

ELFTER 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 1989 bis 31. Dezember 1989)

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

	Seite
<u>Vorbemerkung</u>	1
1. <u>Grenzüberschreitende Informations- verarbeitung</u>	3
1.1 Infrastruktur und Mobilität	3
1.2 Berliner Resolution der Internatio- nalen Konferenz der Datenschutz- beauftragten	4
1.3 Dienstintegrierendes, digitalisiertes Kommunikationsnetz (ISDN)	6
1.4 Datenschutz in der Europäischen Gemeinschaft (EG)	8
1.5 Telekommunikation im Saarland	11
1.6 EG-Statistikverordnung	12
1.7 Abbau der Grenzkontrollen (Schengener Abkommen)	12
2. <u>Bürokommunikation</u>	16
3. <u>Polizei</u>	24
3.1 Die Neuregelung des Saarländischen Polizeigesetzes - SPolG	24
3.2 Neues Polizeiinformationssystem-DIPOL	28
3.3 Informationsverarbeitung im Bereich der Kriminalpolizei	37
3.3.1 Das neue Datenschutzkonzept für das Kriminalpolizeiamt (KPA)	37
3.3.2 PC-Einsatz	40
3.4 Überprüfung eines Polizeireviers	42
3.4.1 Schankkonzessionsdatei	42
3.4.2 Direktzugriff auf das computerisierte Melderegister	44
3.5 Datenschutz in Notruffällen	48

4.	<u>Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes</u>	50
4.1	Novellierung des Bundesdatenschutzgesetzes	50
4.2	Rechtsgrundlagen für die Nachrichtendienste	51
5.	<u>Rechtspflege</u>	54
5.1	Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts	54
5.2	Novellierung des Bundeszentralregistergesetzes	56
5.3	Telefonabhördaten	57
5.4	Aktenübersendung durch die Staatsanwaltschaft	61
5.5	Akteneinsicht für Forschungszwecke	63
5.6	Organisationsuntersuchung bei den Gerichten	64
5.7	Automation im Justizbereich	65
6.	<u>Gesundheit</u>	67
6.1	Maßregelvollzugsgesetz	67
6.2	Gesundheitsamt	69
6.3	Arztbericht an den Betriebsarzt	78
6.4	AIDS-Modellprogramm "Sozialstationen"	78
6.5	Mutterpaß	80
6.6	PC-Einsatz in den Universitätskliniken Homburg	81
7.	<u>Sozialwesen</u>	84
7.1	Rentenreformgesetz	84
7.2	Kinder- und Jugendhilfegesetz	85
7.3	Vertrauensärztlicher Dienst	86
7.4	Sozialpädagogische Familienhilfe	87
7.5	Adoptionsvermittlung	89

7.6	Sozialgeheimnis und Akteneinsichtsrecht des Betroffenen im Wohngeldverfahren	91
7.7	Weitergabe der ärztlichen Verordnung über Orthopädiehilfsmittel durch die AOK an andere orthopädische Fachgeschäfte	93
8.	<u>Statistik und Umfragen</u>	96
8.1	Saarländisches Landesstatistikgesetz	96
8.2	Bürgerumfrage der Landeshauptstadt Saarbrücken	97
8.3	Fragebogenaktion "Energiekonzept"	98
8.4	Umweltumfrage A.U.G.E.	100
9.	<u>Genomanalyse</u>	103
10.	<u>Öffentlicher Dienst</u>	110
10.1	Novellierung des Personalaktenrechts	110
10.2	Zentralisierung und Automatisierung der Beihilfebearbeitung	111
10.3	Telefonnebendaten	113
11.	<u>Probleme aus sonstigen Bereichen</u>	115
11.1	Kontrollmitteilungen an die Steuerbehörden	115
11.2	Auswertung von "Kurmeldescheinen"	116
11.3	Weiterleitung der Todesanzeigen durch die Standesbeamten an das Nachlaßgericht	117
11.4	Benachrichtigung bei der Einschulung	118
11.5	Entsorgung von Aktenmaterial durch eine Rechtsanwaltskanzlei	119
11.6	Auskunftersuchen eines Anwalts gegenüber der Kfz-Zulassungsstelle	119
11.7	Gebäudezusatzerhebung der Stadt Saarbrücken im Zusammenhang mit der Volkszählung'83	120

- | | | |
|------|--|-----|
| 11.8 | Änderung des Gesetzes zu Artikel 10 GG
und der Strafprozeßordnung im Rahmen
der Poststrukturreform | 121 |
| 11.9 | Versendung von Anfragen der Landrats-
ämter an den Verfassungsschutz | 122 |

A n l a g e n v e r z e i c h n i s

- Anlage 1: Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 Seite 124
- Anlage 2: EntschlieÙung der Elften Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 über die Arbeitsgruppe Medien Seite 127
- Anlage 3:: EntschlieÙung der Elften Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 zu den Problemen des ISDN Seite 129
- Anlage 4: Zusatzerklärung der Datenschutzbeauftragten der EG-Länder Seite 133
- Anlage 5: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 über den Datenschutz in der Europäischen Gemeinschaft Seite 135
- Anlage 6: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 zum Entwurf einer EG-Statistikverordnung Seite 138
- Anlage 7: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 zum

Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen Seite 140

Anlage 8: Bericht des Ausschusses für Innere Verwaltung (Landtag des Saarlandes) über die Beratung des gemäß § 20 Abs. 3 Satz 2 SDSG vorgelegten achten und neunten Berichts über die Tätigkeit des Landesbeauftragten für Datenschutz (Lt-Drucksache 9/1038-9/1521) Seite 144

Anlage 9: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zur Neuregelung des Bundesdatenschutzgesetzes Seite 151

Anlage 10: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 30.05.1989 zu den Entwürfen eines Bundesverfassungsschutzgesetzes (BVerfSchG), eines MAD-Gesetzes (MADG) und eines BND-Gesetzes (BNDG) Seite 153

Anlage 11: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (Strafverfahrensänderungsgesetz vom 03.11.1988) Seite 158

- Anlage 12: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zum Entwurf eines Rentenreformgesetzes 1992
Seite 163
- Anlage 13: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 über Genomanalyse und informationelle Selbstbestimmung
Seite 165
- Anlage 14: EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zu den Änderungen des Gesetzes zu Art. 10 GG und der StrafprozeÙordnung im Rahmen der Poststrukturreform
Seite 168

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
Bt-Drucksache	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheid
DIPOL	DV-Infrastruktur für die Polizei
GG	Grundgesetz
HB	Hauptuntersuchungsbericht für die informationstechnische Infrastruktur der Polizei
IK-Ausschuß	Bericht des Ausschusses für Informa- tionstechnologie und Kommunikation
ISDN	Diensteintegrierendes, digitales Fernmeldenetz
KPA	Kriminalpolizeiamt
Lt-Drucksache	Landtagsdrucksache
MAD	Militärischer Abschirmdienst
NJW	Neue Juristische Wochenschrift
OECD	Organisation für europäische wirtschaftliche Zusammenarbeit
PC	Personalcomputer
RSt	Ressortstellungnahme
RVO a.F.	Reichsversicherungsordnung alte Fassung
SAL-Info	Saarland-Informationen für die Presse
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
SPolG	Saarländisches Polizeigesetz
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
TB	Tätigkeitsbericht
Tz	Teilziffer

Vorbemerkung

Im Berichtsjahr stand die Internationalisierung der Informationsverarbeitung durch den steigenden Datenverkehr über die Grenzen hinweg im Blickpunkt der Öffentlichkeit. Die Internationale Konferenz der Datenschutzbeauftragten, die im August 1989 in Berlin stattfand, war ganz diesem Thema gewidmet; aber auch die deutschen Datenschutzbeauftragten haben sich der Problematik angesichts des wachsenden EG-Binnenmarktes verstärkt angenommen. Die Probleme, die sich durch die grenzüberschreitende Informationsverarbeitung ergeben, werden nicht geringer, wenn das "Europäische Haus" sich nach Osten erweitert.

Bestimmend für das Datenschutzgeschehen im Saarland war im Berichtszeitraum die Gesetzgebungstätigkeit vor Abschluß der 9. Legislaturperiode des Landtages. Das Polizeigesetz, das Statistikgesetz, das Maßregelvollzugsgesetz wurden verabschiedet und damit die Rechtsgrundlagen für den Schutz des informationellen Selbstbestimmungsrechts bereichsspezifisch wesentlich verbessert. Auf der Wunschliste notwendiger gesetzlicher Regelungen stehen indessen weitere Vorhaben, die entweder gar nicht erst angepackt oder schon vorzeitig aufgegeben wurden. Im Interesse einer wirksamen Bekämpfung des Krebses muß die Rechtsgrundlage für das regionale Krebsregister überdacht werden. Soll der Datenzugang der Wissenschaft zu dieser hochsensiblen Datensammlung verbessert werden, kann dies nur auf der Grundlage einer ausdrücklichen, gesetzlichen Regelung geschehen, die dem Persönlichkeitsrecht der Betroffenen Rechnung trägt. Die Informationsverarbeitung in den Gesundheitsämtern bedarf einer den verfassungsrechtlichen Anforderungen genügenden Rechtsgrundlage, die ich bereits seit 1978 immer wieder fordere. Besonders bedauerlich ist es, daß die Landesregierung die Novellierung des Saarländischen Datenschutzgesetzes - ein Referentenentwurf lag bereits vor - nicht weiter

verfolgt hat. Der Datenzugang der Forschung ist damit - von besonders geregelten Bereichen wie den Krankenhäusern und den Schulen abgesehen - weiterhin gesetzlich nicht geregelt. Für den Verfassungsschutz ist im Saarland als einzigem Bundesland die Kontrolle durch eine unabhängige Stelle nicht sichergestellt. Die technische Entwicklung schreitet immer weiter voran. Einzelne Komponenten von Bürokommunikationssystemen sowie ISDN-fähige Telefonnebenstellenanlagen sind in der saarländischen Verwaltung bereits installiert. Auch um der neuen Gefährdungssituationen durch technischen Fortschritt gerecht werden zu können, muß das Saarländische Datenschutzgesetz als Auffangnorm für alle Bereiche der öffentlichen Verwaltung fortgeschrieben werden.

Auf Bundesebene waren umfangreiche Gesetzgebungsvorhaben unter Datenschutzgesichtspunkten zu begleiten. Es seien nur erwähnt die Entwürfe zum Bundesdatenschutzgesetz, zum Bundesverfassungsschutzgesetz und zur Regelung der Rechtsgrundlagen für die Nachrichtendienste, zur Strafprozeßordnung, zum Rentenreformgesetz, zum Kinder- und Jugendhilfegesetz, zum Bundeszentralregistergesetz und zum Personalaktenrecht für den öffentlichen Dienst. Ein weiterer Schwerpunkt waren die Überlegungen zur Genomanalyse.

Die Kontrolle der Informationsverarbeitung in den öffentlichen Stellen des Saarlandes wurde dabei keineswegs vernachlässigt. Erfreulicherweise zeichnet sich im Bereich der Polizei und in den Universitätskliniken im Landeskrankenhaus in Homburg eine datenschutzgerechte Regelung für den PC-Einsatz ab, den ich im vergangenen Berichtsjahr einer besonderen Prüfung unterzogen habe.

1. Grenzüberschreitende Informationsverarbeitung

1.1 Infrastruktur und Mobilität

Seitdem automatisierte Datenverarbeitung und Nachrichtenübertragungstechnik sich gegenseitig ergänzend zusammengewachsen sind, ist die Telekommunikation durch Vernetzung des Computers stets auf dem Vormarsch. Informationsverarbeitung und Informationsübermittlung erreichen infolge der in den letzten Jahren stürmisch verlaufenden technischen Entwicklung der Telekommunikation immer neue Dimensionen, die weder durch Ländergrenzen noch durch Entfernungen eingeschränkt werden.

So steht etwa dem IBM-Konzern ein weltweites Netzwerk zur Verfügung, über das Geschäftsdaten, Dokumente, Nachrichten in 75 Länder der Erde weitergeleitet werden können. Bisher nutzte der Konzern diese Infrastruktur nur für die eigene Kommunikation mit Niederlassungen, Lieferanten und Geschäftspartnern. Seit dem 1. Juli 1989, mit dem Inkrafttreten der Strukturreform der Deutschen Bundespost und der Aufhebung des Netzmonopols, dürfen auch Private die von IBM angebotenen, weltweiten Standleitungen einschließlich der verschiedenen, angebotenen Dienste nutzen. Heute schon zählt IBM eine halbe Milliarde Teilnehmer, die Informationen in Sekundenschnelle zwischen verschiedenen Computersystemen übertragen, verarbeiten oder aus Datenbanken zu jeder Tages- und Nachtzeit abrufen können. Zwei Drittel aller Rechnersysteme dieser Welt arbeiten nach IBM-Normen, so daß die Kunden dieses Kommunikationsriesen, ohne sich um technische Besonderheiten der angeschlossenen Endgeräte in den verschiedensten Regionen sorgen zu müssen, bis in die entlegensten Staaten Informationen übermitteln können.

Die Postverwaltungen von 17 europäischen Staaten haben sich zusammengeschlossen, um ein einheitliches, europa-

weites digitales Mobilfunknetz zu errichten. Dadurch werden künftig nicht nur Gespräche "vom Nordkap bis Sizilien" vom Auto aus geführt werden können, sondern es werden auch Texte und Daten (Telefax) auf komfortable Weise übermittelt werden können.

Die Internationalisierung der Informationstechnologie findet ihre Entsprechung in der Mobilität von Arbeit und Kapital.

Großräumige Marketingstrategien, die den Absatz von Massenproduktionen sichern sollen, fördern grenzüberschreitend den Adreßhandel und die Kreditinformation. Im letzten Jahr sind bei einem deutschen Unternehmen, das sich mit Kreditinformationen beschäftigt, die Daten über Personen, die außerhalb der Bundesrepublik den Schwerpunkt ihrer Lebensinteressen haben, auf weit über 20 % gestiegen. Hier zeigt sich schon, wie sich in den kommenden Jahren die Situation verändern wird. Personenbezogene Daten werden in wachsendem Umfang bei der Verwendung von Kreditkarten, zur Buchung für den Reiseverkehr und innerhalb multinationaler Unternehmen transferiert. Die Internationalisierung von Arbeitsmöglichkeiten forciert den Austausch von Arbeitnehmer- und Sozialversicherungsdaten. Internationale Vereinbarungen gewährleisten die Kooperation der Finanzverwaltungen; aus ihrer Sicht ist die Transparenz der Einkommensverhältnisse unabhängig davon, wo die Einkünfte entstehen, unerlässlich und wird deshalb einen zunehmenden Datenaustausch zur Folge haben.

1.2 Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten

Datenschutzbeauftragte aus 22 Ländern haben in Berlin am 28./31. August 1989 unter dem Leitthema "Datenflüsse ohne Grenzen - Neue Aufgaben für den Datenschutz" die Probleme diskutiert, die durch zunehmende Inter-

nationalisierung des Datenverkehrs und die grenzüberschreitende Verflechtung der Informationsverarbeitung entstehen. Neben dem Europarat, der Organisation für wirtschaftliche Zusammenarbeit (OECD) und der Europäischen Gemeinschaft (EG) sowie deren Mitgliedstaaten waren u.a. die Vereinigten Staaten von Amerika, Japan, Kanada, Australien, Schweden und Norwegen vertreten. Die Veranstaltung hat wieder einmal deutlich gemacht, daß der Datenschutz keine exotische, weltfremde Gedankenoperation darstellt. Die Beiträge belegen überdies den internationalen Charakter der Informationsverarbeitung aufgrund einer weltweiten informationstechnologischen Infrastruktur und eine erstaunliche Übereinstimmung in den Erfahrungen innerhalb der nationalen Grenzen.

Die Teilnahme zweier Vertreter aus Ungarn unterstreicht überdies die Bedeutung des Datenschutzes für den Bestand einer demokratischen Gesellschaft. Unübersichtliche und unkontrollierte Informationsverarbeitung verleitet den Bürger, auf seine Grundrechte zu verzichten und sich den eventuell auch nur vermeintlichen Verhaltenserwartungen der speichernden, insbesondere öffentlichen Stellen anzupassen. Besonders bedeutsam war deshalb die Ankündigung der ungarischen Vertreter, daß der Datenschutz in ihrer Verfassung verankert werden soll. Ungarn folgt damit dem Beispiel der Verfassungen Portugals, Spaniens und Österreichs. Auf nicht geringeres Interesse stieß der Hinweis, daß Ungarn die Absicht habe, der Europaratskonvention 108 über den Datenschutz beizutreten. Die Sicherung der informationellen Selbstbestimmung - dies entspricht der Auffassung des Bundesverfassungsgerichts - wird als ein wesentliches Element zur Stärkung der Demokratie gesehen.

Die Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten (Anlage 1) weist auf die praktischen Probleme hin, die durch die Datenübermitt-

lung ins Ausland entstehen. Sie fordert deshalb vor allem gleichwertige, gesetzliche Sicherungen in den Ländern, eine Verbesserung der Rechte des einzelnen beim grenzüberschreitenden Informationsaustausch und eine verstärkte Zusammenarbeit der Datenschutzkontrollorgane.

Die Konferenz setzt im übrigen im Interesse der Intensivierung des Erfahrungsaustausches eine Arbeitsgruppe ein, die die Datenschutzprobleme im Bereich der internationalen Netze und Dienstleistungen beraten soll (Anlage 2).

1.3 Diensteintegrierendes, digitalisiertes Kommunikationsnetz (ISDN)

Im März 1989 hat der Bundespostminister offiziell ISDN in Betrieb genommen. 1990 soll eine Verbindung mit den entsprechenden Netzen von Frankreich, Italien und Großbritannien hergestellt werden. 1993 soll das Netz bundesweit und flächendeckend zur Verfügung stehen; für das Jahr 2000 werden bereits über 7 Millionen, davon 3 Millionen privatgenutzte, Anschlüsse in der Bundesrepublik Deutschland erwartet.

Bei der Einrichtung dieses Netzes handelt es sich zwar zunächst um einen typischen Inlandssachverhalt, der jedoch, wie die technische Entwicklungsperspektive für die Zukunft zeigt, sich alsbald auch im grenzüberschreitenden Datentransfer auswirken wird.

Das derzeitige Konzept der Bundespost sieht vor, Zeitpunkt, Dauer sowie Rufnummer der Beteiligten eines jeden ISDN-Telefongesprächs zu registrieren und über 3 Monate aufzubewahren. Bisher wurden regelmäßig nur die verbrauchten Gebühreneinheiten dem alten Zählerstand hinzuaddiert. Die nunmehr vorgesehene Speicherung der Verbindungsdaten ist bedenklich, weil das grundrecht-

lich geschützte Fernmeldegeheimnis die vom Staat unbeobachtete Kommunikation garantiert. In Zukunft können nicht nur vollständige Listen über Telegramme, sondern auch über alle 3 Monate zurückliegende Telefongespräche, Telefax und Telexverbindungen erstellt werden. Nach dem Fernmeldeanlagen-gesetz ist dies in Strafverfahren ohne Einschränkung auf besonders schwere Straftaten nach Einleitung eines Ermittlungsverfahrens gegen jeden Beschuldigten zulässig (§ 12 Fernmeldeanlagen-gesetz). Dies ist mit Rücksicht darauf, daß hierfür bereits ein Anfangsverdacht für jedwede Straftat ausreicht, eine zu weitgehende Befugnis. Ganz abgesehen davon wächst die Mißbrauchsgefahr angesichts eines so großen, umfassenden Datenbestandes.

Ein Arbeitskreis der Internationalen Konferenz der Datenschutzbeauftragten hat in Berlin angesichts des Gefährdungspotentials bei ISDN gefordert, daß Abrechnungsdaten nur so lange gespeichert werden dürfen, wie dies zur Rechnungsstellung erforderlich ist (Anlage 3). Ferner sollen anonyme Zählleinrichtungen geschaffen und Vermittlungsdaten unverzüglich gelöscht und nur gespeichert werden dürfen, wenn sie für die Abwicklung des Dienstes erforderlich sind. Es sollen Vorkehrungen getroffen werden, daß Teilnehmer, die in ein Teilnehmerverzeichnis aufgenommen werden wollen, nicht Objekt unerwünschter, kommerzieller Werbung werden.

Das leistungsfähige Kommunikationsnetz ISDN wird es zukünftig ermöglichen, daß die Nummer des anrufenden Teilnehmers auf einem Display des Angerufenen erscheint. Diese "elektronische Version des Spiegels an der Haustür" liegt zweifellos im Interesse des Angerufenen, der nicht jedermann telefonisch Rede und Antwort stehen möchte. Zugleich kann aber auch derjenige beeinträchtigt werden, der aus guten Gründen - etwa bei der Telefonseelsorge, bei medizinischer oder psychologischer Beratung im Bereich der AIDS-Hilfe - seine Anonymität gewahrt wissen will. Sowohl der Anru-

fer als auch der Angerufene muß daher in der Lage sein, die Anzeige des anrufenden Teilnehmers zu unterdrücken.

1.4 Datenschutz in der Europäischen Gemeinschaft (EG)

Die Probleme der Internationalisierung erhalten im Bereich der EG eine besondere Note, weil der angestrebte Binnenmarkt und die Dynamik der wirtschaftlichen Integration die Entwicklung zu einem "informationellen Großraum" nachhaltig fördern wird. Trotz der vom Europäischen Parlament bereits im März 1982 geäußerten Erwartung, daß der Datenschutz in der Gemeinschaft geregelt werde, hat die EG-Kommission sich auf die Empfehlung an die Mitgliedstaaten beschränkt, die Europaratskonvention 108 zu ratifizieren. Diese enthält jedoch nur einige Mindestvorschriften über den fairen Umgang mit personenbezogenen Daten und kann die Verabschiedung nationaler datenschutzrechtlicher, gesetzlicher Regelungen und schon gar nicht ein Gesamtkonzept auf EG-Ebene ersetzen. Die Zurückhaltung der EG-Kommission auf dem Gebiet des Datenschutzes steht in auffälligem Gegensatz zu ihren Bemühungen um eine möglichst effektive Nutzung der Kommunikationstechnologie. Das staatliche Monopol in der EG ist aufgehoben und durch Richtlinien soll der Wettbewerb der Endgeräte- und Dienstleistungsanbieter standardisiert und liberalisiert und damit der Wettbewerb gefördert werden. Durch Harmonisierung der technischen Voraussetzungen sollen die Startbedingungen für gemeinschaftsweite Teledienste verbessert werden.

Angesichts solcher Rahmenbedingungen, die die Technik und der Markt mit Sicherheit nutzen werden, erscheint der Datenschutz in der EG in einem düsteren Licht. In 5 von 12 Mitgliedsländern - nämlich in Belgien, Griechenland, Italien, Portugal und Spanien - ist der Datenschutz überhaupt noch nicht gesetzlich geregelt;

ein Umstand, der erschwerend wirkt, weil die ohnehin allein nicht ausreichende Europaratskonvention 108 lediglich von 7 Mitgliedsländern - zuletzt von Dänemark am 23.10.1989 - ratifiziert ist.

Auf der Landkarte Europas gibt es nicht nur "weiße Flecken", Länder, in denen die schutzwürdigen Belange der Betroffenen durch keine gesetzliche Regelung oder sonstige Vorkehrung wie unabhängige Datenschutzkontrollorgane gewährleistet sind. Verunsicherung entsteht überdies auch durch die großen Unterschiede in der Ausgestaltung der - sofern vorhanden - nationalen Verarbeitungsregelungen.

Die Bürger sollten jedoch wissen, ob überhaupt und nach welchen Regeln, ihre Daten europaweit verarbeitet werden. Würde jedes Mitgliedsland der EG durch Kollisionsnormen festlegen, welche nationalen Datenschutznormen anzuwenden sind, würde im Zweifel dem Territorialprinzip zum Durchbruch verholfen. Angesichts der Unsicherheit hinsichtlich der Beurteilungsmaßstäbe wäre dies eine verständliche Reaktion der Mitgliedsländer. Ein einheitliches Regelungsmodell ist darum noch nicht in Sicht.

Die EG bedarf, wenn die supranationalen Tendenzen gefördert werden sollen, eines einheitlichen Konzeptes. Welche Grundregeln dabei jedoch verbindlich für alle Mitgliedsländer sein sollen, ist nicht ohne weiteres zu beantworten. Die Europaratskonvention 108, die übrigens nicht nur für EG-Länder Geltung haben soll, dürfte allein nicht ausreichen.

Es dürfte schwer fallen, eine Rangliste nationaler Gesetzgebung aufzustellen oder gar den Grad der (Un-)Gleichwertigkeit der jeweiligen nationalen Maßstäbe festzustellen. Noch weniger dürfte es gelingen, die nationalen Regelungen zu harmonisieren. Das Ergebnis könnte bestenfalls eine "künstliche Mischung der

unterschiedlichsten nationalen Regelungselemente" sein (vgl. Simitis, Vortrag anlässlich der Berliner Internationalen Konferenz); schlimmer noch wäre ein europäischer Datenschutz "auf kleinstem Nenner".

Hinsichtlich der Kommunikationsnetzwerke sollte jedenfalls ein Regelungskonzept angestrebt werden, das den engen nationalen Ansatz überwindet, Struktur und Auswirkung der gemeinsam genutzten, technischen Infrastruktur berücksichtigt und die Freiheitsrechte sowie die Grundstrukturen einer demokratischen Gesellschaft respektiert (Simitis a.a.o.). Allerdings wäre es wichtig, nunmehr den Grundbestand einer verbindlichen Datenschutzregelung für alle Mitgliedsländer festzustellen und auf den jeweiligen Sachverhalt bezogen spezifische und konkrete Festlegungen zu treffen.

Der Datentransfer in Länder, die keine Datenschutzregelungen getroffen haben, kommt jedenfalls einer Datenfreigabe gleich. Je billiger und einfacher die internationale Telekommunikation wird, "um so mehr werden Freihäfen der Datenverarbeitung möglich, in denen der erforderliche Datenschutz auch für Bürger anderer Länder nicht mehr gewährleistet ist" (Einwag, BfD, anlässlich der Internationalen Konferenz in Berlin). Deshalb ist in solchen Fällen das Übermittlungsverbot die einzige Alternative, den Schutz des Betroffenen sicherzustellen.

In einer Zusatzklärung zur Berliner Resolution der Internationalen Konferenz (Anlage 4) haben die Datenschutzbeauftragten der EG-Länder die Notwendigkeit eines "umfassenden und konsistenten Ansatzes" zur Verwirklichung der Grundsätze des Datenschutzes in den Mitgliedsländern und die Notwendigkeit eines unabhängigen Datenschutzkontrollorgans unterstrichen.

Noch entschiedener haben die deutschen Datenschutzbeauftragten des Bundes und der Länder in ihrer Ent-

schließung vom 26./27.10.1989 (Anlage 5) gefordert, daß dem Datenschutz der gleiche Stellenwert wie der Förderung der technischen Infrastruktur im grenzüberschreitenden Bereich zukommen und die EG ein Gesamtkonzept für die Sicherung des Datenschutzes entwickeln muß. Ferner unterstützen die deutschen Datenschutzbeauftragten die Forderung, eine unabhängige Datenschutzkontrollinstanz auf EG-Ebene einzurichten.

1.5 Telekommunikation im Saarland

Die Staatskanzlei hat mitgeteilt, daß "konkrete Erfolge" im Bereich der Telekommunikation zu verzeichnen seien (SAL-Info Nr. 168/89 vom 12.10.1989). Das enge Zusammenwirken zwischen Lothringen und dem Saarland habe die Ansiedlung der Firma EUCOM in Saarbrücken ermöglicht. Es handele sich dabei um eine gemeinsame Tochter der Bundespost und der France Télécom auf dem zukunftssträchtigen europäischen Markt für Telekommunikationsdienste. Über die Landesgrenze hinweg werde die notwendige Infrastruktur durch eine von französischer Seite zugesagte Glasfaserstrecke geliefert. In Kürze sei u.a. ein Vertrag zwischen dem Saarbrücker Innovations- und Technologiezentrum (SITZ) und Technopôle 2000 in Metz zur Gründung eines grenzüberschreitenden Téléports zu erwarten.

Diese Ankündigungen zeigen, daß die Telekommunikation im Saarland, infolge seiner Lage im Herzen Europas, besonders günstige Startbedingungen hat. Nähere Einzelheiten über den Fortschritt der Projekte sind noch nicht bekannt geworden. Das Saarland trifft dann aber auch mit Rücksicht auf den in seiner Verfassung verankerten Datenschutz eine besondere Verpflichtung.

1.6 EG-Statistikverordnung

Ein Beispiel dafür, wie der Standard des Datenschutzes in der Bundesrepublik Deutschland durch unmittelbare Maßnahmen der EG-Kommission unterschritten werden kann, ist die EG-Statistikverordnung. Die Konferenz der deutschen Datenschutzbeauftragten hat Bedenken erhoben, weil vertrauliche, statistische Daten dem Statistischen Amt der Europäischen Gemeinschaft auch dann übermittelt werden dürfen, wenn sie einen Personenbezug aufweisen. Die Datenschutzbeauftragten haben deshalb in einer EntschlieÙung gefordert (vgl. Anlage 6), daß die Übermittlung personenbezogener Einzelangaben nur ausnahmsweise durch einen weiteren Rechtsakt der EG für bestimmte, statistische Zwecke zugelassen werden darf und daß eine möglichst frühzeitige Anonymisierung sowie die notwendigen organisatorisch-technischen Maßnahmen der Datensicherung zu gewährleisten sind.

1.7 Abbau der Grenzkontrollen (Schengener Abkommen)

Im Schengener Übereinkommen haben Frankreich, die Bundesrepublik Deutschland und die Benelux-Staaten den schrittweisen Abbau der Grenzkontrollen vereinbart. Um die dadurch entstehenden Sicherheitsdefizite auszugleichen, soll es zu einem verstärkten Informationsaustausch zwischen Behörden der genannten Ländern kommen. Die Maßnahmen sollen in einem Zusatzübereinkommen festgehalten werden. Hierzu gehört die Einrichtung eines gemeinsamen, zentralen, automatisierten Informationssystems (Schengener Informationssystem-SIS). In diesem Auskunftssystem sollen insbesondere Informationen zur Fahndung und zur vorbeugenden Verbrechensbekämpfung erfaßt werden. Neben der Ausschreibung zur Festnahme und zur Ermittlung des Aufenthalts von Zeugen in Strafverfahren kommen sensible Daten über die verdeckte Registrierung und gezielte Kontrol-

len von Personen in Betracht. Dabei handelt es sich um Maßnahmen, die etwa der polizeilichen Beobachtung im innerstaatlichen Bereich entsprechen. Zur Sicherung der Außengrenzen der Mitgliedstaaten sollen aber auch abgewiesene oder abzuschiebende Drittausländer in diesem System registriert werden. Nicht zuletzt soll das Informationssystem auch Zwecken der Staatssicherheit dienen. Weitere konventionelle Maßnahmen, die den Informationsaustausch fördern, sind Gegenstand der Verhandlungen, z.B. die spontane Mitteilung von Erkenntnissen, die der Bekämpfung bestimmter Formen der Kriminalität dienen können und die grenzüberschreitende Observation.

Die Konferenz deutscher Datenschutzschutzbeauftragter hat den Entwurf einer Zusatzvereinbarung, in der die Einzelheiten geregelt werden sollen, erörtert und eine EntschlieÙung gefaÙt (vgl. Anlage 7). Nach dem damaligen Stand der Verhandlungen war ein Mindeststandard des Datenschutzes jedenfalls für das Informationssystem auf der Grundlage der Europaratskonvention und der Empfehlungen seines Ministerkomitees über die Nutzung personenbezogener Daten im Polizeibereich bereits vorgesehen. Die Konferenz war der Auffassung, daß diese Elemente Bestandteile des Zusatzübereinkommens bleiben müssen und noch der Verbesserung und der Ergänzung bedürfen.

Insbesondere müssen die Rechte des Betroffenen auf Auskunft, Berichtigung und Klage sowie die Befugnisse der einzurichtenden Kontrollorgane auf nationaler und internationaler Ebene auf den konventionellen Informationsaustausch zur Bekämpfung bestimmter Formen der Kriminalität und den Bereich des Ausländerrechts und des Asylverfahrens erstreckt werden.

Zum Schengener Informationssystem selbst haben die Datenschutzbeauftragten Anregungen im Hinblick auf eine Konkretisierung des Grundsatzes der Verhältnismäßigkeit und des Prinzips der Zweckbindung gegeben.

Die Datenschutzbeauftragten haben im übrigen darauf hingewiesen, daß das Zusatzübereinkommen den deutschen Gesetzgeber nicht der Notwendigkeit enthebt, vor Inkrafttreten des Zusatzübereinkommens die innerstaatlichen Rechtsgrundlagen für die polizeiliche Informationsverarbeitung entsprechend der im Volkszählungsurteil dargelegten Auffassung des Bundesverfassungsgerichts fortzuschreiben. Grenzüberschreitende Observation und Ausschreibung zur verdeckten Registrierung aufgrund internationaler Verträge müssen in einem zweifelhaften Licht erscheinen, solange der Gesetzgeber in der Bundesrepublik die Voraussetzungen solcher Maßnahmen, das Verfahren ihrer Anordnung und die Verwendung der durch sie gewonnenen Erkenntnisse noch nicht geregelt hat. Der deutsche Gesetzgeber darf nicht durch völkerrechtliche Verpflichtungen präjudiziert werden.

Die allgemeine Verpflichtung der Vertragsstaaten in dem Schengener Zusatzübereinkommen, sich unter Berücksichtigung des nationalen Rechts im Interesse der Staatssicherheit gegenseitig Hilfe zu leisten, darf nicht als eigenständige Rechtsgrundlage interpretiert werden, weil die Formulierungen des Abkommens den verfassungsrechtlichen Anforderungen in der Bundesrepublik Deutschland nicht genügen. Nicht zuletzt sind gerade im Bereich des Verfassungsschutzes auf innerstaatlicher Ebene noch Regelungsdefizite festzustellen.

Ferner sind die Datenschutzbeauftragten der Auffassung, daß personenbezogene Daten an Behörden der Mitgliedsländer nicht übermittelt werden dürfen, soweit

diese keine ausreichenden gesetzlichen Grundlagen geschaffen haben.

Eine Gesamtwürdigung des Schengener Abkommens und der Zusatzvereinbarung, die Modellcharakter für die gesamte EG haben dürften, kann zwar nicht außer Betracht lassen, daß durch die Aufhebung der Grenzkontrollen entstehende Sicherheitsdefizite ausgeglichen werden müssen. Die neue Dimension der grenzüberschreitenden Informationsverarbeitung, die durch die Einrichtung eines zentralen, automatisierten Auskunftssystems für alle Mitgliedsstaaten entsteht, weist jedoch bereits über das durch den Wegfall der Grenzkontrolle Notwendige hinaus. Es liegt nahe, daß andere Gründe der inneren Sicherheit Kooperationen der beschriebenen Art, etwa zur präventiven Verbrechensbekämpfung, erfordern. Dies sollte offengelegt und der Öffentlichkeit im Interesse der Nachvollziehbarkeit der Gründe zugänglich gemacht werden.

2. Bürokommunikation

Die Stabsstelle für Informationstechnologie und -kommunikation beim Chef der Staatskanzlei hat "Vorläufige Empfehlungen zur Bürokommunikation" entwickelt. Die Bedeutung dieser Untersuchung für den Einsatz von Informations- und Kommunikationstechniken in der öffentlichen Verwaltung des Saarlandes kann nicht hoch genug eingeschätzt werden. Wirft sie doch ein Schlaglicht auf den gegenwärtigen Stand der Automation in den Behörden und zeigt die Perspektiven für die weitere Entwicklung auf.

Die Situation in der Landesverwaltung umschreiben die "Vorläufigen Empfehlungen" (S. 22) wie folgt:

"In der Landesverwaltung werden bis heute noch vorwiegend autonome PC und Textsysteme eingesetzt. In letzter Zeit ist jedoch in zunehmendem Maße die Tendenz zu erkennen, daß sich dieses Bild ändert. In zunehmendem Maße gewinnen vernetzte PC und autonome Rechnersysteme an Bedeutung, die neben den allgemeinen Bürofunktionen, wie Texterstellung und -bearbeitung, Elektronik-Mail, Terminkalender, usw. u.a. auch Komponenten zur Informationsflußkontrolle und Projektinformationssysteme enthalten sollen. Bei diesen Systemen greift der Anwender über ein Terminal direkt auf die gewünschten Informationen zu. Darüberhinaus wird ihm durch spezielle Rechnerfunktionen die Möglichkeit der Kommunikation mit den "vernetzten Teilnehmern" geboten."

Der verstärkte PC-Einsatz in der Landesverwaltung eröffnet eine neue Dimension der Verfügbarkeit von Informationen am Arbeitsplatz. Diese Geräte erfüllen gleichermaßen Funktionen der Textverarbeitung, der individuellen Datenverarbeitung und ermöglichen durch Netzanschluß die Datenkommunikation einschließlich des Großrechnerzugriffs.

Laut Schreiben der Stabsstelle für Informationstechnologie bei der Staatskanzlei vom 24. Oktober 1989 sind in der Landesverwaltung 47 Textverarbeitungssysteme, 504 Arbeitsplatzrechner (524 Bildschirme), 79 Bereichsrechner und 451 Zentralrechneranschlüsse in Betrieb. Der Ausschuß für Informationstechnologie und Kommunikation (IK-Ausschuß) kommt in seinem Bericht für 1987/88 zu dem Schluß, daß die lokalen PC-Installationen nicht zu Informationsverarbeitungsinselfen verkümmern dürfen. In den "Vorläufigen Empfehlungen" wird eine auf die Bedürfnisse des Landes zugeschnittene Bürokommunikation gefordert und das Mittel zur Verwirklichung dieses Zieles in "einem Verbund möglichst aller im Land installierter Systeme" gesehen (S. 23).

