

LANDTAG DES SAARLANDES

10. Wahlperiode

Drucksache **10/ 451**

19.03.91

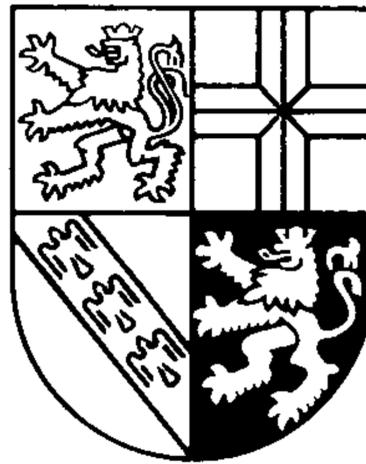
## **ZWÖLFTER BERICHT**

über die

Tätigkeit des Landesbeauftragten für Datenschutz gemäß § 20  
Abs. 3 des Gesetzes zum Schutz vor Mißbrauch personenbe-  
zogener Daten bei der Datenverarbeitung  
(Berichtszeitraum: 1. Januar 1990 bis 31. Dezember 1990)

Ausgegeben: 19.04.91

SAARLAND  
DER LANDESBEAUFTRAGTE FÜR DATENSCHUTZ



12. Tätigkeitsbericht

1990

## INHALTSVERZEICHNIS

	Seite
Vorbemerkung	1
1. <u>Grenzüberschreitende Informations- verarbeitung</u>	7
1.1 "Weltdatenschutztag" Paris 1990	7
1.2 Datenschutz im Europäischen Informationsmarkt	9
1.2.1 Initiativen der Kommission der Europäischen Gemeinschaft	9
1.2.2 Schengener Zusatzübereinkommen	12
1.2.3 EG-Statistikverordnung	14
1.2.4 Deutsch-Deutscher Datenaustausch vor der Vereinigung	15
2. <u>Entwurf eines Saarländischen Daten- schutzgesetzes (SDSG)</u>	19
3. <u>Polizei</u>	25
3.1 Polizeiinformationssystem DIPOL	25
3.2 Spezialdateien	27
3.3 Protokollierung der INPOL-Abfrage	30

4.	<u>Rechtspflege</u>	34
4.1	Stand der Gesetzgebung	34
4.2	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und der organisierten Kriminalität (OrgKG)	36
4.3	Zentraldatei der Staatsanwaltschaft	38
4.4	Beeinträchtigung schutzwürdiger Belange der Betroffenen durch justitielle Vorgänge	41
4.4.1	Diskriminierender Aktenvermerk in einer Pflegschaftssache	42
4.4.2	Einstellungsverfügung der Staatsanwaltschaft	43
4.5	Telefonabhördaten	44
5.	<u>Melderecht</u>	46
5.1	Nach wie vor: Novellierungsbedarf für melderechtliche Bestimmungen	46
5.2	Mangelhafte Datensicherung beim Transport von Meldeunterlagen	47
5.3	Bruch des Wahl- und Meldegeheimnisses	48
5.4	Nochmals: Die gebührenpflichtige Übermittlungssperre	50
6.	<u>Gesundheit</u>	52
6.1	Krankenhaus	52
6.2	Klinisches Krankheitsregister	61
6.3	Gesundheitsamt	62
6.3.1	Amtsärztliche Begutachtung im Vorfeld psychiatrischer Unterbringung	62
6.3.2	Geschlechtskrankenberatungsstelle	66

6.3.3	Sicherung des Auskunfts- und Einsichtsrechts des Betroffenen durch Identitätsprüfung	68
6.3.4	Formulare im jugendärztlichen Dienst (Bilanz)	69
6.3.5	Medizinalpersonendatei (Bilanz)	69
6.4	Krebsregistergesetz	70
6.5	Rechnerunterstützte Programme zur AIDS-Bekämpfung: Computerprogramme KLIMACS und KLINAIDS	71
7.	<u>Soziales</u>	73
7.1	Arztgeheimnis kontra maximale Leistungstransparenz	73
7.2	Übermittlung von Patientenunterlagen durch Krankenhäuser an Krankenkassen	78
7.3	Medizinischer Dienst	78
7.4	Ärztlicher Dienst des Versorgungsamtes	81
7.5	Schulbericht für das Jugendamt	82
7.6	Sozialdatenschutz für das gesprochene Wort	84
8.	<u>Öffentlicher Dienst</u>	86
8.1	Abschottung der Beihilfestellen	86
8.1.1	Landesverwaltung	86
8.1.2	Gemeinden und sonstige öffentliche Stellen	87
8.2	Beihilfe für Familienangehörige	89
8.3	Anerkennung der Beihilfefähigkeit von psychotherapeutischen Maßnahmen	91
8.4	Privatpost für Bedienstete	92

9.	<u>Sonstige Bereiche</u>	94
9.1	Telefon als digitale Telekommunikations- anlage (TK-Anlage)	94
9.2	Verzeichnis (KV-Kataster) kontaminationsverdächtiger Flächen	98
9.3	Gefahr für das Steuergeheimnis: Steuerakten in einem Finanzamt	101
9.4	Technischer Überwachungsverein (TÜV)	102
9.5	Benennung von Zeugen bei der Verfolgung von Ordnungswidrigkeiten	104

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

- Anlage 1: EntschlieÙung der 39. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. März 1990 zum Bundesdatenschutzgesetz und zum Bundesverfassungsschutzgesetz Seite 106
- Anlage 2: EntschlieÙung der 12. Internationalen Konferenz der Datenschutzbeauftragten in Paris (19. September 1990) zu Problemen öffentlicher Telekommunikationsnetze und des Kabelfernsehens (Übersetzung) Seite 110
- Anlage 3: EntschlieÙung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29.01.1991 zum Vorschlag der EG-Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten Seite 116
- Anlage 4: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis Seite 121

- Anlage 5: EntschlieÙung der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Lander und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Neuregelung des Melderechtsrahmengesetzes Seite 125
- Anlage 6: EntschlieÙung der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Lander und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund oder Landern Seite 127
- Anlage 7: EntschlieÙung der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Lander und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Starkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtoffentlich gesprochenen Wortes Seite 129

## 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
AOK	Allgemeine Ortskrankenkasse
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BND	Bundesnachrichtendienst
BSHG	Bundessozialhilfegesetz
Bt-Drucksache	Bundestagsdrucksache
BTX	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheid
DIPOL	DV-Infrastruktur für die Polizei
DOK	Die Ortskrankenkasse
EG	Europäische Gemeinschaft
GG	Grundgesetz
G 10	Gesetz zur Beschränkung der Brief-, Post- und Fernmeldegeheimnisse
ISDN	Integrates Services Digital Network
KLIMACS	Klinisch-medizinisches Analysen- Computer System
KLINAIDS	Klinisches AIDS Computer System
KPA	Kriminalpolizeiamt
KV-Kataster	Verzeichnis kontaminationsverdächtiger Flächen
Lt-Drucksache	Landtagsdrucksache
MG	Meldegesetz
MPI	Medizinisch-psychologisches Institut
NJW	Neue Juristische Wochenschrift
OFD	Oberfinanzdirektion
OrgKG	Geetz zur Bekämpfung des illegalen Rauschgifthandels und der organisier- ten Kriminalität
PC	Personalcomputer

PsychKG	Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke
RSt	Ressortstellungnahme
RVO a.F.	Reichsversicherungsordnung alte Fassung
SDSG	Saarländisches Datenschutzgesetz
SKHG	Saarländisches Krankenhausgesetz
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
SPersVG	Saarländisches Personalvertretungsgesetz
SPolG	Saarländisches Polizeigesetz
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
TB	Tätigkeitsbericht
TK-Anlage	Telekommunikations-Anlage
TÜV	Technischer Überwachungsverein
Tz.	Teilziffer

## Vorbemerkung

Es bedarf weiterer Anstrengungen in der Bundes- und Landesgesetzgebung, um den Schutz der Persönlichkeitsrechte zu gewährleisten. Soweit es derzeit an einer ausreichenden gesetzlichen Grundlage fehlt, müssen Überlegungen angestellt werden, wie in der Übergangszeit den schutzwürdigen Belangen der Betroffenen mehr als bisher Rechnung getragen werden kann.

Defizite der Landesgesetzgebung habe ich in der Vergangenheit immer wieder angesprochen. Initiativen, die eine alsbaldige Verwirklichung der dringend notwendigen Gesetzesprojekte aus dem seit langem präsentierten Katalog erwarten lassen, haben sich im Berichtszeitraum nicht abgezeichnet.

Ich habe wiederholt darauf hingewiesen, daß im Saarland als einzigem Bundesland die unabhängige Datenschutzkontrolle des Verfassungsschutzes nicht ausreichend gesichert ist. Zwar bestehen auch im Saarland parlamentarische Kontrollgremien (Ausschuß für Verfassungsschutz, G-10-Ausschuß und G-10-Kommission). Ihre Unterrichts- und Beteiligungsrechte beschränken sich auf die Entgegennahme von Berichten oder auf die Erteilung von Genehmigungen für die Durchführung von Überwachungsmaßnahmen, die das Brief-, Post- und Fernmeldegeheimnis durchbrechen (G-10-Kommission). Die Überprüfung der Informationsverarbeitung "vor Ort", im Landesamt für Verfassungsschutz selbst, die in anderen Bundesländern von den zuständigen Landesbeauftragten für Datenschutz wahrgenommen wird, kann mangels Kontrollkompetenz hierzulande nicht stattfinden. Datenschutz ohne unabhängige, systematische Kontrolle ist jedoch nicht zu verwirklichen. Ersuchen eines Bürgers auf Überprüfung der Verarbeitung seiner Daten durch den Verfassungsschutz kann der Landesbeauftragte für Datenschutz ebenfalls nicht nachkommen. Eine entsprechende gesetzliche Regelung war im Entwurf zur

Novellierung des Saarländischen Datenschutzgesetzes vorgesehen, den die Landesregierung jedoch in der letzten Legislaturperiode nicht weiter verfolgt und dem Landtag nicht zugeleitet hat.

Die allgemeine Bedeutung dieser Novelle für den Datenschutz im Saarland muß nicht betont werden. Besonders gravierend ist jedoch der sich nunmehr fortsetzende Verstoß gegen elementare Grundregeln des Datenschutzes. Nach Auffassung des Bundesverfassungsgerichts ist "die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung" (BVerfGE 65,1, 46).

Auch die Rechtsgrundlagen für die Informationsverarbeitung des Verfassungsschutzes sind zu novellieren, wie dies auf Bundesebene im vergangenen Jahr bereits geschehen ist.

Seit 1978 werde ich nicht müde, in meinen Tätigkeitsberichten darauf hinzuweisen, daß die verfassungsrechtlichen Anforderungen auch für die Verarbeitung von Gesundheitsdaten besonderer Beachtung bedürfen und deshalb das noch unter national-sozialistischer Herrschaft in Kraft getretene "Gesetz zur Vereinheitlichung des Gesundheitswesens" endlich durch ein modernes Gesundheitsdienstgesetz ersetzt werden muß. An dieser Notwendigkeit ändern auch nichts die inzwischen festzustellenden Fortschritte in der Praxis der Gesundheitsämter.

Defizitär sind auch die Rechtsgrundlagen für den behördlichen Umgang mit Daten psychisch Kranker im Vorfeld psychiatrischer Einweisung in eine Anstalt. Meine Erfahrungen, die ich in diesem Bericht schildere (Tz. 6.3.1), unterstreichen die Notwendigkeit, das Unterbringungsgesetz für psychisch Kranke zu novellieren.

Im Interesse einer wirksamen Bekämpfung des Krebses muß die gesetzliche Grundlage für das regionale Krebsregister überdacht werden. Externe Stellen der Wissenschaft dürfen derzeit mangels einer gesetzlichen Ermächtigung auf personenbezogene Krebsregisterdaten zu Forschungszwecken nicht zugreifen.

Das Archivwesen im Landesbereich bedarf einer verfassungsmäßigen Rechtsgrundlage, die schon seit langem angemahnt ist (7. TB, Tz. 3).

Im Zusammenhang mit der Fortschreibung des Bundesmelde-rechtsrahmengesetzes muß auch das Landesmeldegesetz novelliert werden. Die datenschutzrechtlichen Forderungen im Meldebereich waren bereits Gegenstand einer EntschlieÙung des Ausschusses für Innere Verwaltung (vgl. 10. TB, Anlage 9, Tz. 4 und unten Tz. 5.1).

Nachdem das Justizmitteilungsgesetz bisher nicht verabschiedet ist, muß die Mitteilungspraxis der Gerichte in Zivil- und Strafsachen übergangsweise in einer für die Betroffenen schonenderen Weise als bisher gestaltet werden (vgl. EntschlieÙung des Ausschusses für Innere Verwaltung, 10. TB, Anlage 8, Tz. 4).

Weiterhin muß im Justizbereich das schon seit langem zugesagte Rücklaufverfahren der Staatsanwaltschaft an die Kriminalpolizei in Gang gesetzt werden, damit die Ergebnisse der Strafverfahren zur Fortschreibung der präventiven, kriminalpolizeilichen Datensammlungen zur Verfügung stehen und dadurch den schutzwürdigen Belangen der Betroffenen besser Rechnung getragen werden kann (vgl. EntschlieÙung des Ausschusses für Innere Verwaltung, 10. TB, Anlage 8, Tz. 9).

Seit Inkrafttreten der Bestimmungen des Saarländischen Datenschutzgesetzes war das zuständige Ministerium nicht in der Lage, die Schulen zu veranlassen, die

Dateimeldungen zu dem beim Landesbeauftragten für Datenschutz geführten Register durchzuführen.

Auf Bundesebene hat sich einiges bewegt, wenn man auch noch nicht zufrieden sein kann.

Der Bundestag hat das Bundesdatenschutzgesetz, das Verfassungsschutzgesetz sowie erstmals ein Gesetz für den Militärischen Abschirmdienst sowie für den Bundesnachrichtendienst in einem Artikelgesetz zusammen verabschiedet.

Der Anwendungsbereich des Bundesdatenschutzgesetzes ist insoweit erweitert worden, als im öffentlichen Bereich Akten erfaßt werden und für den öffentlichen sowie den privaten Bereich die Datenerhebung geregelt wird. Das Gesetz enthält andererseits auch Rückschritte gegenüber der bisherigen Praxis. Die Werbewirtschaft sicherte sich das Privileg der listenmäßigen Datenübermittlung, sofern es sich nicht um sensible Daten handelt, die sich auf Gesundheit, Straftaten, Ordnungswidrigkeiten, religiöse oder politische Anschauungen oder arbeitsrechtliche Verhältnisse beziehen. Gravierend könnten sich Einschränkungen der Kontrollbefugnis der Datenschutzbeauftragten auswirken; in bestimmten Fällen sollen Kontrollen nur möglich sein, wenn die Betroffenen zuvor darauf hingewiesen wurden.

Nicht nur beim Bundesdatenschutzgesetz sondern auch bei der Neuordnung der Nachrichtendienste wurden die seit Jahren vorgetragenen Forderungen der Datenschutzbeauftragten nicht berücksichtigt (vgl. Entschließung der DSB-Konferenz, Anlage 1). Der Auskunftsanspruch des Betroffenen gegenüber den Nachrichtendiensten wird zwar grundsätzlich anerkannt; er wird jedoch zu sehr eingeschränkt: Dem Bürger wird die Pflicht zur Begründung seines Auskunftsersuchens auferlegt, während die

Ablehnung der Auskunft unter keinen Umständen begründet werden muß.

Die Diskussion über eine datenschutzgerechte Fassung der Strafprozeßordnung hat sich festgefahren, obwohl hier der dringendste Regelungsbedarf überhaupt besteht. Eine Ländermehrheit hat sich indessen gefunden, die zur Bekämpfung der "Organisierten Kriminalität" moderne Ermittlungsmethoden an die Hand geben will, ohne jedoch eine angemessene Rechtsgrundlage vorzusehen (vgl. unten Tz. 4.2). Die eingriffsintensiven Maßnahmen waren jedoch keineswegs nur auf die "Organisierte Kriminalität" beschränkt, ein Begriff, der ohnehin schwer faßbar ist. Auch die Bundesregierung hat verfassungsrechtliche Bedenken angemeldet.

Die Bundespost installiert mit großem Einsatz an sachlichen, personellen und monetären Mitteln das öffentliche, digitalisierte und integrierte Telekommunikationsnetz (ISDN). Mit dieser neuen Informationsstruktur sind erhebliche Veränderungen der Qualität und Quantität der für den Betrieb verwendeten Daten verbunden. Erste Auswirkungen sind bereits im behördlichen Bereich der Landesregierung durch den Einsatz moderner Telefonanlagen festzustellen (vgl. unten Tz. 9.1). Von besonderer Bedeutung ist die Veränderung des Abrechnungsverfahrens. Es entsteht eine riesige Datenhaltung von Milliarden von Datensätzen über jeden einzelnen Kommunikationsvorgang, die Art der benutzten Dienste (Telefon, Fernschreiber, Bildübermittlung), Teilnehmer des Gesprächs, Beginn und Ende der Verbindung. Die Bundespost lehnt es ab, wenigstens die Zielnummer so zu verkürzen, daß jedenfalls Dritte den angerufenen Teilnehmer nicht mehr identifizieren können. Diese Forderung ist in Frankreich bereits akzeptiert worden (vgl. im einzelnen Entschliebung der DSB-Konferenz, Anlage 7).

Das Gewerberecht bedarf dringend einer datenschutzrechtlichen Überarbeitung (vgl. 10. TB, Anlage 9, Tz. 6).

Ein Lichtblick in der Bundesgesetzgebung bedeutet die Verabschiedung des Kinder- und Jugendhilfegesetzes. Den Jugendämtern wird in sehr konkreter Weise der Umgang mit den Daten ihrer Schutzbefohlenen vorgegeben (vgl. 8. und 9. TB, Tz. 5.2 und 5.3).

Ein wesentlicher Fortschritt in der Beurteilung des grenzüberschreitenden Verkehrs - vielleicht auch als Folge der internationalen Datenschutzkonferenz 1989 in Berlin (vgl. 11. TB, Tz. 1) - ist der offensichtliche Sinneswandel der Kommission der Europäischen Gemeinschaft, den Datenschutz beim Aufbau des Gemeinsamen Marktes in den Mitgliedsstaaten durch eigene Initiativen zu fördern, statt hierin - wie etwa im Grünbuch für den Europäischen Informationsmarkt - ein Hemmnis beim Aufbau gemeinsamer Strukturen zu sehen.

## 1. Grenzüberschreitende Informationsverarbeitung

### 1.1 "Welt Datenschutztag" Paris 1990

Im vergangenen Berichtsjahr stand die Internationalisierung der Informationsverarbeitung infolge des steigenden Informationsverkehrs über die Grenzen hinweg im Blickpunkt der Öffentlichkeit. Die Lösung der grenzüberschreitenden Probleme war bereits das beherrschende Thema der Internationalen Konferenz der Datenschutzbeauftragten 1989 in Berlin (vgl. 11. TB, Tz. 1). Auch die Internationale Konferenz 1990 in Paris widmete sich dem gemeinsamen Anliegen, der Beeinträchtigung schutzwürdiger Belange durch den grenzüberschreitenden Datenaustausch entgegenzuwirken. Eingehend befaßte sich die Konferenz mit Grundsätzen für die Telekommunikation, die bereits in Berlin Gegenstand von Erörterungen waren. Das Zusammenwachsen von Computertechnik und Nachrichtentechnik hat neuartige, interaktive, individuelle Kommunikationsformen entstehen lassen, die Risiken für die Persönlichkeitsrechte auch im grenzüberschreitenden Verkehr zur Folge haben. Die Fortentwicklung des herkömmlichen Telefonnetzes durch Automation der Vermittlungsvorgänge hat zur Folge, daß sämtliche Informationen - nicht nur das gesprochene Wort, sondern auch Daten und Bilder - in Form von Binärziffern über immer leistungsfähigere Netze von Endgerät zu Endgerät transportiert werden. Eine Vielzahl intelligenter Funktionen, ein breites Spektrum neuer Aktivitäten werden möglich, die mit der bisherigen Technik nicht erreicht wurden. Diese Kommunikationsformen werden künftig mit dem dienstintegrierenden digitalen Telekommunikationsnetz (ISDN) und den neuen öffentlichen digitalen Mobilfunksystemen angeboten. Auf der Grundlage des Vorschlags einer Arbeitsgruppe wurde eine Entschließung verabschiedet (Anlage 2). Die wichtigsten Ergebnisse sind folgende:

## a) Teilnehmerverzeichnis

Jedem Teilnehmer an Telekommunikationsdiensten muß das Recht eingeräumt werden, gebührenfrei und ohne Begründung den Eintrag seiner Daten in ein Teilnehmerverzeichnis auszuschließen. Diese Datensammlungen sind inzwischen weltweit die wichtigsten öffentlich verfügbaren personenbezogenen Dateien. Die Risiken nehmen durch den Verkauf der Teilnehmerverzeichnisse ständig zu.

## b) Rufnummernanzeige

Die Einführung einer Einrichtung, die die Anzeige der Nummer des von Anrufern benutzten Anschlusses am Endgerät des angerufenen Teilnehmers anzeigt (Rufnummernanzeige), ist mit der Kommunikationsfreiheit in Einklang zu bringen. Der Anrufer muß die Möglichkeit haben, durch eine technische Vorrichtung seine Rufnummer zu unterdrücken. Er muß im Einzelfall auf die Gefahr hin, daß sein Anruf vom Angerufenen nicht entgegengenommen wird, selbst entscheiden können, ob seine Rufnummer mitgeteilt wird.

## c) Mobilfunk

Die Netzbetreiber von Mobilfunk sind zu verpflichten, den Teilnehmern wirksame Verschlüsselungsverfahren anzubieten und technische Vorkehrungen zur Verhinderung des unbefugten Netzzugangs zu treffen.

## d) Kabelfernsehen

Kabelfernsehgesellschaften, die einzeln abrufbare Programme anbieten (Bestell- und Abrufdienste: "pay per view"), sollen hierzu nur dann berechtigt sein, wenn Verfahren bereit gestellt werden können, die die Gebührenzahlung ohne die Speicherung zuschauer-

bezogener Daten ermöglichen (z.B. im voraus bezahlte Karten oder Decoder). Die Speicherung individueller Zuschauerprofile ist als Eingriff in die Privatsphäre zu verhindern.

## 1.2 Datenschutz im europäischen Informationsmarkt

### 1.2.1 Initiativen der Kommission der Europäischen Gemeinschaft

Da die Internationalisierung der Informationsverarbeitung in der EG mit der wirtschaftlichen Integration und dem Ausbau des europaweiten Telekommunikationsnetzes immer weiter voranschreitet, bedarf es eines länderübergreifenden Datenschutzkonzeptes. Es ist daher zu begrüßen, daß die EG-Kommission nicht zuletzt auch im Hinblick auf die Anregungen der Internationalen Konferenz der Datenschutzbeauftragten 1989 in Berlin (vgl. 11. TB, Tz. 1.2 - 1.4) ein umfangreiches Paket datenschutzrechtlicher Maßnahmen erarbeitet und, soweit geboten, in die Rechtsetzungsprozedur eingebracht hat. Hierbei handelt es sich um folgende Entwürfe, Vorschläge und Mitteilungen (Kom (90) 314 endg. - SYN 287-288):

#### a) "Harmonisierungsrichtlinien"

Ein Schwerpunkt ist der Vorschlag für eine Richtlinie zum "Schutz von Personen bei der Verarbeitung personenbezogener Daten". Dieser Entwurf einer "Magna Charta" des Datenschutzes in der EG verfolgt das Ziel - wie in der Begründung ausgeführt wird - "in allen Mitgliedsstaaten der Gemeinschaft ein gleichwertiges hohes Schutzniveau einzuführen, um die Hemmnisse für den Austausch von Daten abzubauen". Diese sogenannte "Harmonisierungsrichtlinie" wird die Mitgliedsstaaten verpflichten, den teilweise immer noch ungenügenden Datenschutz auszubauen ("keine Datenoasen") und Fehlentwicklungen vorzubeu-

gen. Nicht alle Mitgliedsstaaten haben Datenschutzgesetze verabschiedet und lediglich sieben Länder der EG haben bisher die Europaratskonvention ratifiziert. Der Datenschutz ist in den einzelnen Ländern unterschiedlich geregelt. Der Entwurf überläßt den nationalen Gesetzgebern in vielerlei Hinsicht einen angemessenen Regelungsspielraum. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat einen Arbeitskreis für das Gemeinschaftsrecht der EG eingesetzt, der eine Stellungnahme erarbeitet und eine EntschlieÙung der Konferenz vorbereitet hat (Anlage 3).

- b) Erstreckung der Datenschutzgrundsätze auf Bereiche außerhalb des Gemeinschaftsrechts

Ein EntschlieÙungsentwurf der im Rat vereinigten Vertreter der Mitgliedsstaaten soll die Lücken im Anwendungsbereich der "Harmonisierungsrichtlinie" schließen helfen, die dadurch entstehen, daß bestimmte Bereiche außerhalb des Gemeinschaftsrechts liegen: z.B. Verteidigung, Verbrechensbekämpfung, Geheimdienste. Dieser Entwurf verfolgt das Ziel, die Geltung der Grundsätze der "Harmonisierungsrichtlinie" auf diese Bereiche auszudehnen und verpflichtet die Regierungen der Mitgliedsstaaten, die erforderlichen Gesetzgebungsverfahren einzuleiten.

- c) Anwendung der Datenschutzgrundsätze auf die Organe der EG

Die Kommission hat eine "Erklärung" verabschiedet, in der sie dem Wunsch Ausdruck gibt, daß die Grundsätze der "Harmonisierungsrichtlinie" auf die Organe und Einrichtungen der EG Anwendung finden. Hierzu sollen die erforderlichen Maßnahmen vorgeschlagen werden. Bis diese Maßnahmen getroffen sind,

verpflichtet sich die Kommission, diese Grundsätze in ihrem Zuständigkeitsbereich bereits anzuwenden.

d) Datenschutz in den Beziehungen der EG zu Drittländern

Eine Empfehlung für den Beschluß des Rates betreffend den Beitritt der EG zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ("Europaratskonvention") wird in den Beziehungen zwischen der Gemeinschaft und Drittländern den Schutz der betroffenen Personen gewährleisten.

e) Digitales Kommunikationsnetz und Mobilfunk

Ein weiterer Schwerpunkt ist der Vorschlag für eine Richtlinie zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen, digitalen Kommunikationsnetzen; insbesondere für das dienstintegrierende digitale Telekommunikationsnetz (ISDN) und das öffentliche digitale Mobilfunknetz wurden im Hinblick auf den spezifischen Schutzbedarf Regelungen erarbeitet.

Defizite müssen allerdings bereits jetzt festgestellt werden; folgende Gesichtspunkte sind noch nicht berücksichtigt (Arbeitsergebnisse des AK-Sicherheit der DSB-Konferenz):

- begründungs- und gebührenfreier Ausschluß des Eintrags in ein Teilnehmerverzeichnis
- Kostenfreiheit der Auskunft
- Verbesserung des Fernmeldegeheimnisses durch Verwirklichung einer Strafandrohung in allen Mitgliedsstaaten
- Unterdrückung der Rufnummernanzeige auch im grenzüberschreitenden Telefonverkehr

- Unterdrückung der vollständigen Zielnummer im Kommunikationsnetz und des Standortes im Mobilfunknetz

#### f) Informationssicherheit

Der Vorschlag für einen Beschluß des Rates auf dem Gebiet der Informationssicherheit verfolgt in erster Linie das Ziel, "Privatbenutzern, Verwaltungen und Unternehmen eine wirksame Sicherheit der elektronisch gespeicherten Informationen zu bieten, ohne die Interessen der breiten Öffentlichkeit zu beeinträchtigen". Dies ist angesichts der technischen Entwicklung kostengünstiger, weltweiter Hochleistungskommunikation in einem bislang unerreichten Maßstab umso dringlicher geworden.

Insgesamt sind die Vorschläge geeignet, als Grundlage für die Weiterentwicklung des Datenschutzes und der Datensicherheit in der EG zu dienen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird den Prozeß der Umsetzung in Rechtsetzung und Praxis kritisch begleiten.

Auch die Datenschutzbeauftragten der Mitgliedsstaaten der EG haben sich anläßlich der internationalen Konferenz 1990 mit den Initiativen der EG-Kommission befaßt. Eine gemeinsame Haltung wird nach einem Meinungsaustausch angestrebt. Es werden Möglichkeiten für eine jährliche gemeinsame Konferenz geprüft (Anlage 4).

