher oder persönlicher Inhalt) dem Adressaten auf dem üblichen Postweg zuzuleiten.

Die Dienstanweisung tritt mit Wirkung vom ..... in Kraft.