Die in den Geschäftsbereichen bereits vorhandenen Einrichtungen können somit als "Grundstock" für ein landesweites Bürokommunikationssystem gesehen werden. Ansätze sind jedenfalls schon zu erkennen. Im Umweltministerium und im Innenministerium wurden bereits PC-Netze eingerichtet (IK-Ausschuß Tz. 3.2.1, Tz. 3.8.1). Der Minister des Innern hat für die Bürokommunikation eine "Pilotierung" durchgeführt. Dabei handelt es sich insbesondere um einen Anschluß an den Telex-/Telefax-Dienst der Deutschen Bundespost. Der weitere Ausbau ist beabsichtigt, konkrete Vorstellungen über weitere Realisierungsstufen bestehen indessen nicht. Der Minister für Umwelt plant neben der Automatisierung der Textverarbeitung weitergehende Anwendungen durch Aufbau spezieller und Anbindung an bereits bestehende, außer Haus befindliche Datenbanken. Im Mittelpunkt steht ein fachbereichsübergreifendes Umweltinformationssystem. Die Kommunikation zwischen allen nachgeordneten Dienststellen (z.B. Staatliches Institut für Gesundheit und Umwelt, Landesamt für Umweltschutz, Staatliches Straßenbauamt, Staatliches Straßenneubauamt) und dem Ministerium selbst sowie

eingeschränkt unter den nachgeordneten Dienststellen soll möglichst umgehend realisiert werden (Schreiben des Ministers für Umwelt vom 04.12.1989). Der Minister für Bundesangelegenheiten und besondere Aufgaben stützt sich bei seiner Textverarbeitung ebenfalls auf ein Netzwerk (IK-Ausschuß Tz. 3.9). Ein "lokales Netz" für die Staatskanzlei wird ebenfalls diskutiert.

Für die technische Verwirklichung des Verbundes steht derzeit bereits das bestehende Leitungsnetz der Landesverwaltung zur Verfügung. Die ZDV-Saar soll Übergangsweise als "Datendrehscheibe" dienen, bis etwa ein "Hochleistungs-Hintergrundnetz" (Backbone-Netz) die Kommunikation beliebiger Netzteilnehmer ermöglichen könnte. Eine Arbeitsgruppe hat überdies in Zusammenarbeit mit der Bundespost ein Konzept für digitale Kommunikationsanlagen erarbeitet. Ressortübergreifend wird nach Einschätzungen der Experten die Bürokommunikation frühestens in 5 Jahren verwirklicht werden können ("Vorläufige Empfehlungen" S. 31). Dessenungeachtet werden zunehmend Komponenten in den Geschäftsbereichen als Insellösung installiert, die der Bürokommunikation dienen.

Um die Gefahren für den Bürger erkennen zu können, sollte intensiver der Frage nachgegangen werden, welche praktischen Auswirkungen die Bürokommunikation hat.

Ungeachtet der Tatsache, ob man das Ziel eines völlig "papierlosen Büros" erreicht, wird die Bürokommunikation dazu führen, daß vermehrt personenbezogene Daten automatisiert verfügbar sind. Anstelle von Akten, Notizzetteln, Kalendern, Schreibutensilien dürfte vermehrt der Bildschirm treten, der an ein die verschiedenen Bereiche verbindendes Netz angeschlossen ist. Drucker, Telefaxgeräte, Datenspeicher, etwa in Form von Disketten, können hinzukommen. Über Bildschirm erfährt der Mitarbeiter in der öffentlichen

Verwaltung seine Termine, Mitteilungen und Nachrichten, die in seiner Abwesenheit eingegangen sind. Bereits begonnene Konzepte kann er abrufen sowie mit Hilfe zusätzlicher Informationen aus Datenbanken überarbeiten, den Entwurf seinem Vorgesetzten elektronisch zur Kenntnis geben und zu beteiligende Stellen unterrichten. Den Vorgang kann er im elektronischen Archiv ablegen. Durch die Vernetzung bisher isolierter, hochspezialisierter Arbeitsplatzcomputer werden Möglichkeiten der Kooperation und gemeinsamen Nutzung von Bürofunktionen eröffnet: Dokumentbearbeitung (Texte, Grafiken, Formulare, Tabellen), Ablage, Informationstransport (Dateien, Dokumente, Dialog); Organisationshilfen (Kalender, Sonderspeicher, Taschenrechner). Ressourcen anderer Stellen an Informationen und Büroleistungen werden für die am Netz angeschlossenen Arbeitsplätze nutzbar.

Die Bürokommunikation eröffnet bisher mit konventionellen Mitteln nicht erreichbare Verknüpfungs- und Auswertungsmöglichkeiten von Informationen aus den verschiedensten Lebensbereichen eines Bürgers, in denen er mit der Behörde in Berührung gekommen ist. Hierdurch ist die Gefahr von Persönlichkeitsprofilen gegeben. Das Netz eröffnet insbesondere große Kommunikationsmöglichkeiten. Die Kopie und Versendung etwa einer Akte wird außerordentlich erleichtert. Die Mißbrauchsgefahr im Rahmen eines solchen Systems durch nicht erforderliche und deshalb unnötige Informationsweitergabe und -abrufe wächst.

Gefahren können sich auch ergeben durch den Transport der Informationen. Hierfür kommen vor allem das öffentliche Telefonnetz und das bestehende Leitungsnetz der Landesverwaltung aber auch ein diensteintegrierendes, digitalisiertes Kommunikationsnetz in Betracht. Letzteres wird die Einrichtung der Bürokommunikation innerhalb und außerhalb der Behörden erheblich erleichtern und die Realisierung beschleunigen. Die Informationen

können auf dem Transport nicht nur in ihrer Substanz vernichtet oder verfälscht, sondern gerade in dieser Phase von Unbefugten zur Kenntnis genommen werden. Deshalb kommt der Sicherheit der Kommunikationsnetze besondere Bedeutung zu.

Der Verwaltungsalltag ist vor allem geprägt durch die Beteiligung von verschiedenen Funktionsträgern (Vorgesetzte, Mitarbeiter) innerhalb einer Behörde und von anderen Stellen außerhalb der Behörde. Dies ergibt sich aus der unterschiedlichen Kompetenz- und Zuständigkeitsverteilung, die ein Teil der Rechtsstaatlichkeit öffentlicher Verwaltung ist. Verwaltungsakte unzuständiger Stellen sind fehlerhaft und anfechtbar; welche Stellen, welche Informationen zu welchen Zwecken erheben, speichern, auswerten und weitergeben dürfen, folgt aus der gesetzlichen Befugnis zur Wahrnehmung bestimmter Verwaltungsaufgaben. Der durch die Bürokommunikation hergestellte Informationsverbund hat jedoch die Tendenz, die Verwaltung zu einer Einheit zusammenzuführen, die die Verantwortlichkeit verwischen kann. Wer für was zuständig ist, spielt auch innerhalb der Behörde eine große Rolle (funktioneller Behördenbegriff). Es muß deshalb nicht nur stets feststellbar sein, welche Stelle tätig geworden ist, sondern auch welche Mitarbeiter und Vorgesetzte an der Entscheidung beteiligt waren und wer die Verantwortung zu tragen hat. Dies gilt auch für archivierte (abgelegte) Vorgänge. Die Authentizität der Dokumente muß stets gewährleistet sein; sie müssen vor unbefugter, nachträglicher Änderung nicht nur durch den Verfasser, sondern auch durch privilegierte Benutzer (z.B. Systemverwalter) geschützt werden. Die "Dokumenten-echtheit" sicherzustellen, bedeutet jedoch, daß auch Veränderungen etwa im Mitzeichnungsverfahren nachvollziehbar aufgezeichnet werden müssen. Die Rekonstruktion des Ablaufs eines Vorgangs stellt besondere Anforderungen an die Bürokommunikation.

Eine ungesteuerte und ungezügelter Bürokommunikation würde insbesondere durch ihre Netzkomponente die Verwaltung zu einer Einheit zusammenwachsen lassen, die in einem diametralen Gegensatz zu der rechtsstaatlich verankerten, arbeitsteiligen Kompetenz- und Zuständigkeitsverteilung in der öffentlichen Verwaltung stehen würde. Einer freien Kommunikation zwischen den Behörden und dem unbegrenzten Datenzugang aller Bediensteter innerhalb einer öffentlichen Stelle steht das informationelle Selbstbestimmungsrecht des betroffenen Bürgers entgegen. Die datenschutzrechtlichen Belange - insbesondere die grundsätzliche Zweckbindung der personenbezogenen Daten - sind durch das Bürokommunikationssystem selbst zu gewährleisten, da sonst den Gefahren für die Persönlichkeitsrechte nicht ausreichend begegnet werden kann. Die modernen Techniken dürfen nur eingesetzt werden, wenn die Gefahren für das informationelle Selbstbestimmungsrecht durch technische Vorkehrungen ausgeräumt sind.

Unabdingbare technische Voraussetzung ist, daß jede Behörde und jeder ihrer Mitarbeiter jeweils nur die Informationen erhält und verarbeitet, die zur Wahrnehmung der jeweiligen Aufgaben benötigt werden. Dem mißbräuchlichen Datentransfer, der durch Bürokommunikation erleichtert wird, muß entgegengewirkt werden. Ferner muß im Interesse einer stets feststellbaren, klaren Verantwortlichkeit gegenüber dem Bürger auch nach Zustellung der Entscheidung oder nach Abschluß des Vorgangs stets überprüfbar sein, wer, wann, welche Texte verfaßt, korrigiert, gebilligt, unterschrieben hat. Eine Verfälschung und Manipulation der Texte und Informationen muß ausgeschlossen sein.

Diesen Anforderungen können die herkömmlichen technisch-organisatorischen Sicherungsmaßnahmen nicht genügen. Jedenfalls erscheint es nicht als ausreichend, den Datenschutz in solchen komplexen Systemen lediglich als Gegenstand des Zugriffsschutzes durch

Paßwortvergabe und der Datensicherheit beim Datentransport zu begreifen. Auf meine Forderung, den Datenschutz vor der Einrichtung solcher Systeme bei der Planung zu berücksichtigen, hat die Staatskanzlei zwar zugestanden, daß Überlegungen und Maßnahmen dieser Art "integrierender Bestandteil" des Projekts sein müssen. Man muß sich jedoch fragen, ob das Gefährdungspotential der Bürokommunikation voll erkannt wird, wenn in der Stellungnahme ausgeführt wird, daß es darum gehe, "lediglich die bisherige konventionelle - und datenschutzrechtlich zulässige - Kommunikation zwischen den Behörden zu vereinfachen und zu beschleunigen".

Nach gegenwärtigem Stand der Technik dürfte der Datenschutz noch am ehesten in der Netzkomponente zu gewährleisten sein. Die Möglichkeiten der Sicherheitstechnik für die Kommunikationsnetze wurden erheblich verbessert. Die Datenflüsse im Netz können inzwischen so gesichert und geschützt werden, daß jeder der vielen an das Netz angeschlossenen Benutzer tatsächlich nur auf die Daten zugreifen kann, die er für seine Aufgabenwahrnehmung benötigt. Meiner Forderung nach Netzkontrollprogrammen, die den Verbindungsaufbau zwischen Benutzern, Datenbanken und Programmen steuern und die Vorgänge im Interesse nachträglicher Kontrolle zur Aufdeckung von Mißbräuchen protokollieren, dürften technisch durchaus realisiert werden können. Schwieriger indessen dürfte sich die Entwicklung von Datenschutzkonzepten im übrigen gestalten. Das Bürokommunikationssystem muß nicht nur das ohnehin schon komplizierte Gefüge von Befugnissen und Zuständigkeiten beim Datenzugang, sondern auch die Verantwortlichkeiten innerhalb einer Behörde für das Endprodukt eines Geschäftsvorgangs während des gesamten Bearbeitungs- und Entscheidungsprozesses und vor allem auch danach gewährleisten.

Ich unterstütze die Forderung der Arbeitsgruppe "Organisation der EDV" (Bericht zur Fortentwicklung der

Informations- und Kommunikationstechnik in der Landesverwaltung des Saarlandes vom 29.09.1989), vor weiteren Schritten in der Bürokommunikation eine genaue Analyse der Pilotanwendungen beim Minister des Innern sowie dem Minister für Umwelt durchzuführen. Ich füge hinzu, daß ohne ein umfassendes Datenschutzkonzept, das die Gefahren für das informationelle Selbstbestimmungsrecht ausschließt, Bürokommunikation auch beschränkt auf einzelne Bereiche (Insellösung) nicht zum Einsatz kommen darf.

Auch das grundsätzliche Problem vernetzter Systeme kann nicht ausgespart bleiben, das der Berliner Datenschutzbeauftragte wie folgt beschreibt (Tagesspiegel vom 29.08.1989):

"Die zunehmende Abhängigkeit gesellschaftlicher Abläufe von diesen Systemen erzeugt vielfältige Anfälligkeit. Systemausfälle führen zu Störungen, fehlerhafte Konzepte beeinflussen die Funktionsfähigkeit von Verwaltung und Wirtschaft. Insbesondere ist die Gesellschaft durch bewußte, die vorgegebenen Regeln mißachtende Eingriffe verwundbar. ... Dies alles führt zur Frage nach den Grenzen der Automatisierung."

3. Polizei

3.1 Die Neuregelung des Saarländischen Polizeigesetzes - SPolG

Die Novellierung des Polizeigesetzes war unter Datenschutzgesichtspunkten dringlich geworden, weil das Bundesverfassungsgericht in seinem Volkszählungsurteil eine gesetzliche Grundlage für die zwangsweise Verarbeitung personenbezogener Daten für notwendig erachtet.

Der Verpflichtung der Sicherheitsbehörden, den Rechtsgüterschutz zu gewährleisten, steht das Recht des Bürgers auf informationelle Selbstbestimmung gegenüber. Es führt kein Weg daran vorbei: der Gesetzgeber muß in Ansehung des Interessengegensatzes eine Konfliktsentscheidung treffen. Weder Unterordnung noch Bevorzugung der einen oder anderen Position können zu einer verfassungskonformen Lösung führen. Der Ausgleich zwischen den beiden Verfassungspositionen - Sicherheitsinteresse und Bürgerfreiheit - muß beide zur optimalen Geltung kommen lassen.

Das Gesetz ist mit Rücksicht auf den derzeitigen Stand der Diskussion in der Bundesrepublik ein bemerkenswerter Beitrag zur Fortentwicklung datenschutzrechtlicher Vorschriften im Bereich polizeilicher Informationsverarbeitung. Folgende Regelungen seien erwähnt:

- Die Polizei ist grundsätzlich verpflichtet, personenbezogene Informationen im Rahmen polizeilicher Ermittlungen offen und beim Betroffenen zu erheben (§ 25 Abs. 2, Abs. 3).
- Die (einfache) Informationserhebung ist zur vorbeugenden Bekämpfung von "Straftaten von erheblicher Bedeutung" zugelassen (§ 26 Abs. 2).

- Die Speicherung von zur Vorbeugung erhobener Informationen ist nur zulässig, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, daß Verbrechen oder Straftaten gewerbsmäßig, gewohnheitsmäßig oder bandenmäßig begangen werden sollen (§ 30 Abs. 3). Gleichfalls nur unter diesen Voraussetzungen und zu diesem Zweck sind besondere Formen der Erhebung - wie die Observation, der Einsatz technischer Mittel, von V-Männern und verdeckten Ermittlern - zugelassen (§ 28).
- Auf automatisierte Datenbanken erhält die Vollzugs-polizei einen Direktzugriff (Online-Anschluß) nur, soweit diese Form der Übermittlung personenbezogener Daten unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Erfüllung polizeilicher Aufgaben angemessen ist (§ 35).
- Die Informationsverarbeitung darf nur zu dem Zweck erfolgen, zu dem die Informationen erlangt worden sind. Eine Zweckdurchbrechung ist nur zulässig, soweit die Polizei die Informationen zu diesem Zweck erheben dürfte (§ 30 Abs. 1 Satz 2 und 3).
- Werden Bewertungen in Dateien gespeichert, muß feststellbar sein, bei welcher Stelle die Unterlagen geführt werden, die der Bewertung zugrunde liegen (§ 30 Abs. 4).
- Stellt die Polizei fest, daß unrichtige oder zu löschende Daten übermittelt worden sind, ist dem Empfänger die Löschung oder Berichtigung mitzuteilen (Nachberichtspflicht, § 38 Abs. 3).
- Der Betroffene hat grundsätzlich ein Recht auf unentgeltliche Auskunft; diese umschließt neben den zu seiner Person gespeicherten Informationen auch Herkunft und Empfänger der Information. Ausnahmen hiervon sind nur zulässig, wenn die Erfüllung polizeili-

cher Aufgaben erschwert oder gefährdet würde, dem Wohl des Bundes oder eines Landes Nachteile bereitet würden oder berechnigte Interessen eines Dritten entgegenstehen (§ 40).

Ein wesentliches Element des Ausgleichs zwischen Sicherheitsinteressen und Bürgerfreiheit ist die normenklare Ausgestaltung der Regelungen, damit der Bürger und die Polizei stets wissen können, was die Polizei darf und was sie nicht darf. Die Risiken, die mit unbestimmten, generalklauselartigen Formulierungen verbunden sind, darf der Gesetzgeber bei Konfliktsentscheidungen nicht eingehen. Normensparsamkeit wäre in dieser Lage kein Ausweg.

Die kurze, allerdings unvollständige Übersicht läßt bereits erkennen, daß auch dieses Gesetz - bei allen zweifelsfrei gegebenen Vorzügen - auf die Verwendung unbestimmter Rechtsbegriffe nicht verzichtet hat. Das Gesetz wird alsbald seine Bewährungsprobe bestehen müssen und es wird sich zeigen, ob die Konkretisierung in allen Teilen so gelungen ist, daß Unsicherheiten in der Handhabung nicht aufkommen müssen.

Schwerpunkte unter datenschutzrechtlichen Gesichtspunkten sind die Prävention im Vorfeld konkreter Gefahren und die Zweckbindung der erlangten Informationen. Genau in diesen Bereichen polizeilicher Informationsverarbeitung könnten sich praktische Probleme der Rechtsanwendung ergeben.

Bei der Vorbeugung zumal kann sich polizeiliche Allzuständigkeit und Allgegenwärtigkeit entwickeln, weil die Grenzen ihrer Tätigkeit im Vorfeld konkreter Gefahren nicht ausreichend klar markiert sind.

In meinen verschiedenen Stellungnahmen zum Entwurf habe ich bereits darauf hingewiesen, daß die Voraussetzungen für die Erhebung zur Vorbeugung von Strafta-

ten (§ 26 Abs. 2) zu weit gefaßt sind und der Begriff "Straftaten von erheblicher Bedeutung" einer ausreichend konkreten Handlungsanweisung für die Polizei entbehrt. Das Hessische Polizeigesetz wird übrigens die Voraussetzungen der einfachen Erhebung zur Vorbeugung präziser festlegen und dadurch in seinem Anwendungsbereich vermeiden helfen, daß Alibikontrollen und Ermittlungen "ins Blaue hinein" im Vorfeld konkreter Gefahren durchgeführt werden. Die Unsicherheiten werden nach der Gesetzeslage im Saarland noch dadurch verstärkt, daß die Voraussetzungen der Speicherung zu präventiven Zwecken (§ 30 Abs. 3) enger als die der Erhebung ausgestaltet sind, so daß die Polizei mehr Informationen erheben kann, als sie im Anschluß daran endgültig aufbewahren darf. Unklar ist, ob die Polizei eine Zwischenspeicherung bis zur Entscheidung über eine endgültige Speicherung vornehmen darf. Ohne eine irgendwie geartete Fixierung der Ermittlungsergebnisse können komplexe Vorgänge nicht bearbeitet werden. Die an sich zulässige "Vorgangsverwaltung" entbehrt jeder gesetzlichen Definition, so daß zeitlich nicht näher bestimmte Speicherungen zur Vorbeugung "im Vorfeld konkreter Gefahren" und ohne Vorliegen eines hinreichenden Anfangsverdachts" im Bereich denkbarer, wenn auch bedenklicher Rechtsauslegung liegen (§ 31). Ein solches Ergebnis wäre vor allem deshalb nicht hinnehmbar, weil die Auswertungsschranken einer solchen Zwischenspeicherung nicht klar genug festgelegt sind. Nach der Begründung zum Regierungsentwurf ist die Verwendung zwar "auf das jeweilige Vorhaben" beschränkt; was darunter zu verstehen ist, bleibt indes offen. Den Begriff der "Zweckbindung" hat das Gesetz selbst jedenfalls nicht näher konkretisiert (§ 30 Abs. 1 Satz 2 und Satz 3). Die Verwendungssperre könnte sich mangels eindeutiger gesetzlicher Festlegung orientieren an dem Ziel der vorbeugenden Verbrechensbekämpfung schlechthin, dann wären Auswertungsmöglichkeiten in größerem Umfang unter Einbeziehung aller der Polizei zugänglichen Informationen denkbar.

Die Grenzen polizeilicher Informationsverarbeitung wären dann nicht mehr ausreichend markiert. Die zukünftige Auseinandersetzung um die Zulässigkeit der Erhebung und Verarbeitung von Informationen zur Vorbeugung dürfte spätestens mit dem weiteren Ausbau der Automation im Polizeibereich in eine entscheidende Phase gelangen. Ein komplexes Telekommunikationssystem für die Polizei befindet sich bereits im Stadium konkreter Planung (siehe unten Tz. 3.2). Gerade in diesem Zusammenhang wird deutlich, wie umfassend der Begriff "Vorgangsverwaltung" oder "Vorgangsbearbeitung" gesehen wird. Praktisch jedes Tätigwerden der Polizei wird von Anfang an im Computer dokumentiert. Damit ergibt sich für alle Arten des Tätigwerdens der Polizei und für fast alle Kontakte des Bürgers mit der Polizei jedenfalls theoretisch die ganze Bandbreite elektronischer Auswertungsmöglichkeiten.

Gerade die Gefahren der Automation lassen die Bedeutung der Verwertungssperren unter dem Gesichtspunkt der Zweckbindung deutlich hervortreten. Ich werde ein besonderes Augenmerk darauf richten, daß Prävention und Zweckbindung unter Abwägung der Sicherheitsinteressen einerseits und der schutzwürdigen Belange der Betroffenen andererseits in angemessener Weise praktiziert werden und Auswüchsen insbesondere durch Einsatz der Automation vorgebeugt wird.

3.2 Neues Polizeiinformationssystem - DIPOL

Im Auftrag des Ministers des Innern hat eine Arbeitsgruppe eine neue Konzeption für die informationstechnische Infrastruktur der Polizei im Saarland entwickelt. Der Hauptuntersuchungsbericht (HB) zu diesem Projekt (Stand 01.11.1989) liegt bereits vor. Ein Pilotprojekt soll im Saar-Pfalz-Kreis bereits 1990 durchgeführt werden (HB S. 392). Geplant ist ein integriertes System für die Vorgangsbearbeitung und -ver-

waltung, für die Texterstellung und -bearbeitung sowie für die Textkommunikation (HB S. 550 ff). Unter "Vorgangsverwaltung" werden alle im Rahmen der polizeilichen Aufgabenerfüllung erforderlichen Tätigkeiten und Maßnahmen einschließlich der Registratur verstanden. Schwerpunkte der Automation sind die Anzeigenaufnahme, die Erfassung von Meldungen, Mitteilungen und Feststellungen, die Durchführung der Meldedienste, die Unterrichtung der Führungsebene, die Erstellung der Statistik, die Führung der Ordnungsbücher zur Wiederauffindung von Vorgängen, die Textverarbeitung und die Anbindung an externe Systeme wie das bundesweite polizeiliche INPOL-System.

Das neue System DIPOL im Vorfeld der INPOL-Speicherung soll die wichtigsten Funktionen der saarländischen Polizei integrieren; das Konzept umfaßt alle wesentlichen Elemente einer Bürokommunikation, wenn auch auf Akten nicht gänzlich verzichtet werden soll. Zielvorgaben sind vor allem die Verbesserung der Transparenz von Vorgangs- und Sachzusammenhängen, schnellerer Rückgriff auf Vorgänge und bereits vorhandene Informationen, Vermeidung von Mehrfacherfassungen, zielgerichtete Prävention und Kriminalitätsbekämpfung. Es soll ein "verteiltetes Datenbanksystem" aufgebaut werden, das neben dezentraler, "lokaler" Datenerfassung und -verarbeitung in den örtlichen Polizeidienststellen die Unterhaltung eines zentralen Datenbestandes auf Landesebene einschließt. Eine umfassende Kommunikationsfähigkeit soll vor allem den Meldedienst ersetzen und eine rationelle Arbeitsweise bei der Aufklärungsarbeit ermöglichen. Ein ISDN-fähiges Fernsprechnetz ist für die Polizei vorgesehen (HB S. 392). Damit strebt das Saarland eine polizeiliche Infrastruktur an, die in der überwiegenden Zahl der Bundesländer bisher so nicht verwirklicht ist. Die Vernetzung der Polizeidienststellen untereinander erfordert einen hohen Aufwand. Eine gemeinsame Verfahrensentwicklung

wird allerdings mit Hamburg und Hessen angestrebt (HB S. 362, 371).

Die Integration von Vorgangsverwaltung und Kommunikation in einem System stellt einen Qualitätssprung dar. Bisher waren im Rahmen der Strafermittlung polizeiliche Informationen in automatisierten Verfahren regelmäßig erst nach Aktenabgabe an die Staatsanwaltschaft im zentralen INPOL-System gespeichert worden. In DIPOL werden polizeiliche Vorgänge von Anfang an, mit Beginn der polizeilichen Tätigkeit automatisiert bearbeitet.

Es werden grundsätzlich alle Daten im System erfaßt, die auf lokaler Ebene anfallen: Strafanzeigen, Verkehrsunfälle, Ordnungswidrigkeiten und Vermißtenanzeigen, aber auch jedes Ereignis, jede Mitteilung aus der Bevölkerung oder von anderen Polizeidienststellen.

Fast jede Berührung mit der Polizei, z.B. als Finder, Zeuge, Auskunftsperson, Hinweisgeber, Anzeigenerstatter, Beschuldigter, Verdächtiger, Opfer, Geschädigter, Kontaktperson eines Beschuldigten findet in DIPOL, jedenfalls auf lokaler Ebene, über einen noch nicht näher festgelegten Zeitraum ihren elektronischen Niederschlag, so daß der Betroffene in einem Ausmaß gezielt abgerufen und überprüft werden kann, wie dies auf der Basis konventioneller Informationsverarbeitung, etwa mit Hilfe des bisher üblichen Tagebuches, nicht möglich war. Die Vernetzung eröffnet überdies Möglichkeiten der Verknüpfung von Datenbeständen in bisher nicht vorstellbarem Umfang.

Anfragen und Mitteilungen anderer Polizeidienststellen über Vorgänge und Sachverhalte können unter Suchbegriffen registriert und deshalb leicht auffindbar abgelegt werden. Dadurch wächst die Gefahr, daß nicht aktualisierte und nicht berichtigte Mitteilungen (Kriminaltaktische oder Erkenntnis-Anfragen) den Betroffenen belasten, weil die Nachberichtspflicht nur für

Informationen in Dateien (§ 38 Abs. 3 SPolG) und keinesfalls in allen Bundesländern, geschweige denn in den EG-Mitgliedsstaaten eingeführt ist. Die Mängel konventioneller Informationsverarbeitung können somit durch DIPOL noch verstärkt werden.

Informationen über Personen und Umstände, die auf geplante Straftaten hinweisen, können als Vorgang erfaßt werden und fördern damit die Möglichkeiten polizeilicher Prävention, aber auch der polizeilichen Kontrolle und Überwachung, ohne daß konkrete Gefahren oder ein hinreichender Anfangsverdacht für eine Straftat vorliegen müssen. Gerade die Unschärfen in der Grenzziehung zulässiger, präventiver Polizeitätigkeit, die mit dem neuen Polizeigesetz nicht ausgeräumt wurden, können sich durch die Informationsverarbeitung in DIPOL verstärkt auswirken (vgl. oben Tz. 3.1). Nicht zuletzt fehlt es bisher an einer gesetzlichen Regelung, die die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei bei der Nutzung neuer Informationssysteme festlegt (vgl. EntschlieÙung der DSB-Konferenz vom 5./6.4.1989, Anlage 11, S. 158 ff, 160 f).

Der Qualitätssprung in der polizeilichen Informationsverarbeitung liegt auch darin begründet, daß bereits bei Eingang einer Anzeige neben der Erfassung auf lokaler Ebene, in den Polizeidienststellen, eine parallele Speicherung in einem zentralen Datenbestand auf Landesebene erfolgen soll. Die automatische Speicherung im INPOL-System erfolgt bisher regelmäßig erst, wenn nach Abgabe an die Staatsanwaltschaft ein fortgeschrittener Ermittlungsstand erreicht war. Der Umfang der zentral gespeicherten Datenarten ist nach der bisherigen Planung sogar noch größer als auf der unteren Ebene (HB S. 477 ff); so soll z.B. die Personenbeschreibung nur im Zentralrechner erfaßt werden. Mit Abschluß der Sachbearbeitung sollen die Informationen auf der lokalen Ebene gelöscht und nur mehr im zentralen Bestand gespeichert bleiben (HB S. 457).

Hieraus ergibt sich vom Beginn der Sachbearbeitung an bis zum Ende der Speicherung eine breite, landesweite Nutzungsmöglichkeit für die Polizei, die in diesem Umfang bisher nicht bestanden hat.

Der Umfang der zentralen Speicherung personenbezogener Daten in DIPOL muß unter dem Gesichtspunkt des Verfassungsgrundsatzes der Verhältnismäßigkeit überprüft werden. Weder die polizeiliche Aufgabenwahrnehmung, noch die Bedürfnisse "zentraler Dienste" dürften einen parallelen Datenbestand auf Landesebene als Spiegelbild eines großen Teils der Vorgänge auf der unteren Ebene rechtfertigen.

Zur Bekämpfung der Kriminalität wird jedenfalls die zentrale Speicherung von Delikten minderschwerer Bedeutung nicht mehr als notwendig angesehen. In einem Pilotprojekt wird derzeit im Saarland die Durchführung eines vereinfachten Verfahrens erprobt. Danach sollen z.B. vorsätzliche Körperverletzung, Bedrohung, einfacher Diebstahl, Unterschlagung, Fahren ohne Fahrerlaubnis, Betrug nicht mehr im INPOL-System gespeichert werden. Die Konzeption einer zentralen Datenbank mit umfassender Datenspeicherung steht im Widerspruch zu neuen polizeitaktischen Erwägungen. Ordnungswidrigkeiten wurden schon bisher nicht und Verkehrsstrafsachen werden neuerdings nicht mehr in vollem Umfang in INPOL gespeichert. Die Erforderlichkeit eines zentralen Vorgangsbestandes zur polizeilichen Aufgabenwahrnehmung wird insoweit auch für DIPOL nicht gesehen. Würde ein Vorgang nicht zu einer Speicherung in INPOL führen, besteht aus der Sicht polizeilicher Aufgabenwahrnehmung auch keine Notwendigkeit für eine Dokumentation in einem zentralen Bestand. Es ist auch nicht einzusehen, daß etwa alle Geschädigten, Verletzten, Zeugen, Hinweisgeber und Auskunftspersonen zentral gespeichert werden.

Auch die Wahrnehmung zentraler Dienste, wie die Erstellung von Statistik und Lagebild, setzt nicht unbedingt eine zentrale Speicherung personenbezogener Daten voraus. Doppelzählungen können auch bei dezentraler Erfassung durch mathematische Verfahren vermieden werden, die eine weitgehende Anonymität sicherstellen (vgl. hierzu bereits Bericht des Ausschusses für Innere Verwaltung zu meinem 6. TB, Anlage 8 des 10. TB, Tz. 8). Die Erstellung eines zutreffenden und brauchbaren Lagebildes dürfte nicht davon abhängen, daß die Personalien von Tätern minderschwerer Delikte bekannt sind.

Der auch in der Projektstudie anerkannte Erfahrungsgrundsatz (HB S. 457), daß die überwiegende Zahl der Beschuldigten in deren Wohnort (wieder) in Erscheinung tritt, spricht eher für eine Konzeption, die auf dezentraler Speicherung aufbaut. Es bleibt deshalb zu prüfen, inwieweit ein zentraler Bestand für einen Großteil der Vorgänge erforderlich und deshalb zulässig ist.

In dem komplexen DIPOL-System ist die Berechtigung zum Speichern, Lesen, Verändern, Verknüpfen der Informationen sowie das Ingangsetzen von Verfahren und Dialogen von fundamentaler Bedeutung, weil auf diese Weise der Umgang mit dem System, die gezielte Auswertung der vorgehaltenen Informationen und Nutzung seiner Kommunikationsmöglichkeiten zur Unterstützung der Ermittlungen gesteuert wird. Damit wird das Ausmaß des Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen in einer Art Feinabstimmung festgelegt. Die Projektstudie geht nicht zu Unrecht davon aus, daß die "Zugriffserfordernisse einem abgestuften, aufgabenorientierten System unterliegen...." (HB S. 565). Die Erforderlichkeit für die polizeiliche Aufgabenwahrnehmung allein ist jedoch als Maßstab für die Zulässigkeit der Nutzung des Systems und der Verwertung der vorgehaltenen Informationen nicht ausreichend.

Das Bundesverfassungsgericht hat die Bedeutung des Gesichtspunkts der Zweckbindung deutlich unterstrichen, der auch bei der Verarbeitung von Informationen durch Weitergabe innerhalb der Polizei zu berücksichtigen ist. Auch nach dem neuen Saarländischen Polizeigesetz dürfen Informationen nur zu dem Zweck verarbeitet werden, zu dem sie erlangt worden sind. Die Verarbeitung zu einem anderen Zweck ist nur zulässig, soweit die Polizei die Informationen zu diesem Zweck erheben dürfte (§ 30 Abs. 1 Satz 2 und 3). Hinsichtlich der sogenannten "Vorgangsverwaltung", bei der allerdings unsicher ist, wo deren Grenzen genau verlaufen, ist die Zweckbindung ebenfalls ausdrücklich vorgeschrieben (§ 31 SPolG). Der Direktzugriff auf automatisiert gespeicherte Daten ist deshalb auch keinesfalls mit der Datenübermittlung gleichzusetzen. Denn diese setzt im Einzelfall eine Prüfung der Zulässigkeitsvoraussetzung voraus und ermöglicht überdies eine solche Prüfung durch die datenliefernde Stelle. Informationen, die im Online-Zugriff stehen, sind als tatsächlich übermittelt anzusehen, weil sie der Berechtigte unmittelbar nutzen kann. Die Zugriffsregelung ist deshalb nicht nur ein Instrument der Datensicherung, sondern auch eine Voraussetzung der materiellen Verarbeitungsregelung. Sie ist eine wichtige Ergänzung der Voraussetzungen für eine zentrale und dezentrale Speicherung. Konsequenterweise hat deshalb das SPolG die Zulässigkeit des automatisierten Abrufverfahrens von einer Abwägung zwischen der polizeilichen Aufgabenerfüllung und den schutzwürdigen Belangen der Betroffenen abhängig gemacht (§ 35). Es bedarf deshalb einer eingehenden Prüfung, inwieweit Bedienstete welcher Funktion und welcher Ebene auf einzelne Datenarten und einzelne Verfahren (z.B. Informationsabgleich) und in welchem Stadium der Vorgangsbearbeitung zugreifen dürfen. Aus dem Spektrum der vielfältigen Überlegungen, die noch anzustellen sind, können nur einige wenige Gesichtspunkte aufgegriffen werden.

Die automatisierte Erfassung vom Beginn der Bearbeitung an (z.B. bei Eingang der Anzeige), in einem Stadium, da häufig noch kein hinreichender Anfangsverdacht vorliegt, erfordert eine Beschränkung des Zugriffs auf die zuständigen Sachbearbeiter auf lokaler Ebene. Dies ist regelmäßig zumindest bis zu dem Zeitpunkt erforderlich, da die Ermittlungsakte an die Staatsanwaltschaft abgegeben wird und ein gewisser Stand der Ermittlungen erreicht ist. Nur Informationen mit überregionaler Bedeutung - zu einer solchen Feststellung bedarf es einer Entscheidungsprozedur - können einem weitergehenden Zugriff von Anfang an unterliegen.

Auf Vorgänge, die nicht der unmittelbaren Bearbeitung von Anzeigen dienen, darf ein anderer als der zuständige Sachbearbeiter ohnehin nicht zugreifen. Informationen der "Vorgangsverwaltung" im Sinne des SPolG (§ 31) dürfen nur für das "jeweilige Vorhaben" genutzt werden. Wo die Grenzlinie zwischen Strafermittlung, Gefahrenabwehr einerseits und dieser Art von "Vorgangsverwaltung" andererseits genau verläuft, muß konkret festgelegt werden, weil nur so den Erfordernissen der Zweckbindung Rechnung getragen werden kann.

Besonders problematisch erscheint die Erfassung von Informationen in DIPOL, die zur Prävention oder aufgrund besonderer Erhebungsbefugnisse gewonnen werden. Hierunter fallen insbesondere alle Informationserhebungen und -verarbeitungen im Vorfeld konkreter Gefahren (§ 26 Abs. 2 SPolG), bei Anwendung besonderer Erhebungsformen (Observation, verdeckter Einsatz technischer Mittel, V-Leute und verdeckter Ermittler nach § 28 SPolG) und bei polizeilicher Beobachtung (§ 29 SPolG). Aufgrund der selektiven Auswertungsmöglichkeiten von DIPOL steht der Polizei ein Verdachtverdichtungsinstrument bereits dann zur Verfügung, wenn weder konkrete Gefahren noch ein hinreichender Anfangsver-

dacht vorliegen. Ich halte es deshalb für notwendig, daß wenigstens Informationen, die - in welcher Form auch immer - verdeckt gewonnen werden, in DIPOL nicht erfaßt werden.