#### 1.2.2 Schengener Zusatzübereinkommen

Im 11. Tätigkeitsbericht (Tz. 1.7, S. 12) habe ich über das Schengener Abkommen und seine datenschutzrechtlichen Aspekte berichtet, mit dem die Bundesrepublik Deutschland, Frankreich und die Benelux-Staaten den schrittweisen Abbau der Grenzkontrollen vereinbart

haben. Um die dadurch entstehenden Sicherheitsdefizite auszugleichen, sind ein verstärkter Informationsaustausch zwischen den Behörden der Vertragsstaaten und weitere kompensierende Maßnahmen vorgesehen.

Die Einzelheiten des Verfahrens sind in einem Zusatzübereinkommen festgehalten, welches im Juni 1990 abgeschlossen wurde. Die grenzüberschreitende Informationsverarbeitung hat durch die Einrichtung eines zentralen, automatisierten Informationssystems (SIS) eine neue Dimension erfahren.

Die datenschutzrechtlichen Probleme des vorgesehenen Informationsaustauschs habe ich bereits im einzelnen geschildert (vgl. 11. TB, Tz. 1.7). Die Vertragsregelungen sind außerordentlich kompliziert, so daß der Betroffene wohl kaum noch nachvollziehen kann, wo seine Daten verarbeitet und genutzt werden, wenn sie erst einmal auf der Grundlage des supranationalen Verbindungsnetzes grenzüberschreitend übermittelt sind. Um so mehr fallen die nach wie vor bestehenden Mängel ins Gewicht. Den Bedenken der DSB-Konferenz (vgl. 11. TB, Anlage 6) wurde nur teilweise Rechnung getragen.

Es fehlen nach wie vor Regelungen für das Schengener Informationssystem, die unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes festlegen, wann Informationen aus dem nationalen in den internationalen Fahndungsbestand übernommen werden (Art. 94, 95).

Ebenso fehlt die Festlegung, unter welchen Voraussetzungen und in welchem Umfang die verschiedenen Inlandsbehörden auf die Daten des Informationssystems zugreifen dürfen (Art. 101).

Schließlich konnten sich die Vertragsparteien auch nicht dazu durchringen, die Voraussetzungen konkreter

zu beschreiben, unter denen verdeckte Registrierungen von Personen erlaubt werden sollen (Art. 99).

Die verdeckte Registrierung wird im übrigen von der Voraussetzung des nationalen Rechts abhängig gemacht (Art. 99 Abs. 2). Die in der BRD insoweit bestehenden Regelungsdefizite lassen die durch das Zusatzübereinkommen auftretenden Probleme noch stärker hervortreten.

Wegen des Wegfalls der Grenzen zwischen den Staaten des Schengener Abkommens ist zweifelfrei der grenzüberschreitende Datenaustausch im Sicherheitsbereich zu intensivieren. Insoweit hat das Zusatzübereinkommen Fortschritte gebracht. Damit sind jedoch Gefahren für das informationelle Selbstbestimmungsrecht entstanden, die eine sorgfältige Kontrolle der praktischen Umsetzung des Vertragswerkes erfordern.

### 1.2.3 EG-Statistikverordnung

Die EG-Statistikverordnung, über die ich im letzten Jahr berichtet habe (vgl. 11. TB, Tz. 1.6), ist inzwischen verabschiedet und im Amtsblatt der EG veröffentlicht worden. Erfreulicherweise ist den Forderungen der Datenschutzbeauftragten des Bundes und der Länder (vgl. Entschließung zum Entwurf einer EG-Statistikverordnung vom 26./27.10.1989, 11. TB, Anlage 6) weitgehend Rechnung getragen worden. Übermittlungen personenbezogener Einzelangaben an das Statistische Amt der EG dürfen nach dem verabschiedeten Text nur aufgrund eines eigenen Rechtsaktes der EG für bestimmte statistische Zwecke, nach frühzeitiger Anonymisierung und nach Regelung der notwendigen organisatorisch-technischen Maßnahmen der Datensicherung vorgenommen werden. Auch der Forderung nach ausreichender Sanktion für Verletzungen des Statistikgeheimnis wurde Rechnung getragen. Dagegen erfüllt die Rechtsverordnung nicht die Forderung der Datenschutzbeauftragten

nach einer unabhängigen Datenschutzkontrolle und bleibt insoweit hinter dem nationalen Recht zurück. Es bleibt jedoch zu hoffen, daß die Initiativen der EG zur Harmonisierung datenschutzrechtlicher Bestimmungen (vgl. Tz. 1.2.2) eine unabhängige Datenschutzkontrolle unter Einschluß der Statistik auf der Ebene der Gemeinschaft ermöglichen wird.

#### 1.2.4 Deutsch-deutscher Datenaustausch vor der Vereinigung

Nachdem die Mauer zwischen der BRD und der DDR gefallen war, wuchsen trotz aller Unsicherheiten im Hinblick auf die Rechtslage in der DDR die Informationsinteressen über die bisher trennende Grenze hinweg sprunghaft an. Die Notwendigkeit eines deutsch-deutschen Informationsaustausches ergab sich insbesondere im Bereich der Öffentlichen Sicherheit und Rechtspflege (z.B. Verfolgung wegen Ladendiebstählen, Verkehrsdelikten und Verletzungen der Unterhaltspflicht durch Flucht unter Zurücklassung von Kindern). Schon vor dem endgültigen Wegfall der Personenkontrollen an der "innerdeutschen" Grenze war deshalb als Ausgleichsmaßnahme zur Vermeidung von Sicherheitsdefiziten die Bildung einer Fahndungsunion geplant, um eine schnelle Unterrichtung der Polizeibehörden der DDR und der BRD über Personen sicherzustellen, die von der jeweils anderen Seite zur Strafverfolgung, zum Strafvollzug, zur Strafvollstreckung oder zur Gefahrenabwehr gesucht werden. Das Gesetz über die innerdeutsche Rechts- und Amtshilfe in Strafsachen vom 2. Mai 1953 (BGBl. I S. 161) enthält keine Vorschriften zu der Frage des Datenaustauschs im Bereich der Gefahrenabwehr und der spontanen Datenübermittlung für Strafverfolgungszwecke. Der Prozeß der sozialen, wirtschaftlichen und politischen Einigung führte zu verstärktem, grenzüberschreitendem Datenverkehr, z.B. im Sozialrecht, im Melderecht, im Versicherungs- und Kreditrecht. Vor allem zur Vermeidung von Leistungs-

mißbräuchen strebten die Sozialleistungsträger einen Informationsaustausch an.

Der wechselseitige Datenaustausch setzte nach dem Rechtsverständnis der BRD eine ausreichende, gesetzliche Grundlage voraus, auf die nur übergangsweise - etwa im Bereich der Strafverfolgung - verzichtet werden konnte, wenn die Einhaltung gewisser Minimalanforderungen gesichert war. Dies um so mehr, als die datenschutzrechtlichen Defizite auf dem Gebiet der DDR nicht nur normativer Art waren. Das geschriebene Recht enthielt keine ausdrücklichen Vorschriften über den Datenschutz; besondere Vorschriften, Anordnungen, soweit sie etwa zum Berufsgeheimnis und Bankgeheimnis oder im Hinblick auf die Datensicherung und Ordnungsgemäßheit der Datenverarbeitung bestanden, mußten in ihrer praktischen Wirksamkeit für den Schutz der Grundrechte vor allem deshalb als gering eingeschätzt werden, weil das materialistische Rechtsverständnis keine staatlichem Handeln vorausgehenden Rechte des Bürgers gegen den Staat kennt. Vor allem aber konnte die Verwaltungsorganisation der DDR in keiner Weise rechtsstaatlichen Minimalanforderungen genügen. Die zentralistische Behördenstruktur - in der DDR war z.B. seit 1972 eine zentrale Personen-Datenbank mittels einer Personenkennzahl für jeden Einwohner aufgebaut worden - und die fehlende Trennung von Polizei- und Ordnungsbehörden mußte vor allem Zweifel daran aufkommen lassen, ob die Zweckbindung der übermittelten Daten gewährleistet war. Nicht zuletzt war die Struktur des Staatssicherheitsdienstes nicht durchschaubar und sorgte für zusätzliche Verunsicherung.

Die Vorschläge des Bundesministers der Justiz für eine vorläufige Regelung haben die Datenschutzbeauftragten als unzureichend kritisiert, während die des Bundesministers des Innern die in einem Beschluß der Konferenz vom 23.03.1990 (Anlage 4) enthaltenen Anregungen größtenteils berücksichtigten. Auf diesen Grundsätzen

basierten die "vorläufigen Regeln" der Bundesregierung, die später von wenigen Ausnahmen abgesehen als Anlage VII. des Staatsvertrages vom 18. Mai 1990 über die Schaffung einer Währungs-, Wirtschafts- und Sozialunion zwischen der BRD und der DDR (BGBl. II 1990 vom 29.06.1990) übernommen wurden. Zu den Minimalanforderungen des Datenverkehrs gehörten danach die Beachtung der Grundsätze des Übereinkommens des Europarats über den Schutz des Menschen bei der Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Europaratskonvention) und einige Regeln über die Zweckbindung und das Auskunftsrecht des Betroffenen sowie die entsprechende Anwendung der Datenschutzregelungen des Sozialgesetzbuches. Der Verweis auf die Europaratskonvention konnte allein deshalb nicht ausreichen, weil Rechte der Betroffenen daraus nicht unmittelbar hergeleitet werden können. Die Gewährleistung der Zweckbindung war indessen ein wesentliches Anliegen. War etwa die Kriminalitätsbekämpfung ohne Datenaustausch nicht sichergestellt, so mußte wenigstens die Verwendung der Informationen auf den Anlaß der Erhebung beschränkt werden.

Die Datenschutzbeauftragten wiesen darüberhinaus in ihrer EntschlieÙung darauf hin, daß die Veränderungen in der DDR und im übrigen Ost- und Mitteleuropa auch zu Konsequenzen bei der Sicherheitsüberprüfung und der Informationsverarbeitung durch die Nachrichtendienste in der BRD führen muß.

Die entscheidende Schwachstelle war jedoch, daß die Verwaltungsstruktur der DDR rechtstaatlichen Anforderungen nicht genügte und die Kontrolle durch ein unabhängiges Organ in der DDR nicht gewährleistet war. Ich habe deshalb in meiner Stellungnahme gegenüber dem Ministerium des Innern zur Fahndungsunion gefordert, daß im Interesse der schutzwürdigen Belange des Betroffenen die DDR-Behörden auf Ersuchen verpflichtet

sein sollten, dem Datenschutzbeauftragten des Aufenthaltslandes des Betroffenen Auskunft zu erteilen.

Glücklicherweise waren die vorläufigen Regeln infolge der Rasananz der weiteren Entwicklung nur für eine kurze Übergangszeit in Kraft. Seit dem 3. November 1990 gilt im Gebiet der früheren DDR das Bundesdatenschutzgesetz aufgrund des zweiten Staatsvertrages vom 31. August 1990 und dem hierzu verabschiedeten Einigungsvertragsgesetz (BGBI II 1990 S. 885). Der Bundesbeauftragte für den Datenschutz übt die Kontrolle in den neuen Bundesländern längstens bis zum 31. Dezember 1991 aus. Es ist davon auszugehen, daß in diesen Bundesländern nach und nach Landesbeauftragte ihre Tätigkeit aufnehmen werden.

## 2. Entwurf eines Saarländischen Datenschutzgesetzes (SDSG)

Der Referentenentwurf zur Novellierung des Saarländischen Datenschutzgesetzes (Stand 04.05.1990) wurde mir zur Stellungnahme übersandt.

Der Gesetzentwurf verbessert die Rechtsgrundlagen des Datenschutzes und zieht notwendige Schlußfolgerungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts und Art. 2 Saarländischen Verfassung, indem mit Zustimmung aller im Landtag vertretenen Parteien der Datenschutz als Grundrecht ausdrücklich festgeschrieben wurde.

Positiv hervorzuheben sind insbesondere:

- die Erstreckung des Anwendungsbereiches auf jede Art der Verarbeitung personenbezogener Daten (insbesondere unter Einschluß von Akten); insoweit wird auch die Kontrollbefugnis des Landesbeauftragten klargestellt;
- die Einbeziehung der Datenerhebung sowie der Datennutzung als Phasen der Datenverarbeitung;
- die grundsätzliche Pflicht, die Daten beim Betroffenen zu erheben;
- der Grundsatz der Zweckbindung;
- der grundsätzliche Anspruch auf unentgeltliche Auskunftserteilung, wenn nicht unter den im Entwurf genannten Voraussetzungen das Geheimhaltungsinteresse überwiegt;
- die Regelung der Datenverarbeitung bei Dienst- und Arbeitsverhältnissen des öffentlichen Dienstes sowie für Fernmessen und Fernwirken;

- die Erstreckung der Kontrollbefugnis des Landesbeauftragten auf den Verfassungsschutz.

Gegenüber dem geltenden Saarländischen Datenschutzgesetz vom 17. Mai 1978 waren in folgenden Punkten Rückschritte festzustellen:

- Das Saarländische Datenschutzgesetz galt bisher für alle öffentlichen Stellen; sein Geltungsbereich war im Interesse seiner Auffangfunktion nur insoweit eingeschränkt, als spezielle Gesetze für besondere Bereiche Datenschutzregelungen vorsahen. Im Entwurf sind Gnadensachen völlig, Gerichte und Staatsanwaltschaften und der Landtag mit der Einschränkung ausgenommen, daß insoweit lediglich die Wahrnehmung von "Verwaltungsaufgaben" im Anwendungsbereich des Gesetzes verbleibt.

Die Regelung hätte zur Folge, daß die Kontrollbefugnis des Landesbeauftragten für Datenschutz entsprechend dem Anwendungsbereich des Gesetzes beschränkt ist. Seine Kompetenzen müssen selbstverständlich ihre Grenzen an der richterlichen Unabhängigkeit und der verfassungsrechtlichen Stellung des Parlaments finden. Externe Kontrollen in diesen Bereichen jedoch nur zuzulassen, wenn es sich um die Wahrnehmung von "Verwaltungsaufgaben" handelt, kann im Einzelfall über das Gebotene hinausgehen, weil nicht auf die allein maßgebliche verfassungsrechtliche Substanz abgestellt wird. Man muß fragen, ob das Richterprivileg berührt ist, wenn der Landesbeauftragte riskante, automatisierte Systeme für die Geschäftsstellen oder die Grundbuchämter überwacht, auch wenn sie nicht nur der Wahrnehmung von Verwaltungsaufgaben dienen. Ich kann nicht erkennen, daß der besondere verfassungsrechtliche Rang des Parlaments dadurch tangiert wird, wenn etwa eine ISDN-

fähige Telefonanlage im Landtag, die von der Landtagsverwaltung und von Abgeordneten gleichermaßen genutzt wird, vom Landesbeauftragten für Datenschutz auf ihre datenschutzgerechte Installation überprüft wird. Maßnahmen etwa zum Schutze des Telefon- und Fernmeldegeheimnisses bei der Einrichtung moderner technischer Einrichtungen kann doch wohl keine Beeinträchtigung der parlamentarischen Prerogative oder der Unabhängigkeit des Richters bedeuten. Der Entwurf sollte deshalb auf die verfassungsrechtlich allein maßgeblichen Gesichtspunkte der richterlichen Unabhängigkeit und der parlamentarischen Prerogative abstellen; die Verwendung unbestimmter Rechtsbegriffe wie "Verwaltungsaufgaben" baut unnötige und den genannten Verfassungsgrundsätzen nicht dienliche Hürden auf.

- Die Kontrollbefugnis des Landesbeauftragten wird zudem durch eine Staatswohlklausel beschränkt.
- Verstöße gegen das Datenschutzgesetz sollen nur noch dann als Straftaten verfolgt werden, wenn sie gegen Entgelt oder in Bereicherungsabsicht erfolgen. Die Gefahren für die Persönlichkeitsrechte werden indessen mit fortschreitender Automation größer. Die Entkriminalisierung von Verstößen gegen den Datenschutz stellt einen bedenklichen Rückschritt dar.
- Der Begriff der Datenübermittlung soll nicht mehr wie bisher (§ 14 Abs. 3 Satz 2 SDStG) uneingeschränkt auch für den internen Bereich einer Behörde anwendbar bleiben. Da für die Datenweitergabe innerhalb öffentlicher Stellen die Vorschriften über die Datenübermittlung nur noch entsprechend anwendbar sind, besteht die Gefahr, daß der bisher im Gesetz verankerte "funktionelle Behördenbegriff" an Eindeutigkeit und Klarheit verliert. Dies ist vor allem nachteilig im Hinblick auf die Auffang- und Leitfunktion des Saarländischen Datenschutzgesetzes für

die Datenverarbeitung in anderen öffentlichen Bereichen.

In anderer Hinsicht entsprechen die beabsichtigten Regelungen nicht den Vorgaben des Bundesverfassungsgerichts im Volkszählungsurteil. Aus meiner Stellungnahme möchte ich nur folgende Punkte erwähnen:

- Dem Fortschritt der Technik muß der Entwurf noch stärker Rechnung tragen. Die Gefahren des On-line-Anschlusses erfordern die gesetzliche Festlegung der Protokollierung für jeden Einzelabruf. Die Risiken, die in der Selbstbedienung des Datenempfängers liegen, müssen wenigstens durch nachträgliche Kontrollen gemindert werden. Der Landesbeauftragte ist auch - wie bisher - vor der Einrichtung des automatisierten Direktabrufes innerhalb öffentlicher Stellen zu beteiligen. Auf einem besonderen Berufs- oder Amtsgeheimnis unterliegende Daten darf automatisiert nur aufgrund einer ausdrücklichen, gesetzlichen Ermächtigung zugegriffen werden.
- Die Zweckänderung bei der Verarbeitung gespeicherter Daten rechtfertigt der Entwurf, wenn eine Rechtsvorschrift dies "zwingend voraussetzt" oder es "zur Abwehr erheblicher Nachteile für das Gemeinwohl" erforderlich ist. Durch eine komplizierte Verweisung sind diese generalklauselartigen Voraussetzungen auch für die ausnahmsweise zugelassene Datenerhebung bei anderen Stellen und für die Datenübermittlung anzuwenden. Die Vorschriften sind zu weit gefaßt und wegen ihrer Unbestimmtheit verfassungsrechtlich bedenklich. Der Grundsatz der Zweckbestimmung und das Prinzip der Erhebung beim Betroffenen werden ausgehöhlt; vor allem die Datenweitergabe wird in einem für den Bürger nicht mehr überschaubaren Umfang ausgeweitet.

- Die generelle Zulassung der Verarbeitung personenbezogener Daten für Rechnungsprüfungszwecke, Organisationsuntersuchungen sowie für Ausbildungszwecke ist unverhältnismäßig und deshalb verfassungsrechtlich bedenklich. Regelmäßig sollten anonymisierte Daten und personenbezogene Daten nur dann verwendet werden, wenn dies unumgänglich ist. Werden personenbezogene Daten zu Planungszwecken verarbeitet, ist eine personelle und organisatorische Trennung und Abschottung notwendig, um die Zweckbindung sicherzustellen (vgl. § 32 Abs. 1 Hessisches Datenschutzgesetz).
- Die Einwilligung des Betroffenen darf nicht zu seinem Nachteil mißbraucht werden. Der Manipulationsgefahr gegenüber dem abhängigen und in einer Zwangslage befindlichen Bürger ("faktischer Zwang") muß durch Festlegung der Mindestvoraussetzungen zulässiger Informationsverarbeitung auf freiwilliger Grundlage entgegengewirkt werden.
- Transparenz und Kalkulierbarkeit der Informationsverarbeitung erfordern die Unterrichtung des betroffenen Bürgers über die automatisierte Speicherung (vgl. § 18 Abs. 2 Hessisches Datenschutzgesetz). Außerdem sollten die öffentlichen Stellen zur Protokollierung der Datenübermittlung verpflichtet werden; Prozesse zur Durchsetzung von Schadenersatzansprüchen des Betroffenen haben alsdann größere Aussicht auf Erfolg und die Kontrollen werden effektiver.
- Die Zweckbindung von personenbezogenen Daten, die ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, ist im Gesetz ausdrücklich festzuschreiben. Solche Protokolldaten dürfen nicht zu anderen

- Zwecken verwendet werden (vgl. § 13 Abs. 5 Hessisches Datenschutzgesetz).
- Der Personaldatenschutz, insbesondere die Transparenz der Nutzung von Personalinformationssystemen ist zu verbessern. Dienst- und arbeitsrechtliche Beurteilungen sowie medizinische und psychologische Befunde des Beschäftigten dürfen nicht automatisiert verarbeitet werden (vgl. § 34 Abs. 3 und Abs. 6 Hessisches Datenschutzgesetz).
  - Die bewährte und bürgerfreundliche Zusammenfassung von Kontroll- und Beratungsaufgaben für den öffentlichen und privaten Bereich beim Landesbeauftragten für Datenschutz ist beizubehalten.
  - Die Vorschriften über die Rechtsstellung des Landesbeauftragten für Datenschutz müssen im Interesse der Stärkung seiner Unabhängigkeit weiter konkretisiert werden. Insbesondere darf das Personal der Dienststelle nur mit seinem Einverständnis versetzt und umgesetzt werden.

Es ist zu bedauern, daß der Referentenentwurf bisher nicht in das Gesetzgebungsverfahren eingebracht wurde und deshalb die notwendige Fortschreibung des Gesetzes unterblieben ist. Besonders nachteilig ist die in den Bundesländern einzigartige, weiterbestehende Exemption des Verfassungsschutzes von der Kontrolle durch den Landesbeauftragten für Datenschutz.

### 3. Polizei

#### 3.1 Polizeiinformationssystem DIPOL

Bereits im 11. Tätigkeitsbericht habe ich das zur Verbesserung der Infrastruktur der Polizei geplante Informationssystem DIPOL geschildert (Tz. 3.2). Ziel des Projekts ist die Integration von Vorgangsbearbeitung, -verwaltung, Texterstellung und -bearbeitung sowie Textkommunikation mit Hilfe eines Fernsprechnetzes, das alle Polizeidienststellen verbindet. Die Diskussion über dieses riskante und komplexe Telekommunikationssystem wurde im vergangenen Jahr intensiv fortgeführt, ohne daß ich aus meiner Sicht ein in jeder Hinsicht befriedigendes Ergebnis konstatieren könnte.

Bei der Rechtsfindung über die Grenzen zulässiger Informationsverarbeitung in diesem System darf nicht vergessen werden, daß praktisch jede Berührung des Bürgers mit der Polizei als Finder, Zeuge, Auskunftsperson, Anzeiger, Geschädigter, Opfer, Beschuldigter, Verdächtiger und Kontaktperson eines Beschuldigten ihren elektronischen Niederschlag in DIPOL findet und damit der Polizei der Zugriff auf personenbezogene Daten in bisher nicht gekanntem Umfang eröffnet werden kann.

Neben lokaler, dezentraler Erfassung und Verarbeitung in den örtlichen Polizeidienststellen soll ein zentraler, personenbezogener Datenbestand auf Landesebene eingerichtet werden. Der Qualitätssprung im Vergleich zu der bisherigen konventionellen Arbeitsweise liegt nicht nur in der gezielten Abrufmöglichkeit auf örtlicher Ebene, sondern auch in der Möglichkeit einer schnellen, landesweiten Zusammenführung von Polizeiinformationen mit Hilfe des zentralen Bestandes begründet. Immer wieder habe ich versucht das Problem zu verdeutlichen, inwieweit diese Möglichkeiten genutzt

werden dürfen und inwieweit es möglich ist, den von der Technik ausgehenden Gefahren zu begegnen.

Im Polizeibereich stehen sich zwei gleichrangige Verfassungspositionen gegenüber: Rechtsgüterschutz der Polizei durch Gefahrenabwehr und Verbrechensbekämpfung einerseits und Persönlichkeitsrechte des Bürgers andererseits. Auf der Grundlage des Saarländischen Polizeigesetzes muß eine Lösung gefunden werden, die unter Berücksichtigung beider Gesichtspunkte einen verfassungskonformen Einsatz des Systems gewährleistet.

Mit den Bürgerrechten wäre es jedenfalls nicht vereinbar, wenn DIPOL zu einem Verdachtverdichtungsinstrument ausgestaltet würde, das die Allgegenwärtigkeit und Allzuständigkeit der Polizei im Vorfeld konkreter Gefahren zur Folge hätte. Es muß deshalb dafür gesorgt werden, daß Informationen, die die Polizei aus aktuellem Anlaß etwa über Finder, Anzeiger, Zeugen, Auskunftspersonen, Opfer und Geschädigte dokumentiert, nicht in unverhältnismäßigem Umfang aus Gründen der Vorbeugung genutzt werden. Das Polizeirecht des Saarlandes schreibt eine strenge Zweckbindung vor (§ 25 Abs. 1, § 30 Abs. 1 Satz 2 SPolG). Zweckbestimmung kann die Strafverfolgung, die Gefahrenabwehr, die Gefahrenvorsorge, die vorbeugende Verbrechensbekämpfung oder die sogenannte Vorgangsverwaltung sein. Das Informationssystem hat diese unterschiedlichen Zweckbestimmungen zu berücksichtigen. Es müssen objektive Kriterien gefunden werden, an denen sich die Zugriffsregelung zu orientieren hat.

Mit diesen durch das Gesetz vorgegebenen Schranken ist jedenfalls die geplante, zentrale Datenhaltung nicht vereinbar, die die lokalen Vorkommisse in welcher Form und mit welchem Umfang auch immer, gegebenenfalls sogar für alle Polizeidienststellen personenbezogen abrufbar dokumentiert. Zur vorbeugenden Verbrechensbekämpfung dürfen jedoch aus Strafermittlungsverfahren

lediglich Wiederholungstäter nach einer sorgfältigen Prognoseentscheidung gespeichert werden (§ 30 Abs. 2 SPolG). Diesem Zweck dient das beim Bundeskriminalamt eingerichtete INPOL-System. Diesem bundesweit und teilweise landesweit abrufbaren Datenbestand darf keine weitere, zentrale Datenhaltung hinzugefügt werden, weil sie für präventive Zwecke nicht erforderlich ist und zudem den Betroffenen unverhältnismäßig belasten würde. Die geplante, zentrale Registratur würde vom ersten Tag der Ermittlung an nach Gesichtspunkten der Vorbeugung unbewertete Informationen enthalten. Die Nutzung eines solchen Datenbestandes, die notwendigerweise präventive Auswirkungen haben müßte, wäre mit den strengen Anforderungen des Gesetzes nicht vereinbar.

Der Minister des Innern wird sich an seiner Presseerklärung vom 12. Februar 1990 messen lassen müssen: "So müßten selbstverständlich die Zugriffsregelungen die im Saarländischen Polizeigesetz festgeschriebenen Grundsätze der Zweckbindung verwirklichen. Informationen, die nicht der Strafermittlung und Gefahrenabwehr unmittelbar dienen, dürften nur für die Zwecke des jeweiligen Vorgangs genutzt werden. Die polizeiliche Vorgangsverwaltung durch DIPOL müsse präzise festgelegt werden ...".

Die Diskussion über die Grenzen der Nutzung der in dem riskanten System gespeicherten Informationen ist noch im Gang.

### 3.2 Spezialdateien

Beim Kriminalpolizeiamt des Saarlandes wurde eine spezielle Prostituiertenkartei für den Bereich der Landeshauptstadt mit etwa 600 Personen geführt. Dabei wurde für jede Prostituierte - unabhängig davon, ob im konkreten Fall begründeter Anlaß für Ermittlungen wegen strafbarer Handlungen, Ordnungswidrigkeiten oder

zur Gefahrenabwehr bestand - eine Karteikarte angelegt, die Namen, Anschrift, Geburtsdatum und häufig auch Hinweise oder Verweise auf den Standort oder Arbeitsplatz enthielt.

Neben dieser Kartei wurde eine alphabetisch geordnete Sammlung von Hängeakten geführt, in der Erkenntnisse über das Umfeld, gegebenenfalls Ordnungswidrigkeiten, Anzeigen wegen Verstoßes gegen die Sperrbezirksverordnung, Zeugenvernehmungen beispielsweise wegen eventueller Gewerbsunzucht, Anträge des Verwaltungspolizeiamtes auf Vorführung zum Gesundheitsamt, Abmeldung der Tätigkeit beim Gesundheitsamt gesammelt wurden. Teilweise waren die Erkenntnisse in einem Formblatt strukturiert, auf dem regelmäßig als Freitext eine Vernehmung der Prostituierten über ihre Herkunft und sozialen Verhältnisse aufgezeichnet war. In vielen Fällen war in der Akte ein Lichtbild der Betroffenen abgelegt.

Darüberhinaus wurde jede Prostituierte - auch wenn kein Anlaß für Ermittlungen besteht - in dem automatisierten INPOL-Saarland-Verfahren, das allen saarländischen Polizeidienststellen für Auskünfte zur Verfügung steht, mit dem Hinweis auf ihre Tätigkeit und die Fundstelle für ihre Akte gespeichert. Das Aussonderungsprüfdatum ist regelmäßig auf fünf Jahre festgelegt; jede wie auch immer geartete Erkenntnis verlängerte die Speicherung um den gleichen Zeitraum.

Nach Artikel 2 der Saarländischen Verfassung hat jeder Anspruch auf den Schutz seiner personenbezogenen Daten. Eingriffe in das informationelle Selbstbestimmungsrecht sind nur in überwiegendem Interesse der Allgemeinheit aufgrund eines förmlichen Gesetzes zulässig. Die umfangreiche Datenspeicherung war deshalb auf der Grundlage des Saarländischen Polizeigesetzes zu bewerten.

Aus Gründen der Gefahrenabwehr war die Erhebung von Informationen über Prostituierte nicht gerechtfertigt, wenn nicht im Einzelfall eine konkrete Gefahr vorlag. Die Prostitution ist nicht mehr oder weniger gefahren-geneigt als andere Erwerbszweige. Wollte man gefährde-te Personen schlechthin polizeilicher Kontrolle unter-werfen, müßten ebenso Nachtportiers, Betreiber von Bars und Gaststätten mit Nachtkonzession, Bedienstete von Wach- und Schließgesellschaften einbezogen werden. Die Prostitution als alleiniges Kriterium ist für die Annahme einer konkreten Gefahr im Einzelfall untaug-lich.

Prostitution an sich ist nicht strafbar, so daß diese für sich allein die Speicherung in polizeilichen Da-teien und Unterlagen weder im Hinblick auf ein bisheri-ges noch auf ein zukünftiges Verhalten rechtfertigt (§ 30 Abs. 2 SPolG). Die Prostitution allein liefert überdies noch keine Anhaltspunkte dafür, daß Verbre-chen oder qualifizierte Straftaten begangen werden (§ 30 Abs. 3 SPolG), so daß auch im Vorfeld konkreter Gefahren die Erhebung und Speicherung aus Gründen der Prävention nicht zulässig ist.

Meiner Forderung, die Prostituiertenkartei aufzulösen, die alphabetisch geordnete Sammlung von Hängeakten zu vernichten und die zugehörige Speicherung im automati-sierten Bestand zu löschen, hat das Ministerium des Innern schon deshalb Rechnung getragen, weil der kri-minalistische Wert dieser Datei in keinem Verhältnis zu dem personellen Aufwand stehe.

Die Brisanz der geschilderten, polizeilichen Informa-tionsverarbeitung lag vor allem auch darin begründet, daß Personen, die sich nicht strafbar gemacht haben, in dem landesweiten, automatisierten Informations-system ISA gespeichert wurden.

In meinem letzten Tätigkeitsbericht (8. TB, Tz. 3.4.1 S. 42) habe ich über die Schankkonzessionsdatei eines Polizeireviers im Bereich der Landeshauptstadt berichtet. Hierbei handelte es sich um eine Aktensammlung über etwa 470 Gaststätten, die über eine Findex-Datei erschließbar war. Die Akten enthielten umfangreiche Informationen über Gastwirte, Konzessionsurkunden, Baupläne, Strafregisterauszüge und Polizeiberichte über strafbare Handlungen und Ordnungswidrigkeiten der Konzessionsinhaber sowie sonstige Vorfälle und Beobachtungen über das Verhalten dieser Personen. Ich hatte deutlich gemacht, daß die Führung derartiger Aktensammlungen durch die Vollzugspolizei rechtswidrig ist.

Nachdem der Innenminister zunächst eine gegenteilige Auffassung vertreten hatte, konnte ich im Laufe des Jahres 1990 erreichen, daß er sich meiner Rechtsmeinung anschloß. Das Schutzpolizeiamt wurde angewiesen, die bei den Dienststellen bestehenden Aktensammlungen zu vernichten.

Abgesehen von der rechtlichen Würdigung des Tatbestandes wird deutlich, daß die Notwendigkeit von Spezialdateien neben dem INPOL-System in Zweifel zu ziehen ist. Die Auffassung des Ausschusses für Innere Verwaltung, daß die konventionellen Spezialdateien abzubauen sind, muß unterstrichen werden (Tz. 2.2 der Entschließung vom 09.11.1989, Lt-Drucksache 9/1038-9/1121; Anlage 8 zu meinem 11. Tätigkeitsbericht).

### 3.3 Protokollierung der INPOL-Abfrage

Im Berichtszeitraum wurde die Protokollierung der Nutzung von Personenauskünften aus dem polizeilichen Informationssystem INPOL überprüft.

Bei der Datei INPOL handelt es sich um ein bundesweites Verbundsystem, in das Informationen über Straftäter und Beschuldigte aufgenommen werden. Sinn der Datei ist es, die Arbeit der Polizei bei zukünftigen Strafermittlungsverfahren zu erleichtern. Um mißbräuchliche Zugriffe durch Polizeibeamte auszuschließen, ist durch Erlaß des Innenministers ein stichprobenartiges Überprüfungsverfahren vorgeschrieben. Hierbei hat das Kriminalpolizeiamt, über dessen Terminals alle Auskünfte laufen, an zehn im voraus festzulegenden Tagen im Monat drei Personenerkenntnisfragen nach freier Entscheidung auszuwählen und durch Rückruf bei dem Leiter der Dienststelle, der der anfragende Beamte angehört, die Rechtmäßigkeit des Datenabrufes festzustellen und entsprechend zu protokollieren. Aus Gründen der Effektivität war eine früher einmal vorgesehene, vollständige Protokollierung der Abfragen auf den beschriebenen Umfang zurückgenommen worden.

Bei der Überprüfung dieses Protokollierungsverfahrens hat sich gezeigt, daß im Kriminalpolizeiamt zwar den Vorgaben des ministeriellen Erlasses Rechnung getragen wird, das Verfahren jedoch verbesserungsbedürftig ist. Eine nach dem Zufallsprinzip erfolgte Auswahl von zwölf Personenauskünften, deren Berechtigung in den Dienststellen und Revieren durch meine Mitarbeiter überprüft wurde, hat jedenfalls in vier Fällen zu einem zweifelhaften Ergebnis geführt. Die Einlassung der Beamten ließ eine eindeutige Rechtfertigung der Abfragen nicht erkennen. So erklärte ein Bediensteter, daß er für einen Kollegen nachgefragt habe, an dessen Namen er sich aber nicht mehr erinnere. Ein anderer war mehrere Wochen abwesend, so daß mangels Bezugs der Abfrage zu einem Aktenvorgang davon auszugehen war, daß aufgrund des Zeitablaufs eine Aufklärung nicht mehr möglich oder doch sehr erschwert sein würde.

Zu bemängeln war auch das Protokollierungsverfahren, da durch allgemeine Formulierungen zur Begründung des Abfragegrundes - beispielsweise Strafermittlungen - eine Überprüfung im nachhinein äußerst erschwert wurde. Zudem wurden Abfragen von Dienststellenleitern nicht kontrolliert.

Schließlich wurde festgestellt, daß aus Gründen des Betriebsablaufes Kontrollen des Kriminalpolizeiamtes nur am Vormittag stattfinden, obgleich INPOL-Abfragen rund um die Uhr erfolgen. Bei dieser Verfahrensweise besteht die Gefahr, daß die Kontrollpraxis in den Revieren bekannt ist und daher Anfragen, deren Rechtmäßigkeit zweifelhaft sein könnte, außerhalb der genannten Zeit durchgeführt werden.

Erfreulich ist, daß der Innenminister meinen Beanstandungen und Anregungen Rechnung getragen hat und zukünftig die Protokollierung auf einen Zeitraum von 24 Stunden ausdehnen und hierbei statt drei Abfragen an den ausgewählten Tagen jeweils fünf Abfragen einer Überprüfung unterziehen wird. Protokolliert wird zukünftig neben dem Anlaß der Abfrage auch ein Hinweis auf die der Anfrage zugrundeliegenden Akte und die Tagebuchnummer oder das Aktenzeichen. Schließlich halte ich es für besonders bedeutsam, daß zukünftig nicht mehr eine telefonische Überprüfung stattfindet, sondern in jedem Fall ein schriftliches Verfahren durchgeführt wird, wobei zusätzlich auch Abfragen des Dienststellenleiters durch den nächsthöheren Vorgesetzten überprüft werden.

Gleichwohl ist nicht zu verhehlen, daß auch diese Verfahrensweise die mißbräuchliche Inanspruchnahme des INPOL-Systems nicht ausreichend ausschalten wird. Wünschenswert wäre aus datenschutzrechtlicher Sicht eine umfassende Protokollierung, durch die datenschutzrechtliche Kontrollen in weit größerem Umfang ermöglicht würden. Mit fortschreitender Automation

werden sich die Möglichkeiten der Protokollierung verbessern. Um die Zweckbindung der Protokolldaten zu gewährleisten, sind jedoch nicht zu lange Speicherfristen vorzusehen.

#### 4. Rechtspflege

##### 4.1 Stand der Gesetzgebung

Das Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65,1) hat die Auffassung der Datenschutzbeauftragten bestätigt, daß Eingriffe in das Recht auf informationelle Selbstbestimmung einer gesetzlichen Grundlage bedürfen, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für den Bürger erkennbar ergeben. Obgleich seit dieser Entscheidung bereits mehr als sieben Jahre vergangen sind, müssen für den Bereich der Rechtspflege nach wie vor Regelungsdefizite festgestellt werden.

Bereits in früheren Tätigkeitsberichten habe ich auf die Notwendigkeit eines Justizmitteilungsgesetzes hingewiesen (vgl. zuletzt 8. TB, Tz. 3.2.1 S. 46). Mitteilungen aus gerichtlichen Verfahren werden noch immer auf der Grundlage von Verwaltungsvorschriften, nämlich der "Anordnung über Mitteilungen in Strafsachen (MiStra)" und der "Anordnung über Mitteilungen in Zivilsachen (MiZi)" versendet. Gerichte und Staatsanwaltschaften haben aufgrund dieser Verwaltungsanordnungen vielen anderen Stellen und Institutionen über Straf- und Zivilverfahren und die dabei gewonnenen Erkenntnisse zu berichten. Dabei werden sehr sensible Angaben über den Betroffenen weitergegeben, die die Persönlichkeitsrechte beeinträchtigen. Es steht folglich außer Frage und wird auch von der Justizverwaltung nicht bestritten, daß diese Datenübermittlungen nur auf der Grundlage einer gesetzlichen Regelung erfolgen dürfen. Gleichwohl ist es in der vergangenen Legislaturperiode nicht gelungen, den gesetzgebenden Körperschaften einen verabschiedungsreifen Gesetzentwurf vorzulegen. Ich habe daher den Justizminister wiederum aufgefordert (vgl. bereits meinen 8. TB, Tz. 3.2.2, S. 51), für die Übergangszeit Datenübermittlungen nach MiZi und MiStra nur in eingeschränktem Umfang

zuzulassen. Dies ist notwendig, da das Bundesverfassungsgericht bei Fehlen der gesetzlichen Grundlagen die Weiterführung der bisherigen Verwaltungspraxis nur unter den Einschränkungen gestattet hat, daß Grundrechtseingriffe zur Aufrechterhaltung staatlicher Funktionen unerläßlich sind (BVerfGE 41 S. 251). Eine Stellungnahme hierzu liegt mir noch nicht vor, es bleibt jedoch zu hoffen, daß mein wiederholtes Eintreten für eine restriktive Handhabung Erfolg hat.

Gleichfalls immer noch nicht abgeschlossen ist die Novellierung der Bestimmungen über das Schuldnerverzeichnis. Auch über die damit zusammenhängende Problematik habe ich bereits mehrfach berichtet (vgl. zuletzt meinen 9. TB, Tz. 2.4, S. 40). In das von den Amtsgerichten geführte Schuldnerverzeichnis werden Personen eingetragen, die auf Betreiben ihrer Gläubiger die eidesstattliche Versicherung über ihr Vermögen abgegeben haben (sog. Offenbarungseid) oder gegen die wegen Nichtabgabe der eidesstattlichen Versicherung oder aus anderen privatrechtlichen Gründen Haftvollstreckung angeordnet ist. Da durch die jedermann gestattete Einsichtnahme und die Erteilung von Abschriften und Auszügen an die verschiedensten Institutionen und Privatpersonen Informationen aus dem Schuldnerverzeichnis weitergegeben werden, bedarf es einer dies regelnden gesetzlichen Bestimmung. Die "Allgemeinen Vorschriften über die Erteilung von Abschriften und Auszügen aus dem Schuldnerverzeichnis" genügen als Verwaltungsvorschrift nicht den Anforderungen.

Regelungsbedarf besteht für den Gesetzgeber auch im Bereich des Strafvollzugs. Die Informationsverarbeitung in den Justizvollzugsanstalten, insbesondere die Weitergabe von Informationen über Strafgefangene an andere Stellen bedürfen einer hinreichenden gesetzlichen Grundlage; das Strafvollzugsgesetz ist fortschreibungsbedürftig (vgl. hierzu bereits meinen 8. TB, Tz. 3.3, S. 55).

Bereits in meinem letzten Tätigkeitsbericht habe ich über die Bemühungen berichtet, den Strafverfolgungsbehörden eine rechtstaatlich einwandfreie Grundlage für ihre Arbeit zu geben (vgl. meinen 11. TB, Tz. 5.1, S. 54). Die Bedeutung des Entwurfs zum Strafverfahrensänderungsgesetz aus dem Jahre 1989 kann gar nicht unterschätzt werden; er betrifft einen Kernbereich der Rechtspflege, in dem sich der Mangel normenklarer, gesetzlicher Befugnisse besonders nachteilig auswirken muß. Die Tatsache, daß der Entwurf nicht einmal zur parlamentarischen Beratung gelangte und mithin ausreichende gesetzliche Grundlagen in einigen Bereichen der Informationsverarbeitung für Strafverfolgungszwecke fehlen, wirft schwerwiegende Fragen auf. Der Ablauf der letzten Legislaturperiode des Bundestages markiert einen Zeitpunkt, der die Übergangszeit beenden könnte, die das Bundesverfassungsgericht dem Gesetzgeber bis zur Inkraftsetzung verfassungsmäßiger Rechtsgrundlagen setzt (vgl. Vorbemerkung zu meinem 10. TB S. 2 ff). Es ist nicht auszuschließen, daß die Gerichte mehr und mehr Maßnahmen der Strafverfolgungsbehörden für rechtswidrig erklären, weil die erforderlichen gesetzlichen Grundlagen fehlen.

#### 4.2 Gesetz zur Bekämpfung des illegalen Rauschgift-handels und der organisierten Kriminalität (OrgKG)

Dieser Gesetzesentwurf, den der Bundesrat auf Initiative der Länder Bayern und Baden-Württemberg in das Gesetzgebungsverfahren eingebracht hatte, war insbesondere darauf ausgerichtet, bestimmte Ermittlungsmethoden wie den Einsatz verdeckter Ermittler und technischer Observationsmittel (z.B. Abhörgeräte und Richtmikrofone) sowie die Durchführung von polizeilicher Beobachtung und Rasterfahndung gesetzlich abzusichern. Es wird nicht verkannt, daß bestimmte Erscheinungsformen der Kriminalität im Interesse des Schutzes der Bürger besondere Fahndungsmethoden erfor-

dern. Darauf hat sich der Entwurf jedoch nicht beschränkt.

Im Gegensatz zu den Arbeitsentwürfen des Bundesjustizministers für eine umfassende Novellierung des Strafverfahrensrechts knüpft der Bundesratsentwurf die Eingriffsbefugnisse an zu weit gefaßte Voraussetzungen, die die tiefgreifenden Fahndungsmaßnahmen nicht nur zu Ermittlungen gegen den illegalen Rauschgifthandel und die sog. "organisierte Kriminalität" erlauben und teilweise mit Sicherheit nur die Klein- und Bagatellkriminalität von der Anwendung ausschließen. Zu niedrig war die Schranke für den Einsatz technischer Mittel gegenüber dem an sich Unverdächtigen, sollte er in das Fadenkreuz polizeilicher Überwachungstechnik geraten. Der Anwendungsbereich für Telefonabhörmaßnahmen wurde gegenüber dem geltenden Recht erweitert. Das Richterprivileg für die Anordnung technischer Überwachungsmaßnahmen war zugunsten der Eilkompetenz der Strafverfolgungsbehörden vernachlässigt, nicht einmal die nachträgliche, richterliche Kontrolle war in solchen Fällen zwingend vorgesehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer EntschlieÙung vom 4./5. Oktober 1990 auf die Gefährdungen des informationellen Selbstbestimmungsrechts durch Einschränkungen des Fernmeldegeheimnisses auch im Hinblick auf die Fortentwicklung der Telekommunikation hingewiesen und einschränkende gesetzliche Regelungen gefordert (Anlage 7).

So wünschenswert und notwendig eine umfassende Novellierung der Strafprozeßordnung ist (vgl. Tz. 4.1), so problematisch waren die im OrgKG vorgesehenen Regelungen von Teilaspekten der Materie. Dabei kamen die Rechte Betroffener zu kurz. Die mit besonderen Ermittlungsmethoden für bestimmte Strafverfolgungszwecke erhobenen Daten durften für zu weitgehende andere Zwecke verwendet werden. Es fehlten ausreichende Be-

stimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Der Entwurf forderte Kritik heraus. Selbst die Bundesregierung mußte in ihrer Stellungnahme darauf hinweisen, "daß einzelne Vorschläge unter verfassungsrechtlichen und datenschutzrechtlichen Gesichtspunkten nicht unproblematisch erscheinen und näherer Prüfung bedürfen" (Bt-Drucksache 11/7663, S. 52). Der Entwurf fiel der Diskontinuität des Parlaments anheim.

#### 4.3 Zentraldatei der Staatsanwaltschaft

Im Berichtszeitraum wurde die Zentraldatei der Staatsanwaltschaft Saarbrücken überprüft. Bei dieser Datei handelt es sich um ein zentrales Aktennachweissystem, in dem gegliedert in ein Js-Register (Verfahren gegen namentlich bekannte Beschuldigte) und ein UJs-Register (Verfahren gegen unbekannte Straftäter) personenbezogene Informationen von Beschuldigten und Geschädigten gespeichert werden. Seit Anfang 1987 wird die Zentraldatei in Form eines EDV-Verfahrens betrieben. Die Staatsanwaltschaft bedient sich seither bei der Neuaufnahme, der Fortschreibung, der Abfrage und dem Ausdruck der Registerdaten installierter Terminals und Druckeinrichtungen, die mit der Großanlage der ZDV-Saar durch Standleitung verbunden sind. Die Prüfung des Verfahrens gab Anlaß zu Beanstandungen.

Ich habe insbesondere gerügt, daß die Speicherung der dem Beschuldigten vorgeworfenen Tat nach Strafvorwurfsgruppen erfolgt, in denen bestimmte Delikte zusammengefaßt sind. Aus der Speicherung selbst wird somit nicht ersichtlich, welche konkrete Straftat dem Beschuldigten vorgeworfen wird. In den Strafvorwurfsgruppen sind eine Vielzahl von Straftaten mit ganz unterschiedlichem Unrechtsgewicht gebündelt. Beispielsweise werden Vollrauschdelikte und unterlassene Hilfeleistung oder als weitere Gruppe Hochverrat,

Verbreiten von Propagandamitteln verfassungswidriger Organisationen, Verunglimpfung von Verfassungsorganen und Wehrpflichtentziehung unter derselben Kennzahl zusammengefaßt. Daraus kann sich ein völlig unzutreffendes Persönlichkeitsbild ergeben, das für sich gesehen schon einen schwerwiegenden Grundrechtseingriff darstellt. Dies ist um so problematischer, als die Zentraldatei nicht nur eine für den internen Gebrauch der Staatsanwaltschaft bestimmte Datensammlung ist, sondern Auskünfte und Mitteilungen aus dieser Datei auch an andere Stellen - beispielsweise an den Sozialen Dienst oder an Bewährungshelfer - gehen.

Warum die Staatsanwaltschaft trotz dieser verfassungsrechtlichen Bedenken und meiner nachdrücklichen Forderungen an der Speicherung von Strafvorwurfsgruppen festhält, ist mir nicht ersichtlich. Es wäre ohne nennenswerten Mehraufwand möglich, statt der Speicherung der Kennziffer für eine Strafvorwurfsgruppe von vornherein die konkrete Strafbestimmung zu speichern. Da das Ergebnis des Ermittlungs-/Strafverfahrens ebenfalls gespeichert wird, könnte, soweit sich der Strafvorwurf geändert hat, spätestens bei diesem Arbeitsgang ohne weiteres die beim Ausgang des Verfahrens zutreffende Strafbestimmung gespeichert werden. Hiermit wäre nur ein äußerst geringer Mehraufwand verbunden.

Belastend für den Betroffenen können bestimmte Änderungen der gespeicherten Daten sein. Etwa die Zusammenlegung von Personendatensätzen kann zur Folge haben, daß einem Täter verschiedene Taten, die bisher getrennt gespeichert waren, zugeordnet werden. Zu Recht sieht das Handbuch in solchen Fällen die Protokollierung solcher Bestandsänderungen vor, um eine Kontrolle zu gewährleisten. Das Korrekturprotokoll soll dem Leiter der Zentraldatei vorgelegt werden. Diese Maßnahme zur Verhinderung schwerwiegender Mängel war bislang nicht verwirklicht, obwohl seit Realisie-

rung des EDV-Verfahrens bereits mehr als drei Jahre vergangen waren. Erst auf meine Beanstandung hin hat die Staatsanwaltschaft mit dem nötigen Nachdruck dafür gesorgt, daß der Programmteil "Protokollierung" in die Praxis umgesetzt wurde.

Bei der Prüfung vor Ort hat sich im übrigen gezeigt, daß neben dem EDV-Verfahren ein umfassendes manuelles Karteikartensystem für die bis zum Beginn des Jahres 1987 angefallenen Aktenvorgänge geführt wird. Die einzelnen Karteikarten enthalten hierbei, da eine systematische Aussonderung nicht stattfindet, zum Teil Hinweise auf Straftaten, die mehrere Jahrzehnte zurückliegen. In vielen Fällen sind die zu den Karteikarten gehörenden Akten bereits vernichtet. In anderen Fällen ist mangels systematischer Aussonderung nicht auszuschließen, daß Akten noch vorhanden sind, obwohl die nach den Aufbewahrungsbestimmungen vorgegebenen Fristen bereits abgelaufen sind. Auf entsprechende Fragen haben die Bediensteten der Staatsanwaltschaft erklärt, daß eine systematische Aussonderung von Karteikarten und Aktenmaterial an der fehlenden Personalkapazität scheitere. Auf entsprechende Vorhaltungen in meinem Prüfbericht hat der Leitende Oberstaatsanwalt erklärt, daß eine "permanente Aussonderung" erfolge. Wörtlich hat er mitgeteilt: "Daß es in diesem Bereich aufgrund personeller Engpässe zu Stockungen und Verzögerungen kommen kann, ist richtig, läßt sich indes nicht völlig ausschließen, weil mit den vorhandenen Mitteln der Geschäftsbetrieb insgesamt aufrecht zu erhalten ist. Dazu ist es auch erforderlich, Prioritäten zu setzen." Abgesehen davon hat er die Auffassung vertreten, daß es sich bei dem manuellen Karteikartensystem, jedenfalls soweit es zur Aussonderung vorgesehen ist, um eine interne Datei handele, im Ergebnis also um einen Datenbestand, der nach den datenschutzrechtlichen Bestimmungen zulässig sei.

Die Behandlung der Altfälle durch die Staatsanwaltschaft und die in der Stellungnahme vertretene Rechtsauffassung läßt die völlige Verkennung verfassungsrechtlicher Anforderungen deutlich werden. Nach der Rechtsprechung des Bundesverfassungsgerichts stellt jede Form personenbezogener Datenverarbeitung durch öffentliche Stellen einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Sind vorhandene Datenbestände zur Aufgabenerfüllung der öffentlichen Stelle nicht mehr erforderlich, was bei einem Großteil der alten Datenbestände der Fall sein dürfte, hat demzufolge eine unverzügliche Aussonderung stattzufinden. Eine weitere Aufbewahrung des Datenmaterials würde in nicht gerechtfertigter Weise in Grundrechtspositionen der betroffenen Bürger eingreifen.

Nach einer Entscheidung des Oberlandesgerichts Frankfurt entbehrt die Datenverarbeitung der Staatsanwaltschaft ohnehin der notwendigen gesetzliche Grundlage. Zwar können unerläßliche Datenverarbeitungsmaßnahmen für eine Übergangszeit auch ohne gesetzliche Legitimation hingenommen werden, das Oberlandesgericht hat aber für die zentralen Namensdateien der Staatsanwaltschaft festgestellt, daß diese Übergangszeit mit Ablauf der Legislaturperiode des Bundestages, also im Dezember 1990, endet (vgl. OLG Frankfurt NJW 1989, S. 47). Vor diesem Hintergrund erscheint es um so dringlicher, daß die Staatsanwaltschaft in der Übergangszeit bis zur Verabschiedung verfassungsmäßiger Rechtsgrundlagen personenbezogene Informationen in einer Weise verarbeitet, daß der Betroffene möglichst wenig belastet wird (Prinzip des geringsten Eingriffs).

#### 4.4 Beeinträchtigung schutzwürdiger Belange der Betroffenen durch justitielle Vorgänge

Mich erreichten Eingaben von Bürgern, die sich über diskriminierende Niederlegungen in behördlichen Akten

beschwerten. Änderungen des Akteninhalts sind äußerst schwierig zu erreichen. Ist etwas "schwarz auf weiß" in einer Akte vermerkt, macht es, auch wenn der Akteninhalt nachweislich unrichtig oder subjektiv überzogen bewertet ist, erhebliche Schwierigkeiten, die öffentliche Stelle zu einer Entfernung oder Unkenntlichmachung des entsprechenden Aktenblattes zu bewegen. Auf zwei besonders diskriminierende Aktenvermerke möchte ich exemplarisch eingehen.

#### 4.4.1 Diskriminierender Aktenvermerk in einer Pflugschaftssache

Für eine ältere Dame, die infolge körperlicher Gebrechen nicht mehr in der Lage war, Ihre Angelegenheiten selbst zu besorgen, war mit ihrer Einwilligung eine Gebrechlichkeitspflugschaft angeordnet worden. Der für sie tätige Pfluger wollte ebenfalls mit ihrem Einverständnis das in ihrem Eigentum stehende Hausgrundstück veräußern. Nach Abschluß des notariellen Kaufvertrages mußte die Zustimmung des zuständigen Rechtspflegers eingeholt werden. Die Beteiligung eines Rechtspflegers bei solchen Geschäften ist gesetzlich vorgesehen, um zu verhindern, daß im Rahmen einer Pflugschaft mißbräuchlich über Vermögensgegenstände der unter Pflugschaft stehenden Person verfügt wird. Der zuständige Rechtspfleger beim Amtsgericht nahm seine Aufgabe etwas zu ernst. Zwar obliegt es dem Rechtspfleger, Erkundigungen darüber anzustellen, ob die Gegenleistung für das verkaufte Grundstück erbracht wird. Im vorliegende Fall verstieg sich der Rechtspfleger jedoch dazu, sensible personenbezogene Informationen über die Käuferin des Grundstückes einzuziehen und diese aktenkundig zu machen. Durch einen Zufall wurde dies der Käuferin des Grundstückes bekannt und sie beklagte sich bei meiner Dienststelle über einen sie diskriminierenden Aktenvermerk. In diesem Aktenvermerk wurden telefonisch eingeholte Informationen aus dem Umfeld der Käuferin niedergelegt. Hierbei wurde der

Sozialamtsleiter der Heimatgemeinde der Käuferin wie folgt zitiert: "Frau H. sei kurze Zeit in dem von ihm beaufsichtigten Altenheim als Putzfrau beschäftigt gewesen. Danach habe sie eine zeitlang Sozialhilfe bezogen. Deren Kinder seien irgendwie APO-Mitglieder, jedenfalls nichts anständiges."

Es liegt auf der Hand, daß eine solche Information für die Mitwirkung des Rechtspflegers im Rahmen des Grundstücksgeschäftes völlig unerheblich ist. Jeder Bürger hat aber Anspruch darauf, daß öffentliche Stellen nur solche Informationen über seine Person festhalten, die zur Aufgabenerfüllung erforderlich sind. Ich habe daher die unverzügliche Entfernung des diskriminierenden Aktenvermerkes gefordert. Letztlich ist das Amtsgericht meiner Forderung durch Schwärzung der fraglichen Stellen nachgekommen.

#### 4.4.2 Einstellungsverfügung der Staatsanwaltschaft

Eine Petentin, die von der Staatsanwaltschaft Saarbrücken als Zeugin vernommen wurde, hat sich bei mir über die diskriminierende Protokollierung ihrer Vernehmung beschwert. Der zuständige Staatsanwalt hat über die Vernehmung folgenden Vermerk aufgenommen:

"Vorgeladen erscheint Frau S. Die "Anzeige" sollte inhaltlich mit ihr durchgesprochen werden. Dies war im Hinblick auf ihren krankhaft ausgeprägten rechthaberischen Starrsinn jedoch nicht möglich. Sie vermittelte den Eindruck einer Persönlichkeit mit einer schweren psychischen Störung. Beweise sind mit ihrer Bekundung nicht zu führen."