Ein wichtiger Teilaspekt unter Datenschutzgesichtspunkten ist die Dauer der Speicherung. In automatisierten Verfahren dürfen personenbezogene Informationen nur gespeichert werden, soweit und solange ihre ständige Verfügbarkeit für die Wahrnehmung polizeilicher Aufgaben erforderlich ist. Auch die Projektstudie akzeptiert diesen Grundsatz (HB S. 568). Nach der bisherigen Konzeption soll der Datenbestand nach Beendigung der Sachbearbeitung auf lokaler Ebene gelöscht und teilweise auf Landesebene (hinsichtlich der Anzeigen) zentral weitergeführt werden (HB S. 457). Die Unterhaltung eines zentralen Bestandes in DIPOL muß nicht nur von Beginn der Sachbearbeitung an, sondern vor allem auch nach Beendigung der Ermittlungen und Übernahme in INPOL in Frage gestellt werden. DIPOL sollte sich im wesentlichen auf die Funktionen der Vorgangsbearbeitung beschränken. Diese ist jedoch mit der Erfassung von Anzeigen im INPOL-System abgeschlossen; jedenfalls ist eine Doppelspeicherung unzulässig.

Die Schwächen der Bürokommunikation haben auch im Hinblick auf die neue Konzeption einer Infrastruktur für die Polizei ihr Gewicht. Die Anfälligkeit eines solchen Systems infolge von Fehlern und Schwächen der Hard- und Software sowie infolge der Komplexität der vernetzten Verfahren sollte den Blick für die Grenzen der Automation schärfen. Das System selbst muß, soweit wie möglich, Sicherungs- und Kontrollmöglichkeiten verwirklichen. Aber auch ein Revisionskonzept auf der Grundlage unvorhergesehener Überprüfungen interner und externer Stellen muß von vornherein in die Überlegungen einbezogen werden, um die Schwachstellenanalyse zu ergänzen und insbesondere auch die Berücksichtigung neuer Sicherungskonzepte zu gewährleisten.

3.3 Informationsverarbeitung im Bereich der Kriminalpolizei

3.3.1 Das neue Datenschutzkonzept für das Kriminalpolizeiamt (KPA)

Die Ergebnisse meiner Überprüfung des KPA vom 03./04.09.1986 (vgl. meinen 8. TB Tz. 2) wurden im Unterausschuß für Datenschutz erörtert. Bereits in der Sitzung vom 28.09.1988 hat der Leiter des KPA mitgeteilt, daß eine Arbeitsgruppe die Datenschutzprobleme aufgearbeitet und ein neues Datenschutzkonzept entwickelt habe, mit dessen praktischer Umsetzung Anfang 1989 begonnen werde. Im Laufe des Jahres 1989, zuletzt mit Schreiben vom 30.10.1989 hat der Minister des Innern weitere Einzelheiten der Datenschutzplanung mitgeteilt.

Kernstück ist die Einführung eines vereinfachten Verfahrens bei Ermittlungen im Bereich von Delikten minderschwerer Bedeutung, das aufgrund eines gemeinsamen Erlasses des Ministers des Innern und des Ministers der Justiz als Modellversuch in zwei Polizeirevieren erprobt werden soll. Ziel des Modellprojektes ist vor allem die Beschleunigung des Verfahrens und die Reduzierung der Ersterfassung im INPOL-System. Dem Betroffenen bleibt der Weg zur Vernehmung oder Anhörung in der Polizeidienststelle erspart. Beschuldigte und Zeugen können selbst die erforderlichen Angaben auf einem Anhörbogen eintragen und der Polizei übersenden. Die zeitaufwendige Erstellung von Vernehmungsprotokollen durch die Polizeidienststellen entfällt. Das Verfahren wird bei Privatklagedelikten und u.a. bei einfachem Diebstahl, Unterschlagung, Betrug, Fahren ohne Führerschein angewandt. Unter Datenschutzgesichtspunkten ist von besonderer Bedeutung, daß - anders als bisher - die Beschuldigten in diesem Verfahren nicht mehr im INPOL-System erfaßt werden. Ein weiterer Schritt zur Verminderung des Datenvolumens im INPOL-

System ist der Verzicht auf die Erfassung im Bereich der Verkehrsdelikte. Wird das Verfahren nach der Erprobung landesweit eingeführt, ist damit zu rechnen, daß die jährliche Erfassung in INPOL von etwa 60.000 Fällen um 18.000 Fälle reduziert wird. Die dadurch freierwerdenden Arbeitskapazitäten sollten auch für die vom Parlament angeordneten Maßnahmen zur Verbesserung des Datenschutzes im Bereich der Kriminalpolizei genutzt werden (vgl. Bericht des Ausschusses für Innere Verwaltung vom 09.11.1989, Lt-Drucksache 9/1038-9/1521 Tz. 2.2, Anlage 8).

Vor allem muß es nunmehr möglich sein, den bereits in früheren Tätigkeitsberichten (4. TB Tz. 11; 6. TB Tz. 6.5) wiederholt angemahnten Rücklauf der staatsanwaltlichen und gerichtlichen Entscheidungen an das KPA in die Praxis umzusetzen, damit die Datenbestände der Polizei aktualisiert und fortgeschrieben werden können. Insbesondere die Speicherdauer der Daten kann durch den Ausgang der justiziellen Verfahren beeinflußt werden. Eine Arbeitsgruppe hat bereits die Vorarbeiten für ein dv-gestütztes Verfahren durchgeführt.

Es ist ein wesentliches Anliegen jedes Betroffenen und Überdies ein Element effektiver polizeilicher Aufklärungsarbeit, daß die vorgehaltenen Informationen den Tatsachen und dem letzten Stand der Erkenntnis entsprechen. Die Speicherung über einen Zeitraum von im Regelfall 10 Jahren ist für den Betroffenen von großer Tragweite. Was nützt indessen die angestrebte Reduzierung der Datenbestände durch Verminderung der Erfassung, wenn die Richtigkeit und Vollständigkeit der gespeicherten Daten nicht gewährleistet ist. Deshalb ist es zu begrüßen, daß auch das Parlament eine Verbesserung der internen Kontrolle des kriminalpolizeilichen Meldedienstes befürwortet (Anlage 8 Tz. 2.1). Bisher wurde lediglich bei der Personen- und Sachfahndung die Richtigkeit und Vollständigkeit der Erfassung

überprüft. Die polizeilichen Datensammlungen im übrigen bedürfen jedoch ebenfalls einer solchen Erfassungsprüfung. Die bisher durchgeführten Plausibilitätsprüfungen können allein nicht sicherstellen, daß die auch seitens des Ministeriums durchaus eingeräumten Mängel der Datenerfassung beseitigt werden (vgl. RSt zum 8. TB Tz. 2.1.1). Für den gesamten Bereich der polizeilichen Datenerfassung ist deshalb ein effektiver Prüfdienst einzurichten.

Der Forderung, die Datensammlungen und Systeme zu bereinigen, beginnt das KPA nunmehr nachzukommen. Aus der Kriminalaktenammlung von etwa 100.000 Fällen sind 8.857 Akten überprüft und davon 7.040 ausgesondert worden. Nur noch 20,5 % der überprüften Akten werden weiter aufbewahrt; der Rest wurde vernichtet. Zugleich wurden die jeweils zugehörigen Personendatensätze in INPOL überprüft und 1.050 Fälle gelöscht.

Angesichts der außerordentlich hohen Quote aussondernder Akten muß diese Aktion fortgesetzt werden. Zugleich muß an das Eingeständnis des zuständigen Ressorts erinnert werden, daß bei der Übernahme von Altaktenbeständen in INPOL die an sich notwendige Abwägung im Einzelfall zugunsten eines Verfahrens der "Standardisierung und Verwaltungsvereinfachung" zurückgestellt wurde (RSt zum 8. TB Tz. 2.1.3). Eine "inhaltliche Prüfung" wurde auch bei der Überführung der Erkennungsdienstdatei in den automatisierten Bestand nicht vorgenommen (RSt zum 8. TB Tz. 2.1.5). Die Bereinigung muß deshalb auch unter Einbeziehung aller automatisiert im Polizeibereich vorgehaltenen Daten entsprechend der Forderung des Parlaments erfolgen (Anlage 8 Tz. 2.2).

Bereits im Bericht des Ausschusses für Innere Verwaltung des Landtags zu meinem 6. Tätigkeitsbericht (Lt-Drucksache 9/1110-9/4, Tz. 7) wird die Praxis der Speicherung des Freitodversuches in Polizeidateien

kritisiert und eine Überprüfung der bisherigen Verfahrensweise gefordert (vgl. meinen 6. TB Tz. 6.3.3). Es muß eingeräumt werden, daß bei der Speicherung von sogenannten "personengebundenen Hinweisen" sich erhebliche Verbesserungen ergeben haben. Gleichwohl darf die Problematik der Suizidenten nicht in Vergessenheit geraten (vgl. bereits Ausschuß für Innere Verwaltung am 27.04.1987, 10. TB Anlage 8 Tz. 7).

Die Probleme der Dokumentation treten bei den eingriffsintensiven, erkennungsdienstlichen Maßnahmen besonders zutage. Dazu zählt auch die Fertigung von Lichtbildern. Die Speicherungsgründe und die der Weitergabe - vor allem auch bei Lichtbildern - müssen protokolliert werden, um die Zulässigkeit der Informationsverarbeitung stets nachweisen zu können. Entsprechende Maßnahmen sind für das Jahr 1990 angekündigt.

Im Bereich Kindeskriminalität sollen die Spezialdateien abgebaut werden (vgl. Anlage 8 Tz. 2.3). Das Verfahren für die Erstellung der Kriminalstatistik soll datenschutzgerecht ausgestaltet werden (vgl. bereits Ausschuß für Innere Verwaltung vom 27.04.1987, 10. TB, Anlage 8 Tz. 8).

Der Ausschuß für Innere Verwaltung erwartet, "daß der Beginn der praktischen Umsetzung des neuen Konzepts alsbald die Datenschutzsituation im Polizeibereich verbessern wird" (vgl. Anlage 8 Tz. 2).

3.3.2 PC-Einsatz

Der Einsatz von PC ist mit besonderen Gefahren für das informationelle Selbstbestimmungsrecht verbunden, die im 10. Tätigkeitsbericht (Tz. 4.2 und Tz. 4.3.2) dargestellt wurden. Der Minister des Innern hat eine Dienstanweisung erarbeitet, die den datenschutzrechtlichen Risiken soweit wie möglich vorbeugt. Danach

werden PC bei umfangreichen, strafrechtlichen Ermittlungsverfahren eingesetzt, die mit konventionellen Mitteln nicht zu bewältigen sind.

Die Daten dürfen grundsätzlich nur für die Zwecke des Verfahrens verwendet werden, für das sie im PC gespeichert wurden. Die Verknüpfung mit Daten aus anderen Verfahren ist nur nach vorheriger Prüfung und Genehmigung durch den Datenschutzbeauftragten des KPA zulässig. Diese Verfahrensregelung ist geeignet, die Einhaltung der Zweckbindung und die Beachtung der Verwertungsverbote zu gewährleisten.

Für jedes Verfahren ist eine Errichtungsanordnung zu fertigen, die nach vorheriger Beteiligung des Landesbeauftragten für Datenschutz der Genehmigung durch das Ministerium bedarf. Das KPA führt eine Dateienübersicht. Datenübermittlungen sind nicht zugelassen. Die Zugriffe sind auf die mit der Sachbearbeitung betrauten Bediensteten beschränkt.

Zur Datensicherung ist ein Katalog konkreter Maßnahmen vorgesehen. Zur Zugriffssicherung wird neben Verfahren der Benutzerkennung und der Vergabe von Paßwörtern eine besondere Software eingesetzt, wenn mehrere Verfahren auf einem PC betrieben werden. Die Benutzeraktivitäten werden protokolliert. Die Verwendung privater Hard- und Software ist untersagt.

Die Funktionstrennung ist jedenfalls insoweit aufbauorganisatorisch sichergestellt, als die Systemverwaltung und Programmierung in einer anderen Organisationseinheit als der erfolgt, in der der PC-Einsatz und die Anwendung der Programme durchgeführt wird. Die Programmierung und Systemverwaltung ist zwar noch in einer Organisationseinheit zusammengefaßt, weil eine Trennung dieser Funktionen derzeit noch auf unüberwindliche, organisatorische und personelle Schwierigkeiten stößt. Die mit der Systemverwaltung verbundenen

Risiken sind indessen überwiegend systembedingt; ihnen sollte vor allem durch entsprechende Vorkehrungen der Hersteller begegnet werden (vgl. Entschließung der DSB-Konferenz vom 10.10.1988, 10. TB Anlage 3 Tz. 3). Die Gefahren sind im übrigen im konkreten Fall als nicht so groß anzusehen, daß eine Beanstandung gerechtfertigt gewesen wäre. In der Abwägung der Risiken für die schutzwürdigen Belange der Betroffenen mit den Notwendigkeiten zur Wahrung der inneren Sicherheit konnten die bereits getroffenen Maßnahmen vorerst als ausreichend erachtet werden. Ich habe indessen den Vorbehalt angemeldet, daß eine Funktionstrennung zwischen Programmierung und Systemverwaltung jedenfalls dann zu verwirklichen ist, wenn sich die Personalsituation verbessert hat. Denn die fortschreitende Automation und der vermehrte PC-Einsatz setzen zwangsläufig zusätzliches gut ausgebildetes Fachpersonal voraus.

3.4 Überprüfung eines Polizeireviers

3.4.1 Schankkonzessionsdatei

In einem Polizeirevier im Bereich der Landeshauptstadt habe ich anlässlich einer Überprüfung eine Aktensammlung über etwa 470 Gaststätten festgestellt, die über eine Findexdatei erschließbar ist. Die Akten enthalten Vorgänge über alle seit den 50er Jahren tätig gewesenen Gastwirte im Revierbereich. Neben Konzessionsurkunden, Bauplänen der konzessionierten Räumlichkeiten werden Strafregisterauszüge, Polizeiberichte über strafbare Handlungen und Ordnungswidrigkeiten der Konzessionsinhaber sowie sonstige Vorfälle und Beobachtungen über das Verhalten dieser Personen aufbewahrt. Außerdem geben die Akten Auskunft über den Inhalt von Bierlieferungsverträgen sowie die Umsätze. Ich halte die Vollzugspolizei nicht für berechtigt,

eine spezielle Datensammlung dieses Inhalts vorzuhalten.

Ehemalige und derzeitige Gaststätteninhaber im Zuständigkeitsbereich des Polizeireviers dürfen nicht schon deshalb in Unterlagen der Vollzugspolizei geführt werden, weil möglicherweise in den Räumen strafbare Handlungen oder Ordnungswidrigkeiten begangen werden könnten. Die Datensammlung stellt eine unzulässige Datenvorratshaltung dar. Es werden Informationen über Personen, die größtenteils nicht einmal mehr ihren Beruf in dem Revier ausüben, in einem Umfang vorgehalten, der in keinem Verhältnis zu den Zwecken der Prävention steht.

Zu präventiven Zwecken darf die Polizei Informationen allenfalls über strafbare Handlungen und dies nur in eingeschränktem Umfang speichern. Werden solche festgestellt, sind die im Bereich der Vollzugspolizei eingerichteten Informationssysteme zu nutzen. Die Doppelspeicherung für einen zudem örtlich begrenzten Sonderbereich ist nicht zulässig, weil sonst erfahrungsgemäß die Richtigkeit und Aktualität der Daten nicht gewährleistet ist. Die Einhaltung der Löschungsfristen ist erschwert, weil - wie die vorgefundene Sammlung belegt - der Überprüfungsaufwand nicht zu leisten ist. Zudem gibt die auf einen örtlich begrenzten Bereich beschränkte Sammlung von Informationen über gegebenenfalls strafwürdiges Verhalten einer Person eine nur ungenaue - weil eingeschränkte - Auskunft, die gerade zu präventiven Zwecken nicht ausreicht. Informationen über Konzessionsinhaber dürfen im übrigen nur von den dafür zuständigen Verwaltungspolizeistellen geführt werden.

3.4.2 Direktzugriff auf das computerisierte Melderegister

Für das überprüfte Polizeirevier ist ein automatisierter Direktzugriff auf das computerisierte Melderegister der Landeshauptstadt eingerichtet. Die Datenschutzproblematik eines solchen Anschlusses habe ich bereits dargelegt (vgl. meinen 7. TB Tz. 4.3.1). Die zum Abruf bereitgehaltenen Daten sind insgesamt als an die Vollzugspolizei übermittelt anzusehen, weil sie unmittelbar in den Bestand eingreifen und über diese Daten voll verfügen kann. Die Polizei erhält auf diese Weise Kenntnis auch von Daten völlig unbescholtener und unbeteiligter Bürger. Nicht nur die Rechtsgrundlage für einen solchen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen ist zweifelhaft, sondern es fehlt auch an der gesetzlichen Festlegung der organisatorisch-technischen Maßnahmen der Datensicherung im Interesse eines vorbeugenden Rechtsschutzes. Der Ausschuß für Innere Verwaltung hat darum schon für die Übergangszeit bis zu einer den Anforderungen gerecht werdenden gesetzlichen Regelung es für notwendig gehalten, daß das Abrufverhalten der Polizei durch eine automatisierte Protokollierung überprüft werden kann (Lt-Drucksache 9/1850-9/468, Tz. 4.3; 10. TB Anlage 9). Daß der Ausschuß im übrigen davon ausgeht, daß die melderechtlichen Grundlagen nachgebessert werden müssen, sei in diesem Zusammenhang nochmals erwähnt.

Mittels Online-Anschluß können in dem überprüften Polizeirevier alle Namen und Adressen der Bewohner der Landeshauptstadt abgerufen werden. Damit ist der in der Rechtsverordnung vorgegebene Rahmen abrufbarer Daten nicht völlig ausgeschöpft. Eine weitere Ausdehnung des Direktzugriffs auf einen erweiterten Datensatz ist jedoch nicht gerechtfertigt. Aus den Gesprächen mit den Vollzugsbeamten ist deutlich geworden, daß der automatisierte Abruf von Namen und Adressen

regelmäßig den Informationsbedarf der Vollzugspolizei abdeckt. Insbesondere die häufig erforderliche Überprüfung der Personalien kann in den meisten Fällen kurzfristig durchgeführt werden. Damit können Unsicherheiten über die Identität des Betroffenen auch in seinem Interesse kurzfristig ausgeräumt werden.

Die Überprüfung hat jedoch ergeben, daß in der Mehrzahl der Fälle keine Eilbedürftigkeit gegeben war. Die Überprüfung von Anschriften zu ladender Personen in laufenden Ermittlungsverfahren bedarf jedenfalls keiner Erledigung in Sekundenschnelle. Außerdem wurden die Abfragen überwiegend während der Dienstzeit des Einwohnermeldeamtes abgewickelt. Die Frage ist deshalb erlaubt, ob und inwieweit der automatisierte Direktzugriff auf das Melderegister angemessen und gerechtfertigt ist. Der Minister des Innern ist der Auffassung, daß der Direktabruf nicht nur wegen der Eilbedürftigkeit im Einzelfall und wegen der Zugriffsmöglichkeit außerhalb der Dienstzeiten des Meldeamtes - vor allem bei Nacht - im Interesse der Strafverfolgung und Gefahrenabwehr erforderlich sei. Vielmehr spreche die starke Inanspruchnahme der Meldeämter gerade während der Dienstzeit für die Einrichtung eines Online-Anschlusses.

Grenzen der Automation werden auch in diesem Zusammenhang erkennbar. Die Auffassung des Ausschusses für Innere Verwaltung ist jedenfalls gerechtfertigt, daß die Angemessenheit eines solchen Eingriffs in das informationelle Selbstbestimmungsrecht der an sich Unbeteiligten durch den Direktzugriff auf das Melderegister einer jeden Gemeinde einer sorgfältigen Prüfung bedarf. Dabei ist der etwaige Informationsbedarf der Polizei im Hinblick auf das Kriminalitätsaufkommen ebenso in die Abwägung einzubeziehen wie die konventionelle Auskunftsmöglichkeit aus dem Melderegister. Außer in den Ballungsräumen dürfte ein Online-Anschluß nicht in Betracht kommen. Ein flächendeckender Zugriff

auf alle Melderegister des Saarlandes ist jedenfalls nicht gerechtfertigt.

Die Automation weckt Informationsbedürfnisse; der Informationsfluß vergrößert sich geradezu zwangsläufig. Auch diese allgemeine Erfahrung wurde durch das Prüfergebnis bestätigt. In dem Polizeirevier, das über den Anschluß verfügt, werden nicht etwa nur die Vorgänge im unmittelbaren Zuständigkeitsbereich dieses Reviers, sondern für alle Polizeidienststellen innerhalb und außerhalb des Saarlandes abgewickelt. In einem Fall wurden sogar Daten im Auftrag der Bahnpolizei abgefragt. Die Eingriffsintensität des automatisierten Direktzugriffs auf das Melderegister, die vor allem darin liegt, daß der gesamte im Zugriff stehende Datenbestand als übermittelt gelten muß, tritt bei der "Gruppenauskunft" besonders deutlich zutage. Unter einer Adresse können nämlich alle Bewohner eines Hauses abgefragt werden. Auf diese Weise können an sich Unbeteiligte aus einem konkreten Anlaß in einen unmittelbaren Zusammenhang mit einer strafbaren Handlung gebracht werden (z.B. Alkoholfahrt des flüchtigen Mitbewohners eines Hauses). Unter diesem Gesichtspunkt muß die Funktion des Polizeireviers als Kopfstelle für die automatisierte Abwicklung der Abfragen aller Polizeidienststellen des Landes als problematisch angesehen werden. Das Prinzip, daß die Verhältnismäßigkeit des Direktzugriffs von der Kriminalitätsgeneigtheit eines begrenzten räumlichen Bereiches einer Gemeinde/Stadt abhängig ist, wird spätestens bei dieser "kleinen Rasterfahndung" durch Gruppenauskunft vernachlässigt, wenn unbeteiligte Mitbewohner eines Hauses, in dem ein Verdächtiger wohnt, auch bei Vorfällen außerhalb der Landeshauptstadt ohne weiteres in die automatisierte Überprüfung einbezogen werden. Das Polizeirevier ist inzwischen angewiesen, Auskunftsersuchen dieser Art, "falls unbedingt erforderlich", jedenfalls nur noch für Dienststellen der Vollzugspolizei im Bereich der Landeshauptstadt zuzulassen.

Die Meldedatenübermittlungsverordnung zur näheren Ausgestaltung des Direktabrufverfahrens erinnert an die selbstverständliche Voraussetzung, daß der Direktabruf nur zulässig ist, wenn im Einzelfall die Kenntnis der Daten erforderlich ist (§ 6 Abs. 2). Angesichts der jedenfalls technisch freien Verfügbarkeit über die Meldedaten, die durch den Online-Anschluß gegeben ist, muß an diese Voraussetzung einer jeden Einsichtnahme in das Melderegister durch die Polizei nachdrücklich erinnert werden. Ob die Einhaltung der rechtsstaatlichen Schranken angesichts des jederzeit technisch Machbaren stets gewährleistet ist, muß auch hier gefragt werden. Wenigstens sollte die nachträgliche Überprüfbarkeit der Abrufe gewährleistet sein. Derzeit können die Abrufe lediglich anhand einer konventionell geführten Liste überprüft werden. Dieses Kontrollinstrument kann nicht gewährleisten, daß alle Vorgänge registriert werden. Die Überprüfung hat im übrigen ergeben, daß die Namen derjenigen, die abgerufen wurden, überhaupt nicht und in der überwiegenden Zahl der Fälle auch nicht die Aktenzeichen oder Tagebuchnummern der zugrundeliegenden Vorgänge aufgezeichnet wurden. Diese unzureichende Art der Protokollierung ist nicht prüffähig, weil der Einzelfall nicht den Aktenvorgängen zugeordnet und die Erforderlichkeit des Abrufs nicht beurteilt werden kann. Inzwischen ist dieser Mangel behoben; die Namen der Betroffenen, die Aktenzeichen oder die konkreten Sachverhaltsangaben werden notiert. Stichproben zur Überprüfung der Zulässigkeit des Abrufs sind angeordnet.

Aus der Protokollierung der Einzelvorgänge könnten sich allerdings auch zusätzliche Belastungen für den Betroffenen ergeben, weil seine Daten nicht nur zu Prüfzwecken, sondern auch zu weiteren Recherchen verwendet werden können. Das würde jedoch dem Grundsatz der Zweckbindung zuwiderlaufen, wie er gerade für solche Art polizeilicher Dokumentation - allerdings be-

schränkt auf die Gefahrenabwehr - gesetzlich festgeschrieben ist (§ 31 SPolG). Das Polizeirevier ist zwar inzwischen angewiesen worden, die Protokolldaten nur zu Prüfzwecken zu nutzen. Gleichwohl lege ich Wert darauf, daß die Dokumentation des Abrufverhaltens nur einen möglichst kurzen Zeitraum erfolgen soll.

3.5 Datenschutz in Notruffällen

Die Eingabe eines Notarztes hat zu einer bundesweiten Erörterung geführt. Eine einheitliche, leicht einprägsame Arzt-Notruf-Nummer existiert nicht. Die Rufnummer der zentralen Rettungsleitstelle des Saarlandes ist nicht hinreichend bekannt. Deshalb wird die Polizei-Notruf-Nummer 110 - wie auch in anderen Bundesländern - häufig zur Verständigung des Notarztes oder für die Anforderung eines Krankenwagens benutzt, ohne daß es sich dabei um polizeirelevante Vorfälle handeln muß. Oft noch bevor der Notarzt eintrifft, findet sich die Polizei am Notfallort ein. Bei häuslichen Unfällen, akuten Erkrankungen besteht für die Beteiligung der Polizei jedoch keine Notwendigkeit. Hinzu kommt, daß durch den Notruf über die Polizeinummer nicht nur wertvolle Zeit verloren geht, sondern auch für den Notarzt wichtige Informationen nicht erfragt bzw. lücken- oder fehlerhaft weitergegeben werden. Vor allem begibt sich der Anrufer der Möglichkeit, sein Anliegen nur einem Arzt anzuvertrauen und damit den Schutz der ärztlichen Schweigepflicht für sich in Anspruch nehmen zu können. Erfolgt der Notruf im Zusammenhang mit Verletzungen, die sich der Betroffene bei einem Gesetzesverstoß zugezogen hat, ist sogar die Gefahr der unzulässigen Selbstbezeichnung gegeben.

Die Diskussion darüber, wie dem Hilfesuchenden ein leichter und unmittelbarer Zugang zum Arzt und zur Rettungsleitstelle eröffnet werden könnte, hat noch zu keinem Ergebnis geführt. Eine zumindest für das ganze

Saarland verwendbare Rufnummer ohne Ortskennzahl ist unerläßlich. Der Minister des Innern befürwortet zwar eine solche Lösung, sieht jedoch derzeit keine Realisierungsmöglichkeit. Die Deutsche Bundespost sah sich zur Verwirklichung eines solchen Konzepts noch nicht in der Lage. Auf Bundesebene wird zur Zeit die Einrichtung einer einheitlichen Rufnummer (19222) für den Rettungsdienst angestrebt, die derzeit jedenfalls in Bayern bereits genutzt werden kann. Im Saarland sollte ebenfalls ein solches Projekt alsbald realisiert werden. Zwar kann bereits heute bei Eingang eines Notrufes für ärztliche Hilfe zur Rettungsleitstelle direkt von der Polizei durchgeschaltet werden. Dies erfolgt jedoch erst, nachdem die Polizei bestimmte Informationen abgefragt hat. Es ist deshalb notwendig, bis zur Einrichtung einer einheitlichen Rufnummer für den Rettungsdienst die Telefonnummer der Rettungsleitstelle an exponierter Stelle im Telefonbuch zu veröffentlichen und auf diese Weise für einen besseren und leichteren, unmittelbaren Zugang zum Arzt zu sorgen.

Da jedoch auch nach Einrichtung einer einheitlichen Rufnummer sowie besserer Öffentlichkeitsarbeit nicht auszuschließen ist, daß ärztliche Hilfe über den Polizeinotruf angefordert wird, sollte unverzüglich nachdem der den Anruf entgegennehmende Polizeibeamte den Zweck des Anrufes erkennt, ein unmittelbares Durchschalten zur Rettungsleitstelle erfolgen.

4. Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes

4.1 Novellierung des Bundesdatenschutzgesetzes

Hinter der Bezeichnung "Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes" verbirgt sich ein Artikelgesetz, mit dem das Bundesdatenschutzgesetz und das Bundesverfassungsschutzgesetz novelliert und die gesetzlichen Grundlagen für die Informationsverarbeitung des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes geschaffen werden sollen. So begrüßenswert und notwendig diese Gesetzesvorhaben sind, so bedauerlich ist es, daß die Gesetzentwürfe datenschutzrechtlichen Anforderungen nicht in ausreichender Weise Rechnung tragen. Ich habe in meiner Stellungnahme zu dem Artikelgesetz umfangreiche Änderungen angeregt. Nur auf zwei Schwerpunkte möchte ich hinweisen.

Der Entwurf zur Novellierung des Bundesdatenschutzgesetzes stellt in wesentlichen Fragen des Datenschutzes keine entscheidende Verbesserung gegenüber der derzeitigen Rechtslage dar. Es ist insbesondere verfehlt, das allgemeine Datenschutzrecht aufzuteilen in ein dateibezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz. Wichtige Verwaltungsbereiche werden im Verwaltungsverfahrensgesetz nicht erfaßt und damit der unabhängigen, externen Datenschutzkontrolle entzogen. Schon deshalb wäre es konsequent gewesen, das allgemeine Datenschutzrecht in einem umfassenden Gesetz zu konzentrieren. Die nunmehr vorliegende Konzeption dient weder der Rechtsvereinheitlichung noch der Vereinfachung der Rechtsanwendung noch der Normenklarheit.

Auch in einem anderen Punkt erscheint es mir zweifelhaft, ob der Gesetzentwurf den Anforderungen des Bun-

desverfassungsgerichts hinreichend Rechnung trägt. Das Bundesverfassungsgericht hält eine gesetzliche Festlegung des Verwendungszweckes erhobener Daten für erforderlich, damit der Bürger überschauen kann, über welche ihn betreffenden Informationen die Verwaltung verfügt. Der Entwurf bekennt sich zwar zum Grundsatz der Zweckbindung, den er jedoch durch eine Vielzahl von Ausnahmen durchbricht, so daß die Transparenz und Überschaubarkeit der Datenverarbeitung für den Bürger letztendlich nicht gegeben ist.

Mit dem Gesetzentwurf zur Novellierung des Bundesdatenschutzgesetzes hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz anläßlich ihrer Sitzung am 5./6. April 1989 in Saarbrücken befaßt und die als Anlage 9 beigefügte EntschlieÙung verabschiedet.

4.2 Rechtsgrundlagen für die Nachrichtendienste

Nach dem in der letzten Legislaturperiode gescheiterten Versuch, die Tätigkeit der Nachrichtendienste auf eine verfassungskonforme, gesetzliche Grundlage zu stellen, hat die Bundesregierung mit der Vorlage des Artikelgesetzes einen erneuten Anlauf genommen, in diesem sensiblen Bereich die erforderlichen normativen Grundlagen zu schaffen. Gerade im Bereich der Nachrichtendienste tritt die Spannung zwischen dem informationellen Selbstbestimmungsrecht und den allgemeinen Sicherheitsinteressen besonders deutlich zutage. Bei allem Bemühen um einen Ausgleich zwischen diesen Positionen darf aber nicht vergessen werden, daß die Nachrichtendienste zumeist im Verborgenen arbeiten und deshalb ein besonderes Bedürfnis besteht, die Grenzen zulässiger Eingriffe durch Informationsverarbeitung deutlich zu markieren und für eine Beachtung des Verhältnismäßigkeitsprinzips zu sorgen. Auf diese Weise

muß sichergestellt werden, daß ein wesentliches Element des freiheitlich demokratischen Gemeinwesens keinen Schaden erleidet. Der einzelne Bürger darf nicht durch undurchschaubare Informationsverarbeitung der Nachrichtendienste verunsichert und dadurch veranlaßt werden, auf die Teilnahme am politischen Leben zu verzichten (BVerfGE 65,1, 42 ff).

Dieser Vorgabe werden die vorgelegten Entwürfe in vielerlei Hinsicht nicht gerecht. Für den einzelnen ist nicht deutlich genug erkennbar, wann er die Schwelle von der Ausübung eines Grundrechtes zur verfassungsfeindlichen Bestrebung überschreitet. Es sollte näher geregelt werden, ob, in welchem Umfang und für welchen Zweck das Sammeln und Speichern von Informationen zulässig ist. Nach der derzeitigen Fassung der Gesetzentwürfe ist nicht hinreichend klargelegt, ob auch Informationen über nichtextremistische Organisationen sowie unverdächtige und unbeteiligte Personen verarbeitet werden dürfen, wenn diese lediglich in einem nicht beabsichtigten Zusammenhang mit verfassungsfeindlichen Bestrebungen stehen.

Präziser geregelt werden muß auch der Einsatz nachrichtendienstlicher Mittel. Es muß klargelegt werden, gegen wen sich der Einsatz von V-Leuten, Ton- oder Bildaufzeichnungsgeräten richten darf und was mit den Daten Unverdächtigter zu geschehen hat. Sichert werden muß auch, daß die Befugnis zum Einsatz von nachrichtendienstlichen Mitteln Eingriffe gegen private Dritte nicht rechtfertigt.

Schließlich erscheint mir erforderlich, daß die Zusammenarbeit zwischen Polizei und Nachrichtendiensten präziser geregelt wird. Aus dem Trennungsgebot für Polizei und Nachrichtendienst folgt, daß der Datenaustausch zwischen diesen beiden Bereichen nur nach Maßgabe einschränkender Verwertungsregelungen erfolgen

darf. Diesem Gebot tragen die Gesetzentwürfe über die Nachrichtendienste noch nicht hinreichend Rechnung.

Die Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz haben sich anlässlich ihrer Sitzung am 30. Mai 1989 mit den vorliegenden Gesetzentwürfen befaßt und dabei die als Anlage 10 beigefügte EntschlieÙung verabschiedet.

5. Rechtspflege

5.1 Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts

Auf die Notwendigkeit zur Novellierung der Strafprozeßordnung habe ich bereits in der Vergangenheit mehrfach hingewiesen (vgl. 10. TB Vorbemerkung Seite 3,4; 9. TB Tz. 2.1). Im Berichtszeitraum hat der Bundesminister der Justiz den Referentenentwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vorgelegt. Der Gesetzentwurf, der umfangreiche Regelungen für die Datenverarbeitung der Strafverfolgungsbehörden enthält, stellt zweifelsohne einen beachtlichen Versuch zur Anpassung der Strafprozeßordnung an die Anforderungen des Bundesverfassungsgerichts dar. Dennoch genügt er in einer Reihe von Punkten datenschutzrechtlichen Belangen nicht.

Ich habe in meiner Stellungnahme gegenüber dem Minister der Justiz das Fehlen von Bestimmungen gerügt, die den Persönlichkeitsschutz bei der Erhebung persönlicher Daten von Angeklagten und Zeugen in öffentlicher Sitzung verbessern können. Mein Anliegen zielt darauf ab, Angeklagten und Zeugen die Offenbarung intimer Lebensumstände vor einer sensationsgierigen Öffentlichkeit zu ersparen, soweit dies nicht aus verfahrensrechtlichen Gründen unerlässlich ist. Vor allem in Fällen, in denen der Täter sich schuldig bekennt, erscheint es nicht gerechtfertigt, seinen persönlichen Werdegang, aus dem sich eine Vielzahl von Informationen auch über andere Personen ergeben, in öffentlicher Sitzung nachzuvollziehen.

Mein besonderes Interesse galt dem Zugang zu den Strafakten. Nach der derzeitigen Rechtslage erhalten Angeklagte Akteneinsicht nur über ihren Verteidiger. Ist eine derartige Bestimmung für das Strafverfahren, in dem regelmäßig ein Verteidiger bestellt ist, noch

hinnehmbar, so wirft sie im Bußgeldverfahren, in dem erfahrungsgemäß eine Vielzahl von Personen anwaltlich nicht vertreten ist, besondere Probleme auf. Denn sie eröffnet dem Beschuldigten, der sich über die Beweissituation informieren will, nur die Wahl, entweder einen Anwalt zu beauftragen und damit bei aussichtsloser Rechtslage zusätzliche Kosten in Kauf zu nehmen oder den Bußgeldbescheid von vorneherein zu akzeptieren. Der Auskunftsanspruch des Betroffenen ist eine unabdingbare Voraussetzung für die Gewährleistung des informationellen Selbstbestimmungsrechts. Die derzeitige Rechtslage halte ich deshalb verfassungsrechtlich für problematisch. Ich habe daher gefordert, dem Beschuldigten sowohl im Strafverfahren als auch im Ordnungswidrigkeitenverfahren uneingeschränkt Akteneinsicht zu gewähren.

Andererseits halte ich es für erforderlich, das Akteneinsichtsrecht durch Dritte stärker einzuschränken. Nach dem Gesetzentwurf kann Dritten Akteneinsicht gewährt werden, wenn ein berechtigtes Interesse glaubhaft gemacht wird. Ausreichend für die Gewährung von Akteneinsicht sind hiernach bereits vernünftige Überlegungen, die die vorgesehene Datenverarbeitung in Einklang mit der Rechtsordnung erscheinen lassen. Nach meiner Überzeugung ist ein solch weitgehendes Recht zur Einsichtnahme in Strafverfahrensakten, die schließlich in großem Umfang sensible Daten enthalten, nicht vertretbar. Ich habe daher gefordert, Dritten Akteneinsicht nur dann zu gewähren, wenn sie ein rechtliches Interesse begründen können, das heißt ihr Interesse durch eine Rechtsnorm legitimiert wird.

Auch der Zugriff der Wissenschaft, die nach meinen Erkenntnissen ein starkes Interesse an Strafverfahrensdaten hat, muß eingegrenzt werden. Insbesondere halte ich es für notwendig, daß die Strafakten bei der aktenverarbeitenden Stelle bleiben, also auch zum

Zwecke wissenschaftlicher Auswertung nicht an die forschende Stelle übergeben werden dürfen.

Die Konferenz der Datenschutzbeauftragten hat sich anlässlich ihrer Sitzung am 5./6. April 1989 in Saarbrücken ebenfalls mit dem Gesetzentwurf zur Änderung und Ergänzung des Strafverfahrensrechts befaßt und die als Anlage 11 beigefügte EntschlieÙung verabschiedet. Es bleibt zu hoffen, daß angesichts der vielfachen Anregungen aus dem Kreis der Datenschutzbeauftragten eine gesetzliche Regelung gefunden wird, die dem Recht auf informationelle Selbstbestimmung ausreichend Rechnung trägt.

5.2 Novellierung des Bundeszentralregistergesetzes

Aufgrund gesetzlicher Errichtungsanordnung wird in Berlin das Bundeszentralregister geführt. In dieses Register werden personenbezogene Entscheidungen öffentlicher Stellen eingetragen. Den Schwerpunkt bilden hierbei strafgerichtliche Verurteilungen sowie Entscheidungen über paßrechtliche, waffenrechtliche und gewerberechtliche Verstöße. Neben der Auskunftserteilung an öffentliche Stellen hat das Bundeszentralregister vor allem die Aufgabe, den Bürgern im Wege einer Selbstauskunft staatliche Führungszeugnisse zur Verfügung zu stellen. Es liegt auf der Hand, daß eine derartige Einrichtung mit vielfältigen datenschutzrechtlichen Problemen verbunden ist. Der Bundesminister der Justiz hat den Arbeitsentwurf eines Gesetzes zur Änderung des Bundeszentralregistergesetzes vorgelegt. Der Gesetzentwurf trägt datenschutzrechtlichen Anforderungen bereits in hohem Maße Rechnung. Ich habe in meiner Stellungnahme an den Minister der Justiz weitere Verbesserungen angeregt.

Eine meiner zentralen Forderungen besteht darin, auf die nach dem Gesetzentwurf zugelassene Einrichtung von

Direktabrufverfahren zu verzichten. Die Besonderheit von Direktabrufverfahren ergibt sich daraus, daß die abfragenden Stellen unmittelbar und direkt auf den Datenbestand der speichernden Stelle zugreifen und über diese Daten wie über eigene verfügen können. Die Einrichtung eines Direktabrufverfahrens beinhaltet daher nicht lediglich eine schnellere Form der Übermittlung im Einzelfall, sondern eine qualitativ andere Art der Datenübermittlung. Diesem Gesichtspunkt muß bei der Entscheidung der Frage, ob Direktabrufverfahren zugelassen werden, in besonderem Maße Rechnung getragen werden. Da das Bundeszentralregister seit seiner Errichtung ohne die Möglichkeit von Direktabrufverfahren ausgekommen ist, habe ich große Zweifel an der Notwendigkeit, zum jetzigen Zeitpunkt derartige Verfahren einzurichten. Ich habe den Minister der Justiz daher gebeten, die Erforderlichkeit von Direktabrufverfahren, insbesondere unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit, nochmals zu überprüfen. Es sei indessen klargestellt, daß ein Votum gegen den Online-Anschluß nicht ohne weiteres gleichzusetzen ist mit der Ablehnung automatisierter Verfahren, die die Anlieferung und Verarbeitung von Informationen im Bundeszentralregister betreffen.

5.3 Telefonabhördaten

Zur Unterstützung in Strafermittlungsverfahren werden zunehmend PC eingesetzt (vgl. 10. TB Tz. 4.3.2 und 4.3.3). Bei der Überprüfung eines solchen PC-Verfahrens ergab sich, daß nicht nur auf herkömmliche Ermittlungen zurückgehende Daten über Beschuldigte, Verdächtige und andere Personen vorgehalten wurden, sondern auch Daten aus Telefonabhörmaßnahmen.

Die Polizei hatte auf richterliche Anordnung die Telefonanschlüsse im Lokal eines Motorradclubs und in einer weiteren öffentlichen Gaststätte überwacht. Das

Ermittlungsverfahren war wegen des Verdachts der Bildung einer kriminellen Vereinigung mit dem Schwerpunkt illegaler Betäubungsmittelhandel, Zuhälterei und räuberische Erpressung eingeleitet worden. Auch nach meiner Überzeugung lagen die gesetzlichen Voraussetzungen für die Telefonabhörmaßnahmen vor. Bedenken bestanden jedoch gegenüber der weiteren Verfahrensweise bei der Aufbewahrung der hieraus gewonnenen Informationen.

Die Überwachung des Fernmeldeverkehrs durch Strafverfolgungsorgane und die Verarbeitung der daraus gewonnenen Informationen ist nur in engen durch die Strafprozeßordnung festgelegten Grenzen zulässig. Das Brief-, Post- und Fernmeldegeheimnis ist als Grundrecht geschützt (Art. 10 GG). Zugleich beeinträchtigt jede Maßnahme dieser Art das informationelle Selbstbestimmungsrecht aller Gesprächsteilnehmer, die abgehört werden. Nicht nur die Privatsphäre der Betroffenen wird in außerordentlichem Maße offengelegt, sondern es werden auch an der Straftat völlig Unbeteiligte einbezogen. Deshalb muß - ungeachtet der Schwere der Straftat, zu deren Aufklärung die Telefonüberwachung angeordnet wurde - stets die Prüfung gewährleistet sein, inwieweit die Erkenntnisse für die Strafverfolgung relevant sind. Die Informationen sind zu vernichten, wenn sie für die Strafverfolgung nicht mehr erforderlich sind (§ 100 b Abs. 5 StPO).

Nach dem mir zugänglich gemachten Aktenmaterial wurde die Überwachung der Telefonanschlüsse vom zuständigen Richter für einen Zeitraum von 3 Monaten angeordnet. Da sich aber bereits nach wenigen Wochen abzeichnete, daß sich aus der Überwachung keinerlei Ansatzpunkte für den festgesetzten Ermittlungszweck ergaben, wurde sie am 02.05.1988 - lange vor der bis zum 07.07.1988 angeordneten Laufzeit - eingestellt. Die Kriminalpolizei hat in den Akten vermerkt:

"Es ist nicht abzusehen, daß sich durch die Fortsetzung der Telefonmaßnahmen diesbezügliche Erkenntnisse gewinnen lassen".

Zwar wurde die auf Diskette gespeicherte Arbeitsdatei am 20.10.1988 gelöscht. Im übrigen wurden die Abhörunterlagen jedoch - insbesondere Tonbänder und die Auswertungen - zu den Akten genommen und der Staatsanwaltschaft übergeben.

Zumindest ein Teil der Abhörunterlagen kam für Strafverfolgungszwecke schon von Anfang an nicht in Frage; so konnte ich etwa bei der Akteneinsicht Anfang Oktober 1988 die Speicherung eines Telefongespräches feststellen, in dem von der abgehörten Gaststätte aus eine Getränkebestellung bei einem Saarbrücker Bierverleger getätigt wurde.

Die Staatsanwaltschaft Saarbrücken teilte mir unter dem 2. November 1988 - also 5 Monate nach Einstellung der Abhörmaßnahme - mit, daß die weitere Aufbewahrung der Abhörbänder und Protokollmitschriften erforderlich sei, weil auch "eingestellte Verfahren jederzeit wiederaufgenommen werden können". Diese Auffassung läßt die gesetzlichen Vorgaben völlig außer acht und würde dazu führen, daß die Staatsanwaltschaft berechtigt wäre, Unterlagen aus der Telefonüberwachung auf unabsehbare Zeit vorzuhalten. Erst auf meine nachdrückliche Vorstellung hat der Minister der Justiz Anfang Januar 1989 eine Überprüfung angeordnet, welche - nach Mitteilung des Justizministers - am 17. April 1989 zu der Vernichtung der Unterlagen führte.

Ich will mir nicht anmaßen, die Erforderlichkeit der Aufbewahrung im Interesse der Strafverfolgung zu beurteilen. Was jedoch die Einhaltung der gesetzlichen Verfahrensvorschriften angeht, sah sich auch der Minister der Justiz auf meine Stellungnahme hin zu folgender Feststellung veranlaßt:

"Der Fall und seine Bearbeitung erschien mir ... durchaus dazu angetan, die Staatsanwaltschaft auf die Notwendigkeit der Beachtung und Einhaltung der Vorschriften des § 100 b Abs. 5 und § 101 Abs. 1 StPO hinzuweisen."

Der Minister der Justiz hat die Thematik außerdem zum Gegenstand einer vertieften Erörterung in einer Dienstbesprechung gemacht.

Konkret gibt der lange Zeitraum seit dem Abschluß der Abhörmaßnahmen am 02.05.1988 bis zur Vernichtung der Unterlagen am 17.04.1989 zu der bisher nicht widerlegten Vermutung Anlaß, daß die Staatsanwaltschaft die Prüfungen nicht rechtzeitig und nicht in dem erforderlichen Umfang durchgeführt hat. Spätestens nach Einstellung des Verfahrens wegen Verdachts der Bildung einer kriminellen Vereinigung (noch vor dem 02.11.1988) war ein sorgfältiger Prüfauftrag erforderlich. Daß die Staatsanwaltschaft es an den entsprechenden Bemühungen hat fehlen lassen, ergibt sich schon aus dem ausdrücklichen Prüfauftrag des Ministers vom 04.01.1989, der auf meine Intervention zustande kam. Der Hinweis der Staatsanwaltschaft, daß schließlich die eventuelle Wiederaufnahme eingestellter Verfahren die weitere Aufbewahrung rechtfertige, spricht für eine pauschale, die Interessen nicht hinreichend abwägende Verfahrensweise.

Überdies wurde die in der Strafprozeßordnung vorgeschriebene Benachrichtigungspflicht nicht hinreichend beachtet (§ 101). Die Beteiligten sind von der Telefonabhörmaßnahme zu unterrichten, sobald dies ohne Gefährdung des Untersuchungszwecks geschehen kann. Die Staatsanwaltschaft geht davon aus, daß sie dieser ihrer Verpflichtung mit der Benachrichtigung der überwachten Telefonanschlußinhaber und der Beschuldigten nachgekommen ist. Sie wählt damit eine Interpretation,

die weder dem Wortlaut des Gesetzes hinreichend Rechnung trägt noch dem Recht auf informationelle Selbstbestimmung die notwendige Bedeutung beimißt. Da Telefonabhörmaßnahmen einen besonders tiefen Eingriff in die Privatsphäre der Beteiligten darstellen, erfordert eine verfassungskonforme Interpretation des Gesetzes die Benachrichtigung aller identifizierten oder mühelos identifizierbaren Gesprächsteilnehmer. Nach dieser Auslegung, die im übrigen der Minister der Justiz teilt, hätte die Staatsanwaltschaft alle von ihr ermittelten Gesprächsteilnehmer über die Abhörmaßnahme zu einem die Strafverfolgung nicht mehr gefährdenden Zeitpunkt unterrichten müssen.

Da nach Mitteilung des Justizministers zwischenzeitlich alle Abhörunterlagen vernichtet sind, kann die gesetzlich vorgeschriebene Benachrichtigung nicht mehr in dem erforderlichen Umfang nachgeholt werden. Die Folge hiervon ist, daß Telefongespräche einer ganzen Reihe unbeteiligter Bürger von der Polizei abgehört wurden, ohne daß die Betroffenen - bei zwei Gaststätten dürften es nicht gerade wenige gewesen sein - bis zum heutigen Tag hiervon etwas erfahren haben.

5.4 Aktenübersendung durch die Staatsanwaltschaft

Durch das Landeskrankenhaus Merzig wurde ich auf eine rechtlich fragwürdige Aktenübersendung der Staatsanwaltschaft Saarbrücken an das Arbeitsamt Saarlouis hingewiesen. In der psychiatrischen Abteilung des Landeskrankenhauses Merzig lebt seit Jahren ein Patient, der wegen im Zustand der Schuldunfähigkeit begangener Straftaten zwangsweise untergebracht ist (§ 63 StGB). Im Rahmen der Reintegrationsbemühungen und der Entlassungsvorbereitung versuchte die Klinik den Patienten in einer Werkstatt für Behinderte einzugliedern. Das Arbeitsamt Saarlouis wollte der Durchführung dieser Maßnahme nur unter bestimmten Auflagen zustim-

men, die darauf schließen ließen, daß die Behörde genaue Kenntnis über den Werdegang des Betroffenen hatte. Nachforschungen der Klinik ergaben, daß die Staatsanwaltschaft Saarbrücken der Arbeitsverwaltung auf Anforderung die gesamten Strafakten einschließlich einer Reihe von ärztlichen und psychiatrischen Gutachten übersandt hat.

Ich habe diese Verfahrensweise beanstandet. Zwar erlauben die Richtlinien für das Straf- und Bußgeldverfahren der Staatsanwaltschaft, anderen Behörden Akteneinsicht zu gewähren, wenn diese ein berechtigtes Interesse darlegen. Allerdings genügen diese Richtlinien als Verwaltungsvorschrift nicht den Anforderungen normenklarer, gesetzlicher Regelungen, wie sie das Bundesverfassungsgericht für Eingriffe in das Recht auf informationelle Selbstbestimmung fordert. Lediglich für eine Übergangszeit bis zur Schaffung bereichsspezifischer Vorschriften kann daher ihre Anwendung noch hingenommen werden, wobei allerdings eine verfassungskonforme Auslegung gewährleistet sein muß. Das bedeutet, daß in jedem Einzelfall eine sorgfältige Prüfung erfolgen muß, ob die Gewährung von Akteneinsicht tatsächlich zur Aufgabenerfüllung der einsichtsbegehrenden Stelle erforderlich ist. In einer Reihe von Fällen dürfte es jedenfalls ausreichen, statt der Überlassung der gesamten Akte einzelne Auskünfte zu erteilen.

Im vorliegenden Fall waren Gesichtspunkte nicht erkennbar, die ein berechtigtes Interesse der Arbeitsverwaltung an der Einsichtnahme in die Strafakten hätten rechtfertigen können. Die Frage, ob eine Reintegration für den zwangsweise Untergebrachten in Erwägung zu ziehen ist, obliegt nach den gesetzlichen Bestimmungen allein dem Strafgericht. Es würde in Widerspruch zu dieser Gesetzeslage stehen, wenn die Arbeitsverwaltung die Gewährung von staatlichen Leistungen von einer eigenen Auswertung der Strafakten

abhängig machen könnte. Dies macht deutlich, daß ein berechtigtes Interesse des Arbeitsamtes an der Einsichtnahme in Strafakten von vornherein auszuschließen war. Jedenfalls war die Versendung von Akten zur Einsichtnahme unverhältnismäßig.

Erfreulich stimmt im vorliegenden Fall, daß der Minister der Justiz die Sachbehandlung durch die Staatsanwaltschaft förmlich beanstandet hat. Nachdrücklich zu begrüßen ist auch, daß er den Fall zum Anlaß genommen hat, die Staatsanwaltschaft im Erlaßwege auf die Notwendigkeit einer restriktiven Handhabung der Gewährung von Akteneinsicht hinzuweisen.

5.5 Akteneinsicht für Forschungszwecke

Bereits in der Vergangenheit hatte ich mich häufiger mit der Frage zu beschäftigen, unter welchen Voraussetzungen Akteneinsicht für Forschungszwecke gewährt werden kann (vgl. 9. TB Tz. 8). Auch im letzten Jahr wurden mehrere Vorgänge an mich herangetragen, bei denen es um die Einsichtnahme in Strafakten für Forschungszwecke ging. Da derzeit eine gesetzliche Grundlage für die wissenschaftliche Auswertung von Strafakten fehlt, diese mit der Novellierung der Strafprozeßordnung vielmehr erst geschaffen werden soll (vgl. Tz. 5.1), habe ich generell gefordert, Akteneinsicht nur dann zu gewähren, wenn der Betroffene eingewilligt hat. Hierbei muß sichergestellt werden, daß die Freiwilligkeit - insbesondere bei noch einsitzenden Strafgefangenen - tatsächlich gewährleistet ist und der Betroffene über die wesentlichen Ziele und Verwendungszusammenhänge unterrichtet wird. Der Minister der Justiz hat meine Rechtsauffassung akzeptiert und zugesichert, einer Strafaktenauswertung nur auf der Grundlage der Einwilligung zuzustimmen.

5.6 Organisationsuntersuchung bei den Gerichten

Im Auftrag des Bundesministers der Justiz fand im Berichtszeitraum eine bundesweite Organisationsuntersuchung verschiedener Gerichtszweige statt. Im Saarland erstreckte sich die Untersuchung, die durch private Unternehmensberater durchgeführt wurde, auf das Amtsgericht Ottweiler sowie das Verwaltungsgericht und das Finanzgericht des Saarlandes. Ziel der Untersuchung war die vergleichende Analyse der bestehenden Organisationsstrukturen und die Entwicklung einer möglichst zweckmäßigen Gerichtsorganisation. Zur Datenerhebung wurden Fragebogen eingesetzt, mit denen Organisationsabläufe und Schwachstellen in den einzelnen Gerichten ermittelt werden sollten. Auszufüllen waren die - unterschiedlich ausgestalteten - Fragebogen von den Richtern, Rechtspflegern und sonstigen Bediensteten der Gerichte. Zwar sahen die Fragebogen regelmäßig die Angabe des Namens nicht vor, aus den übrigen - sehr detailliert geforderten - Angaben war jedoch ohne weiteres feststellbar, welcher Bedienstete sich in welcher Weise geäußert hatte. Hieraus resultierte die Gefahr, daß die Bediensteten sich auf die Anonymität der Erhebung vertrauend offen äußerten, im Rahmen der Auswertung die gemachten Angaben dann aber personenbezogen dem Dienstherrn zur Kenntnis gelangten.

Um diese Möglichkeit von vorneherein auszuschließen, habe ich gefordert, daß die ausgefüllten Fragebogen von den Bediensteten in verschlossenem Umschlag unmittelbar an den Unternehmensberater versandt werden. Weiter habe ich darauf gedrängt, daß persönliche Daten der Befragten bei der Auswertung der Fragebogen nicht erfaßt und Angaben, die auf bestimmte Personen schließen lassen, nicht an die Justizverwaltung übermittelt werden. Da für eine derartige Datenerhebung eine spezielle gesetzliche Grundlage fehlt, habe ich darüberhinaus gefordert, daß die Erhebung ausschließ-

lich auf freiwilliger Basis durchgeführt wird. Der Minister der Justiz hat mitgeteilt, daß er meine Vorschläge berücksichtigt.

5.7 Automation im Justizbereich

Der Justizminister beabsichtigt, die Geschäftsstellen und Kanzleien der Amtsgerichte durch Automation zu rationalisieren.

Für den Bereich der Zivilsachen ist beim Amtsgericht Saarbrücken seit etwas über einem Jahr eine Testinstallation "Geschäftsstellenautomation" eingerichtet. Das eingesetzte Verfahren ermöglicht über ein Mehrplatzsystem die Speicherung der Parteidaten, ihrer Prozeßbevollmächtigten, des Streitgegenstandes, des Streitwertes, des zuständigen Richters, des Aktenzeichens sowie der Vorlage- und Sitzungstermine. Über diese Daten lassen sich die typischen Verfahrensabläufe in der Geschäftsstelle automatisiert abwickeln. Daneben wird das System zur Textverarbeitung, insbesondere zur Abfassung von Urteilen, Beschlüssen und Sitzungsniederschriften, genutzt.

Die Bediensteten aller Geschäftsstellen des Amtsgerichts haben Zugriff auf die Speicherungen aus den verschiedenen Geschäftsstellen. Bei der Überprüfung konnte eine nach Aufgaben und Befugnissen differenzierte Zugriffsberechtigung jedenfalls nicht mit ausreichender Sicherheit festgestellt werden. In dem System sind sensible Daten - wie etwa vollständige Urteile oder Sitzungsniederschriften - gespeichert. Ich habe daher gefordert, die Zugriffsberechtigung so festzulegen, daß der Anwender jeweils nur auf die zu seiner konkreten Aufgabenerfüllung notwendigen Daten zugreifen kann.

Nicht geregelt ist bisher, unter welchen Voraussetzungen die gespeicherten Daten gelöscht werden. Offensichtlich geht die Justizverwaltung davon aus, daß die Daten jeweils bis zur rechtskräftigen Entscheidung aufbewahrt werden dürfen. Dies kann aus datenschutzrechtlicher Sicht nicht hingenommen werden. Ungeachtet der Gefahr, daß abgespeicherte Dokumente bewußt oder unbewußt verändert werden können, ist nach Versendung der Schreiben, Urteile und Beschlüsse sowie nach Übernahme in die Akte eine Speicherung in automatisierten Verfahren nicht mehr erforderlich. Ich habe daher auf die Festlegung einer differenzierten Lösungsregelung gedrängt.

Schließlich habe ich gefordert, die bisher fehlende Festlegung organisatorischer und verfahrensrechtlicher Rahmenbedingungen vorzunehmen. Für notwendig halte ich insbesondere den Erlaß einer Dienstanweisung, durch die der Einsatz des Systems geregelt wird, sowie eine schriftliche Dokumentation des Verfahrens.

Eine Stellungnahme des Ministers der Justiz liegt mir bisher noch nicht vor, ich hoffe jedoch, daß meinen Vorschlägen bei der endgültigen Installation des Verfahrens Rechnung getragen wird.

6. Gesundheit

6.1 Maßregelvollzugsgesetz

Im Berichtszeitraum hat der saarländische Minister für Arbeit, Gesundheit und Sozialordnung einen Referentenentwurf für ein Maßregelvollzugsgesetz in das Anhörungsverfahren gebracht. Das Maßregelvollzugsgesetz soll die Durchführung der Unterbringung von psychisch-kranken, behinderten und suchstoffabhängigen Rechtsbrechern in einem psychiatrischen Krankenhaus und einer Entziehungsanstalt regeln. Nach dem erklärten Ziel des Gesetzgebungsvorhabens steht die Behandlung des Untergebrachten im Vordergrund; dem Umgang mit sensiblen psychiatrischen Patientendaten kommt daher große Bedeutung zu.

Der Zwangscharakter des Unterbringungsverhältnisses bringt es mit sich, daß der untergebrachte Patient auf die Verarbeitung der ihn betreffenden personenbezogenen Daten nur einen begrenzten Einfluß hat. Insoweit ist sein Recht auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse eingeschränkt. Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ist ein Eingriff in das informationelle Selbstbestimmungsrecht nur zulässig auf der Grundlage einer bereichsspezifischen, gesetzlichen Regelung, die den Prinzipien der Normenklarheit, Zweckbindung und Verhältnismäßigkeit entspricht. Ich habe es deshalb begrüßt, daß der Referentenentwurf bereits in einem eigenen Abschnitt Regelungen über die Informationsverarbeitung im Maßregelvollzug vorsah. In meiner Stellungnahme habe ich einige Verbesserungs- und Ergänzungsvorschläge gemacht, die im Regierungsentwurf berücksichtigt wurden.

Der Umfang der Erhebung, Speicherung und Nutzung der Patientendaten wird durch die objektiven Kriterien der Erforderlichkeit für Zwecke des Maßregelvollzugs und

der ärztlichen Dokumentationspflicht begrenzt. Damit ist eine routinemäßige und pauschalisierende Datenverarbeitung von vornherein ausgeschlossen. Die Datenübermittlung an Stellen außerhalb der Einrichtung ist nur in den gesetzlich abschließend aufgeführten Fällen zulässig. Um eine nachträgliche Überprüfung zu ermöglichen, ist jede Datenweitergabe zu dokumentieren.

Auch der interne Zugriff auf die Daten ist klar und eindeutig festgelegt. Das Gesetz sieht eine Funktionstrennung zwischen ärztlich-pflegerischem Bereich und administrativem Bereich vor. Jeder in der Einrichtung Beschäftigte darf auf personenbezogene Daten nur insoweit zugreifen, als dies für die jeweilige Behandlung erforderlich ist. Die Einrichtungen des Maßregelvollzugs bilden somit keine Informationseinheit.

Die Transparenz der Datenverarbeitung ist durch ein umfassendes Auskunfts- und Akteneinsichtsrecht gewährleistet. Positiv zu bewerten ist auch, daß der Entwurf ein Verbot der Datenverarbeitung außerhalb der Einrichtung vorsieht. Schließlich ist der Datenzugang der Forschung durch Verweisung auf die entsprechenden Bestimmungen des Saarländischen Krankenhausgesetzes normenklar geregelt.

Kritisiert habe ich in der parlamentarischen Anhörung zum Regierungsentwurf die Vorschriften, die die Voraussetzungen für die Überwachung von Besuchen sowie des Telefon- und Schriftverkehrs regeln. Dabei wird nicht nur in das informationelle Selbstbestimmungsrecht, sondern auch in das Brief- und Fernmeldegeheimnis eingegriffen. Ich habe hierzu dem Parlament Vorschläge für eine weitere Konkretisierung der Eingriffsvoraussetzungen unterbreitet.

Insgesamt trägt der Entwurf den Anforderungen, die das Bundesverfassungsgericht für Eingriffe in das informationelle Selbstbestimmungsrecht aufgestellt hat, weitgehend Rechnung.

6.2 Gesundheitsamt

Im Berichtszeitraum habe ich die Datenverarbeitung in einem Gesundheitsamt überprüft. Das Thema "Datenschutz im Gesundheitsamt" habe ich bereits in meinem ersten Tätigkeitsbericht aufgegriffen. Mit Erlaß vom 05.12.1983 hat der Minister für Arbeit, Gesundheit und Sozialordnung Anordnungen über die Sicherstellung des Datenschutzes bei den saarländischen Gesundheitsämtern getroffen. Wesentlicher Inhalt dieses Erlasses ist die Aufzählung der im Gesundheitsamt zu führenden Dateien. Festgelegt ist, welche Angaben in den einzelnen Dateien gespeichert werden und wie lange sie aufbewahrt werden dürfen. Die Prüfung hat gezeigt, daß im Gesundheitsamt immer noch nicht alle Datenschutzprobleme ausgeräumt sind.

- Zentraldatei

Die Zentraldatei, die die Funktion einer Suchkartei für das Auffinden von Akten hat, enthält Hinweise auf alle amts- und vertrauensärztlichen Gutachten, die über eine Person aus den verschiedensten Anlässen gefertigt werden (z.B. Einstellung und Anstellung eines Beamten, Dienstfähigkeit, Erteilung der Aufenthaltserlaubnis für Ausländer, Fahrtauglichkeit, Jugendschutzuntersuchungen, Bewilligung von Leistungen nach dem Bundessozialhilfegesetz). Die Aufnahme und das Ausscheiden aus der Tuberkuloseüberwachung ist in der Zentraldatei ebenso vermerkt wie das Aktenzeichen der Unterlagen über körperliche und geistige Behinderungen und psychisch-soziale Beratungen. Diese Zusammenfassung von Merkmalen aus der amtsärztlichen Begut-

achtung, der freiwilligen Beratung sowie aus zwangsweiser Informationsverarbeitung aufgrund hoheitlicher Tätigkeit ist datenschutzrechtlich äußerst problematisch. Denn die Zentraldatei wird dadurch zu einem Instrument, das die unzulässige Verknüpfung eines Großteils der Erkenntnisse ermöglicht, die über eine Person beim Gesundheitsamt vorhanden sind. Es ist weder mit der ärztlichen Schweigepflicht, die die Mitarbeiter des Gesundheitsamtes aufgrund von § 203 Abs. 1 und 3 StGB zu wahren haben, noch mit dem vom Bundesverfassungsgericht entwickelten Zweckbindungsgebot zu vereinbaren, daß Unterlagen, die etwa im Rahmen einer auf freiwilliger Basis durchgeführten Beratung angefertigt worden sind, später zu einem anderen Zweck, z.B. einer duldungspflichtigen, amtsärztlichen Untersuchung beigezogen und ausgewertet werden. Das Vertrauensverhältnis zwischen ratsuchendem Bürger und Amtsarzt darf nicht durch eine funktionsübergreifende Informationsverwertung in Frage gestellt werden. Die Gesundheitsämter würden ihren Aufgaben bei der gesundheitlichen Beratung und Aufklärung nicht gerecht werden können, wenn das Vertrauen in den öffentlichen Gesundheitsdienst schwinden würde. Ich habe deshalb gefordert, die Zentraldatei in ihrer jetzigen Form aufzulösen und nach Aufgabengebieten getrennte Karteien aufzubauen. Nur so kann eine Funktionstrennung und dementsprechende Zugriffsberechtigung auf der Grundlage eines Geschäftsverteilungsplans sichergestellt werden.

Schwierigkeiten im Zusammenhang mit der Zentraldatei ergeben sich offensichtlich auch bei der Einhaltung der Löschungspflichten. Die Aufbewahrungsfristen sind je nach Art des Vorgangs unterschiedlich. Amtsärztliche Gutachten werden 10 Jahre, Tuberkuloseakten längstens 30 Jahre aufbewahrt. Weil die Zentraldatei wegen ihres komplexen Inhalts schwer zu kontrollieren ist, blieb in der überprüften Zentraldatei die überwiegende Mehrheit der Vorgänge unbefristet gespeichert. Inzwi-

schen ist das Volumen der in der Zentraldatei registrierten Personen auf eine Zahl angewachsen, die der Hälfte der Einwohnerschaft des Landkreises entspricht, für den das überprüfte Gesundheitsamt zuständig ist.

Das Gesundheitsamt hat inzwischen mitgeteilt, daß die Zentraldatei in der derzeitigen Form nicht mehr fortgeführt wird. Die Angaben zur Behindertenbetreuung werden überhaupt nicht mehr in einer Datei geführt. Für die Tuberkuloseüberwachung und die vertrauensärztlichen Gutachten werden besondere Karteien angelegt. In der Zentraldatei sollen lediglich noch alle amtsärztlichen Gutachten registriert werden. Aber auch insoweit ist eine weitere Überprüfung angezeigt, wie die Zweckbindung insoweit gewährleistet werden kann.

- Gutachterwesen

Die amtsärztlichen Gutachten und Zeugnisse werden zwar aufgrund Rechtsnormen erstellt. Es handelt sich hierbei jedoch überwiegend um lediglich mitwirkungspflichtige Vorgänge, die einer Datenerhebung auf freiwilliger Basis gleichkommen. Informationen, die auf diese Weise gewonnen werden, dürfen nicht in jedem anderen Zusammenhang verwendet werden. Der Betroffene hat die Erhebung und Verwendung seiner Daten nur zu einem konkreten Zweck bestimmt. Wird die Zweckbindung indessen nicht beachtet, können nicht zuletzt dem Arztgeheimnis unterliegende Tatsachen - auch der Amtsarzt unterliegt der Schweigepflicht - in unzulässiger Weise zwischen Ärzten offenbart werden. Was unter Zweckbindung zu verstehen ist, bedarf weiterer Konkretisierung. Gutachten zur Feststellung der Fahrtauglichkeit einer Person sollten bei der Wiederholungsüberprüfung wieder verwendet werden dürfen. Ergebnisse aus solchen Untersuchungen dürfen jedoch nicht etwa für Gutachten zur Vorbereitung einer dienstrechtlichen Entscheidung (Einstellung, Anstellung, Ruhestandsversetzung) genutzt werden. Es ist eine Aufteilung nach Sachgruppen

notwendig, die die Zweckbindung bei der zukünftigen Auswertung gewährleistet. Sollen Informationen aus verschiedenen, in keinem Sachzusammenhang stehenden Anlässen verwendet werden, ist dies ohne Einwilligung des Betroffenen nicht zulässig.

Über die weitere Behandlung der amtsärztlichen Gutachten ist bisher noch nicht entschieden.

- Mütter-/Säuglingsberatung, Vorschulkinder-, Einschulungsuntersuchung

Das Gesundheitsamt bietet im Rahmen der gesundheitlichen Betreuung von Kindern Beratungen an, über deren Inanspruchnahme die Eltern frei entscheiden können. Während die Teilnahme an der Mütter-/Säuglingsberatung und die Vorschulkinderuntersuchung freiwillig ist, besteht eine gesetzliche Verpflichtung, an der Einschulungsuntersuchung teilzunehmen. Die Informationen, die bei diesen verschiedenen Anlässen erhoben werden, werden auf Karteikarten fortgeschrieben, die zu den jeweiligen Untersuchungen herangezogen werden.

Die ohnehin wegen des langen Beobachtungszeitraumes schon sehr umfangreiche Kartei über die Kinder im Zuständigkeitsgebiet des überprüften Gesundheitsamtes war in einzelnen Fällen noch angereichert durch ausführliche Krankenhausentlassungsberichte. Es war nicht mehr feststellbar, wie sie in die Datei gelangten und ob die Erziehungsberechtigten damit einverstanden gewesen sind. Jedenfalls ist eine Rechtsgrundlage für die Aufbewahrung solcher ärztlicher Unterlagen nicht erkennbar, so daß sie auszusondern sind.

Ohne Einwilligung der Erziehungsberechtigten stellt die Fortschreibung der Informationen über Kinder vom Säuglingsalter bis über die Schulentlassung hinaus einen unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht dar. Da die Säuglingsberatung

und die Mütterberatung auf freiwilliger Grundlage erfolgen, ist allein die Einwilligung der Erziehungsberechtigten maßgebend dafür, für welche Zwecke die bei diesen Untersuchungen gewonnenen Erkenntnisse verwendet werden dürfen. Es kann aber nicht ohne weiteres davon ausgegangen werden, daß die Erziehungsberechtigten mit der Verwendung der ärztlichen Unterlagen aus der Mütter-/Säuglingsberatung und Vorschulkinde-
runtersuchung für Zwecke der Einschulungsuntersuchung einverstanden sind. Die Eltern befürchten, daß Feststellungen über Verhaltensauffälligkeiten, Diagnosen und Behinderungen aus dem Vorschulalter sich belastend für die Kinder bei der Einschulung und später auswirken könnten. Sofern anamnestische Erkenntnisse aus der Säuglingsberatungskartei und der Vorschulkinde-
rerkartei an den Schularzt weitergegeben werden, sind die Erziehungsberechtigten hierüber aufzuklären. Ihre ausdrückliche schriftliche Einwilligung ist einzuholen. Die Entscheidung des Ministeriums zu diesem Fragenkomplex steht noch aus (vgl. meinen 10. TB Tz. 8.3).

- Medizinalpersonendatei

Die Datei dient der Überwachung der ärztlichen und nichtärztlichen Medizinalpersonen einschließlich der Apotheker und des Apothekenpersonals, soweit der Beruf ausgeübt wird. Grundlage für die Führung der Datei sind Meldedaten, die die Wohnsitzgemeinden übermitteln. Die Meldeämter übermitteln regelmäßig An- und Abmeldung, Namensänderungen und Tod der Medizinalpersonen (§ 10 Meldedatenübermittlungsverordnung). Für die Überwachungsaufgabe des Gesundheitsamtes ist jedoch nicht die Wohnadresse von Bedeutung, sondern der Ort der Niederlassung oder der Beschäftigung in einem Krankenhaus. Nicht erfaßt werden auf dieser Basis außerdem Personen, die eine Tätigkeit im Gesundheitswesen aufnehmen, ohne daß eine melderechtliche Veränderungsmeldung erfolgt. Ebensowenig ist gewährleistet,

daß Personen, die ihre Berufsausübung aufgeben, aus der Datei herausgenommen werden. Auch der Minister für Arbeit, Gesundheit und Sozialordnung hat erkannt, daß die Kartei für eventuelle Kontrollzwecke im Gesundheitswesen unbrauchbar ist. Die Fortführung der Datei wurde deshalb eingestellt. Konsequenterweise muß darüberhinaus diese unvollständige und nicht mehr aktualisierte Datei vernichtet werden. Eine entsprechende Verfügung ist noch nicht ergangen.

- Organisation

Aus der Sicht des Datenschutzes ist eine eindeutige und klare Zuständigkeitsverteilung von Bedeutung, weil mit ihr die Verantwortlichkeit für die Verarbeitung personenbezogener Daten festgelegt wird. Aus der Zuständigkeit jedes Bediensteten folgt die Zugriffsberechtigung für die in Wahrnehmung der Aufgaben zulässigerweise erhobenen und gespeicherten Daten. Ich hatte Anlaß, auf die Notwendigkeit einer genauen Aufgabenzuweisung an die einzelnen Bediensteten im Organisations- und Geschäftsverteilungsplan hinzuweisen. Aufbau- und Ablauforganisation sollten überdies so gestaltet werden, daß einer unzulässigen Durchbrechung des Zweckbindungsgebotes vorgebeugt wird. Die gleichzeitige Übertragung von Aufgaben zur Bekämpfung übertragbarer Krankheiten nach dem Bundesseuchengesetz, die auch zwangweise durchgeführt werden können, sowie von fürsorglichen Aufgaben (Jugendärztlicher Dienst, Behinderte) führt zu einer Bündelung hoheitlicher und beratender Funktionen. Darin liegt die Gefahr begründet, daß auch die auf freiwilliger Basis angebotenen Leistungen des Gesundheitsamtes Zwangscharakter für den Betroffenen erlangen können. Die Ausstattung insbesondere der kleineren Gesundheitsämter setzt zwar der Funktionstrennung Grenzen. Unerlässlich ist es jedoch, daß der Organisations- und Geschäftsverteilungsplan eine eindeutige Zuordnung der Funktionen festlegt. Eine Zugriffsregelung, die dem unbeschränk-

ten, behördeninternen Datentransfer vorbeugt, ist nur auf der Grundlage einer eindeutigen Aufgaben- und Zuständigkeitsverteilung für alle Bediensteten denkbar.