Ich habe der Staatsanwaltschaft im Rahmen meiner rechtlichen Bewertung des Vorgangs selbstverständlich nicht die Entscheidungskompetenz abgesprochen, eine Bewertung von Zeugenaussage und Persönlichkeit des Zeugen vorzunehmen. Andererseits halte ich die Feststellung eines "krankhaft ausgeprägten rechthaberischen

schen Starrsinns" in Verknüpfung mit dem "Eindruck einer Persönlichkeit mit einer schweren psychischen Störung" ohne nähere, kompetente, medizinische Begründung wegen eines Eingriffs in das informationelle Selbstbestimmungsrecht des Betroffenen für unzulässig. Die Staatsanwaltschaft verwies darauf, daß es das selbstverständliche Recht des sachbearbeitenden Staatsanwalts sei, ein Urteil über die Glaubwürdigkeit des Zeugen, welches unter Umständen negativ oder sogar hart ausfallen könne, zu den Akten zu nehmen. Diese Stellungnahme verkennt, daß es nicht um die Tatsache einer negativen Bewertung der Zeugenaussage geht, sondern darum, daß der diskriminierende Vermerk in tatsächlicher Hinsicht Behauptungen und Bewertungen vornimmt, für die der bearbeitende Staatsanwalt keine Fachkompetenz haben kann. Die Beurteilung der Glaubwürdigkeit einer Person setzt nicht notwendigerweise eine Bewertung der Persönlichkeit voraus, die eine tiefgreifende soziale Abwertung zur Folge hat.

#### 4.5 Telefonabhördaten

In meinem letzten Tätigkeitsbericht (vgl. 11. TB, Tz. 5.3) habe ich über eine Telefonabhöraktion der Staatsanwaltschaft berichtet. Neben anderen Punkten habe ich vor allem gerügt, daß die gesetzlich vorgeschriebene Benachrichtigung der beteiligten abgehörten Personen nicht erfolgt ist sobald dies ohne Gefährdung des Untersuchungszwecks geschehen kann (§ 101 Abs. 1 StPO). Regelmäßig hat daher eine Benachrichtigung stattzufinden, wenn die Abhörmaßnahme beendet ist und - wie im vorliegenden Fall - keinerlei strafprozessual verwertbare Erkenntnisse gebracht hat.

Die Staatsanwaltschaft glaubt ihrer gesetzlichen Benachrichtigungspflicht damit Genüge zu tun, daß sie den überwachten Anschlußinhaber und den Beschuldigten über die Abhörmaßnahme benachrichtigt. Unabhängig von dem zugrundeliegenden Fall, in dem eine Benachrichti-

gung von Gesprächsteilnehmern ohnehin nicht mehr möglich war, weil die entsprechenden Unterlagen vernichtet wurden, habe ich dieser Interpretation der einschlägigen gesetzlichen Grundlage widersprochen. Da Telefonabhörmaßnahmen einen besonders tiefen Eingriff in die Privatsphäre der Beteiligten darstellen, erfordert eine verfassungskonforme Auslegung des Gesetzes die Benachrichtigung aller identifizierten oder mühelos identifizierbaren Gesprächsteilnehmer. Ich habe daher gefordert, daß bei zukünftigen Abhörmaßnahmen entsprechend verfahren wird.

Eine Umfrage des Generalstaatsanwaltes bei den übrigen Staatsanwaltschaften im Bundesgebiet hat ergeben, daß auch diese regelmäßig nur die AnschluBINhaber und Beschuldigten über die Abhörmaßnahme benachrichtigen. Aufgrund dieser Praxis hat sich der Justizminister außerstande gesehen, die Staatsanwaltschaft zu einer umfassenden Benachrichtigung anzuweisen. Er hat lediglich Bereitschaft gezeigt, angesichts sich widersprechender Auffassungen in der Kommentarliteratur zu dieser Frage eine Erörterung der Problematik im Rahmen der Justizministerkonferenz anzuregen mit dem Ziel, zu einer übereinstimmenden Auffassung der Landesjustizverwaltungen und zu einer verbindlichen Auslegungsrichtlinie zu kommen. Ich halte diese Vorgehensweise im Hinblick auf die grundrechtliche Ausgestaltung des Rechts auf informationelle Selbstbestimmung und den besonders tiefgehenden Eingriff einer Telefonabhörmaßnahme für völlig unbefriedigend. Bereits der Gesetzeswortlaut legt meines Erachtens den zu benachrichtigenden Personenkreis abschließend fest und ist deshalb nicht interpretationsfähig. Zu unterrichten sind die "Beteiligten" des Telefongespräches, also alle identifizierbaren Personen, die an dem Telefongespräch "beteiligt" waren.

## 5. Melderecht

### 5.1 Nach wie vor: Novellierungsbedarf für melderechtl liche Bestimmungen

Auf die Novellierungsbedürftigkeit der melderechtl  
ichen Bestimmungen habe ich bereits in meinem 7. Tätig  
keitsbericht (Tz. 4.1 und 4.2) hingewiesen. Auch der  
Landtag des Saarlandes hat in einer EntschlieÙung zu  
diesem Tätigkeitsbericht die Änderung des Melderechts  
in bestimmten Punkten für erforderlich gehalten (Aus  
schuß für Innere Verwaltung - Lt-Drucksache 9/1850  
(9/468) Tz. 4)).

Verfassungsrechtlich problematisch ist vor allem die  
Hotel- und Krankenhausmeldepflicht. Das Melderechts  
rahmengesetz des Bundes und ihm folgend das Meldege  
setz des Landes verpflichtet den Bürger bereits bei  
einem kurzfristigen Hotelaufenthalt, einen Meldevor  
druck auszufüllen und zu unterschreiben, der für die  
Polizei und Meldebehörde zur Einsichtnahme bereitzu  
halten ist. Bei der Aufnahme in Krankenanstalten sind  
die Patienten verpflichtet, die "erforderlichen Anga  
ben" zur Person zu machen; diese Angaben sind in ein  
Verzeichnis aufzunehmen und für die Einsichtnahme  
durch die Polizei und Meldebehörde bereitzuhalten.

Durch die Hotel- und Krankenhausmeldepflicht wird eine  
rein vorsorgliche Polizeikontrolle aufgrund von Melde  
daten ermöglicht, ohne daß tatsächliche Anhaltspunkte  
für eine konkrete Gefahr oder eine aufzuklärende  
Straftat gegeben sind. Eine solch umfassende Regi  
strierung personenbezogener Daten verstößt, jedenfalls  
wenn jeglicher konkreter Anhalt für ein polizeiliches  
Einschreiten fehlt, gegen das Verfassungsprinzip der  
Verhältnismäßigkeit. Die Tatsache des Krankenhausauf  
enthalts unterliegt überdies grundsätzlich der ärztli  
chen Schweigepflicht, die nur bei Gefahr für hohe  
Rechtsgüter durchbrochen werden darf.

Zu dem in der abgelaufenen Legislaturperiode des Deutschen Bundestages eingebrachten Gesetzentwurf zur Änderung des Melderechtsrahmengesetzes hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung vom 4./5. Oktober 1990 geäuÙert (Anlage 5). Die Gelegenheit, die Hotel- und Krankenhausmeldepflicht abzuschaffen, wurde jedoch nicht genutzt. Leider lieÙen sich für eine solche Änderung keine parlamentarischen Mehrheiten finden. Entsprechende Vorstöße durch parlamentarische Minderheiten führten dazu, daÙ eine abschließende Beratung des Gesetzentwurfes nicht mehr möglich war und damit die Vorlage der Diskontinuität des Parlaments anheimfiel. Dies ist um so bedauerlicher, als damit auch für den Landesgesetzgeber wegen der verbindlichen, rahmengesetzlichen Vorgaben die Möglichkeit genommen ist, die Hotel- und Krankenhausmeldepflicht außer Kraft zu setzen.

Gleichwohl dürfen die auch vom Ausschuß für Innere Verwaltung für notwendig gehaltenen Änderungen des Landesmelderechts nicht in Vergessenheit geraten (vgl. Ausschuß für Innere Verwaltung a.a.O.).

#### 5.2 Mangelhafte Datensicherung beim Transport von Meldeunterlagen

Durch Presseberichte wurde ich auf einen Fall aufmerksam, der wieder einmal exemplarisch die Nachlässigkeit öffentlicher Stellen im Umgang mit personenbezogenen Unterlagen offenbart. Vom Einwohnermeldeamt der Landeshauptstadt sollten aussortierte Meldeunterlagen zur Ablagerung in ein anderes städtisches Gebäude gebracht werden. Da sich der Abtransport verzögerte, wurden die Unterlagen vorübergehend im Eingangsbereich und auf dem Bürgersteig vor dem Gebäude deponiert. Vorbeigehende Bürger machten die Presse und meine Dienststelle darauf aufmerksam, daÙ vier große Schubladen,

gefüllt mit Karteikarten im öffentlichen Straßenraum standen und lediglich durch einen aufgelegten Aktenschrank und teilweise Verpackung gesichert waren. Im Eingangsflur des Amtes standen weitere Kästen mit Unterlagen. Für Passanten wäre es ohne weiteres möglich gewesen, Einblick in personenbezogene Unterlagen zu nehmen oder Karteibestände zu entfernen.

Auf meine Nachfrage teilte der zuständige Dezernent der Landeshauptstadt mit, daß der zur Aufsicht bestellte Bedienstete "kurzfristig" zu anderen Aufgaben abberufen worden sei. Das Versäumnis ausreichender Datensicherung hat die Landeshauptstadt eingeräumt und bedauert. Auf meine unverzügliche Intervention wurden die Datenbestände gesichert.

### 5.3 Bruch des Wahl- und Meldegeheimnisses

Parteien, die bisher nicht im Bundestag vertreten sind, müssen beim Landeswahlleiter oder Kreiswahlleiter Unterstützungsunterschriften einer gewissen Anzahl von Wahlberechtigten auf Formblättern vorlegen. Zur Bescheinigung des Wahlrechts wird das Unterstützungsblatt zunächst bei der Wohnortgemeinde des Unterschriftsleistenden eingereicht. Da ein Wahlberechtigter nur eine Partei unterstützen darf, sehen die wahlrechtlichen Bestimmungen vor, daß die zuständige Gemeindebehörde für jeden Wahlberechtigten diese Bescheinigung nur einmal erteilen darf. Um die Kontrolle zu gewährleisten, führen die Gemeinden ein Protokoll. Die Aufzeichnungen müssen sich jedoch auf das beschränken, was zur Feststellung der Identität desjenigen, der eine Unterstützungsunterschrift geleistet hat, unbedingt erforderlich ist. Namen, Anschrift und Geburtsdatum reichen zu diesem Zweck völlig aus.

Eine stichprobenartige Überprüfung von 15 Gemeinden hat jedoch ergeben, daß in mehreren Fällen Verfahrensweisen gewählt wurden, die datenschutzrechtlich nicht

zulässig sind. Zum Teil wurden die Unterstützungsblätter komplett fotokopiert und in Ordnern sortiert aufbewahrt. In anderen Gemeinden wurde eine Liste mit Namen, Anschriften, Geburtsdaten des Unterstützers sowie des unterstützten Wahlvorschlags geführt. Im nachhinein war in diesen Fällen ohne weiteres feststellbar, welcher Wahlberechtigte welche Partei unterstützt hat.

In einer anderen Gemeinde hat die Meldebehörde dem Datensatz des Wahlberechtigten im automatisierten Einwohnermelderegister einen "Merker" beigefügt, wenn ein Wahlberechtigter eine Unterstützungsunterschrift geleistet hatte. Eine solche Verfahrensweise ist unzulässig, da das Meldegesetz die Daten, die gespeichert werden dürfen, abschließend festlegt; Hinweise dieser Art sind jedoch in dieser Aufzählung nicht enthalten. Durch die Speicherung des "Merkers" im automatisierten Einwohnermeldebestand wird die Zweckbindung der Daten unterlaufen, da bei jeder Abfrage der Person - gleich aus welchem Grund - auch die Tatsache der Unterstützungsunterschrift ersichtlich wird. Allein die Tatsache, daß ein Bürger eine bisher im Bundestag nicht vertretene Gruppierung unterstützt, ist jedoch schützenswert, wenn dem Demokratiegedanken ausreichend Rechnung getragen werden soll.

Ich habe die unzulässige Handhabung des wahlrechtlichen Unterstützungsverfahrens bei den betroffenen Gemeinden beanstandet. Darüberhinaus habe ich den Landeswahlleiter und den Minister des Innern als die für das Meldewesen zuständige oberste Landesbehörde über die festgestellten datenschutzrechtlichen Verstöße informiert. Ich habe gefordert, daß sämtliche Gemeinden im Erlaßwege zu einer verfassungsrechtlich einwandfreien Handhabung des Unterstützungsverfahrens angewiesen werden. Insbesondere hielt ich es für notwendig, daß angesichts der unmittelbar bevorstehenden Wahl Anweisungen über die Löschung der Aufzeichnungen

getroffen werden. Nach endgültiger Zulassung einer Partei zur Bundestagswahl werden diese Unterlagen nicht mehr benötigt.

Im Erlaßwege wurde geregelt, daß die Aufzeichnungen auf den notwendigen Umfang beschränkt, die "Merker" im automatisierten Bestand unverzüglich und die Protokollierungen insgesamt spätestens am 10. November 1990 gelöscht werden.

Um so bedauerlicher ist es, daß ich bei einer erneuten Überprüfung in vier Gemeinden am 18. Dezember 1990 - also fast 6 Wochen nach dem festgesetzten Löschungstermin - feststellen mußte, daß in zwei Gemeinden immer noch listenmäßige Aufzeichnungen - in einem Fall sogar jeweils mit der Bezeichnung der unterstützten Gruppierung - vorhanden und in einem weiteren Fall Hinweise auf die Unterstützung in Form eines "Merkers" im automatisierten Bestand gespeichert waren. Erschwerend fällt ins Gewicht, daß trotz der Beanstandung durch meine Dienststelle und der strikten Anweisungen der Aufsichtsbehörde das Grundrecht auf informationelle Selbstbestimmung im Zusammenhang mit der Ausübung des Wahlrechts nicht beachtet wurde.

#### 5.4 Nochmals: Die gebührenpflichtige Übermittlungssperre

Der Bürger hat in bestimmten Fällen gegenüber der Meldebehörde ein Recht auf Sperrung seiner Daten, das er durch einfachen, die Behörde bindenden Widerspruch geltend machen kann. Wer die Weitergabe seiner Daten an die Kirche seines konfessionsverschiedenen Ehepartners oder an Adreßbuchverlage nicht wünscht, im Falle von Alters- und Ehejubiläen auf offizielle Ehrungen keinen Wert legt oder gar wegen Gefahr für Leib oder Leben die Übermittlung seiner Meldedaten unterbinden will, muß von diesem seinem Recht Gebrauch machen können, ohne daß es all zu große Hürden zu überwinden

gilt. Der Bürger ist zu Angaben gegenüber der Meldebehörde in nicht geringem Umfang verpflichtet. Er darf nicht Gefahr laufen, daß in unverhältnismäßig großem Umfang seine Daten anderen Stellen zur Verfügung stehen. Für die Eintragung der Übermittlungs- oder Auskunftssperre wurden allerdings bisher Gebühren erhoben. Dagegen habe ich mich schon 1986 mit aller Entschiedenheit ausgesprochen (vgl. meinen 8. TB, Tz. 12).

Nunmehr hat das Oberverwaltungsgericht des Saarlandes meine Auffassung bestätigt und die entsprechende Gebührenstelle für nichtig erachtet. Dies wird damit begründet, daß die Amtshandlung nicht dem überwiegenden Interesse eines Einzelnen diene. Durch die Eintragung werde lediglich der Grundsatz der Gesetzmäßigkeit der Verwaltung gewahrt, indem durch eine rein behördeninterne Maßnahme die Beachtung der Sperre sichergestellt werde. Ich gehe davon aus, daß nunmehr eine Änderung des allgemeinen Gebührenverzeichnisses erfolgt.

## 6. Gesundheit

### 6.1 Krankenhaus

Die Verarbeitung von Patientendaten in einem Krankenhaus habe ich überprüft. Ich sehe mich zu einer Reihe von Beanstandungen veranlaßt, die jedenfalls in ihrer Summe eine beachtliche Beeinträchtigung schutzwürdiger Belange der Patienten darstellen. Die Wahrung des Arztgeheimnisses und die Respektierung des informationellen Selbstbestimmungsrechts in diesem von den unterschiedlichsten Datenanforderungen geprägten Bereich kann nur gelingen, wenn die Datenschutzvorschriften in jeder Hinsicht sorgfältig beachtet werden. Die Überprüfung des Krankenhauses sollte überdies dazu beitragen, die Umsetzung der neuen, datenschutzrechtlichen Regelungen des Saarländischen Krankenhausgesetzes (SKHG) in der Praxis voranzubringen.

#### - Organisation

Das Krankenhaus bildet keine Informationseinheit. Die im Krankenhaus Beschäftigten dürfen Patientendaten nur für den zur jeweiligen Aufgabenerfüllung gehörenden Behandlungszweck einsehen oder sonst nutzen. Von besonderer Bedeutung für die Abgrenzung der Datenverarbeitungsbefugnisse des Krankenhauspersonals ist der Geschäftsverteilungsplan, der deshalb ständig zu aktualisieren ist.

Ich habe den Mangel einer Dienstanweisung gerügt; die Verarbeitung der Patientendaten ist im einzelnen zu regeln. Die vielfach zu abstrakten Vorschriften des SKHG bedürfen dringend der Konkretisierung, um dem Krankenhauspersonal verständliche und praktikable Handlungsanweisungen zu geben und damit der Gefahr von Datenschutzverstößen in der täglichen Krankenhauspraxis wirksam zu begegnen. Beeinträchtigungen werden zwar nur selten bekannt. Da den Krankenhauspatienten

in erster Linie jedoch andere Sorgen bedrücken, neigt er dazu, Informationsverarbeitungsvorgänge auch dann hinzunehmen, wenn sie eine Beeinträchtigung für ihn darstellen. Wie ich aus eigener Erfahrung weiß, wird diese Einstellung gelegentlich noch durch den freundlichen Hinweis seitens des Krankenhauspersonals gefördert, daß es doch wohl vor allem darauf ankomme, daß "alles andere gut läuft". Nicht zuletzt bleiben die meisten Vorgänge dem Patienten verborgen, der bei fortschreitender Automation schon längst jede Vorstellung von den Verfahrensabläufen und Verwendungszusammenhängen verloren hat.

Eine Dienstanweisung, die ich gefordert habe, sollte Regelungen enthalten über den zulässigen Umfang der Datenerhebung insbesondere bei der Patientenaufnahme, die Notwendigkeit des Hinweises auf die Freiwilligkeit bei bestimmten Angaben, ferner über die Auskunftserteilung an Personen und Stellen außerhalb des Krankenhauses, die zulässigen Datenübermittlungen innerhalb des Krankenhauses, die Beteiligung des krankenhauses-internen Datenschutzbeauftragten, die Datensicherung sowie über Löschungs- und Aufbewahrungsfristen.

Ich habe festgestellt, daß lediglich die Mitarbeiter des Verwaltungsbereiches, nicht jedoch diejenigen, die Zugriff auf die sensiblen Einzelbefunde im ärztlich-pflegerischen Bereich haben, auf das Datengeheimnis verpflichtet worden sind. Ohne die Förmlichkeit eines solchen Vorgangs überbewerten zu wollen, sollte keine Gelegenheit versäumt werden, jedem Mitarbeiter eines Krankenhauses die Geheimhaltungspflichten bewußt zu machen und seine Sensibilität für den Intimbereich des Patienten zu aktivieren.

Die Pflicht zur Bestellung eines internen Datenschutzbeauftragten hat das Krankenhaus wegen Ausscheidens eines Bediensteten aus dem Arbeitsverhältnis vernachlässigt. Wegen Auflösung des Arbeitsverhältnisses mit

dem bisherigen Stelleninhaber war ein interner Datenschutzbeauftragter jedenfalls zeitweise nicht bestellt. Schwerwiegender als die vorübergehende Vernachlässigung dieser gesetzlichen Verpflichtung war der Mangel einer Übersicht über die im Krankenhaus genutzten Dateien, die der interne Datenschutzbeauftragte des Krankenhauses zu führen hat. Fehlt eine solche, wird die interne und die externe Datenschutzkontrolle wesentlich erschwert.

- Patientenaufnahme durch die Krankenhausverwaltung

Rügen mußte ich den Umfang und die Art der Datenerhebung bei der Aufnahme in das Krankenhaus.

Der Name des "Hausarztes" als mitbehandelnder oder nachbehandelnder Arzt ist erst vor der Entlassung und nicht schon bei der Aufnahme zu dokumentieren. Nur so ist gewährleistet, daß der Patient in Kenntnis der Abschlußdiagnose eine Entscheidung zu treffen in der Lage ist, ob und welchem Arzt seiner Wahl das Ergebnis der Krankenhausbehandlung mitgeteilt werden soll. Wird hingegen der Name des sog. "Hausarztes" bereits bei der Aufnahme in das Krankenhaus erfaßt, ist nicht sichergestellt, daß - entsprechend der Gesetzesvorschrift (§ 29 Abs. 4 Nr. 2 SKHG) - die Offenbarung von Arztdateien in Einklang mit dem Willen des Patienten steht.

Ebensowenig dürfen Namen und Telefonnummer einer zu benachrichtigenden Person ohne Hinweis auf die Freiwilligkeit erhoben werden (§ 29 Abs. 4 Nr. 7 SKHG).

Die Frage nach dem Arbeitgeber des Patienten ist grundsätzlich unzulässig. Diese Angabe ist in der Regel weder zur Durchführung der Behandlung noch zur Leistungsabrechnung, noch zur Erfüllung der klinischen Dokumentationspflicht oder einer gesetzlichen Erhebungs- und Speicherungspflicht, erforderlich (§ 29

Abs. 2 SKHG). Allenfalls in Ausnahmefällen, etwa bei unklaren Versicherungsverhältnissen, darf nach dem Arbeitgeber gefragt werden.

Positiv ist mir aufgefallen, daß die Konfession nur gespeichert und an den Seelsorger weitergegeben wurde, wenn der Patient hierzu schriftlich seine Einwilligung erklärt hat.

Bei der Aufnahme von Patienten war die Vertraulichkeit des gesprochenen Worts nicht ausreichend gewährleistet. In dem Raum, in dem sich die Patienten anmelden, befanden sich zwei Erfassungsterminals, so daß nicht auszuschließen war, daß ein Patient in Gegenwart eines anderen nach seinen persönlichen Daten gefragt wurde. Ich habe darauf gedrängt, durch eine Änderung der Raumaufteilung, gegebenenfalls durch bauliche Maßnahmen, die Vertraulichkeit bei der Datenerhebung sicherzustellen.

Die Krankenhäuser sind verpflichtet (§ 28 Abs. 2 MG), ein Verzeichnis aller aufgenommenen Patienten mit Angaben zu führen, die für Behandlungszwecke nicht erforderlich sind und deshalb ausschließlich zur Einsichtnahme durch die Polizei und die Meldebehörde bereit zu halten sind. Eine Nutzung dieser Daten für andere als Polizeizwecke ist unzulässig. Das Krankenhaus hat eine solche besondere Liste nicht angelegt und auch im übrigen keine Vorsorge dafür getroffen, daß der automatisierte Datenbestand insoweit nur zweckgebunden genutzt werden kann. Es besteht insbesondere auch die Gefahr, daß im Falle eines polizeilichen Einsichtnahmebegehrens Patientenlisten mit weiteren Datenarten, die die Polizei nicht einzusehen berechtigt ist, vorgelegt werden müssen. Ich habe Vorkehrungen angemahnt, die die Zweckbindung der Daten gewährleisten.

- Leistungsabrechnung bei Aufnahme eventuell sozialhilfebedürftiger Patienten

Ist ein Patient nicht versichert, sieht er sich häufig weitgehenden Informationsanforderungen seitens der Krankenhausverwaltung ausgesetzt. In der nicht ganz unberechtigten Sorge, daß der nicht versicherte Patient die anfallenden Krankenhauskosten nicht begleichen kann, werden alle Angaben verlangt, die die Inanspruchnahme des Sozialhilfeträgers begründen können (§ 37 BSHG). Nur zu schnell wird der Patient - wie wir aus Eingaben wissen - nach seinen Einkommens- und Vermögensverhältnissen und denen seiner Angehörigen befragt. Zu einer solch umfassenden Datenerhebung ist das Krankenhaus jedoch grundsätzlich nicht berechtigt. Nicht jeder, der nicht versichert ist, ist auch sozialhilfeberechtigt oder ist gar geneigt, Krankenhausleistungen zu erschwindeln. Nur wenn nach den Umständen des Einzelfalls davon ausgegangen werden muß, daß eine nachträgliche Sachverhaltsaufklärung zur Feststellung des Sozialhilfeanspruchs nicht mehr gelingen wird - etwa weil es sich um eine nichtseßhafte Person handelt -, dürfen die relevanten Informationen erhoben werden.

Diese Sozialdaten dürfen jedoch nur für den Kostenübernahmeantrag beim Sozialamt und keinesfalls in einem anderen Zusammenhang etwa im ärztlich-pflegerischen Bereich genutzt werden. Um die Zweckbindung innerhalb der Krankenhausverwaltung sicherzustellen, sind diese Informationen ausschließlich vom Sozialdienst des Krankenhauses zu erheben und unter Verschluß zu halten. Es ist positiv zu vermerken, daß die Datenerhebung der genannten Art in dem überprüften Krankenhaus bereits ausschließlich durch den Sozialdienst erfolgt. Ich habe jedoch angemahnt, daß die für die Begründung des Sozialhilfeantrags erforderlichen Angaben zu den Einkommens- und Vermögensverhältnissen nicht dem behandelnden Arzt zur Kenntnis gelangen.

- Weitergabe medizinischer Daten an die Krankenhausverwaltung zu Statistikzwecken

An die Krankenhausverwaltung dürfen Patientendaten aus dem ärztlichen Bereich nur weitergegeben werden, soweit dies für die Abwicklung des Behandlungsfalls erforderlich ist (§ 29 Abs. 3 SKHG). Die Verwaltung darf zwar Kenntnis von der Einweisungs- und Entlassungsdiagnose erhalten, da sie diese Angaben für die Abrechnung mit den Kostenträgern benötigt. Darüber hinaus dürfen personenbezogene Einzelbefunde, medizinische Angaben und Nebendiagnosen der Krankenhausverwaltung nicht mitgeteilt werden. Dies gilt insbesondere auch für statistische Erhebungen, die von der Verwaltungsabteilung durchgeführt werden. Der mit der Anonymisierung verbundene Verwaltungsaufwand rechtfertigt nicht die Weitergabe personenbezogener medizinischer Angaben an die Krankenhausverwaltung.

- Datensicherheit

Bemängeln mußte ich die Unterbringung der Krankenakten im Ärztlichen Zentralarchiv. Das Zentralarchiv befindet sich im Untergeschoß des Krankenhauses. Der Raum verfügt über ebenerdig liegende Fenster ohne Schutzgitter. Vorbeigehende können von außen erkennen, welchem Zweck der Raum dient. Die Krankenakten sind damit nicht ausreichend gegen Diebstahl und sonstige Beschädigungen, z.B. Brandstiftung, geschützt. Ich habe die Erstellung eines kriminaltechnischen Gutachtens der Beratungsstelle des Kriminalpolizeiamtes zur Sicherung des Archivraumes empfohlen.

- Automatisierte Datenverarbeitung

Mängel mußte ich in bezug auf die automatisierte Datenverarbeitung feststellen. So war der Zeitraum für den Paßwortwechsel zu lang. Die vom System vorgesehe-

nen Beschränkungen der Zugriffsberechtigung waren nicht in dem notwendigen Umfang genutzt. Gefordert habe ich die Bestellung eines Systemverwalters, der die Verbindung mit dem Rechenzentrum koordiniert und der befugt ist, Kennwörter zu ändern und den Zugriff auf die für die Aufgabenerfüllung des einzelnen Sachbearbeiters unerläßlichen Funktionen zu beschränken.

- Datenlöschung

Alle bei der Aufnahme im automatisierten Verfahren abrufbar erfaßten Patientendaten sind seit Einführung des Systems im Jahre 1987 gespeichert. Hierin liegt ein grober Verstoß; alle Patientendaten, die im computerisierten Direktabruf stehen, müssen unmittelbar nach Abschluß der Behandlung bis auf einen Restdatensatz zur Auffindung der Krankenakten gelöscht werden. Der Gesetzgeber hat damit den besonderen Gefahren automatisierter Datenverarbeitung vorzubeugen gesucht (§ 29 Abs. 5 Satz 2 SKHG).