- Formularwesen

Aufgefallen ist mir außerdem, daß das zuständige Ministerium zwar im Wege der Verfügung verschiedene Formulare - z.B. für die Durchführung des Verfahrens zur verkehrsmedizinischen Begutachtung, für die Begutachtung der Beihilfefähigkeit eines Sanatoriumsaufenthalts - eingeführt, den entsprechenden Druckauftrag für die Änderungen aber noch nicht erteilt hat. Dies sollte schnellstmöglich nachgeholt werden.

Dem Formularwesen kommt im Gesundheitsamt besondere Bedeutung zu. Auf der Karteikarte für Vorschulkinder habe ich folgende Abfragearten festgestellt: "übertriebene Ängstlichkeit", "Kontakthemmung", "Stimmungs-labilität", "Eifersucht", "Distanzlosigkeit", "Bindungsschwäche", "Lügen", "Stehlen". Ich habe diese Vorgaben, die nicht nur diskriminierenden Charakter haben, sondern teilweise auch als strafrechtliche Bewertungen keinesfalls verwendet werden dürfen, beanstandet. Verhaltensauffälligkeiten des Kindes sollten jedenfalls nicht aufgrund von Formularrastern vorgeprägt erfaßt werden.

Die auf den Formularen vorgegebenen Erhebungskategorien und Abfragearten routinisieren die Informationsverarbeitung vor allem bei Reihenuntersuchungen. Deshalb muß schon von vornherein dafür Sorge getragen werden, daß keine Datenarten zur Abfrage vorgegeben werden, die eine unzulässige Informationsverarbeitung zur Folge haben oder einer unangemessenen, den Einzelfall nicht ausreichend berücksichtigenden Datenerfassung Vorschub leisten.

- Löschung von Daten

Daten dürfen nur solange gespeichert werden, wie es für die ordnungsgemäße Aufgabenerfüllung unbedingt erforderlich ist. Die Bescheinigungen über die Beratung zur Vorbereitung eines zulässigen Schwangerschaftsabbruches dürfen nur längstens bis zum Ablauf der 22. Woche nach der Empfängnis aufbewahrt werden. Danach ist ein derartiger Eingriff nicht mehr zulässig. Die Löschung trägt dazu bei, daß das Arztgeheimnis ohne jede Konfliktmöglichkeit gewahrt werden kann. Inwieweit die Akten über Behinderte und psycho-soziale Beratungen aufbewahrt bleiben müssen, sollte ebenfalls im einzelnen überdacht werden.

Darüber hinaus halte ich eine Überprüfung der Aufbewahrungszeit für Karteien, die im Rahmen der Säuglingsberatung, der Kindergartenuntersuchung und der Einschulungsuntersuchung angelegt werden, für erforderlich. Die bisher vorgesehene Aufbewahrung bis zur Vollendung des 18. Lebensjahres halte ich jedenfalls in den Fällen für unangemessen, in denen die Erziehungsberechtigten einer Fortschreibung nicht zugestimmt haben.

- Datensicherung

Gemäß § 12 SDSG sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um der Gefahr einer unbefugten Nutzung personenbezogener Daten entgegenzuwirken. Darunter fallen alle Maßnahmen, die geeignet sind, Unbefugten - sowohl Besuchern als auch nicht zuständigen Mitarbeitern - den Zugang zu Datensammlungen und damit eine Kenntnisnahme oder Veränderung von Daten sowie ein Entfernen von Datenträgern zu verwehren. Anlässlich der Überprüfung mußte ich feststellen, daß der zentrale Raum für die Aufbewahrung hochsensibler Gesundheitsakten nicht abgeschlossen war. In Archivräumen, in denen mehrere unter-

schiedliche Datensammlungen aufbewahrt sind, müssen die einzelnen Sammlungen in verschlossenen Schränken oder Karteikästen aufbewahrt werden, um die unterschiedlichen Zugriffsberechtigungen zu gewährleisten.

- Neufassung der gesetzlichen Vorschriften (Gesundheitsdienstgesetz)

Die vorstehenden Ausführungen machen deutlich, daß dringender Handlungsbedarf besteht, Inhalt, Zweck und Ausmaß der Aufgaben des Gesundheitsamtes durch Gesetz zu konkretisieren und auf diese Aufgaben bezogen die Befugnis zur Datenerhebung, -speicherung und -verarbeitung im einzelnen festzulegen. Soll nicht "direktive" Beratung den Bürger entmündigen, muß Aufklärung und freiwillige Mitwirkung stärker als bisher berücksichtigt werden. Die Befugnis zur zwangsweisen Informationsverarbeitung muß normenklar geregelt werden. Soweit die Einwilligung als Rechtsgrundlage in Betracht kommt, muß die freie Entscheidung durch ein Benachteiligungsverbot für den Verweigerungsfall abgesichert werden. Die Voraussetzungen für Löschungs- und Berichtigungsansprüche sind festzulegen. Die bisher maßgebliche Rechtsgrundlage für die Aufgabenwahrnehmung der Gesundheitsämter, das Gesetz über die Vereinheitlichung des Gesundheitswesens (GVG) vom 03.07.1934 mit seinen Durchführungsverordnungen, muß durch ein bereichsspezifisches, allen rechtsstaatlichen Erfordernissen entsprechendes Gesetz ersetzt werden. Der Minister für Arbeit, Gesundheit und Sozialordnung hat die rechtsstaatlichen Defizite des GVG bereits in seiner Ressortstellungnahme zu meinem 4. Tätigkeitsbericht anerkannt. Bis heute vermissen ich jedoch eine entsprechende Gesetzesinitiative.

6.3 Arztbericht an den Betriebsarzt

Eine Klinik hat ohne Einwilligung einer Patientin einen Befundbericht an den Werksarzt des Unternehmens gegeben, bei dem sie beschäftigt ist. Sie hatte gegenüber dem untersuchenden Klinikarzt schriftlich die Einwilligung erklärt, daß der Befund ihrem Hausarzt zu übermitteln sei.

Die Patientin hatte in die Übersendung des Befundberichts an den werksärztlichen Dienst nicht ausdrücklich eingewilligt. Die Tatsache, daß sie eine schriftliche Einwilligung lediglich für die Unterrichtung des Hausarztes abgegeben hat, spricht dafür, daß Datenübermittlungen an andere Stellen nicht gewollt waren.

Eine rechtfertigende Rechtsvorschrift ist nicht ersichtlich. Im Saarländischen Krankenhausgesetz ist abschließend festgelegt, unter welchen Voraussetzungen Patientendaten an Personen und Stellen außerhalb des Krankenhauses weitergegeben werden dürfen. Keine dieser Voraussetzungen lag in dem zu beurteilenden Fall vor. Das Arbeitssicherheitsgesetz, das die Aufgaben des Betriebsarztes festlegt, gibt dem Betriebsarzt keine Befugnis, Befundberichte bei Ärzten oder Krankenhäusern anzufordern. Da der Betriebsarzt den Arbeitnehmer zur Sicherstellung der Arbeitssicherheit allenfalls zu untersuchen, nicht aber auch zu behandeln hat, kann die Zulässigkeit der Weitergabe durch die Klinik etwa unter dem Gesichtspunkt der "Mitbehandlung" nicht in Betracht kommen.

6.4 AIDS-Modellprogramm "Sozialstationen"

Bundesweit wird mit Unterstützung des Bundesministers für Jugend, Familie, Frauen und Gesundheit ein Modellprogramm "Ausbau ambulanter Hilfen für AIDS-Erkrankte im Rahmen von Sozialstationen" durchgeführt. Im Saar-

land sind an dem Projekt neben der AIDS-Hilfe-Saar zwei weitere freie Träger beteiligt. An AIDS erkrankte Personen werden durch die Sozialstationen dieser Einrichtungen gepflegt und versorgt, aber auch psychosozial beraten und betreut.

Das Projekt wird wissenschaftlich begleitet durch ein Sozialforschungsinstitut. Es sollen vor allem Erkenntnisse darüber gewonnen werden, welche Betreuungsleistungen im Rahmen einer ambulanten Versorgung erbracht werden und welche Anforderungen an eine bedarfsgerechte ambulante Versorgung AIDS-Kranker zu stellen sind. Zu diesem Zweck hat das Institut verschiedene Fragebogen entworfen, die von den Mitarbeitern der Einrichtungen ausgefüllt und an das Institut übermittelt werden sollen: "Klientenstammblatt", das für jeden Klienten zu Beginn der Betreuung angelegt wird; "Monatsbericht", der am Ende eines jeden Betreuungsmonats bearbeitet wird; "Leistungsdokumentation", die fortlaufend nach jeder erbrachten Leistung ausgefüllt wird.

Ich habe dieses Dokumentationsprogramm überprüft und einige Verbesserungen vorgeschlagen. Eine Übermittlung an das Institut darf nur erfolgen, wenn die Fragebogen nur solche Angaben enthalten, die keinen Rückschluß auf eine bestimmte Person ermöglichen. Zwar waren die Fragebogen bereits weitgehend anonymisiert. Angesichts der besonderen Sensibilität der Daten habe ich aber besonders strenge Anforderungen an den Grad der Anonymisierung gestellt.

So wird nunmehr auf meinen Vorschlag hin im Stammblatt statt des genauen Datums von Betreuungsbeginn und -ende nur noch Monat und Jahr angegeben; im Monatsbericht wird auf das genaue Datum bei Krankenhausaufnahme und -entlassung verzichtet und stattdessen nur noch die Anzahl der Wochen der stationären Behandlung angekreuzt. Um zu verhindern, daß aus dem Standort der

Sozialstation auf den Wohnort des betreuten Patienten geschlossen werden kann, erhalten alle beteiligten saarländischen Einrichtungen dieselbe Einrichtungsnummer. Schließlich hat das Institut auf meine Anregung hin schriftliche Erläuterungen über den Ablauf der Erhebung, sowie eine Ausfüllanleitung für die Betreuungseinrichtungen erstellt. In der Ausfüllanleitung wird ausdrücklich darauf hingewiesen, daß bei allen offenen Fragen keine Sachverhalte angegeben werden dürfen, die eine Identifizierung des Klienten ermöglichen.

Durch die konstruktive Zusammenarbeit aller Beteiligten ist es gelungen, das Identifikationsrisiko zu minimieren. Damit dürfte die Akzeptanz des Beratungs- und Betreuungsangebots durch HIV-Infizierte und AIDS-Kranke erhöht worden sein.

6.5 Mutterpaß

Im Mutterpaß, den jede Schwangere von ihrem Arzt erhält, wird auch das Ergebnis der Abschlußuntersuchung mit detaillierten Angaben über den Verlauf der Schwangerschaft, der Geburt und des Wochenbetts vermerkt. Eine weitgehend anonymisierte Durchschrift des "Epikrisenblatts" hat der Arzt aus dem Mutterpaß herauszutrennen und zur statistischen Auswertung gemeinsam mit seiner Leistungsabrechnung bei der Kassenärztlichen Vereinigung einzureichen. Durch die gemeinsame Vorlage beider Dokumente bei der Kassenärztlichen Vereinigung wird jedoch die Anonymität des Epikrisenblattes in Frage gestellt, weil aus den Abrechnungsunterlagen die genauen Personalien der Mutter ohne weiteres ersichtlich sind. Die Kassenärztliche Vereinigung konnte ohne Schwierigkeit feststellen, auf welche Frauen sich die Epikrisenblätter beziehen und dadurch Informationen erlangen, die ihr im Rahmen des Abrechnungsverfahrens üblicherweise nicht bekannt werden.

Ich habe vorgeschlagen, daß der Kassenarzt die Epikrisenblätter gesammelt in verschlossenem Umschlag - getrennt von den Abrechnungsunterlagen - bei der Kassenärztlichen Vereinigung einreicht, wo sie getrennt weiterverarbeitet werden. Die Kassenärztliche Vereinigung hat das Verfahren entsprechend geändert. Inzwischen ist allerdings die statistische Auswertung aufgegeben worden, so daß auf die Vorlage der Epikrisenblätter verzichtet werden konnte.

6.6 PC-Einsatz in den Universitätskliniken Homburg

Die Universitätskliniken im Landeskrankenhaus Homburg haben inzwischen einen Entwurf der von mir geforderten Dienstanweisung vorgelegt, mit der die Voraussetzungen eines PC-Einsatzes und die notwendigen Datensicherungsmaßnahmen geregelt werden sollen (vgl. 10. TB Tz. 4.3.1). Dieser Entwurf konnte in weiteren Verhandlungen verbessert werden, so daß eine Trennung der verschiedenen Funktionen beim PC-Einsatz - insbesondere von Programmanwendung und Systemverwaltung - erreicht werden kann.

Der jeweilige Klinikchef, im Verwaltungsbereich dessen Direktor, hat den datenschutzgerechten Einsatz von PC zu überwachen. Er kann diese Funktion einem "Beauftragten" übertragen, der durch Stichproben die Einhaltung der Sicherungsmaßnahmen zu kontrollieren hat.

Für jeden PC ist ein "Systemverantwortlicher" zu benennen, der verpflichtet ist, die Verfahrensdokumentation zu führen sowie die zu seinem PC gehörenden Datenträger sicher aufzubewahren und zu verwalten.

Vor der Inbetriebnahme eines PC sind die jeweils notwendigen Datenschutz- und Datensicherungsanforderungen festzulegen. Hierzu erstellt das Rechenzentrum des

Landeskrankenhauses anhand einer Checkliste eine Schwachstellenanalyse. Festgestellte Schwachstellen sind zu beheben. Programme dürfen erst eingesetzt werden, wenn sie geprüft und förmlich freigegeben sind.

Das Rechenzentrum führt die Generierung des Betriebssystems und der Standardsoftware durch, richtet Benutzerkennungen ein und vergibt die Paßworte, die von jedem Zugriffsberechtigten zu verändern sind.

Ich halte es für unerläßlich, daß bei PC mit Betriebssystemen ohne eigenen Zugriffsschutz und ohne automatische Protokollierung (z.B. MS-DOS) geeignete kompensatorische Datensicherungsmaßnahmen getroffen werden. Werden mehrere Verfahren mit einem derartigen PC betrieben, ist es erforderlich, daß entweder

- nach jeder Anwendung die Dateien auf Disketten übertragen, die Dateien auf Festplatte physikalisch überschrieben (=gelöscht) und die Disketten unter Verschuß gehalten werden, oder
- eine spezielle Datensicherungssoftware eingesetzt wird.

Die Aufgaben des internen Datenschutzbeauftragten werden in der Dienstanweisung ebenfalls festgelegt. Er ist rechtzeitig über Planung, Entwicklung und Einführung von Verfahren, die personenbezogene Daten verwenden, zu informieren. Durch regelmäßige Stichproben überwacht er den ordnungsgemäßen Einsatz dieser Verfahren.

Das Landeskrankenhaus weist darauf hin, daß die Durchführung der im Entwurf der Dienstanweisung vorgesehenen Maßnahmen einen zusätzlichen Personalbedarf verursacht. Ich unterstütze den Entwurf und die sich daraus ergebende Personalforderung. Wird der Entwurf

der Dienstanweisung nicht in Kraft gesetzt, bestehen die Gefahren für die Persönlichkeitsrechte bei der Verarbeitung sensibler Krankheitsdaten fort.

7. Sozialwesen

7.1 Rentenreformgesetz

Im Berichtszeitraum wurde der Entwurf eines Rentenreformgesetzes vorgelegt. Ziel des Gesetzgebungsvorhabens ist es unter anderem, das Rentenrecht neu zu systematisieren, zu vereinfachen und übersichtlicher zu gestalten.

Obwohl im Bereich der gesetzlichen Rentenversicherung in erheblichem Umfang persönliche Daten der Versicherten verarbeitet werden, sah der Entwurf praktisch keine datenschutzrechtlichen Regelungen vor. Insbesondere fehlten Zulässigkeitsvoraussetzungen für die Informationserhebung, -speicherung und -nutzung durch die Rentenversicherungsträger. Nicht geregelt war auch die Datenverarbeitung beim Verband der Rentenversicherungsträger, sowie die Rechtsaufsicht und die Datenschutzkontrolle über die Stelle, die im Auftrag des Verbandes die Datenverarbeitung durchführt. Die Regelungsdefizite waren Anlaß für die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 05./06.04.1989 (Anlage 12). Die Forderungen wurden überwiegend berücksichtigt. In dem inzwischen verabschiedeten Gesetz vermisse ich vor allem eine Regelung über den Umgang mit besonders sensiblen medizinischen Daten im Zusammenhang mit der Feststellung der Berufsunfähigkeit und der Durchführung von Rehabilitationsmaßnahmen.

Im Verlauf des Gesetzgebungsverfahrens ergab sich noch ein weiteres schwerwiegendes Datenschutzproblem: Der Gesetzentwurf erlaubt den automatisierten Direktabruf aller Rentendaten nicht nur durch die Rentenversicherungsträger sondern auch durch sämtliche Krankenkassen und die Bundesanstalt für Arbeit. Darüberhinaus ist der Direktabruf auch durch entsprechende ausländische Stellen zugelassen. Eine so umfassende Erlaubnis zum

Direktabruf hat nicht überschaubare Risiken für die Versicherten zur Folge, weil die Datenflüsse in diesem Abrufverfahren weder begrenzt noch kontrollierbar sind. Dies gilt in besonderem Maße für den Datenabruf aus dem Ausland. Ich habe Vorkehrungen im Gesetz gefordert, die die Eingrenzung der mit dem Direktabruf verbundenen, zusätzlichen Gefahren sicherstellen. Der automatisierte Direktzugriff ausländischer Stellen sollte im übrigen nur zugelassen werden, wenn die Gleichwertigkeit des datenschutzrechtlichen Niveaus im Empfängerland durch gesetzliche Regelungen sichergestellt ist.

7.2 Kinder- und Jugendhilfegesetz

Im Berichtszeitraum hatte ich Gelegenheit, zu dem Entwurf eines Gesetzes zur Neuordnung des Kinder- und Jugendhilferechts Stellung zu nehmen. Ziel des Gesetzes ist die Ablösung des aus dem Jahr 1922 stammenden Jugendwohlfahrtsgesetzes durch eine zeitgemäße Rechtsgrundlage für die Tätigkeit der Jugendämter.

In meiner Stellungnahme habe ich insbesondere kritisiert, daß der Entwurf keine Vorschriften über Voraussetzungen und Umfang der Erhebung, Speicherung, Nutzung und Weitergabe personenbezogener Daten enthält. Gerade in einem Bereich, in dem so tiefgreifend in den persönlichen Lebensbereich der Betroffenen eingewirkt wird, halte ich eine normenklare gesetzliche Regelung der Informationsverarbeitung für dringend erforderlich. Ein besonderes Problem stellt in diesem Zusammenhang die Tatsache dar, daß die Jugendbehörden sowohl Aufgaben auf freiwilliger Basis als auch zwangsweise wahrnehmen. Der Gesetzentwurf muß sicherstellen, daß Erkenntnisse aus der Beratungstätigkeit grundsätzlich nicht bei der sonstigen hoheitlichen Aufgabenerfüllung der Jugendämter verwertet werden. Um die Zweckbindung zu gewährleisten, sind Informationen aus

der Beratungstätigkeit nur ausnahmsweise unter engen, konkret festzulegenden Voraussetzungen in anderem Zusammenhang zu verwenden. Im übrigen sollte ein Verwertungsverbot vorgesehen werden.

Darüberhinaus habe ich angeregt, in das Gesetz spezielle Aufbewahrungsfristen aufzunehmen und auf Familienakten zu verzichten, in denen Vorgänge über alle Familienangehörigen enthalten sind. Gerade bei der Akteneinsicht entstehen sonst zusätzliche Probleme, da die Rechte Dritter angesichts des "Informationsverbundes" über alle Familienangehörigen verstärkt zur Geltung kommen müssen. Schließlich sollte die Novellierung des Jugendhilferechts zum Anlaß genommen werden, die Tätigkeit des Amtspflegers/Amtsvormunds sowie die Adoptionsvermittlung dem Verfahrens- und Datenschutzrecht des Sozialgesetzbuches zu unterwerfen.

7.3 Vertrauensärztlicher Dienst

Ein Petent beschwerte sich darüber, daß der "Vertrauensärztliche Dienst" (nach neuem Recht "Medizinischer Dienst") das vollständige ärztliche Gutachten der Deutschen Klinik für Diagnostik in Wiesbaden an die zuständige Krankenkasse übersandte. Der Petent war deshalb besonders empört, weil es sich um eine umfassende Untersuchung wegen Beschwerden im psychosomatischen Bereich handelte. Der Petent hat vorgetragen, daß er in seinen Äußerungen gegenüber den untersuchenden Ärzten bedeutend zurückhaltender gewesen wäre, wenn er davon gewußt hätte, daß das gesamte Gutachten letztlich der Krankenkasse bekannt würde.

Für die Weitergabe des vollständigen Gutachtens an die Krankenkasse ist eine gesetzliche Grundlage nicht ersichtlich (§ 369 b RVO a.F.). Der Vertrauensarzt hat der Krankenkasse lediglich das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund

mitzuteilen. Der Gesetzgeber stellt darauf ab, daß nur die zur Beurteilung der Krankenkassenleistungen erforderlichen Daten mitgeteilt werden dürfen. Das Erforderlichkeitsprinzip verlangt eine Beschränkung auf die Angaben, die unerläßlich sind, damit die Krankenkasse ihre gesetzlichen Aufgaben erfüllen kann. Die Weitergabe eines Arztberichts in vollem Wortlaut mit detaillierten Angaben über Anamnese, Befunde und Diagnosen ist zur Aufgabenerfüllung der Krankenkasse nicht geboten. Der Vertrauensarzt muß sich in seiner Stellungnahme auf die notwendigen medizinischen Erläuterungen der Krankenkasse gegenüber beschränken. Gerade bei psychiatrisch-psychosomatischen Untersuchungsberichten muß den schutzwürdigen Belangen des Betroffenen in besonderem Maße Rechnung getragen werden.

Der "Vertrauensärztliche Dienst" hat durch die Weitergabe des vollständigen Gutachtens auch sonstige Offenbarungsschranken nicht beachtet (§ 76 Abs. 2 SGB X). Gutachten dürfen, wenn nicht andere gesetzliche Voraussetzungen vorliegen, nur dann weitergegeben werden, wenn der Betroffene nicht widersprochen hat. Um von seinem Widerspruchsrecht Gebrauch machen zu können, ist der Betroffene vorab von der beabsichtigten Offenbarung zu unterrichten. Eine solche Aufklärung hat jedoch im vorliegenden Fall nicht stattgefunden. Der Vorgang hat zu einer schwerwiegenden Beeinträchtigung der schutzwürdigen Belange des Betroffenen geführt.

Eine abschließende Stellungnahme des Vertrauensarztes liegt noch nicht vor.

7.4 Sozialpädagogische Familienhilfe

Seit einigen Jahren bieten die Jugendämter als neue Hilfeform die Sozialpädagogische Familienhilfe an. Die Hilfe besteht in einer intensiven Betreuung durch einen Familienhelfer über einen längeren Zeitraum. Der

Familienhelfer hat die Aufgabe, die Familie in Erziehungsfragen zu beraten, bei der Bewältigung von Alltagsproblemen zu helfen sowie bei der Lösung von Konflikten und Krisen mitzuwirken. Die Sozialpädagogische Familienhilfe ist konzipiert als eine Hilfeform, die die aktive Mitarbeit der Familie erfordert und nur auf freiwilliger Basis in Anspruch genommen wird. Dadurch, daß der Familienhelfer sich stundenweise in der betreuten Familie aufhält, werden ihm eine Fülle von Informationen über die Familienangehörigen bekannt. Damit stellt sich die Frage, welche Informationen, zu welchen Zwecken, an welche Stelle weitergegeben werden dürfen, ohne daß das informationelle Selbstbestimmungsrecht der Familienmitglieder verletzt wird. In Gesprächen mit Sozialarbeitern anläßlich einer Fortbildungsveranstaltung wurden die Datenschutzaspekte erörtert. Meine Auffassungen decken sich weitgehend mit denen von Prof. Dr. Udo Maas (Schriftenreihe Landeswohlfahrtsverband Baden, Karlsruhe 1988).

Ein Problem in diesem Zusammenhang stellen die Berichte dar, die zur Vorbereitung der Entscheidung über die Weitergewährung der Hilfe in regelmäßigen Zeitabständen dem Jugendamt vorzulegen sind. Unbestritten ist, daß sich der Berichtsumfang auf die für den Berichtszweck unbedingt erforderlichen Angaben beschränken muß. Die Familie ist vor Beginn der Hilfe über die regelmäßige Berichterstellung zu informieren. Darüberhinaus ist jeder einzelne Bericht mit der Familie zu besprechen und nur mit deren ausdrücklichen Einverständnis an das Jugendamt weiterzuleiten. Da die Inanspruchnahme der Sozialpädagogischen Familienhilfe auf Freiwilligkeit beruht, bedarf die gesamte Ausgestaltung des Betreuungsverhältnisses, wozu auch die Datenerhebung und -weitergabe gehört, des Einverständnisses der Familienmitglieder. Eine wirksame Einwilligung in eine Datenweitergabe setzt aber die Kenntnis über die zur Übermittlung bestimmten Informationen und den Verwendungszusammenhang voraus. Daß durch diese Ver-

fahrensweise keine unüberwindlichen Hürden aufgebaut werden, zeigt die Praxis eines Jugendamtes, das in dieser Weise verfährt.

Über den Berichtszweck hinaus dürfen grundsätzlich keine Informationen an das Jugendamt weitergegeben werden. Eine Ausnahme gilt insofern, als der Schutz höherwertiger Rechtsgüter eine Offenbarung erfordert, wobei als Maßstab eine Gefahr für Leben oder Gesundheit oder für das Kindeswohl heranzuziehen ist. Keinesfalls darf der Familienhelfer als Informationsquelle für andere Behörden (z.B. Sozialamt) herangezogen werden. Um die Akzeptanz der Sozialpädagogischen Familienhilfe zu gewährleisten, muß auf eine möglichst restriktive Praxis der Datenweitergabe geachtet werden.

7.5 Adoptionsvermittlung

Wer ein Kind adoptieren will, hat gegenüber der Adoptionsvermittlungsstelle seine persönlichen und wirtschaftlichen Verhältnisse offenzulegen. In den von den meisten saarländischen Adoptionsvermittlungsstellen verwendeten Antragsvordrucken werden unter anderem folgende Angaben über die Adoptionsbewerber erfragt: Schulabschluß, berufliche Ausbildung, Arbeitgeber, Vorstrafen, Krankheiten, Behinderungen, frühere Ehen und Gründe für deren Beendigung, Größe der Wohnung nach Quadratmetern und Anzahl der Räume, Nettoeinkommen, Miethöhe, Ratenzahlungen, Höhe und Laufzeit von Schuldverpflichtungen. Paßfotos beider Ehegatten sind ebenso vorzulegen wie polizeiliche Führungszeugnisse, ärztliche Atteste und ein ausführlicher Lebenslauf. In einem Ergänzungsfragebogen, der der Vorbereitung weiterer Gespräche dienen soll, wird u.a. nach gemeinsamen Freizeitinteressen der Familie, angenehmen und unangenehmen Erinnerungen an die eigene Kindheit, den wichtigen eigenen Bedürfnissen, den Auswirkungen der

Kindesaufnahme auf diese eigenen Bedürfnisse, der Partnerbeziehung und bereits vorhandenen Kindern gefragt.

Fragebögen dieses Inhalts werden auch verwendet bei der Vermittlung von Kindern in Pflegefamilien.

Im Erhebungsformular fehlt der gesetzlich vorgeschriebene Hinweis auf die Freiwilligkeit (§ 13 Abs. 2 DSGVO).

Mehrere Bewerber haben sich - stets unter dem Deckmantel der Anonymität, um die Chancen für eine Adoption nicht zu gefährden - an mich mit der Frage gewandt, ob eine solch umfassende Datenerhebung datenschutzrechtlich zulässig ist.

Die Adoptionsvermittlungsstellen benötigen Informationen, um die Eignung der Bewerber für die Adoption eines Kindes beurteilen und gegenüber dem Vormundschaftsgericht eine gutachtliche Stellungnahme abgeben zu können. Die Adoptionsvermittlung ist sowohl für das Kind als auch für die Eltern eine schwerwiegende und bedeutsame Entscheidung, die eine sorgfältige Prüfung erfordert. Im Interesse des Persönlichkeitsrechts der Betroffenen ist die Behörde allerdings auch verpflichtet, den Umfang der Datenerhebung auf das zur Aufgabenerfüllung unerläßliche Minimum zu beschränken. Meine Bemühungen, den Umfang der schriftlichen Abfragen zu reduzieren, blieben weitgehend erfolglos. Abgesehen von einzelnen Datenfeldern (z.B. Frage nach den Gründen für die Beendigung einer früheren Ehe) halten die Adoptionsvermittlungsstellen aus psychologisch-sozialpädagogischen Gründen alle weiteren Angaben und Unterlagen für erforderlich.

Mein weiterer Vorschlag, dann wenigstens nach rechtskräftig erfolgter Adoption die sensibleren Unterlagen zu vernichten oder den Eltern zurückzugeben und nicht

noch mindestens 30 Jahre aufzubewahren, wurde ebenfalls nicht aufgegriffen. Die Adoptionsvermittlungstellen sehen hierfür keine Notwendigkeit, "weil die Fragebogen in den Akten unter Verschluss behalten werden" und es "von Bedeutung sein kann, sich nachzuinformieren, wenn es beispielsweise nach der Vermittlung zu Erziehungsschwierigkeiten kommt". Diese lapidare, mir erst nach über einem Jahr zugegangene Begründung kann ich nicht akzeptieren. Sie wird den Anliegen der Betroffenen nicht gerecht, nicht länger als unbedingt notwendig in behördlichen Unterlagen mit Angaben aus ihrer Intimsphäre erfaßt zu sein. Wenn die Adoption rechtskräftig ist, steht das Kind einem leiblichen Kind gleich. Die Aufbewahrung detaillierter Informationen, die für die Adoptionsentscheidung herangezogen wurden, ist als unzulässige Datenvorratshaltung zu charakterisieren. In den gesetzlich genau umschriebenen Situationen müssen eventuell dann erforderliche Informationen erneut erhoben werden. Nur um eventuelle spätere Nachfragen des Kindes nach seiner Herkunft beantworten zu können, können Informationen in beschränktem Umfang aufbewahrt werden.

7.6 Sozialgeheimnis und Akteneinsichtsrecht des Betroffenen im Wohngeldverfahren

Eine Petentin hat sich darüber beschwert, daß die Wohngeldbehörde den Verwalter ihrer Mietwohnung über ihre finanziellen Verhältnisse sowie über Einzelheiten der Wohngeldgewährung informiert habe. Meine Ermittlungen haben folgendes ergeben:

Der Verwalter hatte die Behörde um Auskunft gebeten, ob und in welcher Höhe Wohngeld bewilligt worden sei. Gegebenenfalls solle das Wohngeld künftig unmittelbar auf das Konto des Vermieters überwiesen werden. Die Wohngeldstelle hat dem Verwalter auf diese Anfrage hin mitgeteilt, daß zur Zeit kein Wohngeld gewährt werde.

Die Befürchtungen der Petentin haben sich zwar nicht in vollem Umfang bestätigt. Die Mitteilung an den Verwalter des Mietshauses, daß zur Zeit kein Wohngeld gezahlt werde, stellt jedoch bereits eine Verletzung des Sozialgeheimnisses dar. Für die Weitergabe dieser Information ist eine Offenbarungsbefugnis nicht erkennbar. Zwar ist das Wohngeld für die Zahlung der Miete bestimmt und insoweit zweckgebunden; der Anspruch entfällt bei Nichtzahlung der Miete (§ 30 Abs. 2 Wohngeldgesetz). Daraus kann jedoch nicht hergeleitet werden, daß es für die Aufgabenerfüllung der Wohngeldstelle erforderlich sei, den Vermieter über den Bezug des Wohngeldes zu unterrichten. Hat die Wohngeldstelle Anhaltspunkte, daß der Leistungsempfänger keine Miete zahlt, so kann sie verlangen, daß dieser die Zahlung der Miete nachweist (§ 60 SGB I). Eine Anfrage beim Vermieter ist nicht erforderlich und damit unzulässig (§ 69 Abs. 1 Nr. 1 SGB X). Eine Überweisung des Wohngeldes unmittelbar an den Vermieter ist nur mit Einwilligung des Mieters zulässig (§ 28 Abs. 1 Wohngeldgesetz). Die Offenbarung des Status eines Sozialleistungsempfängers Dritten gegenüber ist nicht gerechtfertigt. Das Sozialgeheimnis wurde verletzt. Die Gemeinde hat zugesagt, künftig an den Vermieter keine Informationen über das Wohngeldverhältnis mehr weiterzugeben.

Der vorliegende Fall gab mir noch in anderer Hinsicht Anlaß, die Wohngeldstelle auf die Beachtung der Vorschriften über den Sozialdatenschutz hinzuweisen. Der Petentin, die um Akteneinsicht nachgesucht hatte, wurde nicht die vollständige Akte vorgelegt; die Wohngeldstelle hatte zuvor das Schreiben des Verwalters, in dem dieser die Überweisung des Wohngeldes auf das Konto der Vermieterin beantragt hatte, aus der Akte entfernt. Die Wohngeldstelle hat sich vor allem darauf berufen, daß nach ihrer Einschätzung die Petentin den

Inhalt dieses Schreibens zur Wahrnehmung ihrer Rechte nicht kennen müsse.

Ich bin der Auffassung, daß diese Handhabung der Akteneinsicht mit den gesetzlichen Vorschriften nicht in Einklang steht. Den Beteiligten ist Einsicht in die Verfahrensakten zu gewähren, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (§ 25 SGB X). Für die Beurteilung dieser Frage kommt es nicht auf die Bewertung der Behörde an, welche Tatsachen für die Interessenwahrung erforderlich sind. Es genügt vielmehr, daß der Betroffene die Notwendigkeit der Einsichtnahme zur Wahrnehmung seiner rechtlichen Interessen schlüssig darlegt.

Eine großzügige Handhabung der Akteneinsicht ist auch vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts zum Volkszählungsgesetz geboten. Danach gehört es zum Wesensgehalt des grundrechtlich geschützten Rechts auf informationelle Selbstbestimmung, daß der einzelne erkennen kann, "wer was wann und bei welcher Gelegenheit über ihn weiß". Soweit der Akteninhalt nicht wegen berechtigter Interessen Dritter geheimgehalten werden muß (§ 25 Abs. 3 SGB X), sind schwerlich Fälle denkbar, in denen die Sozialverwaltung einem Beteiligten die Akteneinsicht verwehren darf. Meine Intervention hat dazu geführt, daß die Gemeinde sich bereit erklärt hat, der Petentin Kenntnis vom Inhalt des fraglichen Schreibens zu geben.

7.7 Weitergabe der ärztlichen Verordnung über Orthopädiehilfsmittel durch die AOK an andere orthopädische Fachgeschäfte

Ein Petent hat darauf hingewiesen, daß die AOK bei der Versorgung von Patienten mit Orthopädiehilfsmitteln den Lieferauftrag häufig nicht dem von dem Versicher-

ten gewählten Fachgeschäft erteilt, sondern einer Firma, die die Leistungen kostengünstiger anbietet. Ohne Wissen der Versicherten gibt die AOK deren persönliche Daten an verschiedene Sanitätsgeschäfte zur Erstellung von Kostenvoranschlägen weiter.

Die personenbezogenen Daten der Versicherten unterliegen bei der AOK dem Sozialgeheimnis (§ 35 SGB I). Sie dürfen an Dritte nur weitergegeben werden, wenn die Weitergabe zur Aufgabenerfüllung der AOK erforderlich ist (§ 69 Abs. 1 Nr. 1 SGB X). Nicht zu bezweifeln ist zwar, daß die Krankenkassen zur wirtschaftlichen Leistungserbringung verpflichtet sind und deshalb durch geeignete Maßnahmen sicherzustellen haben, daß die Versicherten die vom Arzt verordneten Leistungen zu angemessenen Preisen erhalten. Wenn der Betroffene seinen Leistungsanspruch nicht verlieren will, ist er auch zur Mitwirkung in dem Sinne verpflichtet, daß er einer Weitergabe seiner Daten an verschiedene Leistungserbringer zustimmen muß. Diese gesetzliche Mitwirkungspflicht ist jedoch unter Berücksichtigung des vom Bundesverfassungsgericht in seinem Volkszählungsurteil anerkannten Rechts auf informationelle Selbstbestimmung als Mitwirkungsrecht anzusehen, d.h. der Betroffene muß die Entscheidungsbefugnis haben, der Offenbarung seiner persönlichen Daten zuzustimmen oder eine Versagung der Leistung in Kauf zu nehmen. Von diesem Recht kann der Versicherte bei der gegenwärtigen Praxis der AOK mangels Kenntnis des Verfahrensablaufs keinen Gebrauch machen. Ein Versicherter, der ein Orthopädiefachgeschäft seiner Wahl aufsucht, rechnet wohl kaum damit, daß seine Daten auch an andere Firmen zum Zweck der Erstellung von Kostenvoranschlägen weitergegeben werden.

Ich habe deshalb gefordert, daß die AOK die Versicherten vor einer Einschaltung anderer Firmen unterrichtet, um die Widerspruchsmöglichkeit zu gewährleisten. Meine Bemühungen haben jedoch zu meinem Bedauern zu keinem Erfolg geführt.

8. Statistik und Umfragen

8.1 Saarländisches Landesstatistikgesetz

Bereits in meinem letzten Tätigkeitsbericht habe ich mich umfassend mit dem Regierungsentwurf für ein Landesstatistikgesetz befaßt (vgl. 10. TB Tz. 6.2). Erfreulich ist, daß das Gesetz mittlerweile vom Landtag des Saarlandes verabschiedet wurde und damit für die Datenverarbeitung zu statistischen Zwecken eine gesetzliche Grundlage gegeben ist. Leider konnte ich mich mit meinen Vorstellungen zur Verbesserung des Entwurfes nicht in allen Punkten durchsetzen. Eine wesentliche Änderung gegenüber der Regierungsvorlage wurde in den Ausschußberatungen allerdings erreicht.

Besonders bedeutsam erscheint mir, daß das Gesetz nunmehr den Grundsatz der Freiwilligkeit der Erhebung ausdrücklich festlegt. Soll ausnahmsweise eine zwangsweise Erhebung durchgeführt werden, so bedarf es hierzu einer Anordnung durch Rechtsvorschrift. Auf diese Weise wird sichergestellt, daß sich sowohl der parlamentarische Gesetzgeber als auch der kommunale Satzungsgeber bei der Anordnung einer Statistik der Methodenfrage zu stellen hat und damit der Bürger von unverhältnismäßigen Eingriffen verschont bleibt.

Wenn auch aus meiner Sicht weitere Verbesserungen angezeigt gewesen wären, ist die Verabschiedung des Gesetzes zu begrüßen. Es besteht ein großes Interesse öffentlicher Stellen an der Durchführung statistischer Erhebungen. Das Gesetz wird als Rahmenregelung der Statistik im Landesbereich alsbald seine Bewährungsprobe bestehen müssen.

8.2 Bürgerumfrage der Landeshauptstadt Saarbrücken

Noch vor der Verabschiedung des Landesstatistikgesetzes hat die Landeshauptstadt Saarbrücken eine Bürgerumfrage bei 2.000 nach dem Zufallsprinzip ausgewählten Einwohnern durchgeführt. Themen der Befragung waren die Bewertung von Verkehrsmaßnahmen, die Verkehrsmittelwahl, Einkaufen, Wohnen im Stadtteil und das Verhältnis der Bürger zu Politik und Verwaltung. Die Umfrage wurde in Interviewform durchgeführt. Städtische Bedienstete suchten die ausgewählten Bürger auf und trugen die Antworten in vorbereitete Fragebogen ein. Nicht registriert wurden hierbei Name und Adresse des Befragten. Durch ein Anschreiben des Oberbürgermeisters waren die Bürger zuvor über die Umfrage unterrichtet sowie auf die Freiwilligkeit der Mitwirkung und die Anonymität der Erhebung hingewiesen worden.

Aus der Sicht des Datenschutzes bestanden gegen die Aktion keine durchgreifenden Bedenken. Zwar bedürfen statistische Erhebungen grundsätzlich einer Rechtsgrundlage - welche weder in Form des Landesstatistikgesetzes noch in Form einer kommunalen Satzung vorhanden war -, für die Übergangszeit habe ich als Grundlage der Befragung jedoch eine wirksame Einwilligung für ausreichend gehalten. Leicht gemacht wurde mir diese Entscheidung durch die von der Stadt Saarbrücken beachteten Rahmenbedingungen. Es erfolgte eine ausreichende Unterrichtung der Bürger über die beabsichtigte Datenerhebung, den Verwendungszweck und die Verarbeitungsziele der gewonnenen Daten, die Erhebung erfolgte auf freiwilliger Basis und es wurde eine hinreichende und frühzeitige Anonymisierung der Daten vorgenommen. Einen bedeutsamen Gesichtspunkt habe ich auch darin gesehen, daß die Untersuchung von der Statistikdienststelle der Landeshauptstadt durchgeführt wurde, einer Stelle, die funktionell, räumlich und organisatorisch von der übrigen Verwaltung der Stadt getrennt und

durch weitere Maßnahmen der Datensicherung abgeschottet ist.

Zu bemängeln hatte ich lediglich einen Aspekt, der erst nach genauerem Studium der Fragebogen erkenntlich wurde. Einige Fragen waren ohne Mitwirkung des Befragten durch den Interviewer zu beantworten. Hierbei waren zum Teil Antworten vorgesehen, die der Interviewer nur geben konnte, wenn er die Wohnung des Bürgers betreten hatte. Gefragt wurde beispielsweise nach der Ausstattung der Wohnung, der Belegenheit der Wohnung im Haus sowie dem Verhalten des Bürgers bei der Befragung. Ich habe die Stadt Saarbrücken darauf hingewiesen, daß derartige, vom Interviewer "verdeckt" zu erhebende Informationen von der Einwilligung des Betroffenen zur Mitwirkung an der Umfrage nicht gedeckt sind, da dessen Einwilligung sich nur auf die Beantwortung (offen) gestellter Fragen erstreckt. Ich habe daher gefordert, auf die durch den Interviewer zu beantwortenden Fragen zu verzichten und bereits erhobene Daten zu löschen. Dieser Forderung ist die Stadt Saarbrücken, soweit mir bekannt ist, gefolgt.

8.3 Fragebogenaktion "Energiekonzept"

Ein privater Fernwärmeversorgungsbetrieb führte zusammen mit dem Minister für Wirtschaft in einer Gemeinde eine Umfrage mit dem Ziel durch, für die Gemeinde ein Energiekonzept zu entwickeln. Befragt wurden Grundstückseigentümer über Gebäude, Heizungsart, Warmwasserbereitung und Möglichkeiten der Fernwärmeversorgung. Die Eigentümer wurden mit Namen und Adresse erfaßt.

Ich habe die Fragebogenaktion beanstandet, weil sie in einer Reihe von Punkten datenschutzrechtlichen Anforderungen nicht entsprach. Da die Untersuchung von Anfang an personenbezogen durchgeführt wurde, bedurfte

es zu ihrer Rechtmäßigkeit der Einwilligung der betroffenen Grundstückseigentümer. Eine wirksame Einwilligung im Sinne der Datenschutzgesetze setzt jedoch voraus, daß der Betroffene über die wesentlichen Ziele der Erhebung sowie die weitere Verwendung seiner Daten unterrichtet ist. Eine solche Unterrichtung fand vor der Befragung der Hauseigentümer nicht statt; sie konnte auch nicht stattfinden, weil zu diesem Zeitpunkt die spätere Verwendung der Daten noch nicht abschließend festgelegt war. Zwar war bestimmt, daß die Daten durch das Öko-Institut in Freiburg ausgewertet werden sollten, offen war jedoch, ob die Daten auch für Zwecke der Geschäftsanbahnung zwischen Wärmerversorgern und Hauseigentümern genutzt und welchen Unternehmen die Daten zugänglich gemacht werden sollten. Eine rechtsverbindliche Einwilligung konnten die Befragten somit nicht abgeben.

Gerügt habe ich auch, daß mangels einer schriftlichen Unterrichtung der befragten Personen, wie sie bei solchen Umfragen seit langem üblich ist, der gesetzlich vorgeschriebene Hinweis auf die Freiwilligkeit der Mitwirkung nicht sichergestellt war. Das saarländische Datenschutzgesetz verpflichtet öffentliche Stellen, dem Betroffenen die gesetzliche Grundlage für die Datenverarbeitung zu nennen oder ihn auf die Freiwilligkeit der Mitwirkung hinzuweisen. Der Minister für Wirtschaft war maßgeblich an der Erhebung beteiligt; das war auch für die Befragten ohne weiteres zu erkennen. Einem eventuellen Irrtum, daß es sich um eine zwangsweise Datenerhebung handeln könne, war hier durch einen ausdrücklichen Hinweis auf die Freiwilligkeit vorzubeugen. Um diesem Erfordernis zu entsprechen, sollte die Aufklärung durch ein entsprechendes Schreiben sichergestellt werden.

Angesichts der festgestellten Gesetzesverstöße habe ich gefordert, daß die personenbezogenen Daten und bereits vorliegenden Auswertungen zu löschen und die

Unterlagen zu vernichten sind. Dieser Forderung ist der Minister für Wirtschaft nachgekommen.

8.4 Umweltumfrage A.U.G.E.

Die Aktionsgemeinschaft Umwelt, Gesundheit, Ernährung (A.U.G.E.), ein eingetragener Verein mit Sitz in Hamburg, führte im Berichtszeitraum eine bundesweite Umfrageaktion unter dem Motto "Umweltfreundlicher Haushalt 1989" durch. Die Aktion wurde von zahlreichen Unternehmen der privaten Wirtschaft und namhaften Persönlichkeiten unterstützt. Die Fragebogenaktion, für die die Umweltminister des Bundes und der Länder die Schirmherrschaft übernommen hatten, wandte sich an alle Bundesbürger und verlangte Auskünfte zu umweltrelevanten Themen. Sie war gekoppelt mit einem Preisausschreiben und der Möglichkeit, weitere Informationen - auch von den Sponsoren aus der Wirtschaft - abzufordern.

Hat die aufwendige Aktion - geplant war der Einsatz von 40 Millionen Fragebogen - für sich allein bereits ausgereicht, ein allgemeines Interesse zu finden, so wurde die Öffentlichkeit hellwach, als eine befremdliche Verquickung von Fragen, die dem Umweltschutz dienten, mit solchen, die die werbende Wirtschaft interessierten, offenbar wurde. Anstoß bei den öffentlichen Schirmherrn der Aktion erregte vor allem die Frage nach der bevorzugten Karosserieform beim nächsten Autokauf. Die Einflußnahme der Wirtschaft auf die Fragen ergab sich im übrigen daraus, daß eine Zusendung von weiteren Umweltinformationen gekoppelt war mit dem Einverständnis zur Adressenweitergabe an die Sponsoren. Der saarländische Umweltminister nahm dies zum Anlaß, ebenso wie sein nordrhein-westfälischer Kollege, die Schirmherrschaft niederzulegen.

In datenschutzrechtlicher Hinsicht war - ebenso wie bei der Fragebogenaktion "Energiekonzept" (Tz. 8.3) - zu bemängeln, daß die befragten Personen völlig unzureichend über den Erhebungszweck und die weitere Verwendung ihrer Daten aufgeklärt wurden und damit eine rechtsverbindliche Einwilligung in die Datenverarbeitung nicht vorlag.

Abgesehen davon, verpflichtet das Bundesdatenschutzgesetz bei Meinungsumfragen dazu, die Adreßdaten vor der Auswertung von den Antworten zu trennen und hierdurch eine umfassende Anonymisierung zu gewährleisten. Diesem Erfordernis konnte bereits nach der Konzeption der Erhebung nicht hinreichend Rechnung getragen werden, weil Personen, die am Preisausschreiben teilnehmen wollten oder solche, die weiteres Informationsmaterial anforderten, Namen und Adresse unmittelbar auf dem Fragebogen angeben mußten. Ein weiterer Verstoß gegen das Bundesdatenschutzgesetz ergab sich daraus, daß die Fragebogen von Personen, die um die Zusendung von Informationsmaterial gebeten hatten, von der Aktionsgemeinschaft an die Sponsoren weitergeleitet werden sollten.

Ich habe gemeinsam mit meinem Hamburger Kollegen und anderen Datenschutzbeauftragten der Länder darauf gedrängt, daß die Vorgaben des Bundesdatenschutzgesetzes in vollem Umfang beachtet werden. Auf unsere Initiative hat die Aktionsgemeinschaft die bereits angelaufene Fragebogenaktion gestoppt und beim Rücklauf der bereits versandten Fragebogen eine manuelle Auswertung vorgenommen. Hierbei wurden die Adreßdaten von den Fragebogen abgeschrieben und für die Zusendung von Werbematerial sowie für die Mitwirkung am Preisausschreiben gesondert vorgehalten. Die Fragebogen im übrigen wurden ohne Speicherung von Namen und Adressen ausgewertet und danach vernichtet. Bei allen grundsätzlichen Bedenken gegenüber der anfänglichen Konzeption der Umfrage konnte auf diese Weise den schutzwür-

digen Belangen der Betroffenen Rechnung getragen werden.

Darüberhinaus hat die Aktionsgemeinschaft einen neuen Fragebogen konzipiert, auf dem Namen und Adresse so angebracht waren, daß sie ohne Schwierigkeiten abgetrennt werden konnten. Damit wurde eine anonyme Auswertung der Fragebogen in der Folge sichergestellt. Namen und Adressen konnten, soweit die Betroffenen eingewilligt hatten, für die Mitwirkung am Preisausschreiben und die Zusendung von Informationsmaterial verwandt werden. Gegen diese Verfahrensweise bestehen keine Bedenken.

9. Genomanalyse

Objekt der Genomanalyse ist das in Zellen eines jeden Lebewesens vorhandene genetische Material, das die Entwicklung des Organismus "steuert". Mit den genomanalytischen Verfahren werden Struktur und Funktionsfähigkeit der Erbsubstanz und des sie unmittelbar umgebenden Materials erforscht (Chromosomen-, proteinchemische und DNA-Analyse). Die Untersuchungen eröffnen Möglichkeiten der Früherkennung von genetisch bedingten Erkrankungsrisiken, der Feststellung von Dispositionen und Anfälligkeiten (z.B. bei Schadstoffexposition), der Vererbbarkeit von Krankheiten, der Identifizierung von Beschuldigten im Strafverfahren und der Klärung familiärer Abstammung. Mögliche Anwendungsbereiche sind die pränatale Diagnostik, Reihenuntersuchungen von Neugeborenen, die Aufklärung von Verbrechen, die gerichtliche Vaterschaftsfeststellung, sowie die Feststellung von Krankheitsdispositionen von Arbeit- und Versicherungsnehmern.

Die Genomanalyse bietet die Chance, durch geeignete Verhaltensweisen, bestimmte Erkrankungsrisiken zu verringern, Krankheitsverläufe zu lindern, die Übertragung von Erbkrankheiten durch präkonzeptionelle Beratung zu vermeiden und dadurch auch soziale Belastungen der Allgemeinheit zu mindern. Diesen Vorteilen stehen aus der Sicht des Datenschutzes schwerwiegende Risiken gegenüber. Durch die Entschlüsselung seiner genetischen Eigenschaften kann ein Mensch in seinem Persönlichkeitsrecht und sonstigen schutzwürdigen Belangen nachhaltig beeinträchtigt werden. Dem Betroffenen selbst bisher unbekannt, schicksalhafte Tatsachen über seine eigene Disposition zu unheilbaren Krankheiten können ihn psychisch außerordentlich belasten und ihn zu an sich nicht gewollten Entscheidungen in seiner Lebensgestaltung veranlassen. Die genetische Bedingtheit solcher Informationen hat zur Folge, daß auch Dritte aus der Familie betroffen sein können.

Die Konferenz der Datenschutzbeauftragten hat die Chancen und Risiken erörtert und auf der Grundlage der Vorarbeiten einer Arbeitsgruppe am 26./27.10.1989 eine EntschlieÙung (Anlage 13) gefaÙt. Grundlage waren vor allem der Bericht der Enquôte-Kommission "Chancen und Risiken der Gentechnologie" des Deutschen Bundestages (Bt-Drucksache 10/6775), die Ergebnisse einer Bund-Länder-Arbeitsgruppe und die BeschluÙempfehlung und der Bericht des Ausschusses für Forschung und Technologie (Bt-Drucksache 11/5320).

Die Konferenz war sich bewußt, daß in einer knappen, thesenartigen Stellungnahme nicht alle Gesichtspunkte ausreichend gewürdigt und vor allem nicht alle Möglichkeiten des Fortschritts in den Untersuchungsmethoden berücksichtigt werden können. Eine vorläufige Bewertung war jedoch zum gegenwärtigen Zeitpunkt der Diskussion geboten, um die wichtigsten, generellen Positionen des Datenschutzes zur Geltung zu bringen. Der Dialog mit der Wissenschaft soll jedoch unter Berücksichtigung weiterer und vor allem neuerer Erkenntnisse fortgesetzt werden.

Man muß davon ausgehen, daß die derzeit genutzten Methoden - einmal von denen abgesehen, die sich auf den Phaenotyp beschränken -, da sie Erkenntnisse über genetische Eigenschaften ermöglichen, für den Betroffenen einen weitergehenden Eingriff darstellen, als die sonstigen ärztlichen Untersuchungs- und Diagnosemöglichkeiten. Derzeit ist insbesondere nicht absehbar, ob es immer gelingt, Untersuchungsergebnisse auf den von vornherein festzulegenden Zweck zu begrenzen und dadurch eventuell nicht erforderliche und deshalb zusätzlich belastende ÜberflüÙinformationen zu vermeiden. Vor allem die weitere Verfügbarkeit von Untersuchungsmaterial birgt erhöhte Risiken. Die Zweckbindung der Untersuchung ist aber eine grundlegende Voraussetzung. Auch soweit die Beschränkung der Untersuchungs-

ergebnisse durch Begrenzung des Arbeitsfeldes auf "persönlichkeitsneutrale", "nicht codierende Teile" der Erbsubstanz möglich sein sollten, besteht im Interesse der schutzwürdigen Belange der Betroffenen ein erheblicher Bedarf an Klärung und Sicherung von Methode und Organisation der Verfahren. Dies um so mehr, als der Fortschritt in Methode und Technik derzeit nicht übersehbar ist und deshalb die Auswirkungen von Verfahren und Ergebnissen nicht endgültig eingeschätzt werden können. Der Umgang mit der Erbsubstanz birgt stets die Gefahr ihrer Manipulation.

Die Durchführung der Genomanalyse stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht dar, weil Informationen über den Kernbereich der Persönlichkeit erhoben, verarbeitet und gegebenenfalls offenbart werden; nicht zuletzt aber auch deshalb, weil Unsicherheiten über den Umfang der Entschlüsselung der Erbinformation angesichts des zu erwartenden wissenschaftlichen Fortschritts in der methodischen Ausführung aufkommen müssen.

Auch die freie Selbstbestimmung ist durch die Genomanalyse tangiert. Der freien und autonomen Entscheidung, sich der Genomanalyse zu unterziehen, kommt große Bedeutung zu. Es muß in der freien Entscheidung des Betroffenen liegen, ob wesentliche Grundlagen seines zukünftigen Daseins aufgeklärt werden sollen. Die Pflicht des Staates zur Daseinsvorsorge rechtfertigt nicht eine "prädiktive" oder "direktive" Medizin. Der Betroffene hat überdies ein Recht auf Nichtwissen.

Als Zwischenergebnis ist festzuhalten, daß ein so weitgehender Eingriff in die Persönlichkeitsrechte nur unter Beachtung verfassungsrechtlicher Grenzen aufgrund bereichsspezifischer, normenklarer Regelungen zulässig ist. Die Einwilligung des Betroffenen allein vermag jedenfalls die Beachtung seines informationellen Selbstbestimmungsrechts nicht zu gewährleisten.

Der faktische Zwang in den verschiedensten Formen, etwa im Arbeits- oder Versicherungsverhältnis, erfordert eine generelle Regelung des Einsatzes der Genomanalyse.

Der Bundesminister der Justiz hat inzwischen mitgeteilt, daß zur Personenidentifizierung im Strafverfahren "klare und eindeutige gesetzliche Regelungen über den Einsatz des sogenannten "genetischen Fingerabdrucks" geschaffen werden sollen" (Schreiben vom 03.11.1989 an den BfD). Ein entsprechender Gesetzentwurf werde zur Zeit erarbeitet, der den zulässigen Umfang der gentechnischen Untersuchung sowie die Nutzung der hieraus gewonnenen Erkenntnisse klar umgrenzen und die erforderlichen verfahrensrechtlichen und organisatorischen Sicherungen festlegen solle.

Diese Äußerung des Bundesministers der Justiz ist unter mehreren Gesichtspunkten bedeutsam. Zunächst wird im Ergebnis die Eingriffsqualität auch derjenigen Formen der genomanalytischen Untersuchung im Ergebnis eingeräumt, die sich mit den sog. "persönlichkeitsneutralen" Abschnitten der Erbsubstanz beschäftigen. Es mag dahinstehen, ob für diese Bewertung die Untersuchung dieses "nicht codierenden" Teils an sich oder die damit verbundenen sonstigen Gefahren der Offenbarung aus dem Kernbereich der Privatsphäre ausschlaggebend waren. Darüberhinaus werden die Zweifel an einer ausreichenden, gesetzlichen Ermächtigung für genomanalytische Untersuchungen bestätigt, die der Identifikation im Strafverfahren dienen sollen. Nicht zuletzt wird die Zweckbindung als verbindliches Prinzip akzeptiert, das eine Zweckorientierung der Untersuchung und eine an diesem Zweck ausgerichtete Nutzung der Ergebnisse der Analyse erfordert. Nur unter dieser Voraussetzung kann einer unverhältnismäßigen Beeinträchtigung der Betroffenen vorgebeugt werden.

Auch dürfte der Schlußfolgerung nichts mehr entgegengehalten werden können, daß Analysen zur gerichtlichen Feststellung der Abstammung ebenfalls einer gesetzlichen Regelung bedürfen, weil die geltenden zivilprozessualen Vorschriften den Eingriff nicht rechtfertigen. Der weitere Gang des Gesetzgebungsverfahrens muß indessen abgewartet werden.

Offen ist nach wie vor die Frage, inwieweit der Forderung nach einer gesetzlichen Regelung der vorgetragenen Grundsätze im übrigen gefolgt wird.

Die Genomanalyse kann in erster Linie genetisch bedingte Eigenschaften feststellen. Ob jemand krank wird aufgrund einer genetischen Disposition und wann dies geschieht, ist regelmäßig durch Genomanalyse nicht ohne weiteres festzustellen. Es darf nicht verkannt werden, daß neben der Erbsubstanz auch Einflüsse aus Umwelt, sozialer Umgebung und eigenverantwortlichem Verhalten den weiteren Lebensverlauf beeinflussen und damit endgültige Aussagen über den weiteren Werdegang des Einzelnen relativieren können. Vorbeugung und adäquate Lebensführung können jedenfalls nicht völlig außer Betracht bleiben. Der Zusammenhang zwischen genetischer Konstitution und dem Risiko, tatsächlich krank zu werden, kann mit wissenschaftlichen Methoden derzeit nicht ausreichend sicher gewichtet werden.

Allerdings wäre es wohl möglich, mit Hilfe der Genomanalyse Menschen auszuwählen, die gegen bestimmte Stoffe besonders widerstandsfähig sind. Damit wird die Verwendung dieser Untersuchungsmethode im Arbeitsleben schon im Ansatz fragwürdig. Nur zu leicht gibt man sich der Täuschung hin, in welchem Ausmaß die gesundheitsschädigende Wirkung von Schadstoffen beherrschbar ist. Es darf andererseits auch nicht zu einer Selektion des "genbehinderten" Arbeitnehmers kommen. Der Ausbau des Arbeitsschutzes hat jedenfalls Vorrang gegenüber der Kündigung oder der Ablehnung eines Be-

werbers für einen Arbeitsplatz. Vorsorgeuntersuchungen mit Hilfe der Genomanalyse sind jedoch mit allen bereits geschilderten Risiken für den Betroffenen belastet. Die bisher bestehende Risikoverteilung im Arbeitsleben muß gewahrt bleiben.

Im Versicherungswesen darf im konkreten Einzelfall nicht die gesamte genetische Konstitution zur Risikodifferenzierung herangezogen werden. Die Folge wäre, daß gewisse Risiken nicht mehr versichert werden könnten, und Versicherungsleistungen gerade demjenigen entzogen würden, der sie besonders benötigt. Das widerspräche der Gefahrengemeinschaft und auch dem öffentlichen Interesse an einem funktionierenden Versicherungsschutz. Das gesetzliche Fragerecht des Versicherers muß neu geregelt werden.

Der Schutz des ungeborenen, werdenden Lebens ist ein fundamentales Anliegen; der Schutz des Lebens ist im Grundgesetz verankert. Die vorgeburtliche Diagnostik aufgrund der Genomanalyse darf deshalb nicht der Einstellung Vorschub leisten, die Geburt behinderter Kinder oder von Kindern mit hohem Gesundheitsrisiko sei von vornherein unerwünscht. Immerhin sollen derzeit etwa 3 Prozent der Neugeborenen behindert sein, davon haben etwa 1 Prozent Herzfehler. Die Diagnostizierbarkeit einer angeborenen Behinderung im Mutterleib, sollte vor allem dazu beitragen, den Start ins Leben zu verbessern. Da die Zahl der feststellbaren Defekte in Zukunft ansteigen wird, darf die Genomanalyse kein Einfallstor für eine pränatale Selektion menschlichen Lebens werden. Fehlgeleitete Vorstellungen von einer Bevölkerungseugenik könnten erhebliche Folgen für die allgemeine Einstellung gegenüber Behinderten und deren Lebenssituation haben. Die derzeit festzustellende Toleranz gegenüber Behinderten könnte jedoch angesichts der Diagnosemöglichkeiten in Gefahr geraten. Auch die routinemäßige Durchführung von Untersuchungen an Neugeborenen stößt auf Bedenken. Der Schutz des

Lebens vor und nach der Geburt erfordert, daß nicht alle Erkenntnismöglichkeiten ausgeschöpft werden. Die freie Entscheidung der Eltern, eine solche Untersuchung durchzuführen, muß überdies stets sichergestellt sein.

Der Fortschritt der Medizin ist auf solche genomanalytische Untersuchungen angewiesen, die dazu beitragen können, daß kausal bisher nicht beherrschbare Krankheiten geheilt werden können oder ihnen durch Prophylaxe vorgebeugt wird. Deshalb sollten alle Möglichkeiten der Wissenschaft genutzt werden. Voraussetzung ist jedoch, daß sich Probanden in Kenntnis aller Risiken freiwillig zur Verfügung stellen. Um den besonderen Risiken zu begegnen sollte der Einsatz der Genomanalyse für wissenschaftliche Zwecke gesetzlich abgesichert werden.

10. Öffentlicher Dienst

10.1 Novellierung des Personalaktenrechts

Der Personaldatenschutz bedarf dringend einer gesetzlichen Regelung. Die allgemeinen Datenschutzgesetze haben sich als ungeeignet erwiesen, die Informationsverarbeitung im Arbeitgeber-/Arbeitnehmerverhältnis angemessen zu regeln. Auf die Regelungsdefizite - auch des öffentlichen Dienstrechts - habe ich in früheren Tätigkeitsberichten immer wieder hingewiesen (4. TB Tz. 3; 7. TB Tz. 7).

Der Bundesminister des Innern hat nunmehr - gestützt auf den Bericht einer Interministeriellen Arbeitsgruppe - einen Entwurf zur Änderung und Ergänzung des Bundesbeamtengesetzes zur Neuordnung des Personalaktenrechts erarbeitet. Ob das Gesetzgebungsverfahren hinsichtlich dieses noch in der Ressortabstimmung befindlichen Entwurfs in dieser Legislaturperiode abgeschlossen werden kann, ist offen. Es handelt sich jedenfalls um eine wichtige Gesetzgebungsmaßnahme zur Regelung des Personaldatenschutzes, wenn auch mit dem Personalaktenrecht vorwiegend nur ein Teilaspekt aufgegriffen wurde.

In meiner mit anderen Datenschutzbeauftragten abgestimmten Stellungnahme habe ich einige Verbesserungen vorgeschlagen. Sollte das Gesetzgebungsverfahren des Bundes in dieser Legislaturperiode nicht zum Abschluß kommen, muß ich an die Forderung des Ausschusses für Innere Verwaltung vom 30.09.1988 (Lt-Drucksache 9/1850-9/468 Tz. 5) erinnern, daß bis zur Verabschiedung rahmenrechtlicher Bestimmungen durch den Bundesgesetzgeber alle Regelungsmöglichkeiten auf Verwaltungsebene auszuschöpfen sind. Soweit eine rahmenrechtliche Regelung nicht erforderlich ist, kann der Landesgesetzgeber nicht mehr länger warten, die notwendigen gesetzlichen Vorkehrungen zu treffen.

10.2 Zentralisierung und Automatisierung der Beihilfebearbeitung

Die Landesverwaltung will zum 01.01.1990 ein automatisiertes Verfahren zur Berechnung und Zahlbarmachung der Beihilfe einsetzen. Damit zusammenhängend wird die Beihilfebearbeitung, für die bisher jedes Ressort selbst zuständig war, für alle Landesbehörden zusammengefaßt. Bei der Oberfinanzdirektion - Zentrale Besoldungs- und Versorgungsstelle (OFD-ZBS), die bereits für die gesamte Landesverwaltung Gehälter, Vergütungen, Löhne und Versorgungsleistungen berechnet und auszahlt, wird eine zentrale Beihilfestelle eingerichtet.

Eine Zentralisierung bietet aus datenschutzrechtlicher Sicht Vorteile. Die gemeinsame Bearbeitung von Personalangelegenheiten und Beihilfe entfällt. Somit wird der Gefahr besser vorgebeugt, daß Beihilfedaten zweckfremd verwendet werden.

Um Beihilfe zu erhalten, muß der Bedienstete unter anderem Arztrechnungen und Arzneimittelverordnungen vorlegen, die durch die Angaben über Diagnose und Therapiemaßnahmen Aufschlüsse über seinen Gesundheitszustand und den seiner Angehörigen geben. So müssen z.B. psychotherapeutische Maßnahmen bereits vor der Behandlung von der Beihilfestelle genehmigt werden. Einzelne Beihilfeberechtigte haben - wie ich erfahren habe - aus Sorge, daß Erkrankungen dem Dienstherrn bekannt werden und bei Personalentscheidungen, z.B. Beförderungen, eine Rolle spielen könnten, entweder auf notwendige Behandlungsmaßnahmen oder auf die Einreichung der Rechnungen verzichtet.

Das in § 17 Abs. 2 Beihilfeverordnung festgelegte Zweckbindungsgebot ist in allen öffentlichen Stellen

durch eine strikte organisatorische, personelle und räumliche Abschottung der Beihilfestelle zu gewährleisten. Vor allem ist dafür zu sorgen, daß die in kleinen Behörden immer noch übliche organisatorische Zusammenfassung mit der Personalsachbearbeitung aufgegeben wird. Im Bereich der Landesverwaltung ist eine solche Abschottung durch Zentralisierung zu erreichen. Allerdings muß auch bei der dafür vorgesehenen OFD dafür gesorgt werden, daß die Funktionstrennung zwischen Personalverwaltung und automatisierter Abwicklung der Beihilfebearbeitung hergestellt wird. Kleine Behörden, vor allem kleinere Gemeinden, können die notwendigen organisatorischen Vorkehrungen nicht bieten. Deshalb ist in solchen Fällen die Möglichkeit zu erwägen, eine externe öffentliche Stelle mit der Bearbeitung der Beihilfe zu betrauen.

Das bereits beim Bund und anderen Bundesländern eingesetzte System BABSY unterstützt im Rahmen einer Dialogverarbeitung die Sachbearbeitung in vielfältiger Weise etwa bei der Dateneingabe, der Kontrolle der Beihilfefähigkeit der geltend gemachten Aufwendungen, der Festlegung der Bemessungssätze, der Erstellung der Bescheide. Es bietet dabei auch die Möglichkeit, Arztrechnungen und andere Leistungsabrechnungen anhand von Gebührenziffern (z.B. der Gebührenordnung für Ärzte) oder Tarifen zu überprüfen. Diagnosen und die einzelnen erbrachten Leistungen werden jedoch nicht in der Datenbank gespeichert.

Der Zugriff der einzelnen Sachbearbeiter und der Prüfer ist auf die Daten der Beihilfefälle zu beschränken, für die sie zuständig sind. Ein Zugriff ausschließlich unter Eingabe des Namens eines Beihilfeberechtigten sollte nur einer besonderen Clearingstelle erlaubt sein, um Anträge ohne Personalnummer dem zuständigen Bearbeiter zuweisen zu können. Dadurch wird die Möglichkeit des Bearbeiters eingeschränkt, unab-

hängig von einem konkreten Antrag gezielt Beihilfedaten einzusehen.

Abgesehen von der Beurteilung dieses einzelnen Automatisationsverfahrens dürfen die durch die zunehmende automatisierte Verarbeitung von Personaldaten für die Persönlichkeitsrechte der Betroffenen entstehenden Gefahren nicht aus den Augen verloren werden. Durch immer neue Verfahren - so auch durch die fortschreitende, ressortübergreifende Automation im Personalbereich der Landesregierung (vgl. meinen 10. TB Tz. 7.2 zu DIAPERS) - werden die Personaldaten nahezu umfassend edv-gestützt verarbeitet. Die einzelnen Systeme sind, um die Aktualität der Grunddaten sicherzustellen und um die Abwicklung zu vereinfachen, miteinander durch eine einheitliche Ordnungsnummer, die Personalnummer, verknüpft. Es stellt sich immer mehr die Frage nach der Sozialverträglichkeit des Einsatzes automatisierter Verfahren im Personalbereich. Jedenfalls hat der Gesetzgeber mehr als früher organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung der Persönlichkeitsrechte entgegenwirken (BVerfGE 65,1 ff, 44). Entsprechende Forderungen habe ich bereits früher (vgl. meinen 7. TB Tz. 7.2) und im Zusammenhang mit der zurückgestellten Novellierung des Saarländischen Datenschutzgesetzes vorgetragen. Insbesondere müssen die automatisierten Verfahren, die der Auswertung von Personaldaten dienen, von vornherein und abschließend unter Beteiligung der Personalvertretung festgelegt und die Transparenz aller Möglichkeiten dieser Art für den einzelnen Bediensteten gewährleistet sein.

10.3 Telefonnebenaten

Der Minister der Finanzen hat zum 01.08.1989 neue Fernsprechrichtlinien für die Landesbehörden in Kraft gesetzt, die meine im 10. TB (Tz. 7.1) nochmals aufge-

griffenen Forderungen weitgehend berücksichtigen. Hervorzuheben sind insbesondere die folgenden Verbesserungen:

- Bei Privatgesprächen darf die Nummer des angerufenen Gesprächspartners (Zielnummer) nur unter Weglassung der beiden letzten Ziffern gespeichert werden.
- Bei dienstlichen Gesprächen, die nicht der Dienstaufsicht unterliegen, wird - sofern sie von hierfür bestimmten Nebenstellen aus geführt werden - die Zielnummer überhaupt nicht erfaßt. Beispielfhaft erwähnen die Richtlinien Telefonate von Personalratsmitgliedern oder von Personen, die nach § 203 StGB einem besonderen Berufsgeheimnis unterliegen (Ärzte, Psychologen, Berater in einer Erziehungsberatungsstelle usw.).

Nicht übernommen wurde mein Vorschlag, auch bei (sonstigen) Dienstgesprächen die Zielnummer nur verkürzt zu speichern. Meines Erachtens erfordert auch eine sicherlich notwendige, stichprobenweise Kontrolle - wie die Praxis in Hessen zeigt - keine Erfassung der vollständigen Zielnummer. Auch die Landeshauptstadt Saarbrücken hat in einer kürzlich abgeschlossenen Dienstvereinbarung für den Bereich der Stadtverwaltung sich dahin festgelegt, daß bei dienstlichen wie auch bei privaten Telefonaten die Zielnummer nur um die beiden letzten Stellen verkürzt gespeichert werden darf.

11. Probleme aus sonstigen Bereichen

11.1 Kontrollmitteilungen an die Steuerbehörden

Einer lang andauernden Praxis entsprechend übermitteln insbesondere öffentliche Stellen den Finanzbehörden Informationen über die Auszahlung von Geldbeträgen, die nicht einem direkten Steuerabzug unterliegen. Dazu gehören zum Beispiel Zahlungen aus dem Landeshaushalt an Unterrichtende und Vortragende im Nebenberuf oder an Bauunternehmer für Leistungen bei der Errichtung öffentlicher Bauten oder der Instandsetzung von Straßen. Mit diesen Kontrollmitteilungen sollen den Finanzämtern Ansatzpunkte für die Überprüfung von Steuererklärungen an die Hand gegeben werden. Eine Rechtsgrundlage für diese Datenübermittlungen ist derzeit nicht gegeben. Der Erlaß einer Kontrollmitteilungsverordnung ist zwar inzwischen durch Änderung der Abgabenordnung gesetzlich vorgesehen (§ 93 a AO), sie ist bisher jedoch noch nicht in Kraft gesetzt.

Ich habe daher den Finanzminister auf die Rechtswidrigkeit der derzeitigen Verfahrensweise hingewiesen und ihn aufgefordert, das Kontrollmitteilungsverfahren bis zum Erlaß der Rechtsverordnung einzustellen. Der hessische Finanzminister hat rechtsstaatlichen Überlegungen Vorrang eingeräumt und mit Erlaß vom 2. November 1999 alle Behörden des Landes angewiesen, von solchen Datenübermittlungen abzusehen, soweit sie nicht durch eine spezielle gesetzliche Regelung angeordnet sind. Eine Stellungnahme des saarländischen Finanzministers liegt mir bisher noch nicht vor; es bleibt daher abzuwarten, ob im Saarland den durch die Verfassung vorgegebenen Anforderungen in gleicher Weise Rechnung getragen wird. Wie ich dem 9. Bericht des Datenschutzbeauftragten des Saarländischen Rundfunks entnehme, hat jedenfalls diese Anstalt des öffentlichen Rechts im Berichtsjahr keine Kontrollmit-

teilungen über die an freie Mitarbeiter gezahlten Honorare an die Finanzbehörde übermittelt.

11.2 Auswertung von "Kurmeldescheinen"

Im Auftrag des Wirtschaftsministeriums erstellte ein wirtschaftswissenschaftliches Institut ein Konzept für die Fremdenverkehrsentwicklung im Saarland. Ein Petent führte mir gegenüber Klage darüber, daß zur Feststellung der Übernachtungszahlen in einigen saarländischen Gemeinden Hotelmeldescheine rechtswidrig ausgewertet worden seien. Da die Untersuchungen bereits längere Zeit zurücklagen, waren die Ermittlungen meiner Behörde erschwert. Der Verdacht, daß melderechtliche Unterlagen rechtswidrig verwertet worden seien, hat sich jedoch nicht bestätigt. Bei der Prüfung in einer Gemeinde konnte lediglich festgestellt werden, daß der Verkehrsverein, der im Auftrag der Gemeinde die Kurabgaben erhebt, personenbezogene Unterlagen an das wissenschaftliche Institut weitergeleitet hat.