- Krankenhaussozialdienst

Überprüft habe ich auch den Sozialdienst des Krankenhauses, der nach dem SKHG in jedem Krankenhaus einzurichten ist. Schwerpunkt der Arbeit des Sozialdienstes, die regelmäßig von einem Sozialarbeiter wahrgenommen wird, ist die psychosoziale Beratung, die Hilfestellung bei der Beantragung von Rehabilitationsmaßnahmen und anderer Sozialleistungen und die Alten- und Pflegeheimvermittlung.

Sorgfältig habe ich die Informationsbeziehungen zwischen dem Sozialdienst einerseits und dem ärztlich-pflegerischen sowie dem Verwaltungsbereich andererseits untersucht. Der Sozialdienst darf nur tätig werden, wenn der Patient eine sozialarbeiterische Betreuung wünscht. Um dieses Ziel zu erreichen, ist es jedoch notwendig, daß die Datenerhebung grundsätzlich

beim Betroffenen selbst erfolgt. Nur so ist sichergestellt, daß sich die Aktivitäten des Sozialdienstes in Übereinstimmung mit dem Willen des Betroffenen vollziehen. Lediglich in der Phase der Kontaktaufnahme dürfen dem Sozialdienst Patientendaten aus der Verwaltung und dem medizinisch-pflegerischen Bereich zur Verfügung gestellt werden. Es muß aber streng darauf geachtet werden, daß sich der Umfang der Daten, die von diesen Stellen an den Sozialdienst weitergegeben werden, auf das für die Kontaktaufnahme unbedingt notwendige Maß beschränkt.

Weiter bin ich der Frage nachgegangen, wer Zugriff auf die beim Sozialdienst geführten Akten haben darf. Die Unterlagen dürfen nur dem Sozialarbeiter selbst zur Verfügung stehen. Etwa der Verwaltungsdirektor des Krankenhauses, dessen Dienstaufsicht der Sozialarbeiter untersteht, darf keinen Zugang zu diesen Unterlagen haben. Zwischen Patient und Sozialarbeiter besteht - wie zwischen Arzt und Patient - ein persönliches Vertrauensverhältnis, dessen Verletzung überdies strafbewehrt ist (§ 203 Abs. 1 Nr. 5 StGB). Für eine Offenbarung selbst gegenüber dem Vorgesetzten besteht auch keine Notwendigkeit, weil der Sozialdienst die Beratung des Patienten und die Wahrnehmung seiner Belange gegenüber dem Leistungsträger in Sozial- und Rehabilitationsfragen in eigener Kompetenz durchführt.

In diesem Zusammenhang habe ich darauf hingewiesen, daß bei einem Wechsel des Sozialarbeiters die Unterlagen nur mit Einwilligung der Patienten weitergegeben werden dürfen. Im übrigen sind die Angaben nach Entlassung des Patienten aus dem Krankenhaus zur Aufgabenwahrnehmung nicht mehr erforderlich und sind daher kurzfristig zu löschen.

Die Überprüfung hat im konkreten Fall ergeben, daß der Sozialdienst im wesentlichen den datenschutzrechtlichen Anforderungen Rechnung trägt. Die Darlegung mei-

ner Rechtsauffassung hat vor allem den Zweck, den Sozialdienst im Krankenhaus in seiner Eigenständigkeit zu bestärken. Darauf muß im Interesse der Zweckbindung der bei dem Krankenhausdienst anfallenden Daten besonderer Wert gelegt werden.

- Telefondatenerfassung bei Patienten

Beanstandet habe ich die Verfahrensweise bei der Erfassung von Nebendaten bei Telefonaten von Patienten. Das Krankenhaus hat jedes Telefongespräch zur Gebührenabrechnung mit Datum, Uhrzeit, Zielnummer, Anzahl der Gebühreneinheiten, Gebührenbetrag automatisch registriert. Die Ausdrucke mit diesen Daten werden 10 Jahre lang aufbewahrt, dem Patienten wurde nur der Gesamtbetrag der zu entrichtenden Telefongebühren mitgeteilt.

Die Speicherung der vollständigen Zielnummer verletzt das Fernmeldegeheimnis. Sie ist auch nicht erforderlich, weil eine um die letzten beiden Ziffern verkürzte Erfassung der Zielnummer die Gebührenabrechnung ermöglicht, ohne daß der Angerufene offenbart wird. Der Ausdruck mit den Einzeldaten ist - auch bei verkürzter Zielnummerregistrierung - dem Patienten auszuhängen. Für den Gebühreneinzug durch das Krankenhaus ist die Kenntnis des Gesamtgebührenbetrages ausreichend.

Das überprüfte Krankenhaus hat sich äußerst kooperativ gezeigt; die Erfüllung meiner Forderungen wurde mir zugesagt.

Aus der Überprüfung habe ich den Eindruck gewonnen, daß die Datenschutzvorschriften des SKHG praktikabel sind.

## 6.2 Klinisches Krankheitsregister

Bereits in früheren Tätigkeitsberichten habe ich mich mit der datenschutzrechtlichen Problematik klinik-interner Krankheitsregister befaßt. Das Tumorregister im Landeskrankenhaus war Gegenstand meines 6. Tätigkeitsberichts (Tz. 8.1), über das Tumorregister im Winterbergkrankenhaus habe ich im 10. Tätigkeitsbericht (Tz. 8.1) berichtet.

Bei beiden Registern mußte ich im wesentlichen folgende Defizite feststellen: die mangelhafte Unterrichtung des Patienten vor seiner Speicherung im System, die Nichtbeachtung der Grundsätze der Funktionstrennung bei der automatisierten Datenverarbeitung und das Fehlen von Lösungsfristen für die gespeicherten Daten.

Im Berichtszeitraum habe ich mich noch einmal mit den Verantwortlichen in Verbindung gesetzt und auf eine Lösung dieser Problembereiche gedrängt. Obwohl noch nicht alle Fragen bis in Detail geklärt sind, kann ich schon jetzt eine grundsätzliche Annäherung der Standpunkte konstatieren.

Akzeptiert wird, daß eine Unterrichtung des Patienten nach Abschluß der Behandlung und vor seiner Speicherung im System erfolgen muß. Während mit dem Verantwortlichen in Homburg über die Form der Unterrichtung Einigkeit besteht - es soll, wie von mir gefordert, ein spezielles Merkblatt erarbeitet werden - wird diese Frage mit dem Winterberg-Krankenhaus noch diskutiert.

Das Problem der Funktionstrennung ist beim Tumorregister des Winterberg-Krankenhauses mittlerweile zufriedenstellend gelöst. Die Funktionen der Programmierung, der Systemverwaltung und der Anwendung werden von verschiedenen Personen wahrgenommen. Der Programmierer

hat keinen Zugriff auf personenbezogene Daten. Ausschließlich die Dokumentationskräfte und die von der Klinikleitung im Vertretungsfall Ermächtigten haben als Anwender Zugriff auf die personenbezogenen Daten. Die Aufgaben der Systemverwaltung werden vom Leiter der EDV-Abteilung der Klinik wahrgenommen. Das Tumoregister Homburg hat ebenfalls eine Funktionstrennung zugesagt.

Ebenfalls eingeführt werden sollen bestimmte Lösungsfristen.

Beide Kliniken haben im übrigen meiner Forderung entsprechend zugesagt, den Verfahrensablauf und die datenschutzrechtlichen Fragen in einer Dienstanweisung detailliert zu regeln.

### 6.3 Gesundheitsamt

#### 6.3.1 Amtsärztliche Begutachtung im Vorfeld psychiatrischer Unterbringung

Ein Petent hat sich mit der Beschwerde an mich gewandt, daß ein Gesundheitsamt zu Unrecht eine Akte mit Vermerken über seinen psychischen Zustand führe.

Die Überprüfung und Feststellung des Sachverhalts bereitete gewisse Schwierigkeiten, da die Kontakte zwischen den einzelnen beteiligten Dienststellen in der Akte des Gesundheitsamtes nur unzureichend dokumentiert waren.

Der Besuch bei dem Gesundheitsamt ergab folgendes:

Der Petent hat sich mit zahlreichen Anfragen und Beschwerden an verschiedene Polizeidienststellen des Saarlandes gewandt. Dabei ging es um die Probleme eines Suchtabhängigen, für den er sich intensiv einsetzte. In einem Fall mußte die Polizei wegen eines

Notrufs tätig werden. Gegen den Petenten wurde dieserhalb wegen Vortäuschens einer Straftat ermittelt. Wegen der Häufung der Beschwerden haben die Polizeidienststellen teils direkt, teils über den zuständigen Landrat als Unterbringungsbehörde, Kontakt zu dem Gesundheitsamt aufgenommen. Es kam dann in der Folgezeit zu "Gesprächen" zwischen dem Petenten und dem Amtsarzt im Gesundheitsamt - einmal auch im Beisein eines Polizeibeamten -, deren Ergebnisse der Amtsarzt in Vermerken festgehalten hat. Diese enthalten Beurteilungen über den Geisteszustand des Petenten. Der Amtsarzt stellt fest, daß er "keine sicheren Hinweise für das Vorliegen einer echten Psychose" finde.

Es ließ sich nachträglich nicht mehr feststellen, ob der Petent sich durch das Gesundheitsamt auf freiwilliger Basis hat beraten lassen oder ob es sich um eine auf faktischem Zwang beruhende Begutachtung gehandelt hat. Während die Polizei den Sachverhalt so darstellt, als sei dem Petenten aus "fürsorglichen Gründen" empfohlen worden, die Hilfe des Gesundheitsamtes in Anspruch zu nehmen, war der Amtsarzt - nach seiner Darstellung - der Auffassung, daß er im Rahmen eines Unterbringungsverfahrens gutachterlich tätig geworden sei. Der Petent läßt sich jedenfalls dahin ein, daß er den Rat und die Hilfe des Gesundheitsamtes nicht für sich, sondern für den Suchtabhängigen in Anspruch nehmen wollte, für den er sich einsetzte.

Zwar fehlen derzeit hinreichend konkrete gesetzliche Regelungen über die Vorgehensweise der Behörden gegenüber psychisch Kranken, die möglicherweise untergebracht werden müssen. Aber nicht einmal die derzeit geltenden, rudimentären, gesetzlichen Bestimmungen über die Unterbringung psychisch Kranker rechtfertigen im vorliegenden Fall die Informationserhebung und -verarbeitung durch das Gesundheitsamt. Die Voraussetzungen für eine gutachterliche Tätigkeit des Gesundheitsamtes im Rahmen eines Unterbringungsverfahrens

waren nicht gegeben. Abgesehen davon, daß ich es für zweifelhaft halte, ob ein hinreichender Anlaß für die Einleitung eines Unterbringungsverfahrens gegeben war, fehlte es jedenfalls in formeller Hinsicht an einem entsprechenden Auftrag der zuständigen Verwaltungsbehörde, ein Gutachten zu erstellen. Das Gesundheitsamt darf erst nach Aufforderung durch die zuständige Behörde in Angelegenheiten des Gesundheitswesens gutachterlich tätig werden (§ 1 Satz 2 Nr. 3 der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens). Die Vorschriften setzen zwingend die förmliche Einleitung der Ermittlungen im Unterbringungsverfahren durch den Landrat voraus. Daraus ergibt sich im Umkehrschluß, daß das Gesundheitsamt keine Befugnis hat, von sich aus oder auf Veranlassung etwa der Vollzugspolizei tätig zu werden.

Dem Akteninhalt ließ sich nicht entnehmen, daß der Landrat als Unterbringungsbehörde das Gesundheitsamt konkret beauftragt hat, den Petenten zwecks Durchführung eines Unterbringungsverfahrens zu untersuchen. Die Begutachtung erfolgte somit ohne die für eine derartige Maßnahme zwingend erforderliche Ermächtigung.

Ist das Gesundheitsamt jedoch von Gesetzes wegen nicht zum Tätigwerden befugt, ist die Speicherung personenbezogener Daten und die Aufbewahrung von Unterlagen sensiblen, psychiatrischen Inhalts nicht zulässig.

Nimmt jemand freiwillig die Beratung des Gesundheitsamtes in Anspruch, bedarf die Dokumentation des Beratungsverlaufs und des Beratungsergebnisses der Einwilligung des Betroffenen. Das informationelle Selbstbestimmungsrecht begründet den Anspruch des einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. In dieses Recht darf nur aufgrund eines bereichsspezifischen und normenklaren

Gesetzes eingegriffen werden. Eine gesetzliche Ermächtigung, die es dem Gesundheitsamt erlaubt, Aufzeichnung über eine psychiatrische Beratungstätigkeit zu fertigen, ist nicht ersichtlich, so daß Rechtsgrundlage nur die Einwilligung des Betroffenen sein kann. In der Akte des Petenten befanden sich jedoch weder eine schriftliche Einwilligungserklärung, noch sonst ein Hinweis, daß er mit der Dokumentation seines Gesundheitszustandes einverstanden gewesen ist.

Das Gesundheitsamt ist meiner Argumentation gefolgt und hat die über den Petenten geführte Akte vernichtet.

Das Gesetz über die Unterbringung von Kranken und Süchtigen vom 10.12.1969 muß fortgeschrieben werden. Gerade im Vorfeld der Unterbringung ergeben sich Unsicherheiten über den zulässigen Umfang der Datenverarbeitung. Das Auftreten des psychisch Kranken weckt häufig Aggressionen. Sein oft querulatorisch erscheinenden Ersuchen verursachen den Behörden zusätzlichen Aufwand. Die Notwendigkeit einer Unterbringung scheint sich aus der Sicht des psychiatrisch nicht geschulten Laien in nicht wenigen Fällen geradezu anzubieten. Es liegt nahe, daß die Behörden Informationen über Ereignisse, Vorkommnisse sammeln und möglicherweise sogar mit einschlägigen Bemerkungen versehen dem Gesundheitsamt übermitteln. Die Untersuchungen und Ermittlungen zur Vorbereitung einer Entscheidung, die das Wohl des Kranken zu berücksichtigen hat, stellt einen tiefen Eingriff in das Persönlichkeitsrecht des Betroffenen dar. Eine ohne seine Einwilligung stattfindende Informationsverarbeitung bedarf einer detaillierten gesetzlichen Ermächtigung. Es bedarf einer eindeutigen, gesetzlichen Festlegung unter welchen Voraussetzungen seine personenbezogene Daten erhoben und gespeichert werden dürfen. Geregelt werden müssen die Datenübermittlungsbefugnisse zwischen den beteiligten Behörden, die Dauer der Aufbewahrung der ge-

speicherten Informationen und der Auskunftsanspruch des Betroffenen.

Ich muß bedauern, daß die datenschutzrechtlichen Ansätze im Entwurf eines Gesetzes "über Hilfen und Schutzmaßnahmen für psychisch Kranke" - PsychKG - (Lt-Drucksache 7/2121) nicht weiter verfolgt worden sind. Im einzelnen habe ich hierzu bereits einige konkrete Vorstellungen entwickelt (3. TB, Tz. 7.2).

Ich nehme den vorliegenden Fall zum Anlaß, an meine Forderung zu erinnern, das Unterbringungsgesetz zu novellieren.

#### 6.3.2 Geschlechtskrankenberatungsstelle

Nach dem Gesetz zur Bekämpfung der Geschlechtskrankheiten müssen Prostituierte in regelmäßigen Zeitabständen gegenüber dem Gesundheitsamt einen Nachweis über ihren Gesundheitszustand in bezug auf Geschlechtskrankheiten erbringen. Bei den Gesundheitsämtern sind deshalb Geschlechtskrankenberatungsstellen eingerichtet, die die Einhaltung dieser Verpflichtung überwachen und bei Feststellung einer Geschlechtskrankheit die entsprechenden Maßnahmen treffen.

Anläßlich eines Prüfbesuchs bei einem Gesundheitsamt konnte ich feststellen, daß die Datenverarbeitung in bezug auf Prostituierte dort im wesentlichen den Anforderungen des Datenschutzes entspricht. Es gab jedoch auch einige Punkte, die ich beanstanden mußte.

Anläßlich ihrer Vorstellung beim Gesundheitsamt "empfiehlt" das Gesundheitsamt den Prostituierten, sich bei der Polizei zu melden.

Von einer derartigen "Empfehlung" ist in Zukunft abzu-  
sehen. Der Hinweis des Gesundheitsamtes hat die Prostituierten in der Vergangenheit regelmäßig veran-

läßt, die Kriminalpolizei aufzusuchen, die sie befragte, ihre Angaben nebst den Personalien in einer speziellen Prostituiertendatei speicherte.

Diese Erhebungs- und Speicherungspraxis ist jedoch nach dem neuen saarländischen Polizeigesetz unzulässig (siehe dazu oben Tz. 3.2). Es besteht deshalb kein Anlaß, die Prostituierten anläßlich ihrer Untersuchung beim Gesundheitsamt zu einem Gang zur Polizei zu bewegen. Die Empfehlung würde überdies einen faktischen Zwang zu einem Handeln ausüben, das von Gesetzes wegen nicht geboten ist.

Das Gesundheitsamt hat meiner Forderung entsprochen. Empfehlungen der genannten Art werden nicht mehr erteilt.

Bei den Prostituierten wird alle 3 Monate ein Aids-Test auf freiwilliger Basis durchgeführt. Das Einverständnis wird lediglich mündlich erklärt. Ich halte demgegenüber aus Beweissicherungsgründen eine schriftliche Einwilligungserklärung für zwingend geboten. Dazu teilte mir das Gesundheitsamt mit, daß auf eine schriftliche Einverständniserklärung der Prostituierten zur Durchführung des HIV-Tests aus Gründen der Anonymität und Vertraulichkeit verzichtet werden müsse. Diese Begründung ist für mich nicht nachvollziehbar, da die Tatsache der Durchführung des Tests im Gesundheitsamt ohnehin bekannt ist.

Anlaß zur Beanstandung gab auch der Umstand, daß die über die Prostituierten angelegten Akten und Karteikarten nicht wie vorgesehen nach 10 Jahren nach Aufgabe der Tätigkeit als Prostituierte vernichtet wurden.

Bemängeln mußte ich außerdem, daß die Unterlagen teilweise nicht in den Räumlichkeiten der Geschlechtskrankenberatungsstelle, sondern in einem Dienstzimmer des Verwaltungsbereichs in einem einfachen Holzschrank

archiviert wurden. Das Gesundheitsamt bildet keine Informationseinheit. Durch technische Maßnahmen muß sichergestellt sein, daß auf die beim Gesundheitsamt geführten Akten und Unterlagen nur die Bediensteten Zugriff nehmen können, die die Daten zu ihrer Aufgabenerfüllung benötigen. Das Gesundheitsamt hat zugesagt, meinen Forderungen zu entsprechen.

### 6.3.3 Sicherung des Auskunfts- und Einsichtsrechts des Betroffenen durch Identitätsprüfung

Ein Gesundheitsamt hat die Kopie einer vor längerer Zeit angefertigten Röntgenaufnahme zur Vorlage beim behandelnden Arzt herausgegeben. Der Betroffene behauptet, daß jemand unter seinem Namen beim Gesundheitsamt vorgesprochen und das Dokument erhalten habe. Da das Gesundheitsamt bei der Aushändigung der Kopie die Identität des Antragstellers nicht überprüft hat, war nicht auszuschließen, daß die Röntgenaufnahme tatsächlich einem Unbefugten überlassen wurde.

Verlangt ein Bürger Auskunft über gespeicherten Informationen oder Einsicht in die über ihn geführten Akten oder sollen ihm Kopien dieser Unterlagen ausgehändigt werden, hat sich die Behörde über die Berechtigung zur Wahrnehmung solch höchstpersönlicher Individualrechte zu vergewissern. In solchen Fällen hat der Betroffene regelmäßig durch Vorlage von Ausweispapieren (Bundespersonalausweis, Reisepaß) seine Identität nachzuweisen, damit verhindert wird, daß personenbezogene Daten in falsche Hände gelangen. Das Gesundheitsamt hat inzwischen angeordnet, um ähnliche - wie eingangs geschilderte Vorfälle - zu vermeiden, daß solche Identitätsprüfungen durchgeführt werden. Es ist bedauerlich, daß solche Selbstverständlichkeiten einer besonderen Anordnung bedürfen.

#### 6.3.4 Formulare im Jugendärztlichen Dienst (Bilanz)

Anläßlich der Überprüfung eines Gesundheitsamtes hatte ich beanstandet, daß die bei der Mütter-/Säuglingsberatung und der Vorschulkinderuntersuchung erhobenen Untersuchungsbefunde bei der Einschulungsuntersuchung herangezogen und verwertet werden, ohne daß die Erziehungsberechtigten um ihr Einverständnis gebeten werden (vgl. meinen 11. TB, Tz. 6.2). Das zuständige Ministerium hat diese Beanstandung zum Anlaß genommen, die bei den jugendärztlichen Untersuchungen verwendeten Formulare neu zu gestalten. Die ärztlichen Unterlagen aus der Mütter-/Säuglingsbetreuung und Vorschulkinderuntersuchung werden nunmehr für Zwecke der Einschulungsuntersuchung nur noch verwendet, wenn sich die Erziehungsberechtigten schriftlich damit einverstanden erklärt haben.

Darüber hinaus hat das zuständige Ministerium weitere Probleme, die in der Vergangenheit im Zusammenhang mit der Einschulungsuntersuchung angefallen sind, in dem Formular aufgearbeitet.

So werden die Erziehungsberechtigten ausdrücklich auf ihr Recht hingewiesen, Einsicht in die Unterlagen zu nehmen und zu verlangen, daß das Ergebnis der Untersuchung mit ihnen besprochen wird.

Eine Weitergabe der bei der Untersuchung festgestellten Befunde an die Schule erfolgt nur, wenn die Erziehungsberechtigten hierzu ihr Einverständnis schriftlich erklärt haben.

#### 6.3.5 Medizinalpersonendatei (Bilanz)

In meinem 11. Tätigkeitsbericht, Tz. 4.2 hatte ich darüber berichtet, daß der Minister für Arbeit, Gesundheit und Sozialordnung die Fortführung der bei den Gesundheitsämtern eingerichteten Medizinalpersonendatei eingestellt hat. Ich hatte gefordert, daß konsequenterweise die vorhandenen Datensammlungen vernich-

tet werden müssen. Im Berichtszeitraum hat das zuständige Ministerium meiner Forderung entsprochen und den Gesundheitsämtern die Vernichtung des alten Datenbestandes aufgegeben.

#### 6.4 Krebsregistergesetz

Im Berichtszeitraum ist die Absicht des Bundesministers für Jugend, Familie, Frauen und Gesundheit bekannt geworden, ein Bundeskrebsregistergesetz einzuführen. Durch dieses Gesetz sollen einheitliche Vorgaben für die Führung regionaler Krebsregister geschaffen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die neu entstandene Diskussion im Zusammenhang mit der Einrichtung von Krebsregistern zum Anlaß genommen, ihre Position in einer gemeinsamen EntschlieÙung darzulegen (vgl. Anlage 6). Die Datenschutzbeauftragten lehnen eine Meldung ohne Einwilligung des Betroffenen ab, weil die Ziele von bevölkerungsbezogenen Krebsregistern mit weniger belastenden Methoden der Registrierung erreicht werden können. Es bestehen daher unter dem Gesichtspunkt des Verfassungsgrundsatzes der Verhältnismäßigkeit Bedenken gegenüber dem Meldemodell des Saarländischen Krebsregistergesetzes, das eine Beteiligung des betroffenen Patienten nicht vorsieht. Besondere Beachtung verdient das in Baden-Württemberg entwickelte und zwischenzeitlich in einer Pilotstudie erprobte dezentrale Anonymisierungsmodell; der behandelnde Arzt meldet die personenidentifizierenden Angaben verschlüsselt an das Register.

Ich habe gegenüber dem zuständigen Ministerium noch einmal darauf gedrängt (s. bereits meinen 8. TB, Tz. 4.7), die Novellierung des Saarländischen Krebsregisters in Angriff zu nehmen. Vor allem die Nutzung der Krebsregisterdaten zu wissenschaftlichen Zwecken be-

darf einer gesetzlichen Regelung. Das Persönlichkeitsrecht des Betroffenen und der Informationsanspruch der Wissenschaft bedürfen eines Ausgleichs, den der Gesetzgeber unter Berücksichtigung beider Positionen festlegen muß.

#### 6.5 Rechnerunterstützte Programme zur AIDS-Bekämpfung: Computerprogramme KLIMACS und KLINAIDS

Die Bundesregierung hat als Beitrag zu einer wirkungsvolleren Bekämpfung von AIDS Computerprogramme entwickelt, mit deren Hilfe auf Arbeitsplatzrechnern in bestimmten Kliniken u.a. die Krankengeschichte, der Behandlungsablauf, Befunde und Therapie von AIDS- - Patienten und HIV-Infizierten dokumentiert werden sollen. KLIMACS ist für die ambulante und KLINAIDS für die stationäre Behandlung vorgesehen. KLINAIDS wurde jedoch schon bald als nicht "essentiell" für das Ziel des Gesamtprojekts angesehen (Antwort des Parlamentarischen Staatssekretärs Seehofer vom 19. September 1989 auf schriftliche Anfrage; Bt-Drucksache 11/5226). Schon frühzeitig stellte das Ministerium für Jugend, Familie, Frauen und Gesundheit Erwägungen über den Nutzen dieses Programms an (Schreiben vom 26.09.1989).

Für den technischen Ablauf der Programminstallation und der Programmdurchführung hat das Kuratorium AIDS der Paul-Ehrlich-Gesellschaft im Auftrag des Bundesministers für Arbeit ein Handbuch erstellt, das nach Abstimmung mit dem Bundesbeauftragten für den Datenschutz durch einen datenschutzrechtlichen und datenschutztechnischen Teil ergänzt wurde.

Im Interesse der Optimierung der medizinischen Behandlung kommt der EDV-gestützten Dokumentation besondere Bedeutung zu. Zugleich darf nicht verkannt werden, daß wegen der außerordentlichen Sensibilität der in den Arbeitsplatzrechnern mit Hilfe dieser Programme gespeicherten Datenbestände die technisch perfekte

Durchführung der Datensicherung unabdingbare Voraussetzung ist.

Meine Nachforschungen haben ergeben, daß die beiden Programme auch in einer saarländischen Klinik angewandt werden. Leider mußte ich feststellen, daß trotz aller meiner bisherigen Bemühungen um die Datensicherung beim Computereinsatz in Krankenhäusern (vgl. meinen 10. TB, Tz. 4 S. 21) den Anforderungen der Datensicherung nicht Rechnung getragen wurde. Dies muß angesichts der besonderen Sensibilität der fraglichen Daten um so mehr befremden. Ich hatte mich sogar an der Erarbeitung einer Dienstanweisung für die Datensicherung in der fraglichen Klinik beteiligt, ohne daß diese mittlerweile in Kraft gesetzt wurde.

Eine Reihe technischer Maßnahmen, die dem Zugriff Unbefugter entgegenwirken, waren speziell für die Programme entwickelt worden; die Klinik sah sich nicht veranlaßt, entsprechende Vorkehrungen vor der Benutzung der Programme zu treffen. Die Sicherungssoftware, die Dateien und Betriebssystem zuverlässig schützt und eine lückenlose Zwangsprotokollierung der Benutzung gewährleistet, war nicht installiert. Nicht einmal der Zugang zu dem Raum, in dem der Computer abgestellt ist, war gesichert. Ferner war die Funktionstrennung zwischen Systemverwalter und Anwender, wie ich sie in meinem Datensicherungskonzept vorgeschlagen habe (10. TB S. 34), nicht vollzogen.

Die Klinik hat zugesagt, sich um eine Datensicherungssoftware zu bemühen, die den Anforderungen gerecht wird. Bis zur Realisierung dieser organisatorisch-technischen Maßnahmen werden keine Daten des fraglichen Personenkreises mit Hilfe von KLIMACS auf PC gespeichert. Die Benutzung von KLINAIDS wurde wegen der Unklarheiten über Ziel und Zweckmäßigkeit des Einsatzes zurückgestellt. Der vorhandene Datenbestand wurde gelöscht.

## 7. Soziales

### 7.1 Arztgeheimnis kontra maximale Leistungstransparenz

Der Gesetzgeber hat das Recht der gesetzlichen Krankenversicherung als Fünftes Buch im Sozialgesetzbuch geregelt. Ein eigenes Kapitel ist dem Thema Datenschutz gewidmet. Die Ärzte und Krankenhäuser stehen im Zentrum vielfältiger Informationsanforderungen von zahlreichen Stellen, nicht zuletzt von Sozialleistungsträgern. Die Zielsetzung des Gesetzgebers war insbesondere, den Datentransfer zwischen den am Leistungsgeschehen beteiligten Ärzten und Sozialversicherungen normenklar und einschränkend zu regeln. Das Vertrauensverhältnis zwischen Arzt und Patient, das strafbewehrte Arztgeheimnis, darf nicht durch einen Datenfluß ausgehöhlt werden, der nicht streng am Maßstab der Erforderlichkeit orientiert ist. Ob dieses Ziel in der Praxis erreicht worden ist, muß man bezweifeln.

Ärzte haben sich wiederholt mit der Frage an mich gewandt, ob aus datenschutzrechtlicher Sicht die Forderung der gesetzlichen Krankenversicherung gerechtfertigt ist, daß zu Abrechnungszwecken die Diagnosen stets anzugeben sind. Die Kassenärztlichen Vereinigungen und die AOK haben erklärt, daß kein Entgelt für ärztliche Leistungen gezahlt wird, wenn nicht die Diagnose angegeben ist. In einem Sonderrundschreiben hat die Kassenärztliche Vereinigung Saarland die Ärzte darauf hingewiesen, daß im Abrechnungsvordruck (Krankenschein) im dafür vorgesehenen Feld "Diagnosen bzw. Befunde in angemessener Kürze, aber so präzise zu formulieren sind, daß sich daraus die Plausibilität der abgerechneten Leistungen auch im Rahmen der Wirtschaftlichkeitsprüfung erkennen läßt". Zahlreiche Ärzte waren in die Zwangslage versetzt, zwischen der Wahrung des Arztgeheimnisses und eventueller Strafverfolgung einerseits und den wirtschaftlichen Notwendig-

keiten einer personal- und materialaufwendigen Praxisführung entscheiden zu müssen.

In dieser Situation habe ich in Stellungnahmen gegenüber der Kassenärztlichen Vereinigung, der AOK und dem Ministerium für Gesundheit und Soziales keinen Zweifel daran gelassen, daß ich die Angabe der Diagnose zu Abrechnungszwecken nicht für zulässig halte. Die Vermischung insbesondere von Funktionen der Abrechnung, der Plausibilitäts- und Wirtschaftlichkeitsprüfung ist unzulässig und durch das Gesetz nicht gerechtfertigt.

Angesichts der Schwere des Eingriffs in die Persönlichkeitsrechte der Patienten, die in der Offenbarung intimster medizinischer Daten durch den Arzt liegt, ist eine konkrete gesetzliche Befugnis notwendig, die die Ärzte als Leistungserbringer zur Weitergabe der medizinischen Angaben zu Abrechnungszwecken berechtigt. Eine solche liegt jedoch nicht vor.

Beim kassenärztlichen Versorgungssystem ist von einem zumindest faktischen Zwang bei der Verarbeitung patientenbezogener Daten auszugehen, wenn man ärztliche Leistungen in Anspruch nehmen will und dafür den Datentransfer an die beteiligten Stellen in Kauf nehmen muß. Ein Zwang zur Angabe personenbezogener Daten setzt jedoch voraus, daß der Gesetzgeber deren Verwendungszweck bereichsspezifisch und präzise bestimmt (BVerfGE 65,1, 44).

Die an der kassen- und vertragsärztlichen Versorgung teilnehmenden Ärzte sind indessen aufgrund ausdrücklicher gesetzlicher Vorschrift lediglich verpflichtet, in den Abrechnungsunterlagen "die von ihnen erbrachten Leistungen einschließlich des Tages der Behandlung, bei zahnärztlichen Behandlungen auch mit Zahnbezug" mitzuteilen (§ 294, § 295 Abs. 1 Ziff. 1 SGB V). Ferner sind auf den Vordrucken die Arztnummer sowie die Krankenversicherungsnummer des Patienten anzugeben (§

295 Abs. 1 Ziff. 2 SGB V). In dieser abschließenden Aufzählung sind Angaben zu Diagnosen nicht enthalten. Daß eine routinemäßige Weitergabe medizinischer Angaben zu Abrechnungszwecken nicht in Betracht kommt, ergibt sich aus der Textinterpretation ebenso wie aus einer systematischen Betrachtung des Fünften Buches des Sozialgesetzbuches.

Angaben von Diagnosen zu Abrechnungszwecken werden ausdrücklich nur Krankenhäusern auferlegt (§ 301 SGB V). Deshalb kann nur gefolgert werden, daß Diagnoseangaben im übrigen nicht zugelassen sind. Der Wortlaut des Gesetzes läßt jedenfalls keine andere Interpretation zu.

Der Gesetzgeber hat im übrigen die Übermittlung patientenbezogener Angaben durch niedergelassene Ärzte, soweit sie zur Aufgabenerfüllung durch die Kassenärztlichen Vereinigungen und die Krankenkassen etwa zur Wirtschaftlichkeitsprüfung und Plausibilitätskontrolle erforderlich ist, konkret geregelt.

Für die Wirtschaftlichkeitsprüfung ist im einzelnen festgelegt, daß patientenbezogene Daten nur in eingeschränktem Umfang aufgrund von Stichproben zur Verfügung stehen, im übrigen aber solche nur nach Durchschnittswerten und Richtgrößen auf der Grundlage von nicht auf den Versicherten bezogenen Daten erfolgt (§ 106 SGB V).

Plausibilitätskontrollen sollen nach dem Willen des Gesetzgebers nicht generell, sondern folgerichtig ebenfalls nur auf der Grundlage von Stichproben erfolgen. Hierzu sind Gesamtverträge zwischen den Kassenärztlichen Vereinigungen und den Krankenkassen abzuschließen (§ 83 Abs. 2 SGB V). Außerdem liegen Untersuchungen vor, die in Diagnosen auf Krankenscheinen kein Plausibilitätskriterium erkennen können und damit die Geeignetheit und Erforderlichkeit der Diagnose in

Frage stellen (Forschungsgruppe AOK Dortmund DOK 82/41).

Für Zwecke der Qualitätsprüfung ärztlicher Leistungen kann ebenfalls eine routinemäßige Diagnoseangabe nicht verlangt werden, weil eine sorgfältige Kontrolle im Einzelfall ohnehin die Einsichtnahme in die vom Arzt zu führende Dokumentation erfordert. Eine auch im Interesse des Patienten liegende derartige Kontrolle ist den Kassenärztlichen Vereinigungen generell als Aufgabe übertragen. Wegen des Mangels einer förmlichen gesetzlichen Befugnis - die Aufgabenzuweisung allein reicht auch nach der Systematik des Gesetzes (§ 294 SGB V) nicht aus - hat die Kassenärztliche Vereinigung des Saarlandes bis zur gesetzlichen Bereinigung des Formmangels ohnehin auf die Vorlage von ärztlichen Unterlagen zu diesem Zweck verzichtet. Die routinisierte Übermittlung der Diagnosen aus Gründen der Qualitätsprüfung ist nach der Vorschrift für die Aufgabenzuweisung nicht gerechtfertigt.

Für die Gewährung von Krankengeld aufgrund einer Arbeitsunfähigkeitsbescheinigung sind zwar Angaben über die Art der Erkrankung notwendig, weil die Dauer der Leistung bei wiederholter Erkrankung wegen desselben Leidens beschränkt ist (§ 48, § 292 Abs. 1 SGB V). Die routinemäßige Diagnoseangabe zu Abrechnungszwecken kann aber auch hieraus keinesfalls hergeleitet werden. Ebenso wenig kann die Verpflichtung der Krankenkasse, im Einzelfall den Medizinischen Dienst einzuschalten, einen solchen umfassenden Datentransfer rechtfertigen.

Abgesehen vom Mangel einer ausreichenden gesetzlichen Ermächtigung ist bisher die Erforderlichkeit einer routinemäßigen Diagnoseangabe zu Abrechnungszwecken nicht dargelegt. Diagnoseangaben könnten etwa in Betracht kommen, wenn im Gebührenverzeichnis die ärztliche Leistung nicht hinreichend konkret beschrieben ist. Der beanstandete routinemäßige Datentransfer ist

spätestens mit Einführung der Automation im Abrechnungswesen, die auch einen selektiven Zugriff auf den Datenbestand eröffnet, besonders bedenklich. Eine strenge Erforderlichkeitsprüfung ist deshalb um so mehr angebracht. Jedenfalls ist die Angabe der Diagnose auf dem Krankenschein zu Abrechnungszwecken bis zu einer ausdrücklichen, gesetzlichen Regelung nicht zulässig.

Es ist sehr zu bedauern, daß AOK, Kassenärztliche Vereinigung und das zuständige Ministerium sich ohne Rücksicht auf die Erfordernisse verfassungsgemäßer Rechtsgrundlagen zugunsten der Routine und übernommener Verwaltungsübung entschieden haben. Es stehen überdies im Einzelfall ausreichende andere Kontrollinstrumente zur Verfügung, die eine routinemäßige Diagnoseübermittlung im Zusammenhang mit der Abrechnung erübrigen dürften. Die Vertreterversammlung der Kassenärztlichen Vereinigung in Hessen hat deshalb empfohlen, ohne einen förmlichen Beschluß zu fassen, dem Persönlichkeitsrecht des Patienten einen höheren Stellenwert beizumessen als abrechnungstechnischen Erfordernissen.

Meine Bedenken blieben unberücksichtigt. Die Ärzte sind nach wie vor gehalten, die Diagnose allein zu Abrechnungszwecken in jedem Krankenschein anzugeben, wenn sie nicht finanzielle Nachteile hinnehmen wollen.

Die Auseinandersetzung in den Medien hat zu einer großen Verunsicherung in der Ärzteschaft geführt (vgl. Spiegel 08.10.1990: "Die Kassen verlangen von den Ärzten einen Bruch ihrer Schweigepflicht"). Peinlich berührt war ich von der teilweise vereinfachenden Argumentationsweise und der unverhohlenen Drohung gegenüber einzelnen Ärzten, daß Krankenscheine nicht zur Abrechnung angenommen werden, wenn die Diagnosen nicht angegeben sind.

## 7.2 Übermittlung von Patientenunterlagen durch Krankenhäuser an Krankenkassen

Ein Krankenhaus hat die Frage gestellt, ob es verpflichtet sei, einer Krankenkasse als Sozialleistungsträger die "Fieberkurve" eines Patienten wegen Verlängerung der Kostenzusage zu überlassen. Die "Fieberkurve" ist ein Krankenblatt, in dem Angaben zur Medikation und Therapie, sowie Laborbefunde eingetragen werden.

Der Gesetzgeber hat indessen abschließend geregelt, welche Angaben die Krankenhäuser den Krankenkassen bei Krankenbehandlung zu übermitteln haben (§ 301 SGB V). Die von der Krankenkasse verlangte Information fällt nicht unter den Katalog der nach dieser Vorschrift zu übermittelnden Angaben. Ich habe deshalb empfohlen, von einer Weitergabe der "Fieberkurve" abzusehen.

## 7.3 Medizinischer Dienst

Seit dem 01.01.1990 gibt es im Saarland, wie in allen anderen Bundesländern, eine neue Institution, den Medizinischen Dienst der Krankenversicherung im Saarland. Es handelt sich um eine Arbeitsgemeinschaft als Körperschaft des öffentlichen Rechts, der als Mitglieder die Allgemeine Ortskrankenkasse für das Saarland, der Landesverband der Betriebskrankenkassen Rheinland-Pfalz und Saarland, die Landwirtschaftliche Krankenkasse für das Saarland, der Verband der Angestelltenkrankenkassen e.V. und der Verband der Arbeiter-Ersatzkassen e.V. angehören. Der Medizinische Dienst tritt an die Stelle des "Vertrauensärztlichen Dienstes", der als unselbständige Abteilung bisher der Landesversicherungsanstalt zugeordnet war.

Die Rechtsgrundlage für die Tätigkeit des Medizinischen Dienstes ergibt sich aus dem Fünften Buch des Sozialgesetzbuches (SGB V). Er hat die Aufgabe, für

die Krankenkassen Gutachten zu erstellen als Entscheidungshilfe für die leistungsrechtliche Beurteilung im Einzelfall. Eine Beteiligung des Medizinischen Dienstes kommt in Betracht etwa bei Beurteilung der Arbeitsunfähigkeit, bei Feststellung der Schwerpflegebedürftigkeit oder bei Prüfung der Voraussetzungen von Kurmaßnahmen.

Darüber hinaus sollen die Krankenkassen den Medizinischen Dienst zu Rate ziehen, wenn es um allgemeine medizinische Fragen der gesundheitlichen Versorgung und Beratung der Versicherten geht.

Im Berichtszeitraum hatte ich Gelegenheit, mit dem Geschäftsführer des Medizinischen Dienstes verschiedene datenschutzrechtlichen Probleme, die in der Praxis aufgetreten sind, zu erörtern.

Diskutiert wurde die Frage, in welchem Umfang der Medizinische Dienst Informationen aus Krankenhausberichten an die Krankenkasse weitergeben darf. Ich habe meine bereits früher vertretene Auffassung unterstrichen, daß die Weitergabe des vollen Wortlauts des Arztberichts an die Krankenkasse mit detaillierten Angaben über Anamnese, Befund und Diagnose unzulässig ist (11. TB, Tz. 7.3). Der Krankenkasse sind lediglich "das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund" mitzuteilen (§ 277 SGB V, § 369b Abs. 2 RVO a.F.). Aus dem Wortlaut des Gesetzes ergibt sich eindeutig, daß allenfalls die zum Verständnis des Gesamtzusammenhangs unerläßlichen Einzelangaben offenbart werden dürfen.

Beauftragen die Krankenkassen eine Klinik oder einen niedergelassenen Arzt unmittelbar mit der Erstellung eines Gutachtens, ist das Original zunächst dem Medizinischen Dienst zuzuleiten, der alsdann die Informationen mit der gesetzlich gebotenen Einschränkung an die Krankenkassen weiterzuleiten hat. Der Umfang der

Offenbarung der unter das Arztgeheimnis fallenden Daten kann nicht davon abhängen, von welcher Stelle das ärztliche Gutachten erstattet wird.

Meine Rechtsauffassung wird von dem Geschäftsführer des Medizinischen Dienstes geteilt; er hat angeordnet, daß keine Krankenhausberichte oder ärztliche Gutachten im Original an Krankenkassen weitergegeben werden dürfen.

Übereinstimmung konnte auch dahin erzielt werden, daß der Medizinische Dienst personenbezogene Daten nur erheben und erfassen darf, soweit dies für seine Prüfungen, Beratungen und gutachterlichen Stellungnahmen erforderlich ist. Er ist nicht berechtigt, den Patienten, unabhängig von der konkreten Fragestellung des zu erstattenden Gutachtens, einer umfassenden Untersuchung zu unterziehen und die Ergebnisse zu dokumentieren. Eine Beratungsfunktion in dem Sinne, daß der Medizinische Dienst im Einzelfall über den konkreten Gutachterauftrag hinaus eine umfassende Untersuchung durchführt, um den Betroffenen über Gesundheitsgefährdungen und ihre Vermeidung zu beraten, hat der Gesetzgeber dem Medizinischen Dienst nicht zugewiesen.

Gegenstand der Erörterung war schließlich die Frage nach der Aufbewahrungsdauer der Unterlagen. Hierzu hat der Gesetzgeber eine eindeutige Entscheidung in dem Sinne getroffen, daß die personenbezogenen Daten nach 5 Jahren zu löschen sind (§ 276 Abs. 2 Satz 3 SGB V). Keine Einwände habe ich jedoch gegen den Vorschlag, den Versicherten nach Ablauf der Frist die für sie wichtigen Originalbefunde zu übergeben. Damit wäre einerseits dem gesetzgeberischen Anliegen Rechnung getragen, daß personenbezogene Informationen nicht länger als 5 Jahre vorgehalten werden. Andererseits kann der Versicherte, wenn es im Einzelfall in seinem Interesse einmal erforderlich sein sollte, auf die Informationen zurückgreifen.

#### 2.4 Ärztlicher Dienst des Versorgungsamtes

Aufgrund der Anfrage eines Klinikchefs habe ich mich mit der Behandlung medizinischer Unterlagen beim Versorgungsamt befassen müssen.

Für die Bearbeitung von Anträgen nach dem Schwerbehindertengesetz fordert das Versorgungsamt regelmäßig Befundberichte der behandelnden Ärzte, häufig aber auch von Krankenhäusern die kompletten Krankenpapiere an. Auch bei Leistungsansprüchen des sozialen Entschädigungsrechts (Kriegsopferversorgung, Impfschäden, Opferentschädigung) werden häufig medizinische Gutachten benötigt. Die Unterlagen werden uneingeschränkt den Sachbearbeitern vorgelegt. Kopien der Krankenakten und sonstigen medizinischen Unterlagen werden zu den Verwaltungsakten genommen, sofern die Originale an die datenliefernden Stellen zurückzusenden sind.

Die Ärzte des Versorgungsamtes oder die externen Gutachter werten zwar als medizinische Sachverständige die Krankenunterlagen aus. Die Entscheidung über den anzuerkennenden Grad der Behinderung wird jedoch von nichtärztlichen Bediensteten des Verwaltungsbereiches getroffen. Das Versorgungsamt ist daher der Auffassung, daß dort auch die vollständigen medizinischen Unterlagen zur Verfügung stehen müssen.

Ich halte es nicht für vertretbar, daß Krankenakten mit Angaben über Krankheitsvorgeschichte, Einzelbefunde, Behandlungen, Operationsberichte den medizinisch nicht vorgebildeten Mitarbeitern der Verwaltung zugänglich sind und in Verwaltungsakten aufbewahrt werden.

Krankenpapiere sollten als Arztsache deklariert unmittelbar dem Ärztlichen Dienst des Versorgungsamtes zugeleitet, dort ausgewertet sowie aufbewahrt und -

soweit notwendig - von dort dem Einsender wieder zurückgesandt werden. Der "Ärztliche Dienst" hat der Versorgungsverwaltung die medizinischen Informationen zur Verfügung zu stellen, die für die Sachbearbeitung - etwa für die Festsetzung des Grades der Behinderung oder für die Entscheidung über den Leistungsanspruch - unerlässlich sind. Das Verhältnis zwischen "Ärztlichem Dienst" und Verwaltung des Versorgungsamtes sollte ähnlich gestaltet werden wie das zwischen dem Medizinischen Dienst und den Krankenkassen (vgl. oben Tz. 7.4). Die Ablauforganisation des Versorgungsamtes sollte in diesem Sinne geändert werden.

Leider ist es mir trotz mehrfacher Erinnerung bisher nicht gelungen, das zuständige Ministerium dazu zu bewegen, zu meinem Vorschlag Stellung zu nehmen.

#### 7.5 Schulbericht für das Jugendamt

Ein Sozialarbeiter eines Jugendamtes hat sich mit der Frage an mich gewandt, unter welchen Voraussetzungen und in welchem Umfang Schulen verpflichtet sind, Informationen über ihre Schüler an das Jugendamt weiterzugeben.

Eng verwoben mit der Informationspflicht öffentlicher Stellen ist die Frage nach der Verantwortlichkeit datenliefernder und datenempfangender Stellen für die Rechtmäßigkeit der Datenübermittlung. Die Gesetzgebung hat dieses Problem bisher ausgespart. Erst die Novelle zum Bundesdatenschutzgesetz enthält hierzu Regelungen (§ 15 Abs. 2 BDSG, BGBl. I. 1990, S. 2954).

Fordert das Jugendamt einen Schulbericht im Rahmen eines Verfahrens an, das auf freiwilliger Grundlage durchgeführt wird, ist eine Datenweitergabe nur mit Einwilligung der Eltern zulässig. Dabei sind die Eltern vorab darüber aufzuklären, in welchem Umfang eine Zusammenarbeit zwischen Schule und Jugendamt

stattfindet und welche Angaben weitergegeben werden. Jeder einzelne Bericht ist den Eltern bekanntzugeben, mit ihnen zu besprechen und nur mit ausdrücklicher Einwilligung an das Jugendamt weiterzugeben.

Bei Maßnahmen des Jugendamtes, die auf gesetzlicher Grundlage ohne Einwilligung der Eltern durchgeführt werden (z.B. Mitwirkung bei Entziehung der elterlichen Sorge), ist die Datenweitergabe auch ohne Einwilligung zulässig. Aber auch in diesen Fällen empfiehlt es sich, daß sich Schule und Jugendamt um die Einwilligung der Eltern zur Datenweitergabe im Interesse der Stärkung des Vertrauensverhältnisses zwischen Eltern und Jugendamt bemühen.

Unabhängig davon, ob die Datenweitergabe der Einwilligung der Eltern bedarf, dürfen jedenfalls nur die Daten weitergegeben werden, die das Jugendamt zur Erfüllung seiner Aufgaben unbedingt benötigt. Im Einzelfall ist stets eine Prüfung notwendig, ob überhaupt ein Bericht und gegebenenfalls in welchem Umfang Informationen erforderlich sind. Dabei trägt das Jugendamt besondere Verantwortung, weil die datenliefernde Stelle die Notwendigkeit der Informationsanforderung im Einzelfall nicht überprüfen kann (vgl. § 15 Abs. 2 Satz 2 BDSG). Das Jugendamt sollte deshalb folgendes beachten:

- Das Jugendamt hat vor jeder Anforderung eines Schulberichts sorgfältig zu prüfen, ob ein Schulbericht im Einzelfall tatsächlich erforderlich ist.
- Die Befragung muß auf den individuellen Fall abgestellt werden. Das Jugendamt hat die Beantwortung möglichst konkreter Fragen zu verlangen. Die Schule soll nicht von vornherein dazu verleitet werden, mehr Informationen an das Jugendamt weiterzugeben, als zur Erfüllung seiner Aufgaben notwendig sind. Bedenklich wäre in diesem Zusammenhang vor allem die

Verwendung eines standardisierten Fragebogens, da solche zwangsläufig die konkrete Einzelfallsituation nicht ausreichend berücksichtigen. Die Erforderlichkeit der Information für die Aufgabenwahrnehmung des Jugendamtes sollte sich aus der Datenanforderung ergeben. Im Zweifel ist die Schule berechtigt, die Erforderlichkeit einer Information zu überprüfen und Rückfrage zu halten (vgl. § 15 Abs. 2 Satz 1 BDSG).

- Die Möglichkeit der Berichts-anforderung gegenüber der Schule kann das Jugendamt nicht von eigenen Erhebungen bei den Betroffenen entbinden. Die Datenerhebung beim Betroffenen hat stets Vorrang vor der Befragung anderer Personen und Stellen. So ist etwa die Beschreibung des Erscheinungsbildes des Kindes in einem Schulbericht von vornherein unzulässig. Denn es handelt sich um eine Information, die dem Jugendamt schon aus eigener Anschauung bekannt sein muß.
- Bei der Berichts-anforderung ist darauf zu achten, daß nur solche Fragen gestellt werden, die die Schule allein aus dem schulischen Umgang mit dem Schüler und seinen Eltern beantworten kann. Am wenigsten problematisch sind dabei die Angaben über tatsächliche Verhältnisse (z.B. Fehlzeiten). Größte Zurückhaltung ist dagegen geboten, wenn es sich um Wertungen und Meinungen handelt. Auf jeden Fall unzulässig ist die Weitergabe von Bewertungen und Vermutungen, für die es keine tatsächlichen Anhaltspunkte gibt.

#### 7.6 Sozialdatenschutz für das gesprochene Wort

Mehrere Sozialhilfeempfänger haben sich darüber beklagt, daß bei ihren Vorsprachen beim Sozialamt Unbeteiligte mithören können, welche Anliegen sie mit dem Sachbearbeiter besprechen. Häufig hielten sich noch andere Personen - Besucher oder nicht zuständige Mit-

arbeiter - im Raum oder im Nachbarzimmer auf, zu dem die Verbindungstüren geöffnet waren.

Die Datenschutzvorschriften des Sozialgesetzbuches verpflichten den Sozialleistungsträger, organisatorische und technische Vorkehrungen zum Schutz des Sozialgeheimnisses zu treffen. Der Hilfesuchende muß Gelegenheit haben, vertraulich mit dem Sachbearbeiter zu reden, ohne daß Dritte mithören können.

## 8. Öffentlicher Dienst

### 8.1 Abschottung der Beihilfestellen

#### 8.1.1 Landesverwaltung

Ein unzulässiger Eingriff in die Persönlichkeitsrechte ist stets dann gegeben, wenn Tatsachen, die den Arbeitnehmer persönlich betreffen, weiter aufgedeckt werden, als dies die unabdingbare Folge seiner Einordnung in den Arbeitsbereich ist. Deshalb ist der Grundsatz der Zweckbindung bei der Verarbeitung von Personaldaten gerade auch im Bereich des öffentlichen Dienstes einzuhalten, weil der Dienstherr mit Rücksicht auf seine Fürsorgepflicht einen besonderen Vertrauensschutz gegenüber dem Bediensteten zu gewährleisten hat. Dies gilt vor allem für die sensiblen Informationen, die im Zusammenhang mit der Festsetzung von Beihilfen anfallen (Beihilfeverordnung § 17 Abs. 2). Ebensowenig wie die gesetzliche Krankenkasse dem Arbeitgeber Informationen über den Gesundheitszustand seiner Arbeitnehmer offenbaren darf, dürfen Angaben aus Beihilfeanträgen dem Dienstherrn zur Verfügung stehen.

Mit der Zentralisierung der Beihilfebearbeitung bei der Oberfinanzdirektion (OFD) ist im Bereich der Landesverwaltung ein entscheidender Fortschritt erzielt worden, indem die Beihilfegewährung von der Personalsachbearbeitung getrennt erfolgt. Denn die Gefahren der Zweckdurchbrechung treten insbesondere dann auf, wenn Beihilfe- und Personalangelegenheiten in derselben Organisationseinheit bearbeitet werden.

Die notwendige organisatorische und personelle Trennung von der Personalsachbearbeitung ist jedoch für den Bereich der OFD mit ihren 2.600 Bediensteten noch nicht erreicht. Insoweit sind sogar weitergehende Gefahren für die schutzwürdigen Belange der betroffe-

nen Bediensteten infolge der Kompetenzüberlagerung mit anderen sensiblen Bereichen nicht auszuschließen.

Einer Abteilung der OFD, die zugleich die Aufsicht über die Finanzämter führt und insoweit auch für alle Personalentscheidungen zuständig ist, ist die Festsetzung von Löhnen, Vergütungen und Gehältern sowie Versorgungsbezügen (zentrale Besoldungsstelle) und die Beihilfebearbeitung für den gesamten Landesbereich übertragen. Die Gefahr einer unverhältnismäßigen Durchleuchtung ergibt sich aus einer Überschneidung der Zuständigkeiten im Bereich der OFD, die jedenfalls auf der Ebene des Abteilungsleiters und des Behördenleiters zu Interessenkollisionen führen muß. Schließlich trägt der Vorgesetzte Verantwortung für die Ordnungsgemäßheit der Aufgabenwahrnehmung und muß deshalb auch von seinem Kontrollrecht Gebrauch machen dürfen. Sensible Informationen über die wirtschaftlichen Verhältnisse aus der Steuersachbearbeitung, der Kindergeldgewährung, der Auseinandersetzung über Vermögens-, Versorgungs- und Unterhaltsansprüche in Ehescheidungs- und Sorgerechtsverfahren ebenso wie Krankheitsdaten können sich in einer die Zweckbindung nicht beachtenden Weise bei Personalentscheidungen auswirken.

Die notwendige Abschottung der zentralen Beihilfestelle wird jedenfalls für den relativ großen Bereich der OFD nicht in dem gebotenen Ausmaß erreicht. Zwar wurde der Postlauf inzwischen dahin geregelt, daß die Eingänge der Beihilfestelle unmittelbar zugehen. Die Gefahren für die Bediensteten müssen jedoch durch weitere organisatorische Maßnahmen - insbesondere eine andere Aufbauorganisation - gemindert werden. Bisher ist noch keine Entscheidung getroffen.

#### 8.1.2 Gemeinden und sonstige öffentliche Stellen

Das Risiko, daß Beihilfedaten bei Personalentscheidungen verwendet werden, ist in kleineren Verwaltungen,

insbesondere in kleineren Gemeinden noch größer als im Bereich der Landesverwaltung. Auch dort ist durch organisatorische, personelle und räumliche Abschottung der Beihilfestelle von der allgemeinen Personalsachbearbeitung das in der Beihilfeverordnung festgelegte Verbot einer zweckfremden Verwendung von Beihilfedaten sicherzustellen. Weil dies in kleineren Verwaltungen nur schwer zu realisieren ist, habe ich bereits in meinem letzten Tätigkeitsbericht (Tz. 10.2) angeregt, eine Übertragung der Beihilfebearbeitung an eine externe, öffentliche Stelle zu erwägen. Der Minister des Innern hat meine Forderung strikt abgelehnt, den kommunalen und den sonstigen, der Aufsicht des Landes unterliegenden Behörden die Möglichkeit zu eröffnen, die Festsetzung der Beihilfe einer anderen öffentlichen Stelle zu übertragen. Er ist der Auffassung, daß den datenschutzrechtlichen Belangen Rechnung getragen wird.