Zwar wurden dem Institut keine Meldeunterlagen zur Verfügung gestellt, die festgestellte Verfahrensweise mußte ich gleichwohl beanstanden, da sie mit den Bestimmungen des Saarländischen Datenschutzgesetzes nicht in Einklang steht. Für die Erstellung eines Fremdenverkehrskonzeptes war eine personenbezogene Datenübermittlung nicht erforderlich. Namen und Anschriften der Kurgäste waren für die Untersuchung nicht von Interesse, so daß es ausreichend gewesen wäre, wenn dem Institut anonymisierte Daten zur Verfügung gestellt worden wären. Die Unterlagen sind inzwischen dem Verkehrsverein wieder zurückgegeben worden.

11.3 Weiterleitung der Todesanzeigen durch die Standesbeamten an das Nachlaßgericht

Über die Aufgabe des Standesbeamten, bei Sterbefällen dem Finanzamt auch Angaben über den Nachlaß zu liefern, hatte ich in meinem 8. Tätigkeitsbericht (Tz. 11.1) berichtet. Eine befriedigende Lösung des Problems, vor allem eine ausreichende Aufklärung der Hinterbliebenen, daß die Datenangabe freiwillig erfolgt, ist bisher nicht erreicht worden.

Inzwischen habe ich erfahren, daß die Standesämter im ehemals bayerischen Teil des Saarlandes Informationen über den Nachlaß auch dem Amtsgericht übermitteln. Die Verpflichtung, dem Nachlaßgericht jeden beurkundeten Todesfall mitzuteilen, beruht auf einem Gesetz aus dem Jahre 1902. Dem Nachlaßgericht soll dadurch ermöglicht werden, die ihm nach diesem Gesetz obliegende Aufgabe der Erbenermittlung und der Vermittlung der Auseinandersetzung zwischen den Beteiligten zu erfüllen. In dem bayerischen Gesetz wird dem Standesbeamten aber nicht auferlegt, die Hinterbliebenen nach Art und Wert des Nachlasses zu befragen. Das Nachlaßgericht ist aufgrund der ihm zur Verfügung stehenden gesetzlichen Befugnisse selbst in der Lage, diese Angaben zu erheben.

Der Minister des Innern hat daraufhin die Standesbeamten angewiesen, dem Nachlaßgericht nur noch die eigentlichen Beurkundungsdaten des Sterbefalles mitzuteilen. Dem Hinterbliebenen, der den Sterbefall anzeigt, soll ein "Fragebogen zur Ermittlung der Erben" ausgehändigt werden, den dieser auszufüllen und an das Nachlaßgericht weiterzuleiten hat. Ich begrüße diese Regelung, die die Funktion des Standesbeamten und seinen gesetzlichen Auftrag in angemessener Weise berücksichtigt.

11.4 Benachrichtigung bei der Einschulung

Der Computer hilft zwar das Massengeschäft in der Verwaltung zu bewältigen. Nur zu leicht werden jedoch dabei die schutzwürdigen Belange einzelner beeinträchtigt.

Die Gemeinde als Träger der Grundschulen versendet bei der Einschulung Benachrichtigungen. Die Adreßaufkleber für diese Mitteilungen enthalten Namen und Adresse des erstmals schulpflichtigen Kindes. Stimmt der Namen des Kindes nicht mit dem der Erziehungsberechtigten überein, können der Briefträger, aber auch Mitbewohner im Haus erkennen, daß das Kind nicht bei seinen leiblichen Eltern lebt. Regelmäßig handelt es sich in solchen Fällen um ein Pflegekindschaftsverhältnis. Die Pflegeeltern und das Kind haben ein Interesse daran - vor allem bei späterer Adoption -, daß von Anfang an die volle Integration in den Familienverband auch anderen gegenüber gewährleistet ist.

Ich habe deshalb gefordert, daß die Adresse bei der Einschulungsbenachrichtigung nicht mehr die Namen des Kindes, sondern ausschließlich die der gesetzlichen Vertreter oder Erziehungsberechtigten enthält. Wenigstens bei Namensverschiedenheit in der Adressierung an das Kind und die Pflegeeltern sollte dafür gesorgt werden, daß die schutzwürdigen Belange berücksichtigt und nur die Namen der "Eltern" ausgedruckt werden. Auch hierbei kann die Automation das Verfahren erleichtern. Durch einen automatisierten Abgleich kann die Namensverschiedenheit im Einzelfall leicht festgestellt werden. Die Vorteile der Automation liegen auf der Hand; sie müssen im Interesse der Menschen aber auch voll genutzt werden.

11.5 Entsorgung von Aktenmaterial durch eine Rechtsanwaltskanzlei

Der Fall einer Aktenentsorgung durch eine Saarbrücker Rechtsanwaltskanzlei macht deutlich, daß die notwendige Sensibilität im Umgang mit personenbezogenen Unterlagen noch nicht ausreichend entwickelt ist. Im Zuge einer Kanzleiauflösung wurden nicht mehr benötigte Akten, ausgesondertes Schriftgut und Satzsetzwürfe in Plastiksäcke verpackt für die Sperrgutabfuhr bereitgestellt. Da die Säcke über Nacht auf dem Bürgersteig lagerten, wurden sie vermutlich auf verwertbare Gegenstände durchsucht. Jedenfalls fanden Passanten am nächsten Morgen Aktenmaterial auf dem Bürgersteig verstreut. Durch die herbeigerufene Polizei wurden auch hochsensible Unterlagen wie Gerichtsentscheidungen in Erbaueinandersetzungen sowie Akten über Familien- und Scheidungsangelegenheiten gefunden.

Es bedarf keiner näheren Erläuterung, daß durch einen derartig sorglosen Umgang mit personenbezogener Unterlagen in rechtswidriger Weise in das Persönlichkeitsrecht der betroffenen Bürger eingegriffen wurde. Die Polizei hat daher folgerichtig ein Strafverfahren wegen Verletzung von Privatgeheimnissen (§ 203 StGB) eingeleitet. Nachdem ich von dem Vorfall Kenntnis erlangt habe, habe ich zudem die Rechtsanwaltskammer unterrichtet, die aufsichtsrechtliche Maßnahmen gegen den Rechtsanwalt eingeleitet hat.

11.6 Auskunftersuchen eines Anwaltes gegenüber der Kfz-Zulassungsstelle

Ein Petent beklagte sich bei meiner Dienststelle über die unbefugte Auskunftserteilung durch eine Kfz-Zulassungsstelle. Eine Untersuchung des Vorgangs ergab, daß einem Rechtsanwalt von der Zulassungsstelle mitgeteilt worden war, daß der Petent Halter eines bestimmten

Fahrzeuges und bei welcher Versicherung das Fahrzeug angemeldet ist. Der Rechtsanwalt hatte gegenüber der Zulassungsstelle wahrheitswidrig angegeben, er benötige diese Informationen zur Durchsetzung von Ansprüchen aus einem Verkehrsunfall. Da in Wirklichkeit ein Unfall nicht stattgefunden hatte, war die Datenübermittlung rechtswidrig. Denn das Straßenverkehrsgesetz gestattet der Kfz-Zulassungsstelle die Mitteilung von Informationen an Privatpersonen lediglich dann, wenn sie im Zusammenhang mit Ansprüchen aus der Teilnahme am Straßenverkehr stehen. Ein solcher Fall lag jedoch nicht vor.

Ich habe den Rechtsanwalt auf die Rechtswidrigkeit der Auskunftserteilung hingewiesen. Da der Anwalt die formularmäßig beantragte Auskunft einem Fehler seines Büros zuschrieb, habe ich außerdem gefordert, daß das Personal über die Rechtslage unterrichtet und belehrt wird. Auf Maßnahmen gegenüber der Kfz-Zulassungsstelle habe ich verzichtet. Die Zulassungsstelle durfte aufgrund der Antragstellung durch die Rechtsanwaltskanzlei darauf vertrauen, daß die Voraussetzungen für eine rechtmäßige Datenübermittlung vorliegen.

11.7 Gebäudezusatzerhebung der Stadt Saarbrücken im Zusammenhang mit der Volkszählung'83

In meinem 8. Tätigkeitsbericht (Tz. 4.2) habe ich über eine von mir beanstandete, rechtswidrige Datenerhebung der Stadt Saarbrücken im Zusammenhang mit der Volkszählung'83 berichtet. Die Stadt hatte gleichzeitig mit dem "amtlichen" Teil der Volkszählung eine kommunale Zusatzerhebung durchgeführt. Die hieraus gewonnenen Daten wurden zum Aufbau einer kommunalen Gebäudedatei gespeichert, ohne daß hierfür eine ausreichende Rechtsgrundlage vorhanden war. Nachdem das Bundesverfassungsgericht die Volkszählung'83 blockiert und das zugrunde liegende Gesetz für nichtig erklärt hatte,

hat die Stadt Saarbrücken den amtlichen Teil der Erhebungsbögen vernichtet. Meiner Aufforderung aus dem Jahre 1984, auch die Informationen aus der Zusatzerhebung zu vernichten ist die Landeshauptstadt bisher nicht nachgekommen. Auch das Statistische Landesamt ist in einer Prüfung zu dem Ergebnis gelangt, daß die Durchführung der Erhebung sowie die Verarbeitung der Daten unter Mißachtung des geltenden Rechts erfolgt ist und deshalb jede weitere Nutzung dieser Daten zu unterbleiben hat. Auf Initiative der Staatskanzlei wurde zwischenzeitlich der Minister des Innern als Kommunalaufsichtsbehörde mit der Angelegenheit beauftragt. Ein endgültiges Ergebnis liegt noch nicht vor. Ich gehe davon aus, daß die Stadt durch kommunalaufsichtsrechtliche Mittel dazu angehalten wird, die rechtswidrig erhobenen Daten zu löschen.

11.8 Änderung des Gesetzes zu Art. 10 GG und der Strafprozeßordnung im Rahmen der Poststrukturreform

Die Datenschutzbeauftragten des Bundes und der Länder haben ähnlich wie der Arbeitskreis der Internationalen Konferenz in Berlin (Anlage 3) die Informationsverarbeitung in komplexen Netzen und Systemen in einer Entschließung kritisiert (Anlage 14). Im Rahmen der Poststrukturreform ist aufgrund eines Antrags aus dem Bundestag die Überwachung des Fernmeldeverkehrs durch die Nachrichtendienste und die Strafverfolgungsbehörden erweitert worden. Während in der Vergangenheit neben dem Briefverkehr nur Telefongespräche und Fernschreiben kontrolliert und ausgewertet werden durften, ist dies in Zukunft für alle Dienste des Fernmeldeverkehrs (z.B. Btx, Temex, Telefax, ISDN) unter Einbeziehung von Abrechnungs-, Verbindungs- und Nutzungsdaten grundsätzlich zulässig. Die durch den Fortschritt der Telekommunikation vermehrt anfallenden "elektronischen Spuren" des Bürgers sollen in die Überwachungs- und Kontrollmöglichkeiten der Nachrichtendienste und

Strafverfolgungsbehörden voll einbezogen werden. Die Datenschutzbeauftragten haben vergebens gefordert, vor einer Erstreckung der gesetzlichen Kontrollbefugnisse auf die neuen Formen des Fernmeldeverkehrs die Auswirkungen eingehend zu diskutieren.

11.9 Versendung von Anfragen der Landratsämter an den Verfassungsschutz

Durch eine Fehlzustellung der Posteingangsstelle beim Ministerium des Innern wurde ich auf einen Vorgang mit datenschutzrechtlicher Bedeutung aufmerksam. Zugestellt wurde mir ein Schriftstück, in dem die Ausländerbehörde eines Landratsamtes sich beim Landesamt für Verfassungsschutz nach Erkenntnissen über einen sowjetischen Staatsbürger erkundigte. Das Schreiben wurde offen auf dem Dienstweg versandt und gelangte durch eine Verwechslung in meine Dienststelle.

In Anbetracht der Sensibilität derartiger Anfragen und der Tatsache, daß - wie im konkreten Fall bewiesen - Fehlzustellungen nicht auszuschließen sind, habe ich die offene Versendung gerügt. Ich habe den Minister des Innern gebeten, durch Weisung sicherzustellen, daß auch bei Versendung von Schriftstücken dieser Art auf dem Dienstwege eine Kuvertierung vorgenommen wird. Gleichzeitig habe ich die Anfragepraxis der Ausländerbehörden unter Berücksichtigung datenschutzrechtlicher Belange problematisiert.

Auf meine Initiative hin hat der Minister des Innern eine generelle Weisung an die Landräte erlassen, beim Versand von Schriftstücken mit personenbezogenen Daten diese so zu kuvertieren und zu beschriften, daß sie ungeöffnet dem Endadressaten zugestellt werden können. Im übrigen hat er mir mitgeteilt, daß die Ausländerbehörden von ihm angewiesen worden sind, auf routinemäßige Anfragen an den Verfassungsschutz im Zusammen-

hang mit der erstmaligen Erteilung einer Aufenthaltserlaubnis sowie vor Erteilung der Aufenthaltserlaubnis in Form des Sichtvermerkes zu verzichten.

Anlage 1

Berliner Resolution der Internationalen Konferenz
der Datenschutzbeauftragten vom 30. August 1989

Die Telekommunikation befindet sich weltweit in einer raschen Entwicklung. Über internationale Datennetze werden in wachsendem Umfang auch personenbezogene Daten transferiert, etwa im Zusammenhang mit der Verwendung von Kreditkarten, bei Reise-Buchungs-Systemen und innerhalb multinationaler Unternehmen. Die Nutzung dieser Technologie kann bedeutende Vorteile mit sich bringen. Aber zugleich wird es schwieriger, die Rechte derer zu schützen, deren persönliche Daten rund um die Welt übermittelt werden.

Der Europarat, die OECD, die Vereinten Nationen und weitere internationale Organisationen haben Empfehlungen und Leitlinien zum Datenschutz verabschiedet. Sie enthalten einen gemeinsamen Bestand von Grundsätzen für eine faire Praxis, wie sie etwa in der Konvention des Europarats (Konvention No. 108) und in den OECD-Leitlinien zum Ausdruck kommen. Sie bezwecken den Schutz der Privatheit des einzelnen.

Bisher haben sich acht Staaten durch Beitritt zur Konvention des Europarats international verpflichtet, einen bestimmten Datenschutzstandard einzuhalten. Die Datenschutz-Kontrollinstanzen dieser Länder haben in gewissem Umfang die Befugnis, den grenzüberschreitenden Datenfluß zu kontrollieren, wenn dies zum Schutz einzelner nötig ist. Bei dieser Kontrolle ergeben sich allerdings schwerwiegende praktische Probleme. Daten-Übermittlung ins Ausland bedeutet deshalb für den einzelnen in der Mehrzahl der Fälle, daß er nicht mehr die Gewißheit haben kann, daß die Grundsätze, die in nationalen Gesetzen und in den verschiedenen internationalen Übereinkommen festgelegt sind, auf seine oder ihre Daten angewandt werden. Zum Beispiel kann es dann

keine Garantie geben, daß die Daten auf dem neuesten Stand und genau sind und nur für bestimmte Zwecke verwendet werden. Der einzelne kann auch sein Recht, einen Datenschutzbeauftragten anzurufen, nicht wahrnehmen.

Das Problem eines wirksamen internationalen Datenschutzes läßt sich nur durch gleichwertige gesetzliche Sicherungen in den übermittelnden und empfangenden Ländern lösen. Diese Lösung wird auch von den oben genannten Empfehlungen und Leitlinien vorgezeichnet.

Nach Auffassung der Datenschutzbeauftragten muß bei der Entwicklung und Nutzung internationaler Datendienste dem Datenschutz die gleiche Priorität gegeben werden, wie der Förderung der Datenverarbeitung und der Telekommunikation. Sie empfehlen deshalb:

- Die Regierungen sollten sowohl einzeln als auch im Rahmen internationaler Organisationen darauf hinarbeiten, daß so bald wie möglich gleichwertige gesetzliche Sicherungen geschaffen werden.
- Wer personenbezogene Daten über die Grenzen vermittelt, muß den Schutz beim Empfänger prüfen, daß die Beachtung der Rechte der Betroffenen tatsächlich sichergestellt wird.

Das Ziel dieser Maßnahme muß sein:

- Die Datenschutzgrundsätze der Konvention 108 und der OECD-Leitlinien werden unabhängig von einer grenzüberschreitenden Übermittlung gewährleistet;
- international operierende Datenverarbeitungssysteme müssen so aufgebaut sein, daß der einzelne ohne unzumutbare Schwierigkeiten seine Datenschutzrechte wahrnehmen kann;

- Berichtigungen, Aktualisierungen und Löschungen von Daten müssen auch im Ausland nachvollzogen werden, wenn die Daten zuvor dorthin übermittelt worden sind;

- die durch den internationalen Datenaustausch erhöhten Gefahren für das Recht des einzelnen, über die Verwendung ihrer Daten zu bestimmen, müssen durch internationale Zusammenarbeit der Datenschutzbeauftragten ausgeglichen werden.

Anlage 2

EntschlieÙung der Elften Internationalen Konferenz
der Datenschutzbeauftragten vom 30. August 1989
über die Arbeitsgruppe Medien

Die Ausarbeitung des Entwurfs für eine EntschlieÙung war AnlaÙ zu einem sehr nützlichen Informationsaustausch zwischen den teilnehmenden Delegationen.

Die Empfehlungen und Entscheidungen, die wir in unseren jeweiligen Ländern ausgesprochen bzw. getroffen haben, sollten die internationale Dimension der Netze und Dienstleistungen berücksichtigen.

Die Informationen über die Entwicklungen, die sich jenseits unserer Grenzen vollziehen, dürfen uns nicht ausschließlich von unseren nationalen Organen übermittelt werden.

Die Netze und Dienstleistungen werden in unseren jeweiligen Ländern nicht gleichzeitig bzw. im selben Rhythmus weiterentwickelt.

Unsere Erfahrungen haben gezeigt, daÙ die Effizienz des Datenschutzes in diesem Bereich - über die Prinzipien hinaus - auf praktischen Maßnahmen beruht, über die von den nationalen Verwaltungsinstanzen Informationen nicht leicht zu erhalten sind.

Daher beschließt die Konferenz, daÙ diese Arbeitsgruppe ihre Arbeit in Berlin fortsetzt und daÙ nach Möglichkeit jede Delegation ihre Erfahrungen, insbesondere in folgenden Bereichen, einbringen sollte:

- detaillierte Rechnungslegung
- Modalitäten zur Aufnahme in die Teilnehmerverzeichnisse, Verwendung der Teilnehmerverzeichnisse

- verschiedene Kategorien der Telematischen Dienste (elektronische Post, Fernkäufe, Informationsdienste, usw.)
- Fernmeßverfahren
- ISDN
- Zelluläres Telefon (digitaler Mobilfunk)
- automatische Anrufeinrichtungen
- Sicherheit der Netze
- Kabelnetze für Dialogfernsehen.

Anlage 3

EntschlieÙung der Elften Internationalen Konferenz
der Datenschutzbeauftragten vom 30. August 1989
zu den Problemen des ISDN

Die Datenschutzbeauftragten:

- 1) begrüÙen die bisherige die ISDN-Probleme betreffende Tätigkeit des Arbeitskreises Medien und unterstreichen die Bedeutung dieser Fragen,
- 2) nehmen den von dem Arbeitskreis vorgelegten EntschlieÙungsentwurf zur Kenntnis,
- 3) erklären sich bereit, die in diesem Vorschlag enthaltenen Grundsätze und aufgezählten Dienstmerkmale unter Berücksichtigung der jeweiligen nationalen Bedingungen weiter zu verfolgen, und
- 4) unterstützen die diesen Fragenbereich betreffende Arbeit des Sachverständigenausschusses des Europarates zu Datenschutzfragen.

Beschluß der Internationalen Konferenz
der Datenschutzbeauftragten vom 30. August 1989
zu I S D N
auf Vorschlag der Arbeitsgruppe Medien

Die nationale und internationale Entwicklung der Telekommunikation ist derzeit gekennzeichnet durch die Einführung diensteintegrierender, digitalisierter Netze. Diese sind die Träger vielfältiger Dienste.

Die Entwicklung führt sowohl für die Netzträger als auch für die Diensteanbieter zur Verarbeitung von erheblich mehr personenbezogenen Daten als dies bei bisherigen Netzen der Fall war. Diese Situation erfordert nationale und internationale Vorkehrungen zum Schutz personenbezogener Daten.

Die Internationale Konferenz der Datenschutzbeauftragten stellt fest, daß hierzu erhebliche Anstrengungen erforderlich sind. Insbesondere darf der Datenschutz nicht als Hindernis für die Entwicklung des Internationalen Informationsmarktes gesehen werden, sondern er stellt vielleicht eine notwendige Ergänzung der technischen Entwicklung dar, die für die Akzeptanz der neuen Telekommunikationstechnologien unerlässlich ist, er stellt vielleicht sogar ein beschleunigendes Element dieser Entwicklung dar.

Sie geht bei offenen Netzen von folgenden Grundsätzen aus:

- Abrechnungsdaten dürfen nur und nur so lange gespeichert werden, wie dies erforderlich ist, um Rechnungen zu erstellen oder auf eventuelle Anfechtungen zu reagieren; ferner zur Erstellung detaillierter Rechnungen, die ausschließlich für diejenigen Teilnehmer bestimmt sind, die sie angefordert haben. Die Ver-

einfachung der Tarifsysteme kommt dem Datenschutz entgegen.

- Für bestimmte Telekommunikationsdienste (Telefon, Kabelfernsehen mit Rückkanal, Datenübermittlungsdienste, Autobahngebühreneinzug usw.) müssen anonyme Zahleinrichtungen geschaffen werden. Ungeachtet der Abrechnungsprobleme macht es die Mehrwertigkeit der Netze erforderlich, diese mit den technischen Möglichkeiten eines anonymen Zugangs auszustatten.
- Daten, die für die Vermittlung erforderlich sind, sind unverzüglich zu löschen; Inhaltsdaten dürfen nur gespeichert werden, wenn sie für die Abwicklung des Dienstes erforderlich sind.
- Vorkehrungen sollten getroffen werden, die jenen Teilnehmern, die wünschen, in Teilnehmerverzeichnisse aufgenommen zu werden, garantieren, daß sie nicht Objekt unerwünschter kommerzieller Werbung werden. Das Recht, daß unentgeltlich in den Teilnehmerverzeichnissen kein Eintrag erscheint, sollte angestrebt werden. Daten, die die Erreichbarkeit von Teilnehmern sicherstellen sollen, dürfen nicht zur Erstellung von Personenprofilen führen, die eine Verhaltenskontrolle erlauben.
- Maßnahmen zur Datensicherung insbesondere gegen den Zugang nicht autorisierter Personen, die Manipulation, das Mithören oder zur Gewährleistung der Authentizität des Senders müssen auf höchstem technischen Niveau und zu akzeptablen Preisen angeboten werden.
- Angemessene Kontrollinstitutionen sind sowohl national als auch international einzurichten.

- In lokalen Netzen und bei Telekommunikationsendgeräten ist bereits bei der Normierung und Genehmigung auf den Datenschutz Rücksicht zu nehmen.

Insbesondere erfordern folgende Dienstmerkmale besondere Aufmerksamkeit:

- Die Anzeige des anrufenden Teilnehmers muß sowohl vom Anrufer als auch vom Angerufenen unterdrückt werden können; Mißbrauch muß durch Maßnahmen im Netz verhindert werden.
- Freisprecheinrichtungen müssen so gestaltet werden, daß nur mit Kenntnis der Gesprächsteilnehmer mitgehört oder aufgezeichnet werden kann.
- Beim Zugang zu Anrufbeantwortern, Voice- und Mailboxsystemen sowie Datenübermittlungsdiensten sind hinreichende Zugangssicherungen einzuführen.

Anlage 4

Zusatzklärung
der Datenschutzbeauftragten der EG-Länder

Die Datenschutzbeauftragten der Länder der Europäischen Gemeinschaft sind der Überzeugung, daß die Existenz und die Aktivitäten der Gemeinschaft einerseits besondere Vorkehrungen des Datenschutzes erforderlich machen, andererseits aber auch verbesserte Möglichkeiten bieten, den Datenschutz über nationale Grenzen hinaus wirksam zu machen.

- Der für Ende 1992 angestrebte EG-Binnenmarkt ist auf den freien Austausch von auch personenbezogenen Informationen gerichtet, etwa in den Bereichen Direktmarketing/Adressenhandel und Kreditinformation.
- Entscheidungen der Europäischen Gemeinschaften verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung und Verarbeitung personenbezogener Daten - so etwa im Bereich der Landwirtschaftsstatistik - und zur grenzüberschreitenden Datenübermittlung - so beispielsweise im Umwelt-, Gesundheits- und Sozialbereich.
- Einige Länder der Europäischen Gemeinschaft arbeiten an einem Pilot-Projekt für gemeinsame polizeiliche Fahndungsdateien (Schengener Informationssystem) - gewissermaßen als Ersatz für die wegfallenden Kontrollen an den Binnengrenzen.
- Die Einrichtungen der EG selbst führen zunehmend personenbezogene Datenbanken. Diese Einrichtungen unterliegen jedoch keinem Datenschutzgesetz und sind daher nicht an die Grundsätze des Datenschutzes gebunden.

Die Europäische Gemeinschaft und ihre Mitgliedsstaaten werden aufgefordert, in ihre Planungen für "Europa'92" die Notwendigkeit eines umfassenden und konsistenten Ansatzes zur Verwirklichung der Grundsätze des Daten-

schutzes in den Mitgliedsländern und in bezug auf die Aktivitäten der Gemeinschaft selbst einzubeziehen.

Im einzelnen schlägt die Konferenz vor:

- Durch entsprechende Rechtsakte der Europäischen Gemeinschaft sollten die Grundsätze der Europaratskonvention 108 für alle Mitgliedsstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden.

- Eine unabhängige Datenschutzkontrollinstanz sollte eingerichtet werden. Sie sollte die Einrichtungen der EG in allen Datenschutzfragen beraten, die Verarbeitung personenbezogener Daten innerhalb der Einrichtungen der EG kontrollieren, Eingaben von Betroffenen entgegennehmen und mit den nationalen Datenschutzorganen zusammenarbeiten.

Die Commission Nationale de l'Informatique et des Libertés (die französische Datenschutzkommission) wird gebeten, diese Vorschläge alsbald dem Vorsitzenden des Ministerrats sowie den Präsidenten des Europaparlaments und der EG-Kommission zu unterbreiten und um Unterstützung zu werben.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 über den

•

Datenschutz in der Europäischen Gemeinschaft

Angesichts der für das Jahr 1993 zu erwartenden Errichtung eines Binnenmarktes in der Europäischen Gemeinschaft zählt der grenzüberschreitende Datenaustausch zu den drängenden, ungelösten Problemen des Datenschutzes.

Eine internationale Datenverarbeitung ist nicht nur eine Grundbedingung für eine gemeinschaftsweite privatwirtschaftliche Tätigkeit. Auch für den öffentlichen Bereich gewinnt die Problematik zunehmend an Bedeutung. Der Abbau der Grenzkontrollen in der Europäischen Gemeinschaft und das vor diesem Hintergrund geschlossene "Schengener Übereinkommen" über die verstärkte informationelle Zusammenarbeit der Polizeibehörden Frankreichs, der Bundesrepublik Deutschland und der Benelux-Staaten sind dafür ein signifikantes Beispiel.

Ebenso werden die technischen Voraussetzungen für internationale Datenübermittlungen immer weiter verbessert. Schon 1993 soll europaweit das digitale, diensteintegrierende Kommunikationsnetz (ISDN) zur Verfügung stehen.

In der Europäischen Gemeinschaft wird die Dynamik der wirtschaftlichen Integration die Entwicklung zu einem "informationellen Großraum" nachhaltig fördern. Dies hat zur Folge, daß die Informationsverarbeitung insbesondere in den Bereichen Umweltschutz, Forschung,

Arbeitsmarkt, soziale Sicherung, Statistik und öffentliche Sicherheit erheblich zunehmen wird.

Die Beratungen der Internationalen Konferenz der Datenschutzbeauftragten im August 1989 in Berlin haben erneut gezeigt, daß die auf supranationaler Ebene vorhandenen Regelungen, wie etwa die Europaratskonvention von 1981, zwar wichtige Prinzipien für einen fairen Datenumgang enthalten, aber keineswegs ausreichen, den etwa in der Bundesrepublik Deutschland oder Frankreich durch das nationale Datenschutzrecht erreichten Stand der Sicherung des informationellen Selbstbestimmungsrechts des Bürgers zu gewährleisten, abgesehen davon, daß eine Reihe von Mitgliedsstaaten der Gemeinschaft die Konvention noch nicht ratifiziert hat.

Besonders bedenklich ist die Untätigkeit der EG im Bereich des Datenschutzes. Rechtsakte der EG verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung, Verarbeitung und Übermittlung personenbezogener Daten, etwa im Bereich der Statistik. Die Telekommunikationspolitik der EG ist auf einen forcierten Ausbau europaweit standardisierter und operierender Telekommunikationsdienste und -netze gerichtet. Zwischen den verschiedenen nationalen Datenschutzrechten der Mitgliedsstaaten bestehen im Hinblick auf Verarbeitungsvoraussetzungen, Rechte der betroffenen Personen und Kontrollmöglichkeiten große Unterschiede.

Die Konferenz bekräftigt daher die auf der Internationalen Konferenz in Berlin einmütig erhobenen Forderungen,

- daß bei der Entwicklung und Nutzung grenzüberschreitender Datennetze und Datendienste dem Datenschutz der gleiche Stellenwert zukommen muß, wie der Förderung der technischen Infrastruktur,

- daß die EG ein Gesamtkonzept für die Sicherung des Datenschutzes sowohl in den Mitgliedsländern als auch bei ihren eigenen Aktivitäten entwickeln muß, das insbesondere die Gleichwertigkeit des Schutzniveaus in der gesamten Gemeinschaft herstellt, und
- daß auf der EG-Ebene eine unabhängige Datenschutzzinstanz einzurichten ist, die die Institution der Gemeinschaft in allen Datenschutzfragen berät, die Verarbeitung personenbezogener Daten durch die EG-Gremien überwacht, Eingaben von Bürgern entgegennimmt und mit den nationalen Datenschutzorganen zusammenarbeitet.

Die Konferenz der Datenschutzbeauftragten erklärt ihre ausdrückliche Bereitschaft, ihre Kenntnisse und Erfahrungen bei der Realisierung dieser Maßnahmen einzubringen. Ansprechpartner sind dabei zum einen die Organe der Gemeinschaft, insbesondere das Europäische Parlament, zum anderen die an der Willensbildung der EG beteiligten deutschen Behörden des Bundes und der Länder.

Anlage 6

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 zum

Entwurf einer EG-Statistikverordnung

Die Kommission der Europäischen Gemeinschaften hat den Entwurf einer Verordnung des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften vorgelegt.

Diese Verordnung darf nicht hinter dem datenschutzrechtlichen Standard der amtlichen Statistik in der Bundesrepublik Deutschland zurückbleiben.

Die nationalen Statistikämter sollen nach dem Vorschlag der EG-Kommission die Befugnis erhalten, vertrauliche statistische Daten dem Statistischen Amt der Europäischen Gemeinschaften auch dann zu übermitteln, wenn sie einen Personenbezug aufweisen. Es ist nicht auszuschließen, daß auf nationaler Ebene kurzfristig für bestimmte statistische Zwecke vorgefallene personenbezogene Datenbestände (z.B. noch nicht anonymisierte Daten aus dem Mikrozensus) durch das Statistische Amt der EG abgerufen werden. Deshalb muß in der EG-Verordnung festgelegt werden, daß die Übermittlung personenbezogener Einzelangaben nur ausnahmsweise durch einen weiteren Rechtsakt der EG für bestimmte statistische Zwecke (z.B. für die Produktions-, Industrie- und Außenhandelsstatistik) zugelassen werden darf und daß eine möglichst frühzeitige Anonymisierung stattfindet sowie notwendige organisatorisch-technische Maßnahmen der Datensicherung getroffen werden.

Die unabhängige Datenschutzkontrolle auf Gemeinschaftsebene ist bisher nicht gewährleistet. Der geplante Beratende Ausschuß kann diese Kontrolle nicht ersetzen.

Im Gemeinschaftsrecht sind bisher für die Verletzung des Statistikgeheimnisses keine ausreichenden Sanktionen vorgesehen. Nicht einmal alle Mitgliedsstaaten stellen einen derartigen Verstoß unter Strafe.

Die Teilnehmer der 11. Internationalen Konferenz der Datenschutzbeauftragten in Berlin haben am 30. August 1989 diesen Fragenkreis diskutiert und sind übereingekommen, sich auf nationaler und internationaler Ebene für eine stärkere Berücksichtigung datenschutzrechtlicher Belange im Verordnungsentwurf einzusetzen.

Die Konferenz der Datenschutzbeauftragten appelliert daher an die Bundesregierung und den Ministerrat, vor einer Verabschiedung des Verordnungsentwurfs die aufgezeigten Mängel zu beseitigen, damit den Persönlichkeitsrechten der Gemeinschaftsbürger auch bei der ständig zunehmenden Zahl europäischer Statistiken und bei der für 1990 in den meisten anderen EG-Mitgliedsstaaten vorgesehenen Volkszählung Rechnung getragen wird.

Anlage 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 zum

Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen

1. Am 14. Juni 1985 unterzeichneten die Regierungen Frankreichs, der Bundesrepublik Deutschland und der Beneluxstaaten in Schengen/Luxemburg ein Abkommen über den schrittweisen Abbau der Grenzen zwischen ihren Ländern. Dabei knüpften sie den Wegfall der Grenzkontrollen an eine Reihe von Maßnahmen, die die befürchteten Sicherheitsdefizite ausgleichen sollen. Die Maßnahmen sollen in einem Zusatzübereinkommen festgehalten werden. Hierzu gehört die Errichtung eines gemeinsamen automatisierten Informationssystems für den Bereich der Fahndung (Schengener Informationssystem - SIS). Dieses System dient vor allem der Ausschreibung zur Festnahme und zur Zurückweisung an der Grenze, der verdeckten Registrierung und der Ermittlung des Aufenthalts von Zeugen im Strafverfahren. Überdies sollen der Informationsaustausch zum Zwecke der Bekämpfung bestimmter Formen der Kriminalität verstärkt, die ausländer- und asylrechtlichen Entscheidungen vereinheitlicht und ein gemeinsames Verfahren für intensivierete Kontrollen an den Außengrenzen festgelegt werden.
2. Die Vertragsstaaten verpflichten sich in dem Entwurf zum Zusatzübereinkommen, Datenschutzvorschriften für das Schengener Informationssystem entsprechend den Grundsätzen der Datenschutzkonvention des Europarates und der Empfehlung des Ministerkomitees des Europarats an die Mitgliedsstaaten über die Nutzung personenbezogener Daten

im Polizeibereich als Mindeststandard zu erlassen. Die Konferenz begrüßt dies und stellt zugleich fest, daß nach dem gegenwärtigen Stand der Verhandlungen auch die in der Erklärung der Datenschutzorgane Frankreichs, Luxemburgs und der Bundesrepublik Deutschland vom 16.03.1989 enthaltenen Forderungen in wesentlichen Bereichen erfüllt werden sollen. Der Vertragsentwurf sieht für das Schengener Informationssystem vor: Auskunfts-, Berichtigungs- und Klagerechte für die Betroffenen; Kontrollorgane auf nationaler und internationaler Ebene; eine Zweckbindung der Daten. Diese Elemente müssen Bestandteile des Zusatzübereinkommens bleiben, bedürfen aber noch der Verbesserung und Ergänzung, damit sich durch den grenzüberschreitenden Datenaustausch keine gravierenden Verschlechterungen für den Datenschutz ergeben.

2.1 Die Datenschutzbeauftragten fordern für das SIS insbesondere

die

- Festlegung der Voraussetzungen, nach denen unter Berücksichtigung der Verhältnismäßigkeit (zum Beispiel nach der Schwere der Straftaten) Informationen aus dem nationalen in den internationalen Fahndungsbestand übernommen werden sollen,
- Festlegung, unter welchen Voraussetzungen und in welchem Umfang die verschiedenen Inlandsbehörden auf die Daten zugreifen dürfen,
- konkrete Beschreibung der Voraussetzungen, unter denen verdeckte Registrierungen erlaubt werden sollen (Straftatenkatalog),
- präzisere Beschreibung der Kriterien, nach denen Zweckdurchbrechungen zur Verhütung einer Straftat mit erheblicher Bedeutung sowie aus schwer-

wiegenden Gründen der Staatssicherheit erlaubt werden sollen, und

- Aufnahme einer Verpflichtung, Zweckänderungen zu Kontrollzwecken zu dokumentieren.

2.2 Die Regelungen über den Datenschutz - insbesondere die Rechte der Betroffenen und die Datenschutzkontrolle - müssen auf die im Zusatzübereinkommen vorgesehene konventionelle Verarbeitung personenbezogener Daten ausgedehnt werden. Dies gilt vor allem für den Informationsaustausch in den Bereichen des Ausländerrechts und des Asylverfahrens.

3. Der Entwurf des Zusatzübereinkommens enthält eine pauschale Verpflichtung der Vertragsparteien, daß ihre nationalen Sicherheitsdienste sich untereinander unter Berücksichtigung des nationalen Rechts und nach Maßgabe ihrer jeweiligen Zuständigkeit bei der Abwehr von Nachteilen für die Staatssicherheit Hilfe leisten.

Die Datenschutzbeauftragten weisen vorsorglich darauf hin, daß eine solche Bestimmung nach deutschem Verfassungsrecht keine tragfähige Grundlage für einen umfassenden Datenaustausch der Geheimdienste darstellt.