Eine Umfrage bei 15 Städten und Gemeinden hat allerdings ergeben, daß nur in 2 Kommunen von einer einigermaßen befriedigenden Abschottung der Beihilfestelle die Rede sein kann. Nur in diesen beiden Fällen ist die Beihilfefestsetzung von der eigentlichen Personalsachbearbeitung wenigstens personell und räumlich - wenn auch innerhalb des Personal- oder Hauptamtes - getrennt. In den übrigen Gemeinden wird die Beihilfe vom Personalsachbearbeiter festgesetzt; häufig erledigt dies der Leiter der Personalabteilung selbst. Daß dabei Informationen aus der Beihilfebearbeitung bewußt oder auch unbewußt bei der Vorbereitung von Personalentscheidungen verwendet werden, liegt in einer solchen Situation nahe.

Den Behörden, die die notwendige Abschottung der Beihilfestelle nicht leisten können, sollte die Möglichkeit der Aufgabenübertragung auf eine externe, öffentliche Stelle - etwa die Ruhegehalts- und Zusatzversorgungskasse des Saarlandes - offenstehen.

## 8.2 Beihilfe für Familienangehörige

Für Angehörige von öffentlichen Bediensteten können sich - wie ich aus Anfragen entnehmen konnte - Beeinträchtigungen ergeben, weil sie keinen eigenen Beihilfeanspruch haben. Sie müssen dem Beihilfeberechtigten zur Inanspruchnahme jeder Art von beihilfefähiger Leistung die Belege zur Vorlage an die Beihilfestelle übermitteln. So kann eine getrennt lebende Ehefrau gezwungen sein, dem beihilfeberechtigten Ehemann hochsensible Gesundheitsdaten - etwa über eine psychotherapeutische Behandlung - zu offenbaren. Es ist nicht auszuschließen, daß solche Informationen zur Grundlage eines Scheidungsbegehrens gemacht werden. Aber auch die Eltern-Kind-Beziehung kann schwer belastet werden, wenn der beihilfeberechtigte Vater Kenntnis von gynäkologischen Befunden - etwa dem legalen Schwangerschaftsabbruch seiner volljährigen, unverheirateten Tochter - erfährt.

Ich bin der Auffassung, daß den Familienangehörigen ein eigener Beihilfeanspruch eingeräumt werden sollte. Übergangsweise könnten die schutzwürdigen Belange der Familienangehörigen - wenn auch unvollkommen - durch die Möglichkeit berücksichtigt werden, daß sie die Belege der Beihilfestelle unmittelbar vorlegen.

Der Minister des Innern lehnt ein eigenständiges Antragsrecht der Angehörigen ab, da die Beihilfe als Teil der Alimentation des Beamten als höchstpersönlicher Anspruch nicht teilbar sei. Den Familienangehörigen stehe zu Lebzeiten des Bediensteten kein eigener Anspruch auf Alimentation zu.

Im übrigen ist der Minister des Innern der Auffassung, daß das Antragsrecht nicht vom Nachweis der Leistung getrennt werden kann. Lediglich in eng begrenzten Ausnahmefällen soll den Familienangehörigen die Di-

rektvorlage der Belege an die Beihilfestelle eingeräumt werden.

Ich bin der Auffassung, daß eine "organisatorische" Lösung ohne Anerkennung eines eigenen Beihilfeanspruchs lediglich übergangsweise, bis zur Änderung der Rechtsgrundlage, weiterhelfen kann. Wird Angehörigen die Möglichkeit eingeräumt, Arztrechnungen, Arzneimittelverordnungen unmittelbar bei der Beihilfestelle einzureichen, muß der beihilfeberechtigte Bedienstete jedoch stets selbst den Antrag stellen. Sein Akteneinsichtsrecht muß zwar nicht unbedingt dazu führen, daß er die Belege nachträglich zur Kenntnis nimmt, weil diese regelmäßig nach Beendigung der Sachbearbeitung an den Betroffenen zurückgegeben werden. Bis zu diesem Zeitpunkt könnte jedoch die Kenntnisnahme durch den Beihilfeberechtigten, wenn er dies ausdrücklich gegenüber der Beihilfestelle verlangt, nicht ausgeschlossen werden. Spätestens jedoch mit der Zustellung des Beihilfebescheides erfährt der Bedienstete die Höhe des Betrags und die Art der Leistung. Im Falle der Ablehnung müssen die tragenden Gründe dem Beihilfeberechtigten mitgeteilt werden, so daß auch insofern die Offenbarung notwendige Folge des ausschließlichen Anspruchs des beihilfeberechtigten Bediensteten ist.

Die früher in der gesetzlichen Krankenversicherung geltende Rechtslage, wonach nur dem Versicherten selbst ein eigener Anspruch eingeräumt war, ist durch das Gesundheitsreformgesetz geändert worden (§ 10 SGB V). Auch im Beihilferecht können die Probleme in befriedigender Weise nur gelöst werden, wenn die Rechte der Familienangehörigen in gestörten Familienverhältnissen als eigenständige Ansprüche ausgestaltet werden.

Einer solchen Lösung stehen "hergebrachte Grundsätze des Beamtentums" nicht entgegen (Art. 33 Abs. 5 GG). Hierzu zählen nur die Prinzipien, die das Bild des

Beamtentums in seiner überkommenen Form so prägen, daß ihre Beseitigung auch das Wesen des Beamtentums antasten würde. Das ist hier nicht der Fall. Den "hergebrachten Grundsätzen des Beamtentums" kommt zwar Verfassungsrang zu; der Vorrang des informationellen Selbstbestimmungsrechts darf jedoch hierdurch nicht geschmälert werden.

### 8.3 Anerkennung der Beihilfefähigkeit von psychotherapeutischen Maßnahmen

Bevor ein Beihilfeberechtigter eine psychotherapeutische Behandlung beginnt, hat er bei der Beihilfestelle zu beantragen, daß diese Therapie als beihilfefähig anerkannt wird. Das Antragsformular sieht nur die einfache Angabe der Diagnose vor und keine ausführliche, medizinische Begründung (vgl. 9. TB, Tz. 7.2). In Zweifelsfällen kann allerdings die Beihilfestelle nach einem Erlaß des Ministers des Innern ein Gutachten über die Notwendigkeit der Behandlung einholen. Ein Psychiater hat sich bei mir darüber beschwert, daß die Beihilfestelle sich nicht mit einer kurz gefaßten Stellungnahme zufrieden gebe, sondern die Beihilfegewährung von der Vorlage eines umfassenden Gutachtens abhängig mache.

Die Erstellung eines ausführlichen Gutachtens mit detaillierten, medizinischen Einzelheiten und Befunden halte ich nicht für geboten. Es ist äußerst fraglich, ob der medizinisch und psychologisch nicht vorgebildete Sachbearbeiter der Beihilfestelle in der Lage ist, sich mit detaillierten Angaben eines Gutachtens fachlich auseinanderzusetzen. In der Stellungnahme sollte daher nur das Ergebnis und lediglich die für das Verständnis unerläßlichen Befunde dargestellt werden. Ich habe den Minister des Innern gebeten, seinen Erlaß in diesem Sinne zu präzisieren.

#### 8.4 Privatpost für Bedienstete

Der Personalrat des Umweltministeriums hat sich an mich gewandt, weil im Entwurf einer neuen Dienstanweisung für die Poststelle festgelegt werden sollte, daß nicht mehr wie bisher alle persönlich adressierten Posteingänge ungeöffnet an den Bediensteten weitergeleitet werden, sondern nur noch dann, wenn sie ausdrücklich die Vermerke "persönlich" oder "vertraulich" tragen.

Diese Verfahrensweise halte ich für problematisch. Üblicherweise werden im Postverkehr Briefe nur mit dem Namen und der Anschrift des Adressaten versehen. Es ist daher durchaus möglich, daß private Postsendungen dieser Art auch ohne besondere weitere Kennzeichnung an die Dienstanschrift eines Bediensteten gerichtet sind. Dies gilt um so mehr, als die Abläufe in einer Behörde Außenstehenden im einzelnen nicht bekannt sind. Wird ein solcher Brief geöffnet, liegt darin ein Verstoß gegen Art. 10 GG, der den brieflichen Verkehr gegen die Kenntnisnahme durch die öffentliche Gewalt schützt. Bedienstete, die unrechtmäßig Kenntnis vom Inhalt eines Briefes erlangen oder andere zu einer solchen veranlassen, könnten sich nach § 202 Strafgesetzbuch strafbar machen.

Es darf zwar nicht verkannt werden, daß Briefe mit durchaus dienstlichem Inhalt mit einer an den zuständigen Bediensteten gerichteten Adressierung in öffentlichen Stellen eingehen und dadurch dienstliche Vorgänge dem weisungsbefugten Vorgesetzten und der Behördenleitung nicht unmittelbar zur Kenntnis gelangen. Das Post- und Briefgeheimnis ist jedoch ein so hohes Rechtsgut, daß der Dienstherr sich darauf verlassen muß, daß der Bedienstete solche ihm ungeöffnet zugegangenen Vorgänge nachträglich auf den Dienstweg bringt. Das Kontroll- und Aufsichtsrecht des Dienst-

vorgesetzten rechtfertigt jedenfalls nicht die Durchbrechung des Post- und Briefgeheimnisses.

Das Ministerium hat eine Änderung seiner Dienstanweisung zugesagt. Ein verbesserungsbedürftiger Entwurf liegt vor, der erkennen läßt, daß das Briefgeheimnis von Bediensteten gewahrt bleiben soll.

104

## 9. Sonstige Bereiche

### 9.1 Telefon als digitale Telekommunikationsanlage (TK-Anlage)

Zum diensteintegrierenden, digitalen Telekommunikationsnetz (ISDN) habe ich mich im Anschluß an die internationalen Konferenzen der Datenschutzbeauftragten geäußert (11. TB S. 6 und oben Tz. 1.1, 1.2 lit c). Nach einer Verlautbarung der Oberpostdirektion Saarbrücken werden im Jahre 1993 alle acht Fernvermittlungsstellen des Saarlandes digitalisiert sein, so daß "eine flächendeckende Versorgung mit ISDN gewährleistet ist" (SZ 19.04.1989).

Die Gefahren der neuen Technik liegen insbesondere darin begründet, daß Verbindungsdaten ohne größeren Aufwand, in bisher nicht praktiziertem Umfang gespeichert und ausgewertet werden können und die Bundespost bisher an der Konzeption einer umfassenden Speicherung festzuhalten gewillt ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben sich in einer grundlegenden EntschlieÙung zu dem Gefährdungspotential von ISDN geäußert (Anlage 7). Weitere Gefährdungen für das "Recht am gesprochenen Wort" ergeben sich durch neue Funktionen (Leistungsmerkmale), die das System zur Verfügung stellt.

Einen ersten Einstieg in ISDN haben verschiedene Behörden des Saarlandes durch Installierung ISDN-fähiger Telefonanlagen gewonnen. Die Landesregierung hat überdies beschlossen, die Landesbehörden Zug um Zug mit TK-Anlagen auszustatten. Wenn auch das Netz derzeit erst teilweise digitalisiert ist, können die neuartigen Funktionen jedenfalls behördenintern (in-house) bereits genutzt werden, von denen einige mit der Digitalisierung der gesamten Vermittlungs- und Übertragungstechnik regelhaft für alle Benutzer, andere wiederum jedenfalls auf Antrag zur Verfügung stehen wer-

den. Die derzeitigen behördeninternen Erfahrungen sind deshalb auch für die weitere Entwicklung von ISDN von Bedeutung.

Das Grundrecht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) schützt in "bestimmten Grenzen, ebenso wie das Recht am eigenen Bild, das Recht am gesprochenen Wort" (BVerfGE 34/238 ff), 246). Staatliche Maßnahmen, die das "Recht am eigenen Wort" (BVerfGE a.a.O. 248) unter strikter Wahrung der Verhältnismäßigkeit einschränken können, liegen nach Auffassung des Bundesverfassungsgerichts etwa im Bereich der Strafverfolgung und Rechtspflege. Auch das dienstliche Gespräch genießt den Grundrechtsschutz. Es ist die individuelle Angelegenheit des jeweiligen Gesprächspartners, in welchem Stil er kommuniziert, welche Gesprächstaktik er verfolgt, wie er sich und seine Aufgaben präsentiert. Der Schutz der unbefangenen Kommunikation muß als Grundvoraussetzung persönlicher Identitätsbildung auch bei Dienstgesprächen beachtet werden.

Im einzelnen habe ich bei der Überprüfung der TK-Anlage im Bereich des Ministeriums für Bildung und Sport sowie Wissenschaft und Kultus folgendes festgestellt:

In Chefanlagen sind die Funktionen "Konferenzschaltung" und "Lauthören" installiert, die das unbemerkte Mithören ermöglichen. Beim "Lauthören" wird die Anlage so geschaltet, daß alle im Raum Anwesenden das Gespräch beider Teilnehmer verfolgen können, ohne daß der andere Anschlußinhaber dies erkennen muß. Bei einer Konferenzschaltung können Nebenstellen beteiligt werden; auch hier ist nicht auszuschließen, daß ein sich völlig passiv verhaltender Teilnehmer lediglich zuhört, ohne daß dies von den anderen erkannt wird. Die Gefahr steigt, wenn die Zahl der zuschaltbaren Stellen erhöht wird.

In der Telefonzentrale können sich Vermittlungsplätze "aufschalten" oder ein Tonbandgerät anschließen, wodurch ebenfalls das Mithören ermöglicht wird. Beim "Aufschalten" ertönt zwar ein Signal, das jedoch in seiner Bedeutung den Bediensteten nicht bekannt war. Überdies ist die Notwendigkeit einer solchen Einrichtung nicht zu erkennen. Weniger eingriffsintensive Mittel sind vorzuziehen. Es reicht völlig aus, wenn durch ein akustisches Signal auf einen weiteren Gesprächswunsch hingewiesen wird, ohne daß die Telefonzentrale das Gespräch selbst abhört.

Die "Rufnummeranzeige" ist derzeit an 24 Geräten der Anlage möglich. Diese elektronische Version des "Spion an der Haustür" beeinträchtigt den Anrufer, weil dieser nicht selbst über seine Identifizierung durch den Angerufenen entscheiden kann. Der Angerufene seinerseits kann von sich aus das Gespräch eines Anrufers, der sich nicht zu erkennen gibt, ohne weiteres ablehnen. Die Anzeige der Rufnummer sollte der anrufende Teilnehmer jedoch unterdrücken können. Auch für öffentliche Stellen mit sensiblen dem Amts- und Berufsgeheimnis unterliegenden Funktionen, die im Interesse des freien Zugangs auf die Anonymität des Publikums Wert legen sollten, ist eine solche Möglichkeit von großer Bedeutung. Beim weiteren Ausbau von ISDN wird diese Einrichtung noch an Bedeutung gewinnen.

Gravierender ist, daß einige Funktionen, die die Anlage anbietet, zwar "gesperrt", die Möglichkeit ihrer Aktivierung jedoch nicht ausreichend gesichert war. Werden die Schutzmechanismen nicht oder unzureichend genutzt, entstehen Mißbrauchsgefahren durch Schaltung etwa folgender Leistungsmerkmale:

Die Verbindungsdaten von bestimmten Nebenstellen können in der Weise registriert ("gefangen") werden, daß sie gesondert ausgewertet werden können. Das Merkmal "Direktansprechen" in Chefanlagen kann so geschaltet

werden, daß sogar das Belauschen von Äußerungen anderer Personen in dem Raum möglich wird, in dem sich die Telefonanlage des Angerufenen befindet. Die Installation einer "Voice-box" oder die Ablage von individuellen Telefonverzeichnissen darf nur zugelassen werden, wenn ausreichende Vorkehrungen gegen unbefugten Abruf, auch mit Hilfe des Betriebsterminals, getroffen sind.

Es müssen alle durch die Anlage vorgegebenen Sicherungsmaßnahmen genutzt werden, um die mißbräuchliche Nutzung auszuschließen. Nicht hinnehmbar war, daß die Systemverwaltung durch den Hersteller wahrgenommen wurde und somit die Aktivierung aller wesentlichen Funktionen ihm überlassen waren. Den Gefahren für das "Recht am gesprochenen Wort" war deshalb nicht ausreichend vorgebeugt.

Der Umfang und die Art der Wartung der Anlage war nicht festgelegt. Dies ist insbesondere notwendig für die Fernwartung (Wartung über Telefon), die die Nutzung neuer Programme oder den Abruf von Daten - auch personenbezogener Art - aus der Anlage ermöglicht, ohne daß der Anlagenbetreiber davon Kenntnis erhält.

Die Auswertemöglichkeiten der gespeicherten Gebühren-daten für dienstliche und private Gespräche waren nicht auf den zulässigen Umfang beschränkt. Die von den Herstellern zur Verfügung gestellte Software sieht im Regelfall universelle Auswertemöglichkeiten nach jedem beliebigen Datum vor.

Der Zugang zu den Räumen, in denen Nebenstellenanlagen sowie ihre Komponenten aufgestellt sind, war nicht geregelt. Defizite dieser Art sind auch im Hinblick auf die Gefahren für die Verletzung des Fernmeldegeheimnisses sowie für die Anlagensicherheit zu beseitigen.

Die bei Inbetriebnahme der Anlage erforderliche Zustimmung des Personalrats war hinsichtlich der Organisationseinheiten aus dem Innenressort nicht eingeholt worden (§ 84 Ziff. 1, 2 und 6 SPersVG).

Als Prüfungsergebnis ist insgesamt festzuhalten:

Das "Recht am gesprochenen Wort", der Schutz der unbefangenen Kommunikation und das informationelle Selbstbestimmungsrecht", die im dienstlichen Verkehr ebenso wie bei sonstigen Telefongesprächen zu beachten sind, erfordern teilweise zusätzliche technische Vorkehrungen, die nur der Hersteller zu installieren vermag. Soweit die betreibende Stelle die Mängel nicht durch eigene Maßnahmen abzustellen vermag, habe ich darauf gedrungen, daß der Hersteller zur Entwicklung geeigneter Systemkomponenten angehalten wird. Erst recht besteht ein dringender Bedarf dieser Art im Hinblick auf den Ausbau von ISDN.

Ferner war wenigstens vorerst dafür zu sorgen, daß die Bediensteten über die Risiken und Schwächen der Anlage aufgeklärt wurden. Transparenz ist ein Mindestanfordernis.

Die Nutzung der vom Hersteller von TK-Anlagen angebotenen Leistungsmerkmale und die Datensicherung durch organisatorisch-technische Maßnahmen sind für den Behördenbereich durch generelle Anweisungen zu regeln. Ich habe den Minister der Finanzen aufgefordert, eine entsprechende Richtlinie zu erlassen.

#### 9.2 Verzeichnis (KV-Kataster) kontaminationsverdächtiger Flächen

Im Rahmen eines Forschungsprojekts erstellt der Stadtverband Saarbrücken ein Verzeichnis kontaminationsverdächtiger Flächen. Erfasst werden Standorte, an denen mit boden- und wassergefährlichen Stoffen umgegangen

wurde oder derzeit noch wird. Mit Hilfe von Adreßbüchern, Branchentelefonbüchern, Stadtplänen, historischen, zeitgenössischen Karten, Luftaufnahmen werden Produktionsbetriebe - etwa der eisenschaffenden Industrie -, Dienstleistungsunternehmen - wie Tankstellen, Reinigungsbetriebe, Reparaturwerkstätten - oder Infrastruktureinrichtungen - wie Stadtwerke, Schlachthöfe - kartographisch auf Meßtischblättern lokalisiert. Die dazugehörigen Informationen werden automatisiert gespeichert. Derzeit sind etwa 2.500 kontaminationsverdächtige Flächen in der beschriebenen Weise bearbeitet.

Die Erhebung soll zunächst dazu führen, daß Flächen dieser Art überhaupt erst einmal erfaßt werden. Die so gewonnenen Informationen sollen aufgrund von Bodenproben verdichtet und einer abschließenden Hauptbewertung zugeführt werden. Die Aufnahme einer Fläche in das Kataster signalisiert, daß ein Kontaminationsverdacht nicht auszuschließen ist, aber nicht in jedem Fall sich tatsächlich bestätigen muß. Jedenfalls kann aus der Zugehörigkeit eines Betriebs oder einer Einrichtung zur Branche allein nicht auf Grad und Intensität der Kontamination geschlossen werden.

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, worin eine nicht unerhebliche Beeinträchtigung der betroffenen Eigentümer liegt, weil der Verkehrswert des Grundstücks erheblich gemindert werden kann. Dies fällt um so mehr ins Gewicht, als die Tatsache der Wertminderung durch Kontamination nicht auszuschließen ist, im Ergebnis aber wegen der noch ausstehenden Bewertung unsicher bleibt und demnach auch das Ausmaß einer eventuellen Nutzungsbeschränkung nicht endgültig eingeschätzt werden

kann. Die sich hieraus ergebenden Unwägbarkeiten hat der betroffene Eigentümer allenfalls hinzunehmen, wenn die Einrichtung und der Dauerbetrieb eines Katasters, das auf Erhebungen ohne Einwilligung des betroffenen Eigentümers beruht, auf der Grundlage einer bereichsspezifischen gesetzlichen Regelung erfolgt. So wichtig und notwendig solche Untersuchungen und ein solches Verzeichnis im Allgemeininteresse ist, sind Eingriffe durch die Speicherung von sensiblen Informationen der beschriebenen Art nur zulässig, wenn Erhebung und Bewertungsverfahren sowie die Verwertung, insbesondere die Erteilung von Auskünften im einzelnen gesetzlich geregelt sind. Vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts sind Informationseingriffe der vorliegenden Art allein auf der Grundlage des Landesdatenschutzgesetzes nicht mehr zu rechtfertigen.

Es wird jedoch nicht verkannt, daß im Interesse eines wirksamen Umweltschutzes eine auf mehr Transparenz zielende Rechtsentwicklung wegen der Gemeinschaftsgewandtheit und -bezogenheit der Person nicht im Widerspruch zum informationellen Selbstbestimmungsrecht steht. Die Weiterentwicklung der Rechtsgrundlagen im Umweltbereich sind zudem durch das Recht der Europäischen Gemeinschaft vorgezeichnet; die Mitgliedsstaaten sind grundsätzlich zu einer die Informationsfreiheit begünstigenden Gesetzgebung verpflichtet (Richtlinie des Rates vom 07.06.1990 über den freien Zugang zu Informationen über die Umwelt EG-ABl-L 158/56). Gleichwohl kann nach der einschlägigen EG-Richtlinie die Vertraulichkeit personenbezogener Daten nicht unberücksichtigt bleiben (Art. 3 Abs. 2 a.a.O.). Um so mehr ist es notwendig, daß die Erhebungs-, Bewertungs- und Auskunftsverfahren durch den Gesetzgeber abschließend und im einzelnen geregelt werden.

Der Minister für Umwelt bereitet derzeit ein Bodenschutzgesetz vor, in dem ich gefordert habe, auch die

Verarbeitung von personenbezogenen Daten in und aus dem Kataster gesetzlich zu regeln. Ich begrüße es, daß die Landesregierung die Notwendigkeit einer solchen gesetzlichen Regelung erkannt hat und das Fachministerium derzeit den Entwurf eines solchen Gesetzes erarbeitet.

Da es sich meiner Kenntnis entzieht, ob dieser Entwurf die vom Stadtverband erarbeitete Konzeption eines KV-Katasters berücksichtigt und die Errichtung sowie den Betrieb einer kommunalen Registrierstelle der angestrebten Art abdeckt, habe ich den Minister für Umwelt um Klarstellung gebeten. Da wegen ihrer Warn- und Schutzfunktion Einrichtungen der vorgenannten Art im überwiegenden Allgemeininteresse liegen, sollte die angestrebte gesetzliche Regelung auch bereits bestehende Kataster einschließen, damit ihre Nutzung in rechtstaatlicher Weise gewährleistet ist. Sollte jedoch das Fachministerium eine gesetzliche Grundlage für das existierende KV-Kataster des Stadtverbandes Saarbrücken nicht vorsehen, muß unweigerlich die Frage nach seinem weiteren Bestand gestellt werden.

Übergangsweise können zur Abwendung einer konkreten Gefahr - etwa zum Schutz von Bewohnern, Besuchern, Kunden, Arbeitnehmern und Nachbarn - Informationen weitergegeben werden. Die Registerstelle hat die Erforderlichkeit einer solchen Offenbarung zu vertreten. Solange eine Gefahrenbeurteilung nicht durchgeführt ist, dürfen im übrigen personenbezogene Daten nur für Zwecke der Bauleitplanung und für baupolizeiliche Zwecke übermittelt werden.

### 9.3 Gefahr für das Steuergeheimnis: Steuerakten in einem Finanzamt

Wegen Raummangels wurden Akten eines Finanzamtes in zum Teil nicht mehr verschließbaren Holzrollschränken außerhalb der Dienstzimmer auf Fluren aufbewahrt. Die

Gefahr einer unbefugten Kenntnisnahme oder Entwendung von dem Steuergeheimnis unterliegenden Akten war nicht auszuschließen. Die vom Vorsteher unverzüglich eingeleiteten Maßnahmen wie Reparaturen der Holzschränke und Erlaß einer schriftlichen Anordnung, die Schränke verschlossen zu halten, war in Anbetracht der Sensibilität der Akten nicht ausreichend, zumal die Aufbewahrung der Steuerakten nicht nur vorübergehend in den Fluren erfolgte.

Holzschränke stellen keinen ausreichenden Schutz gegen mißbräuchliche Nutzung der Daten dar, da neben dem Material der Schränke insbesondere die eingebauten Schlösser Einbruchversuchen nur unzulänglich standhalten. Ich habe deshalb die Unterbringung der Akten in Blechschränken mit Sicherheitsschloß gefordert. Sowohl das Finanzamt wie die zwischenzeitlich eingeschaltete Oberfinanzdirektion teilten meine Bedenken. Da die Haushaltsmittel des Finanzamtes eine sofortige Realisierung nicht zuließen, konnten erst Ende 1990 die erforderlichen Schränke aufgestellt werden. Bis zum Redaktionsschluß dieses Berichtes waren fast alle Akten in die neuen Schränke umgeräumt.

#### 9.4 Technischer Überwachungsverein (TÜV)

Aufgrund einer Eingabe habe ich das medizinisch-psychologische Institut (MPI) des TÜV-Saarland überprüft. Dieses Institut ist eine amtlich anerkannte Untersuchungsstelle, die bei der Prüfung der Wiederteilung einer Fahrerlaubnis an alkoholauffällige Kraftfahrer gutachterlich tätig wird.

Grundlage des Gutachtens sind ein vom Probanden auszufüllender Fragebogen zum Verkehrsverständnis, zur Vorfahrtsberechtigung und zum logischen Denkvermögen, ein psychologisches Einzelgespräch etwa zu Trinkgewohnheiten und zur persönlichen Situation sowie eine allgemeine medizinische Untersuchung. Als abschließen-

de Bewertung kommen die Merkmale positiv (keine Probleme), negativ/Nachschulung (leichte Fälle) oder negativ/Beratungsstelle in Betracht.

Die Ergebnisse werden in Akten erfaßt, aber auch edv-mäßig aufbereitet. Die Löschung der Daten wird nicht automatisch überwacht.

Ich habe gefordert, daß bei empfohlener Nachschulung auf die Freiwilligkeit der Teilnahme hinzuweisen, sowie deutlich zu machen ist, daß es den Betroffenen freisteht, an einer Gruppennachschulung des Instituts teilzunehmen oder aber Einzelgespräche zu wählen. Auch ein Hinweis auf das Recht, eine Nachschulung abzubrechen, erschien mir geboten.

Hinsichtlich der automatisierten Verarbeitung habe ich angemahnt, daß die Dateien mir zu melden sind. Die Speicherung von Einzelbefunden unter dem Stichwort "Zusatzbefund" habe ich vor allem wegen der Unbestimmtheit dieses Begriffs für nicht zulässig gehalten. Die Erforderlichkeit eines solchen Kriteriums war nicht gegeben, weil der Gutachter ohnehin die zugrundeliegenden Akten einsehen muß, wenn er ein zutreffendes Bild von dem Probanden gewinnen will. Schließlich habe ich gefordert, daß die noch nicht vollständige Dokumentation des EDV-Verfahrens fertiggestellt wird.

Wenn auch der TÜV als Träger des Instituts - anders als ich - die Auffassung vertritt, das MPI sei keine öffentliche Stelle im Sinne des SDSG und falle deshalb nicht in den Anwendungsbereich des Gesetzes, so hat es sich doch meine Forderungen und Anregungen zu eigen gemacht. Einige sind bereits umgesetzt, die Anmeldung zum Register, die Konkretisierung der Löschungskriterien, sowie eine Vervollständigung der Dokumentation erwarte ich demnächst.