4. Der Vertragsentwurf verpflichtet jeden Vertragsstaat, Ausländer aus dritten Staaten an der Grenze zurückzuweisen, wenn ein anderer Vertragsstaat ihn "zur Einreiseverweigerung" ausgeschrieben hat. Es ist nicht vorgesehen, daß der vollziehende Staat die Gründe der Ausschreibung zur Kenntnis nimmt und rechtlich überprüft. Die Datenschutzbeauftragten fordern die verbindliche Festlegung der sachlichen Voraussetzungen solcher Ausschreibungen und die Ermöglichung einer Überprüfung.

5. Die Datenschutzbeauftragten machen darauf aufmerksam, daß das Zusatzübereinkommen den deutschen Gesetzgeber nicht von der dringenden Notwendigkeit enthebt, vor Inkrafttreten des Zusatzübereinkommens für die polizeiliche Datenverarbeitung verfassungskonforme Rechtsgrundlagen zu schaffen.
6. Bevor die einzelnen Vertragsstaaten ihre im Entwurf des Zusatzübereinkommens vorgesehene Verpflichtung, spezielle nationale Regelungen für das Erheben und Nutzen von Daten zu erlassen, nicht erfüllt haben, dürfen Daten an diese Staaten auf der Grundlage des Zusatzübereinkommens nicht übermittelt werden.

Landtag des Saarlandes

9. Wahlperiode

Drucksache 9/1038-9/1521

09.11.1989

Bericht

des Ausschusses für Innere Verwaltung

Über die Beratung des gemäß § 20 Absatz 3 Satz 2 des Datenschutzgesetzes vorgelegten achten und neunten Berichts über die Tätigkeit des Landesbeauftragten für Datenschutz.

Der Landtag wolle beschließen:

Der Landtag nimmt nachstehenden Bericht zur Kenntnis.

1. Der Ausschuß hat die beiden Tätigkeitsberichte des Landesbeauftragten für Datenschutz aus den Jahren 1986 und 1987 beraten. Dabei ergab sich die Chance, nicht nur eine "Momentaufnahme" der Datenschutzproblematik in bestimmten Bereichen der öffentlichen Verwaltung zu erhalten, sondern auch Entwicklungen und Trends in der Gestaltung eines gewaltmäßigenden Individualrechtsschutzes feststellen zu können.
2. Im Berichtszeitraum wurde das Kriminalpolizeiamt überprüft. Der Ausschuß begrüßt die Ankündigung des Ministers des Innern, ein neues Datenschutzkonzept im Bereich der Kriminalpolizei einzuführen. Der Ausschuß erwartet, daß der Beginn der praktischen Umsetzung des neuen Konzeptes alsbald die Datenschutzsituation im Polizeibereich verbessern wird.
 - 2.1 Die Richtigkeit und Vollständigkeit der im zentralen INPOL-System der Kriminalpolizei erfaßten Daten über Verdächtige und Beschuldigte ist bisher

nicht ausreichend gewährleistet. Unrichtige Daten belasten jedoch nicht nur den Betroffenen, sondern beeinträchtigen auch die Effizienz der Polizeiarbeit. Die interne Kontrolle des kriminalpolizeilichen Meldedienstes muß verbessert werden.

- 2.2 Das Kriminalpolizeiamt hat etwa die Hälfte des Bestandes an Altakten - nämlich 62.000 Fälle - in einem "standardisierten Verfahren" gesichtet; 29.000 Fälle wurden ausgesondert, der Rest in das automatisierte INPOL-System übernommen.

Es ist erfreulich, daß eine große Zahl von Akten vernichtet wurde, die für die vorbeugende Verbrechensbekämpfung nicht mehr erforderlich waren.

Es müssen auch weiterhin alle technischen, organisatorischen und personellen Möglichkeiten genutzt werden, die automatisiert vorgehaltenen Daten im Polizeibereich zu bereinigen.

- 2.3 Der Unterausschuß begrüßt die Absicht des Kriminalpolizeiamtes, die konventionellen Spezialdateien abzubauen. Er ist der Auffassung, daß die Voraussetzungen für die Erfassung Erwachsener im automatisierten Kriminalaktennachweis nicht ohne weiteres auf Kinder angewendet werden dürfen. Deshalb wird begrüßt, daß vor der Speicherung von Daten über Kinder ein in der Jugendkriminalität besonders erfahrener Dienst eingeschaltet werden soll.

3. Ein Schwerpunkt datenschutzrechtlicher Probleme bildet in den Berichtsjahren der Verkehrsbereich.

- 3.1 Bei der Landeshauptstadt wurden die Anliegerparkausweise durch die Meldebehörde ausgestellt. Die Stadt verlangt u.a. Angaben über die Anzahl der in einem Haushalt lebenden Erwachsenen.

Die Angaben der Antragsteller werden zugleich für die Korrektur des Melderegisters genutzt. Diese Verwendung personenbezogener Daten steht nicht in Einklang mit dem ursprünglichen Zweck der Datenerhebung.

- 3.2 Die Praxis der Führerscheinstellen wurde erörtert, vor der Erstellung eines Führerscheines regelmäßig ein "Leumundszeugnis" von den Polizeidienststellen am Wohnort des Antragstellers einzuholen. Der Ausschuß hat Zweifel, ob die routinemäßige Stellungnahme des Polizeireviers geeignet ist, der Führerscheinstelle in allen Fällen verwertbare Informationen über den Führerscheininhaber zu verschaffen.

Deshalb ist zu prüfen, ob und inwieweit die Einhaltung solcher Stellungnahmen der örtlichen Polizeidienststellen angesichts der sonstigen Möglichkeiten zulässiger Informationsbeschaffung weiterhin stattfinden soll.

- 3.3 Der Ausschuß mißbilligt die immer wieder vereinzelt festzustellende Praxis der Führerscheinstellen, Angaben über Verkehrsverstöße, die als Ordnungswidrigkeiten oder Straftaten geahndet wurden, in den Führerscheinkarteien zu vermerken. An die Einhaltung des dahingehenden Erlasses des Ministers für Wirtschaft wird erinnert.

- 3.4 Durch die Automatisierung des Verkehrsordnungswidrigkeitenverfahrens - SAAROWI - ist die Vollzugs- und Verwaltungspolizei entlastet und der Verwaltungsablauf wirtschaftlicher gestaltet worden.

Der Ausschuß begrüßt, daß inzwischen wieder die Möglichkeit geschaffen wurde, daß der Verwarnte sein Bußgeld sofort dem Polizeibeamten bezahlen

kann, ohne daß sein Name im Computer festgehalten wird.

Der Minister des Innern wird gebeten, zu prüfen, ob für die Verwarngelder derjenigen, die vor Ort nicht angetroffen werden, die sog. "Zahlkartenverwarnung" eingeführt werden kann.

4. Aus dem Justizbereich wurden einzelne Verstöße erörtert. Der Ausschuß sah jedoch keinen Anlaß für grundsätzliche Bedenken, daß die Geheimhaltung durch Gerichte, Staatsanwaltschaft und Anwälte generell nicht gewährleistet sei.

- 4.1 Neben den genannten Einzelfällen wurde - wie schon anläßlich der Beratung des 6. Tätigkeitsberichtes (vgl. Bericht des Ausschusses für Innere Verwaltung vom 27.04.1987, Lt-Drucksache 9/1110-914) - die Mitteilungspraxis der Gerichte in Zivil- und Strafsachen gegenüber anderen Stellen unter Berücksichtigung konkreter Fälle diskutiert.

Der Ausschuß erinnert an seine früher dargelegte Auffassung, wonach bis zum Vorliegen der notwendigen bundesgesetzlichen Regelung alle geeigneten Maßnahmen getroffen werden müssen, die die notwendige Abwägung zwischen den schutzwürdigen Belangen der Betroffenen und die im allgemeinen Interesse liegende Unterrichtung anderer Stellen im Einzelfall sicherstellen.

- 4.2 Die Auffassung des Ministers der Justiz wird mit Befriedigung zur Kenntnis genommen, daß das Strafvollzugsgesetz durch den Bund novelliert werden muß. Für die Übergangszeit wird der Minister der Justiz gebeten, den Umfang der Datenerhebung insbesondere für Kurzzeitgefangene auf das wirklich notwendige Maß zu beschränken.

5. Im Sozialbereich können zwar einige Fortschritte festgestellt werden; die Gefahren für die Persönlichkeitsrechte sind infolge der Automation jedoch eher gewachsen.
- 5.1 Die Aufbewahrung von Amtshilfeersuchen für Sicherheitsbehörden durch die Sozialhilfeträger hat zu unverhältnismäßigen Belastungen für die Betroffenen geführt. Die Amtshilfeersuchen der Sicherheitsbehörden sollten getrennt von den jeweiligen Fallakten aufbewahrt werden, um einer zu weiten Streuung derartiger Informationen innerhalb des Sozialleistungsbereiches vorzubeugen.
- 5.2 Ein Jugendamt hat rechtsirrig die Auffassung vertreten, daß bei der Amtsvormundschaft und Amtspflegschaft für nichteheliche Kinder das Sozialgeheimnis nicht zu beachten sei. Der Ausschuß unterstützt den Standpunkt des Landesbeauftragten und des zuständigen Ressorts, daß die Daten dieser Kinder, die der Beratung und der Hilfe durch das Jugendamt besonders bedürfen, ebenso wie die Daten von Sozialleistungsempfängern geschützt sein müssen.
- 5.3 Zwar war es dem Landesbeauftragten für Datenschutz stets möglich, in den beispielhaft geschilderten Fällen eine Übereinstimmung in der Rechtsauffassung mit dem zuständigen Ministerium herzustellen. Dieses sollte jedoch durch mehr Aufklärung und Unterrichtung die Umsetzung des Datenschutzes im nachgeordneten Bereich fördern.
- 5.4 Der Ausschuß hat sich mit den datenschutzrechtlichen Aspekten der Rentenversicherungsnummer befaßt. Die im Sozialleistungsbereich zu verzeichnende Massendatenverarbeitung hat einen verstärkten Einsatz der Automation zur Folge. Wesentliches Instrument automatisierter Verfahren ist die als

Ordnungsnummer verwendbare Rentenversicherungsnummer, die deshalb in allen Sozialversicherungsbereichen benutzt wird. Zahlreiche andere Behörden und vor allem auch Arbeitgeber erhalten Kenntnis von dieser Nummer. Durch die beabsichtigte Einführung eines Sozialversicherungsausweises, der ebenfalls mit einer Versicherungsnummer der Rentenversicherung versehen werden soll, wird nicht nur der größte Teil der ständig Beschäftigten in der Bundesrepublik erfaßt, sondern auch andere nicht versicherungspflichtige Personen, z.B. Schüler, Werkstudenten, Hausfrauen mit Nebenbeschäftigung. Dies rückt die Rentenversicherungsnummer noch weiter als bisher in die Nähe eines unzulässigen Personenkennzeichens. Die Rentenversicherungsnummer schafft zwar nicht den gläsernen Menschen. Der Staat sollte jedoch nicht nur auf die Möglichkeiten der Informations- und Kommunikationstechnik setzen und sein ohnehin schon großes Instrumentarium an Kontrollmöglichkeiten nur, wenn es unerläßlich ist, erweitern.

5.5 Seit Jahren umstritten ist die Frage, ob und inwieweit die Krankenhausärzte Entlassungsberichte über ihre Patienten an die Krankenkassen übersenden müssen. Als ein positives Ergebnis der Gesundheitsreform ist jedoch zu vermerken, daß der Umfang der Mitteilungspflicht der Krankenhäuser nunmehr einschränkend geregelt ist (§ 301 SGB V). Somit sind routinemäßige Anforderungen umfassender Entlassungsberichte in Zukunft nicht mehr zulässig.

6. Bewerber um Arbeitsplätze im öffentlichen Dienst haben Beschwerde gegen die Durchführung von Tests geführt. Der Ausschuß weist darauf hin, daß Einstellungstests sich auf die Feststellung der Eignung für den angestrebten Arbeitsplatz beschränken müssen.

7. Der Datenschutz droht in Einzelfällen - wie die EG-Verordnung zur Einführung der Weinbaukartei zeigt - durch die Rechtsetzung der Europäischen Gemeinschaft unterlaufen zu werden. Belange des Datenschutzes müssen jedoch auch auf Europaebene entschiedener vertreten werden. Der Ausschuß unterstreicht deshalb die Notwendigkeit, den Datenschutz in den Gremien der Europäischen Gemeinschaft institutionell stärker zu verankern. Da die Bundesländer die Hauptlast des Vollzugs auch der Europanormen tragen, ist ihre rechtzeitige Beteiligung vor den Beratungen auf der Ebene der Europäischen Gemeinschaft unerläßlich.

8. Die Rechtsverordnung zur Regelung der Datenverarbeitung im Schulbereich stellt zwar einen wesentlichen Fortschritt für den Datenschutz dar. Bisher sind die Schulen jedoch der seit 1979 bestehenden Pflicht, ihre Dateien zum Datenschutzregister anzumelden, nicht nachgekommen. Um das Meldeverfahren rationell durchführen zu können, ist eine wesentliche Voraussetzung die Vereinheitlichung der Dateien im Schulbereich, die als wesentliches Ziel der Rechtsverordnung angesehen wurde.

Der Minister für Kultus, Bildung und Wissenschaft wird deshalb gebeten, die Meldung der Dateien im Hinblick auf den Zeitablauf seit Bestehen dieser gesetzlichen Meldepflicht nunmehr zu vollziehen und die hierfür erforderlichen rechtlichen und tatsächlichen Voraussetzungen sicherzustellen.

Anlage 9

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat bei Stimmenthaltung von Bayern in ihrer Sitzung vom 5./6. April 1989 zur

Neuregelung des Bundesdatenschutzgesetzes

folgende EntschlieÙung gefaÙt:

1. Die Datenschutzbeauftragten begrüßen die Beschlüsse des Bundesrates zur Neufassung des Bundesdatenschutzgesetzes. Sie sehen darin eine Bestätigung ihrer bisher dazu vertretenen Meinung und erinnern an ihre Beschlüsse vom 14. März 1986 und vom 6. Juni 1988.
2. Die Datenschutzbeauftragten betonen nochmals die Notwendigkeit,
 - die Datenerhebung im Bundesdatenschutzgesetz zu regeln;
 - die Verarbeitung personenbezogener Daten in Akten in das Bundesdatenschutzgesetz einzubeziehen;
 - die lückenlose Kontrolle durch die Datenschutzbeauftragten zu gewährleisten;
 - im öffentlichen und nicht-öffentlichen Bereich, ungeachtet aller erforderlichen Differenzierung, einen gleichwertigen Datenschutz sicherzustellen.
3. Die Datenschutzbeauftragten weisen schließlich mit Nachdruck darauf hin, daß eine Verabschiedung des Regierungsentwurfs ohne die gebotene Nachbesserung, aber auch eine weitere Verzögerung des Gesetzge-

bungsvorhabens die Gefahr einer Rechtszersplitterung verstärken würde, die sich schon jetzt deutlich abzeichnet.

Anlage 10

EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Lander und der Datenschutzkommission Rheinland-Pfalz vom 30.05.1989 zu den Entwurfen eines Bundesverfassungsschutzgesetzes (BVerfSchG), eines MAD-Gesetzes (MADG) und eines BND-Gesetzes (BNDG)

I.

Mit den von der Bundesregierung vorgelegten Entwurfen sollen die nach der Rechtsprechung des Bundesverfassungsgerichts erforderlichen bereichsspezifischen Rechtsgrundlagen fur die Informationsverarbeitung der Verfassungsschutzbehörden und Nachrichtendienste geschaffen werden. So dringend die Beseitigung der bestehenden Regelungsdefizite auch ist, mussen sich neue Gesetze gerade in diesem Bereich in besonderem MaÙe daran messen lassen, daÙ in die Freiheitsrechte der Burger nicht unverhaltnismaÙig eingegriffen wird. Dieser Vorgabe werden auch die nunmehr vorgelegten Entwurfe in vielerlei Hinsicht nicht gerecht.

II.

1. Da sich der zulassige Umfang der Informationsverarbeitung nach den Aufgaben der datenverarbeitenden Stelle bemisst, bedarf es einer abschlieÙenden, moglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Fur den Einzelnen muÙ erkennbar sein, wann er die Schwelle von der Ausubung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Die in § 3 Abs. 1 verwendeten Begriffe, wie etwa "Bestrebungen gegen die freiheitliche demokratische Grundordnung" oder "Gefahrdung aus-

wärtiger Belange" stellen dies nicht sicher. Insbesondere bleibt unklar,

- ob der Begriff der Bestrebungen das Handeln einer Mehrzahl von Personen in einem gewissen Grad von Organisiertheit voraussetzt oder auch das Tätigwerden einer einzelnen Person beinhaltet;
- ob es zulässig sein soll, Informationen auch über solche Bestrebungen zu sammeln und zu speichern, die erkennbar nicht gegen die freiheitliche demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen gegen diese Grundordnung gerichteten Bestrebungen mitwirken;
- ob und ggf. in welchem Umfang Informationen über nicht extremistische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung (-versuche) sind.

Zur weiteren Umschreibung der Aufgaben könnte auch der Inhalt von § 92 StGB mit herangezogen werden.

2. Bei einer derartig vagen Umschreibung der Aufgaben wäre es um so notwendiger, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten je nach dem, welche seiner ganz unterschiedlichen Aufgaben (Spionageabwehr, Extremismus- und Terrorismusbeobachtung, Sicherheitsüberprüfung) der Verfassungsschutz wahrnimmt, differenziert, präzise und für den Bürger transparent zu regeln. Stattdessen sieht der Entwurf pauschale Befugnisse für den Verfassungsschutz vor. Außerdem fehlen Regelungen darüber, ob und ggf. in welchem Umfang, für welche Zwecke und mit welchen Speicherungsfristen Daten über unverdäch-

tige und unbeteiligte Personen erhoben und gespeichert werden dürfen.

3. Unklar ist, welche rechtlichen Grenzen dem Einsatz nachrichtendienstlicher Mittel gesetzt sind. Außerdem muß klargestellt werden, daß die Befugnis zum Einsatz nachrichtendienstlicher Mittel kein genereller Rechtfertigungsgrund für Verstöße gegen Straftatbestände ist, gegen wen sich der Einsatz nachrichtendienstlicher Mittel richten darf und was mit den ggf. dabei über Unverdächtige gewonnenen Daten geschehen darf. Auch im Übrigen sollten beim Einsatz nachrichtendienstlicher Mittel, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, entsprechende Schutzrechte wie im Gesetz zu Art. 10 Grundgesetz vorgesehen werden (z.B. Verwertungsverbot, Unterrichtungen).
4. Der Entwurf regelt im wesentlichen lediglich die Speicherung personenbezogener Daten in Dateien, obwohl die Informationstechnik es schon heute ermöglicht, auch komplexe Datensammlungen - bestehend aus Akten, Dateien und anderen Unterlagen - gezielt mit Hilfe automatischer Verfahren zu erschließen.
5. Bei der Regelung insbesondere für die gemeinsamen Verbunddateien der Verfassungsschutzbehörden sollte auch klargestellt werden, daß in Textdateien nur Daten über solche Personen gespeichert werden dürfen, die selbst in Verdacht stehen, eine der im Gesetzentwurf aufgezählten Straftaten zu planen, zu begehen oder begangen zu haben. Darüber hinaus ist sicherzustellen, daß in der Datei die für die Bewertung und Überprüfung von Textzusätzen maßgeblichen Unterlagen angegeben werden.

6. Die Frage, ob Einsicht in amtliche Register zulässig sein soll, kann nur bereichsspezifisch geregelt werden. Die Zulässigkeit der Einsichtnahme in Register rechtfertigt nicht die Einrichtung von on-line-Anschlüssen.
7. Das Zweckbindungsgebot ist sowohl für Übermittlungen an den Verfassungsschutz als auch für solche durch den Verfassungsschutz nicht ausreichend berücksichtigt. Die nunmehr vorgesehenen Übermittlungseinschränkungen reichen vor allem deshalb nicht aus, weil die übermittelnde Stelle nicht ausdrücklich verpflichtet wird zu prüfen, ob schutzwürdige Belange entgegenstehen. Auch innerhalb des Bundesamtes für Verfassungsschutz darf nicht jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden.
8. Aus dem Trennungsgebot für Polizei- und Nachrichtendienste folgt insbesondere, daß die Übermittlung von Daten, die die Polizei unter Einsatz dem Verfassungsschutz vorenthaltener Befugnisse, z.B. bei Hausdurchsuchungen, gewonnen hat, nur nach Maßgabe einschränkender Verwertungsregelungen erfolgen darf. Die Ansatzpunkte, die im Entwurf der letzten Legislaturperiode enthalten waren, sollten wieder aufgegriffen werden.

Die Informationshilfe der Grenzpolizeien für den Verfassungsschutz muß einschränkend geregelt werden.

9. Es fehlen auch befriedigende Lösungsregelungen. Abgesehen davon, daß die Löschung von Daten in Akten nicht einmal erwähnt wird, sollten schon im Gesetz Regelfristen für die Überprüfung und Löschung der verarbeiteten Daten festgelegt werden. Dabei sollte zwischen den einzelnen Aufgabenberei-

chen des Bundesamtes für Verfassungsschutz unterschieden werden.

10. Die Einschränkungen des Auskunftsrechts der Bürger sind bereichsspezifisch im Bundesverfassungsschutzgesetz zu regeln. Ein Auskunftsanspruch besteht in der Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht. Im übrigen bedarf es einer Abwägung im Einzelfall. Die Ablehnung ist gegenüber dem Betroffenen soweit zu begründen, daß er sachgerecht darüber entscheiden kann, ob und welche Rechtsmittel er einlegen will. Außerdem ist der Betroffene auf sein Recht hinzuweisen, sich an den Datenschutzbeauftragten zu wenden.
11. Die Datenschutzbeauftragten begrüßen es, daß die Beteiligung des Verfassungsschutzes an Sicherheitsüberprüfungen und Überprüfungen im Rahmen des vorbeugenden personellen Sabotageschutzes in einem eigenen Geheimschutzgesetz geregelt werden sollen. Sofern über die Sicherheitsüberprüfung hinaus eine Mitwirkung an anderen Verfahren für unabdingbar gehalten wird, sind diese gesetzlich zu regeln.
12. Soweit die Entwürfe für ein MAD-Gesetz und ein BND-Gesetz auf das Bundesverfassungsschutzgesetz verweisen, gilt die hierzu geäußerte Kritik. Die in den Entwürfen vorgesehene Verweisungstechnik erhöht für den Bürger die Schwierigkeit, aus den Gesetzen klar zu erkennen, welche personenbezogenen Daten die Dienste bei welcher Gelegenheit über ihn verarbeiten dürfen. Darüber hinaus bestehen Zweifel, ob die für das Bundesamt für Verfassungsschutz vorgesehenen Befugnisse pauschal auch für den Militärischen Abschirmdienst notwendig sind, der als Teil der Streitkräfte ein gegenüber dem Bundesamt für Verfassungsschutz deutlich unterschiedliches Operationsgebiet hat.

EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Lander und der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zum Entwurf eines Gesetzes zur nderung und Erganzung des Strafverfahrensrechts (Strafverfahrensnderungsgesetz vom 03.11.1988)

Die Konferenz begrußt, daÙ ein Entwurf zur Regelung des Datenschutzes im Strafverfahrensrecht vorgelegt worden ist und daÙ darin fur die besonderen Ermittlungs- und Fahndungsmethoden eigenstandige Befugnisnormen vorgesehen sind sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht in die StrafprozeÙordnung aufgenommen werden sollen.

Die im Entwurf vorgesehenen Datenschutzregelungen sind an den verfassungsrechtlichen Grundsatzen der VerhaltnismaÙigkeit und Normenklarheit zu messen. Weil im Bereich der Grundrechtsausubung nach der Rechtsprechung des Bundesverfassungsgerichts alle wesentlichen Entscheidungen vom Gesetzgeber selbst zu treffen sind, ist die gesamte Informationsverarbeitung wegen ihres Eingriffscharakters in der StrafprozeÙordnung prazise und umfassend gesetzlich zu regeln.

Der vorliegende Entwurf entspricht den sich aus dem Recht auf informationelle Selbstbestimmung ergebenden Anforderungen noch nicht; er ist im ubrigen unvollstandig. Die Datenschutzkonferenz hebt deshalb unter gleichzeitiger Bezugnahme auf ihren BeschluÙ vom November 1986 folgende Kritikpunkte hervor:

1. Zu den Regelungen über die Ermittlungs- und Fahndungsmethoden

- Die Erhebung und Weiterverarbeitung personenbezogener Daten durch Strafverfolgungsorgane greift empfindlich in das Persönlichkeitsrecht der Bürger ein. Umso wichtiger ist es, nach dem Grad der Betroffenheit im Gesetz Abstufungen vorzunehmen. Zwischen dem Beschuldigten, dem Verdächtigen, dem von Vorfeldermittlungen Betroffenen und dem erkennbar nicht Verdächtigen (z.B. Geschädigten, Zeugen) sollte daher unterschieden werden. Vor allem die Regelungen über "Kontakt- und Begleitpersonen", "andere Personen" und "Dritte" werden dem nicht gerecht.

- Es muß klargestellt werden, daß die Ermittlungsgeneralklausel keine Eingriffe gestattet, die in ihrer Eingriffstiefe den besonders geregelten gleichkommen. So wären z.B. die Voraussetzungen des Einsatzes von V-Leuten besonders zu regeln. Auch weiterentwickelte "besondere Fahndungs- und Ermittlungsmethoden" dürfen nicht auf die Ermittlungsgeneralklausel gestützt werden. In die Strafprozeßordnung sind Verfahrensregelungen aufzunehmen, die eine Information etwa der zuständigen Parlamentsausschüsse über die beabsichtigte Anwendung vorsehen. Vor dem Einsatz qualitativ neuer Methoden müssen auf jeden Fall gesetzliche Regelungen geschaffen werden.

- Der Entwurf betont zu recht, daß bei jeder einzelnen Ermittlungs- und Datenverarbeitungsmaßnahme der Grundsatz der Verhältnismäßigkeit zu beachten ist. Dies muß bereits in einzelnen Befugnisnormen zum Ausdruck kommen. Die bislang vorgesehenen Straftatenkataloge sind mit dem Ziel einer Einschränkung zu überprüfen; die bloße Anknüpfung an den Begriff der "Straftat mit er-

heblicher Bedeutung" ohne weitere Differenzierung reicht nicht aus.

- Die Anordnung von Ermittlungs- und Fahndungsmethoden, die besonders stark in das Recht auf informationelle Selbstbestimmung eingreifen, ist dem Richter vorzubehalten. Gleiches gilt, wenn mit solchen besonderen Methoden erhobene Daten für andere Strafverfahren oder für andere - polizeiliche - Zwecke verwendet werden sollen.
- Wegen der Tiefe der Eingriffe bei besonderen Ermittlungs- und Fahndungsmethoden darf der Richtervorbehalt - von besonderen Eilfällen abgesehen - nicht durch Entscheidungen der Staatsanwaltschaft oder der Polizei ersetzt werden. Soweit ausnahmsweise die Staatsanwaltschaft oder die Polizei eine Anordnung treffen muß, dürfen erlangte Daten nicht weiter verwendet werden, wenn die richterliche Bestätigung ausbleibt; erhobene Daten sind zu löschen.
- Die Verwendung von durch besondere Ermittlungs- oder Fahndungsmethoden erlangten Daten für polizeiliche Zwecke muß neben dem Richtervorbehalt voraussetzen, daß das Polizeirecht vergleichbare Eingriffe gestattet oder daß die Daten zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben erforderlich sind.

2. Zu den besonderen Regelungen über die Datenverarbeitung

Regelungen über die Datenverarbeitung im Strafverfahren setzen eine Gesamtkonzeption über die Informationsverarbeitung bei den Strafverfolgungsbehörden voraus. Notwendig sind insbesondere klare Bestimmungen über die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei. Der vorliegende Entwurf

läßt den hierzu notwendigen Konsens jedoch nicht erkennen.

- Der Gesetzgeber sollte möglichst genau regeln, welche Arten von Daten für "Zwecke des Strafverfahrens", für Zwecke anderer Strafverfahren oder für die Aufklärung künftiger Straftaten in automatisierten Dateien landes- oder bundesweit zur Verfügung stehen sollen und in welchem Verhältnis hierzu das Bundeszentralregister steht.
- Der Gesetzgeber muß, auch um Doppelspeicherungen zwischen staatsanwaltschaftlichen und polizeilichen Informationssystemen zu vermeiden, eindeutig festlegen, wem die Entscheidungsbefugnis über die bei der Strafverfolgung angefallenen Daten zusteht und für welche Zwecke sie verwendet werden dürfen.
- Daten, die für bloße Tätigkeitsnachweise gespeichert werden (Vorgangsverwaltung), dürfen für andere Zwecke nicht verwendet werden und müssen nach kurzen Fristen gelöscht werden.
- Die vorgesehene Speicherung von Daten über Personen, die "bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen", oder die "Opfer einer Straftat werden könnten", gibt zu Bedenken Anlaß, weil das Anlegen von Dateien über besondere Personengruppen wie z.B. Prostituierte, Homosexuelle und ausländische Gastwirte als erlaubt angesehen werden könnte.
- Die Datenspeicherung über Personen, die mangels hinreichendem Tatverdacht freigesprochen worden sind oder bei denen das Ermittlungsverfahren eingestellt oder die Anklage nicht zugelassen worden ist, darf nur unter engeren Voraussetzungen erfolgen.

3. Zur Akteneinsicht

Strafakten sind wegen ihres teilweise sehr sensiblen Inhalts geheimzuhalten. Sie dürfen deshalb auch anderen öffentlichen Stellen nur unter engeren Voraussetzungen zugänglich sein. Nicht am Strafverfahren beteiligte Personen dürfen auch über Rechtsanwälte allenfalls in besonderen Ausnahmefällen Einsicht oder Auskunft aus Strafakten erhalten.

4. Fehlende Regelungen

Regelungsbedürftig sind außerdem vor allem:

- die engere Festlegung der Zulässigkeit erkennungsdienstlicher Behandlungen und der Voraussetzungen für den Fahndungsabgleich sowie die weitere Verwendung der dabei gewonnenen Daten,
- die Verbesserung des Schutzes der Persönlichkeitsrechte bei der Erhebung persönlicher Daten von Angeklagten und Zeugen in Strafverfahren,
- der allenfalls begrenzte Einsatz der Genomanalyse im Strafverfahren.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zum Entwurf eines Renten-Reform-Gesetzes 1992

Die Rentenversicherung erfaßt den weit überwiegenden Teil der Bevölkerung mit Daten über das Einkommen sowie über familiäre und gesundheitliche Verhältnisse. Sowohl Pflichtmitglieder als auch freiwillige Versicherte haben nur einen sehr begrenzten Einfluß auf die Erhebung, Speicherung, Verwendung und Weitergabe ihrer Daten. Dies führt zu Eingriffen in das Recht auf informationelle Selbstbestimmung, die einer verfassungsmäßigen gesetzlichen Grundlage bedürfen.

Der Zwang zur Angabe personenbezogener Daten im Rahmen des Versicherungsverhältnisses setzt voraus, daß der Gesetzgeber den Verwendungszweck sowie Art und Umfang der erforderlichen Daten präzise bestimmt. Die Verwendung der Daten ist grundsätzlich auf den gesetzlich bestimmten Zweck zu begrenzen. Bei Anwendung dieser Grundsätze sind zur Verbesserung des Datenschutzes Änderungen oder Ergänzungen des Rentenreformgesetzes notwendig. Dies gilt insbesondere in folgenden Punkten:

1. Für die Erhebung, Verarbeitung und Offenbarung von Versichertendaten, insbesondere von Gesundheitsdaten, bedarf es konkreter Befugnisnormen, die auf die verschiedenen Aufgaben der Rentenversicherungsträger abstellen.
2. Um die zweckgebundene Verwendung der Versichertendaten sicherzustellen, müssen auch die Aufgaben der Rentenversicherung normenklar und übersichtlich im Gesetz dargestellt werden.

3. In das Gesetz sollten Regelungen über Aufbewahrungs- und Lösungsfristen aufgenommen werden.
4. Im Gesetz ist klarzustellen,
 - welche versicherungserheblichen Daten im Versicherungskonto gespeichert werden dürfen;
 - welche Stellen am sog. Rentenauskunftsverfahren teilnehmen und worüber Auskünfte erteilt werden;
 - welche Aufgaben der Deutschen Bundespost im Zusammenhang mit der Rentenversicherung obliegen und welche Datenübermittlungen zwischen Rentenversicherungsträgern, Bundespost und anderen Beteiligten erfolgen;
 - welche Daten in der Zentraldatei bei der Datenstelle der Rentenversicherungsträger (VDR) geführt werden und wer auf diese Daten Zugriff hat.
5. Um für die eigenen Mitarbeiter der Rentenversicherungsträger den Sozial- und Personaldatenschutz zu gewährleisten, sollte die organisatorische und personelle Trennung der Sachbearbeitung von der Personaldatenverarbeitung vorgeschrieben werden.
6. Eine eindeutige Klarstellung der Rechtsaufsicht und der Datenschutzkontrolle über die Datenstelle der Rentenversicherungsträger ist erforderlich.

Anlage 13

EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Lander sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 ber

Genomanalyse und informationelle Selbstbestimmung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Lander sowie der Datenschutzkommission Rheinland-Pfalz hat den AbschluÙbericht der Enqute-Kommission des Deutschen Bundestages "Chancen und Risiken der Gentechnologie" (Drucksache 10/6775) zum AnlaÙ genommen, die Risiken fr die informationelle Selbstbestimmung jedes Betroffenen abzuwgen gegenber den Chancen, die die Genomanalyse bringt. Durch die Offenlegung genetischer Daten eines Menschen kann dieser in seinem Persnlichkeitsrecht und sonstigen schutzwrdigen Belangen nachhaltig beeintrchtigt werden. Informationen aus dem Kernbereich der Privatsphre, die dem Betroffenen selbst bisher unbekannt waren, knnen ihn zu einem an sich ungewollten Verhalten in seiner Lebens- oder Berufsgestaltung veranlassen; ihre Kenntnis kann zu einer psychischen und sozialen Zwangslage fr den Betroffenen fhren. Wegen der genetischen Bedingtheit solcher Informationen knnen sich daher auch entsprechende Auswirkungen auf dritte Personen, insbesondere die Familie, ergeben. Das Bekanntwerden solcher Informationen kann den Betroffenen in seinem sozialen Umfeld diskriminieren mit der mglichen Folge gesellschaftlicher Ausgrenzung.

Um den besonderen Risiken bei der Anwendung der Genomanalyse zu begegnen, bedarf es der gesetzlichen Absicherung folgender Grundstze:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muß sich auch auf die weitere Verwendung der genetischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muß zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschußinformationen bringt. Überschußinformationen sind unverzüglich zu vernichten.
4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
5. Die Genomanalyse im gerichtlichen Verfahren muß auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschußinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, daß genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.
6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.
8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, daß ein Schwangerschaftsabbruch straffrei bliebe.

Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muß vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muß berücksichtigt werden.

Die Konferenz versteht ihre Stellungnahme als Beitrag zur Diskussion mit allen Institutionen, die an den Fragen der Genomanalyse arbeiten. Sie legt Wert darauf, den Dialog mit der Wissenschaft fortzusetzen und dabei neue wissenschaftliche Erkenntnisse einzubeziehen.

EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Lander sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zu den nderungen des Gesetzes zu Art. 10 GG und der StrafprozeÙordnung im Rahmen der Poststrukturreform

Der im Rahmen der AusschueÙberatungen zur Poststrukturreform aus den Reihen des Bundestages eingebrachte Entwurf zur nderung des Gesetzes zu Art. 10 GG (Gesetz zur Beschrnkung des Brief-, Post- und Fernmeldegeheimnisses) soll die Verfassungsschutzbehörden des Bundes und der Lander, den Militrischen Abschirmdienst und den Bundesnachrichtendienst u.a. dazu ermchtigen, den Fernmeldeverkehr zu iberwachen und aufzuzeichnen. Bisher war den Diensten nach dem Gesetz zu Art. 10 GG nur gestattet, "den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf Tontrger aufzunehmen". Auch die iberwachungsvorschriften der StrafprozeÙordnung (§§ 100a, 100b) sollen entsprechend verndert werden.

Whrend in der Vergangenheit neben dem Briefverkehr nur Telefongesprche und Fernschreiben kontrolliert und ausgewertet werden durften, soll dies nach dem Entwurf in Zukunft fur den gesamten Fernmeldeverkehr (z.B. Btx, Temex, Telefax, Datel-Dienste, ISDN) zulssig sein. Daraus lieÙe sich ableiten, daÙ auch Abrechnungs-, Verbindungs- und Nutzungsdaten sowie im Rahmen elektronischer Dienste gespeicherte Inhaltsdaten (z.B. bei Mailboxen, Btx usw.) kontrolliert werden durfen. Damit wurde jedenfalls fur den Bereich der StrafprozeÙordnung auch eine ruckwirkende Kontrolle legalisiert. Nicht auszuschlieÙen ist auÙerdem, daÙ Dienstebetreiber dazu verpflichtet werden, fur iberwachungszwecke in groÙerem Umfang Daten zu speichern, als fur

ihre betrieblichen Belange erforderlich und zulässig ist.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß derart weitgehende Eingriffe in Grundrechte einer gründlichen Prüfung durch alle Beteiligten bedürfen. Deshalb sollten im Rahmen der vom Bundestag als dringlich angesehenen Poststrukturreform das Gesetz zu Art. 10 GG und die Strafprozeßordnung nur insoweit geändert werden, als dies in einem unmittelbaren Zusammenhang zu den geplanten ordnungspolitischen Änderungen der Telekommunikation steht. In Betracht käme insofern lediglich die Einbeziehung der Betreiber privater Telekommunikationsdienste in die Regelungen, die bislang nur für die Post gelten.