### 9.5 Benennung von Zeugen bei der Verfolgung von Ordnungswidrigkeiten

Ein Petent hatte darunter zu leiden, daß häufig parkende Kraftfahrzeuge die Zufahrt zu seiner Garage versperren, so daß er sich veranlaßt sah, Anzeigen zu erstatten.

Im Rahmen des dann eingeleiteten Ordnungswidrigkeitenverfahrens ging den Beanzeigten ein Verwarnungsgeldangebot und ein Anhörbogen zu, der den Verkehrsverstoß benannte und als Beweismittel den Petent als Anzeiger und Zeugen angab. Auf diese Tatsache führte der Petent Repressalien durch die Nachbarschaft wie Drohungen und Beschmieren der Hauswand zurück. Er wollte erreichen, daß auf die Mitteilung des Zeugen in diesem Verfahrensstadium verzichtet wird.

Im Hinblick darauf, daß die Benennung des Zeugen dessen verfassungsrechtlich geschützten Persönlichkeitsrechte berührt, hat das Ministerium des Innern auf meine Anregung hin die Bußgeldstellen angewiesen, im Einzelfall und auf Wunsch des Zeugen zunächst auf dessen Benennung zu verzichten und lediglich den allgemeinen Hinweis aufzunehmen, daß als Beweismittel ein Zeuge zur Verfügung steht.

In der Folge hatte ich dann Anlaß, der Frage nachzugehen, ob die Benennung des Zeugen im Bußgeldbescheid - aber auch im Anhörbogen oder Verwarnungsgeldangebot, wenn der Wunsch nach völliger Geheimhaltung nicht geäußert wird - die Wohnanschrift beinhalten muß oder ob die Namensnennung ausreicht. Dabei muß neben dem Recht des Beanzeigten auf ein faires Verfahren auch das verfassungsrechtlich geschützte Persönlichkeitsrecht des Zeugen berücksichtigt werden. Im Hinblick darauf, daß sich die Verteidigungsmöglichkeiten durch die Mitteilung der Anschrift nicht verbessern, habe ich diese Angabe nicht für erforderlich gehalten.

Den schutzwürdigen Interessen sowohl des Beanzeigten als auch des Anzeigers wird durch die namentliche Benennung ohne Wohnanschrift in angemessener Weise Rechnung getragen. Ich habe meine Auffassung dem Ministerium des Innern vorgetragen mit der Bitte, entsprechend zu verfahren.

Anlage 1

## E n t s c h l i e ß u n g

der 39. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. März 1990 zum Bundesdatenschutzgesetz und zum Bundesverfassungsschutzgesetz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz (gegen die Stimme Bayerns) begrüßt die mit den am 13.03.1990 vorgelegten Vorschlägen der Koalitionsfraktionen verbundene Absicht, die längst fällige Novellierung des Bundesdatenschutzgesetzes und des Bundesverfassungsschutzgesetzes noch rechtzeitig vor dem Ende der Legislaturperiode zu verabschieden.

Die Vorschläge zum Bundesdatenschutzgesetz beseitigen eine Reihe von Schwächen des Regierungsentwurfes. Hervorzuheben ist insoweit

- daß nunmehr für den öffentlichen Bereich die Verarbeitung personenbezogener Daten in Akten und die Datenerhebung durch öffentliche Stellen in den Geltungsbereich des Bundesdatenschutzgesetzes einbezogen werden,
- daß künftig der Bundesbeauftragte für den Datenschutz durch das Parlament gewählt werden soll,
- daß der Betroffene bei Ablehnung der Auskunftserteilung darauf hingewiesen wird, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

Demgegenüber weisen auch die Vorschläge noch Schwächen und Defizite auf. Dazu gehören u.a.:

- Die unzureichende Kontrollbefugnis des Bundesbeauftragten für den Datenschutz bei der Datenverarbeitung in Akten,
- ein Widerspruchsvorbehalt für die Betroffenen gegen eine Kontrolle ihrer Daten durch den Bundesbeauftragten für den Datenschutz, der systematische Prüfungen gefährdet und deshalb entbehrlich ist, weil es für die Datenschutzbeauftragten schon immer selbstverständlich war, die Daten von Betroffenen nicht gegen deren erklärten Willen in Kontrollen einzubeziehen,
- die verfassungswidrige Erstreckung des Widerspruchsvorbehaltes in der Neufassung auf die Landesbeauftragten für den Datenschutz,
- das Fehlen eines gesonderten Gesetzesvorbehaltes für die Einrichtung von Direktzugriffsverfahren in besonders sensiblen Bereichen,
- der zu weite Katalog erlaubter Zweckänderungen und die unzureichende Unterrichtung des Betroffenen über die Zweckänderung.

Im Bereich der Datenverarbeitung durch nichtöffentliche Stellen verschlechtern einzelne vorgeschlagene Regelungen die Rechte der Betroffenen im Vergleich zum geltenden Gesetz, etwa bei der Übermittlung von Daten an den Adressenhandel. Sie bleiben im übrigen weit hinter den Vorschlägen für den öffentlichen Bereich zurück. Weder die Verarbeitung in Akten noch die Datenerhebung werden einbezogen. Auch die höchst unzureichenden Kontrollbefugnisse der Datenschutzaufsichtsbehörden sind nicht wesentlich verbessert worden.

Schließlich erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen für die Verarbeitung von Arbeitnehmerdaten sowie von Regelungen für den Kredit- und Versicherungsbereich.

Zu den Vorschlägen der Koalition für das Bundesverfassungsschutzgesetz stellen die Datenschutzbeauftragten des Bundes und der Länder fest:

Die Vorschläge bringen gegenüber dem Vorentwurf der Bundesregierung Verbesserungen. Dies gilt insbesondere für:

- Den Schutz des in Wohnungen nichtöffentlich gesprochenen Wortes vor heimlichem Mithören und Aufzeichnen,
- die Einschränkung der Speicherung von Daten über Minderjährige,
- die konkretisierenden und einschränkenden Regelungen für den Einsatz nachrichtendienstlicher Mittel,
- die präzise Definition der "Bestrebungen" gegen die freiheitlich-demokratische Grundordnung,
- die Anknüpfung der Sammlung und Verarbeitung von Daten an das Vorliegen tatsächlicher Voraussetzungen.

Hingegen sind u.a. folgende datenschutzrechtliche Anforderungen noch nicht erfüllt:

- Die Befugnisse zur Datenverarbeitung müssen differenziert den unterschiedlichen Aufgaben zugeordnet werden.

- Die Datenspeicherung ist nicht so präzise geregelt, daß er Bürger dem Gesetz entnehmen kann, unter welchen in seiner Person liegenden Voraussetzungen der Verfassungsschutz über ihn Daten speichern darf.
- Die Zweckbindung der Daten innerhalb des Verfassungsschutzes ist nicht gewährleistet.
- Das Auskunftsrecht des Bürgers auch gegenüber den Verfassungsschutzbehörden wird zwar nummehr erstmals anerkannt.

Die vorgeschlagene Regelung schränkt aber den Auskunftsanspruch zu sehr ein. So wird dem Bürger eine Pflicht zur Begründung seines Auskunftsersuchens auferlegt, während die Ablehnung der Auskunft unter keinen Umständen begründet werden muß.

- Die vorgesehenen Regelungen zur Sicherheitsüberprüfung ersetzen nicht eine bereichsspezifische, präzise Rechtsgrundlage in einem Geheimschutzgesetz für das Überprüfungsverfahren.

Die Datenschutzbeauftragten gehen davon aus und halten es für notwendig, daß die bestehenden Mängel der Gesetzentwürfe in den anstehenden Parlamentsberatungen behoben und ihre Anregungen aufgegriffen werden.

Anlage 2

## E n t s c h l i e ß u n g

der 12. Internationalen Konferenz  
der Datenschutzbeauftragten  
in Paris (19. September 1990)  
zu Problemen öffentlicher Telekommunikationsnetze  
und des Kabelfernsehens  
(Übersetzung)

Nachdem die XI. Internationale Konferenz der Datenschutzbeauftragten in ihrer EntschlieÙung vom 31. August 1989 allgemeine Grundsätze zu dienste-integrierenden digitalen Netzen (ISDN) aufgestellt hat, begrüÙt sie den zweiten Bericht der Arbeitsgruppe "Telekommunikation und Medien", der zeigt, daÙ diese Grundsätze konkretisiert und auf der technischen Ebene garantiert werden sollten. Diese Grundsätze sind auf jede Form der Telekommunikation einschließlich analoger Formen und bestimmter Formen massenmedialer Kommunikation (insbesondere Kabelfernsehen) anzuwenden. Öffentliche und private Netzbetreiber sollten diese Prinzipien ebenso verwirklichen wie Anbieter von Telekommunikationsdiensten.

## I.

## Teilnehmerverzeichnisse

Verzeichnisse von Teilnehmern an Telekommunikationsdiensten sind inzwischen weltweit die wichtigsten öffentlich verfügbaren personenbezogenen Dateien. Die Konferenz stellt mit Sorge fest, wie schwierig es ist, die Nutzung dieser Daten weltweit zu kontrollieren. Die Risiken nehmen durch den Verkauf der Teilnehmerverzeichnisse auf elektronischen Datenträgern zu.

Personenbezogene Daten, die von Netzbetreibern erhoben und gespeichert werden, müssen dem Zweck entsprechen, dem Betroffenen einen Telekommunikationsdienst zur Verfügung zu stellen und ihm den Zugang zum Netz zu ermöglichen; die Daten müssen für diesen Zweck erheblich sein und dürfen nicht darüber hinausgehen.

Ein Teilnehmerverzeichnis sollte nur solche personenbezogenen Daten enthalten, die unbedingt zur hinreichend sicheren Identifikation bestimmter Teilnehmer erforderlich sind. Die Teilnehmer haben auch das Recht, einen Hinweis auf ihr Geschlecht (und auf ihren Wohnort)\* auszuschließen. Andererseits schließt dies die Veröffentlichung zusätzlicher Daten auf Wunsch des Teilnehmers nicht aus.

Teilnehmer haben das Recht, gebührenfrei und ohne Begründung den Eintrag ihrer Daten in ein Teilnehmerverzeichnis auszuschließen.

Bei der Erhebung von Bestandsdaten sollte der Netzbetreiber den Betroffenen vollständig darüber aufklären, ob er zur Aufnahme seiner Daten in ein Teilnehmerverzeichnis unabhängig von der Form der Veröffentlichung verpflichtet ist oder nicht.

Bestandsdaten, die einen Mitbenutzer des Endgerätes betreffen, dürfen nur mit dessen Zustimmung in ein Teilnehmerverzeichnis aufgenommen werden.

Die Weitergabe von Bestandsdaten durch einen Netzbetreiber an Dritte zu Werbezwecken darf nur mit der freiwilligen und informierten Zustimmung des Betroffenen erfolgen, es sei denn, dieser hat nach innerstaatlichem Recht die Möglichkeit, der Weitergabe zu widersprechen.

Bestandsdaten von Teilnehmern, die einen Eintrag in das Teilnehmerverzeichnis ausgeschlossen oder sich entschieden haben, ihren Namen nicht für Werbezwecke nutzen zu lassen, sollten in keinem Fall an Dritte weitergegeben werden.

Besondere Aufmerksamkeit muß der höchsten räumlichen Ebene gewidmet werden, auf der dem Verzeichnis Teilnehmerdaten entnommen werden können.

Die Konferenz betrachtet mit Sorge die wachsenden Gefahren der telefonischen Direktwerbung und wird diese Probleme eingehender untersuchen.

## II.

### Anzeige der vom Anrufer benutzten Rufnummer

Die Einführung einer Einrichtung, die die Anzeige der Nummer des vom Anrufer benutzten Anschlusses am Endgerät des angerufenen Teilnehmers vor der Herstellung der Verbindung ermöglicht, wirft ernste Fragen des Schutzes der Privatsphäre auf.

Es ist wichtig, den Schutz der Privatsphäre des einzelnen Teilnehmers - der anrufenden und der angerufenen Person - mit den Erfordernissen der Kommunikationsfreiheit in Einklang zu bringen. Dies wird durch die Beachtung der folgenden Grundsätze erreicht:

Der Anrufer muß die Möglichkeit haben, durch eine einfache technische Vorrichtung im Einzelfall zu entscheiden, ob er seine Rufnummer anzeigen lassen will oder nicht, auf die Gefahr hin, daß sein Anruf von der angerufenen Person nicht entgegengenommen wird.

Dieses Verfahren zur Unterdrückung der Rufnummernanzeige muß für den Teilnehmer gebührenfrei sein.

Bei der Anwendung dieser Grundsätze sollen die folgenden Maßnahmen getroffen werden:

Teilnehmer müssen das Recht haben, gebührenfrei in das Teilnehmerverzeichnis einen Hinweis darauf aufnehmen zu lassen, daß sie kein Verfahren zur Anzeige der vom Anrufer benutzten Rufnummer anwenden.

Es ist notwendig, die Offenbarung übermittelter Informationen über den Anrufer an Dritte einzuschränken.

Ausnahmsweise darf die Unterdrückung der Rufnummernanzeige entsprechend dem innerstaatlichen Recht außer Kraft gesetzt werden, wenn Personen über Notruf die Feuerwehr oder den Notarzt anrufen.

Der Netzbetreiber kann die Unterdrückung der Rufnummernanzeige auch außer Kraft setzen, um auf Antrag der angerufenen Person den Urheber belästigender Anrufe festzustellen.

Diese Grundsätze sollen bei der Abwicklung internationaler Telefongespräche in gleicher Weise beachtet werden.

### III.

#### Mobilfunk

Netzbetreiber, die ein Mobilfunknetz betreiben und anbieten, sollten Teilnehmer über die Sicherheitsrisiken informieren, die normalerweise - insbesondere bei fehlender Verschlüsselung der übermittelten Nachrichten - mit der Benutzung eines Mobilfunknetzes verbunden sind. Der Betreiber sollte dem Teilnehmer vor allem empfehlen, das Mobilfunknetz nicht zur Übermittlung vertraulicher Nachrichten zu benutzen, solange Probleme der Datensicherheit bestehen.

Netzbetreiber sollten verpflichtet sein, den Teilnehmern am Mobilfunknetz wirksame Verschlüsselungsverfahren anzubieten.

Wirksame technische Vorkehrungen sollen getroffen werden, um den unbefugten Netzzugang über mobile Endgeräte zu verhindern.

Die Speicherung von Verbindungsdaten muß strikt auf den kurzen Zeitraum des Verbindungsaufbaus zwischen Teilnehmer und Netz beschränkt werden. Das Tariffsystem soll so gestaltet werden, daß die Orte, an denen Mobiltelefone benutzt worden sind, nicht Teil der Abrechnungsdaten sind. Besondere Beachtung verdient die Frage, inwieweit die Speicherung der vollständigen Rufnummer der angerufenen Person für Abrechnungszwecke notwendig ist.

#### IV.

##### Gebührenabrechnung

Inwieweit die Speicherung der vollständigen Nummer des angerufenen Teilnehmers für Zwecke der Gebührenabrechnung im allgemeinen erforderlich ist, sollte noch näher untersucht werden.

#### V.

##### Kabelfernsehen

Die Speicherung individueller Zuschauerprofile durch Kabelfernsehgeseilschaften, die einzeln abrufbare ("pay per view") Programme anbieten, ist ein Eingriff in die Privatsphäre des Kunden.

Deshalb sollten Kabelfernsehgeseilschaften "pay per view"-Programme nur dann anbieten, wenn die Kunden eine praktikable und wirtschaftliche Möglichkeit (z.B.

im voraus bezahlte Karten oder Decoder) haben, die Programme zu empfangen, ohne daß zuschauerbezogene Informationen gespeichert werden.

Messungen der Sehbeteiligung und Tantiemen dürfen nicht auf der Grundlage zuschauerbezogener Daten berechnet werden.

Die Konferenz befürchtet, daß in naher Zukunft im Bereich des Kabelfernsehens zahlreiche Datenschutzprobleme entstehen werden und wird die Entwicklung deshalb eingehend überwachen.

\* bezüglich des Klammerzusatzes bestehen unterschiedliche Auffassungen

Anlage 3

## E n t s c h l i e ß u n g

der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29.01.1991 zum Vorschlag der EG-Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

## I.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem "informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

## II.

Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den "Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1980 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt aller-

dings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

### III.

Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinienentwurf aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

### IV.

Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienentwurf für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in "Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.
2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf

die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet; die Transparenz des Datenumgangs geht für den einzelnen verloren.

3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.
4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur "nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.
5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem "angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländer übersichtlich und praktikabel auszugestalten.

6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene "Gruppe für den Schutz personenbezogener Daten" erfüllt - betrachtet man ihre Struktur, Aufgaben und Kompetenzen - diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser - aus den nationalen Datenschutzorganen zusammengesetzten - "Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der "Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der "Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.

7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.

Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.

Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlages führen wird. Die Konferenz wird diese EntschlieÙung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

Anlage 4

## E n t s c h l i e ß u n g

der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis

1. Das Engagement der Bevölkerung in der DDR für den Schutz ihrer personenbezogenen Daten z.B. beim Staatssicherheitsdienst zeigt, wie elementar die Persönlichkeitsrechte von den Bürgern in der DDR verstanden werden und daß sie das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Selbstbestimmungsrechts wahrnehmen.

Die Konferenz der Datenschutzbeauftragten begrüßt Bemühungen, auch in der DDR angemessene Datenschutzregelungen zu schaffen.

2. Obwohl in der DDR keine hinreichenden Datenschutzregelungen bestehen, werden bereits jetzt mehr personenbezogene Daten als früher ausgetauscht. Dieser Datentransfer wird noch zunehmen. Aktuelle Anlässe, wie der Austausch von Daten bei Verkehrsunfällen, sowie im Rahmen der Gefahrenabwehr und der Strafverfolgung haben in der Öffentlichkeit besondere Aufmerksamkeit gefunden.

Der Prozeß der sozialen, wirtschaftlichen und politischen Einigung führt zu verstärktem grenzüberschreitenden Datenverkehr, z.B. im Sozialrecht, im Melderecht, im Versicherungs- und Kreditrecht. Dies wirft Fragen des Datenschutzes auf. Für die Bundesrepublik gelten das allgemeine Datenschutzrecht und besondere Gesetze wie z.B. das Gesetz über die

innerdeutsche Rechts- und Amtshilfe in Strafsachen vom 2. Mai 1953 sowie Vereinbarungen.

Bei der Verwirklichung technischer Maßnahmen insbesondere bei dem Ausbau der Telekommunikationsdienste und bei der automatisierten Datenverarbeitung muß der Datenschutz beachtet werden.

3. Die Datenschutzkonferenz hält es für geboten, daß der Austausch personenbezogener Daten zwischen Behörden und öffentlichen Stellen in der Bundesrepublik Deutschland und in der Deutschen Demokratischen Republik erst durchgeführt wird, wenn gewährleistet ist, daß nach folgenden Grundsätzen verfahren wird:

- Die Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der Verarbeitung personenbezogener Daten vom 28. Januar 1981 sind zu beachten.
- Die Übermittlung personenbezogener Informationen unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines Gesetzes der Bundesrepublik Deutschland verstoßen würde oder schutzwürdige Belange bei den betroffenen Personen beeinträchtigt würden. Die Übermittlung personenbezogener Informationen unterbleibt insbesondere dann, wenn Grund zu der Annahme besteht, daß die Verwendung der übermittelten Informationen nicht in Einklang mit rechtsstaatlichen Grundsätzen steht oder dem Betroffenen aus der Verwendung der Informationen erhebliche Nachteile erwachsen, die im Widerspruch zu rechtsstaatlichen Grundsätzen stehen.

- Der Empfänger darf personenbezogene Informationen nur zu dem durch die übermittelnde Stelle angegebenen Zweck und unter den von ihr vorgeschriebenen Bedingungen nutzen.
- Personenbezogene Informationen dürfen ausschließlich an die in den Abkommen oder Absprachen genannten Behörden übermittelt werden. Eine Übermittlung an andere Stellen darf nur mit vorheriger Zustimmung der übermittelnden Stelle erfolgen.
- Der Empfänger unterrichtet die übermittelnde Stelle und den zuständigen Datenschutzbeauftragten auf Ersuchen über die Verwendung der übermittelten Informationen und über die dadurch erzielten Ergebnisse.
- Die übermittelnde Stelle ist verpflichtet, auf die Richtigkeit der zu übermittelnden Informationen zu achten. Erweist sich, daß unrichtige oder zu vernichtende personenbezogene Informationen übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. Dieser ist verpflichtet, die Berichtigung oder Vernichtung vorzunehmen.
- Dem Betroffenen ist auf Antrag über die zu seiner Person vorhandenen Informationen sowie über den vorgesehenen Verwendungszweck Auskunft zu erteilen. Eine Verpflichtung zur Auskunftserteilung besteht nicht, soweit eine Abwägung ergibt, daß eine Auskunft den Verwendungszweck oder schutzwürdige Interessen Dritter gefährden würde.
- Die Übermittlung und der Empfang personenbezogener Informationen sind aktenkundig zu machen.

- Zur Gewährleistung dieser Grundsätze sind die verfahrensmäßigen Sicherungen vorzusehen. Dazu kann es gehören, besondere Stellen mit der Datenübermittlung zu beauftragen. Die Kontrolle der Datenübermittlung durch unabhängige Datenschutzbeauftragte muß gewährleistet sein.
4. Die Verarbeitung personenbezogener Daten bei den Sicherheitsbehörden der Bundesrepublik Deutschland muß im Hinblick auf die politischen Veränderungen in der DDR und im übrigen Mittel- und Osteuropa über die bereits getroffenen Maßnahmen hinaus überprüft werden. Diese Notwendigkeit besteht u.a. bei:
- dem Verfahren der Sicherheitsüberprüfung,
  - der Datenerhebung und Datenübermittlung des Bundesgrenzschutzes anlässlich von Grenzkontrollen an die Nachrichtendienste,
  - der Bereinigung der Datensammlungen der Verfassungsschutzbehörden.

Anlage 5

## E n t s c h l i e ß u n g

der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Neuregelung des Melderechtsrahmengesetzes

Der dem Deutschen Bundestag vorliegende Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes hält weiter an der Hotel- und Krankenhausmeldepflicht fest. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz hat erhebliche Bedenken, ob dem Bund die Gesetzgebungskompetenz zur Regelung dieser Frage zusteht. In jedem Fall ist zu bedenken:

Zweck der allgemeinen Meldepflicht ist es, die Identität der Einwohner und deren Wohnungen festzustellen und diese Basisinformation für die Bewältigung einer Vielzahl von Verwaltungsaufgaben zur Verfügung zu stellen. Bei einem kurzfristigen Aufenthalt in einem Hotel oder Krankenhaus entfällt dieser Zweck. Lediglich die Polizei hat ein Interesse an der Feststellung dieser Tatsachen. Schon deshalb paßt die Hotel- und Krankenhausmeldepflicht nicht in die Systematik des Melderechts, es handelt sich vielmehr um materielles Polizeirecht.

Polizeiliche Datenverarbeitung setzt voraus, daß Gefahren abgewendet oder Straftaten verfolgt bzw. verhütet werden sollen. Hotelgäste und Krankenhauspatienten können jedoch nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen werden. Vielmehr ist zu berücksichtigen, daß es sich im Regelfall

um Bürger handelt, die ein Recht darauf haben, von polizeilichen Ermittlungen unbehelligt zu bleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz ist darüber hinaus der Auffassung, daß den Bürgern in allen Meldegesetzen ein Widerspruchsrecht gegen die Weitergabe ihrer Daten an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung eingeräumt werden muß.

Anlage 6

## E n t s c h l i e ß u n g

der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund oder Ländern

1. Die Datenschutzbeauftragten haben schon in ihren Entschlüssen vom 14. Dez. 1981 und 27. April 1982 zur Schaffung gesetzlicher Grundlagen für die Errichtung und Führung bevölkerungsbezogener epidemiologischer Krebsregister Stellung genommen. Wenn sich der Gesetzgeber zugunsten solcher Register, deren Nutzen auch unter Medizinern nicht unumstritten ist, entscheiden sollte, entspricht es dem gesetzlichen Auftrag der Datenschutzbeauftragten darauf zu achten, daß die Errichtung und Führung solcher Register in einer Weise geschieht, die auf das Persönlichkeitsrecht der Krebskranken in größtmöglichem Umfang Rücksicht nimmt.
2. Würde den Ärzten die Befugnis eingeräumt, ihre Krebskranken in jedem Fall ohne deren Einwilligung mit Namen an ein solches Register zu melden, würde dies einen äußerst schwerwiegenden Eingriff in deren durch Art. 1 i.V.m. Art. 2 Abs. 1 GG geschütztes Persönlichkeitsrecht darstellen, eine weitere Durchbrechung der ärztlichen Schweigepflicht zur Folge haben und damit das Arzt-/Patientenverhältnis erheblich belasten. Die Krebskranken würden ohne ihre Einwilligung zentral in einem Register gespeichert werden und zwar so, daß die registerführende Stelle feststellen kann, welche Personen an Krebs erkrankt und zum Register gemeldet worden sind.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß die Einrichtung eines Krebsregisters auf einer solchen Grundlage (Melderechtsmodell) nicht in Betracht kommt.

Sie sind nach wie vor der Meinung, daß das Krebsregister nur mit Einwilligung der Patienten oder auf anonymer Basis geführt werden können. Für beides gibt es bereits Modelle (Einwilligungsmodell und dezentrales Verschlüsselungsmodell). Die Datenschutzbeauftragten sehen in diesen Modellen gangbare Wege zur Führung bevölkerungsbezogener Krebsregister, die auch noch fortentwickelt werden können.

Sollten weitere Modelle, die das Persönlichkeitsrecht der Krebskranken in gleicher Weise wahren, weiterentwickelt werden, sind die Datenschutzbeauftragten selbstverständlich bereit, auch sie in Erwägung zu ziehen.

Anlage 7

## E n t s c h l i e ß u n g

der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes

Wegen der dynamischen technischen Entwicklung auf dem Gebiet der Telekommunikation ist es dringlich, das Grundrecht auf freie Entfaltung der Persönlichkeit gegen neue Gefährdungen zu schützen. Den Risiken für das Recht auf unbeobachtete Kommunikation muß rechtzeitig begegnet werden:

- Die Einführung von ISDN macht es möglich, daß auch nach Beendigung von Telefongesprächen über einen bestimmten Zeitraum gespeichert wird, wer wann mit wem wie lange telefoniert hat.
- Der zunehmende Einsatz von Funkdiensten im Telekommunikationsverkehr (z.B. mobile Telefone, Satellitenkommunikation) ist mit der Speicherung von noch mehr Daten über die Telefonverbindungen verbunden und erleichtert die Möglichkeit des Abhörens und Aufzeichnens der Gesprächsinhalte.
- Zunehmend stehen Abhöranlagen zur Verfügung, mit denen aus der Masse der geführten Telefongespräche bestimmte Telefonate gezielt herausgegriffen, aufgezeichnet und nach bestimmten Gesichtspunkten ausgewertet und gespeichert werden können.

Das Grundgesetz läßt Einschränkungen des Fernmeldegeheimnisses unter gewissen Voraussetzungen auf gesetzlicher Grundlage zu. In den vergangenen Jahren hat der Gesetzgeber diese Eingriffsmöglichkeiten mehrmals erweitert und hierbei alle Telekommunikationsdienste (wie z.B. Telefax und Btx) einbezogen. Zudem hat die Rechtsprechung den Anwendungsbereich extensiv ausgelegt. Vor diesem Hintergrund ist es erforderlich:

- Die gesetzlichen Regelungen präziser und enger zu fassen,
- bei Entwicklung, Auswahl und Einsatz von Telekommunikationstechniken darauf zu achten, daß bei deren Betrieb die Speicherung personenbezogener Daten nach Dauer und Umfang auf das wirklich Notwendige beschränkt wird,
- erlaubte Eingriffe in das Grundrecht nach Art. 10 auf das unerläßliche Maß zu beschränken und eine strenge Zweckbindung der dabei gewonnenen Daten sicherzustellen,
- eine wirksame Kontrolle solcher Eingriffe durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

Neben die Ausweitung der Möglichkeiten der Überwachung der Telekommunikation treten zunehmend weitere Techniken der heimlichen Datenerhebung (z.B. durch Videoaufnahmen, Abhörgeräte, Richtmikrofone), durch die das Recht auf ungestörte Kommunikation auch außerhalb des Fernmeldebereiches gefährdet ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, daß der Gesetzgeber diesen Gefährdungen des Rechts auf informationelle Selbstbestimmung seine Aufmerksamkeit zuwendet. Sie unterstützt in diesem Zusammenhang die Einwände der Bundes-

regierung in deren Stellungnahme zum Gesetzentwurf des Bundesrates zur Bekämpfung der organisierten Kriminalität. Die Datenschutzbeauftragten sehen in der Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes einen Schwerpunkt ihrer weiteren Arbeit.