BREMISCHE BÜRGERSCHAFT
Landtag
12. Wahlperiode

Drucksache 12/815

Zwölfter Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag), dem Präsidenten des Senats den 12. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1989 zum 31. März 1990 (§ 33 Abs. 1 Bremisches Datenschutzgesetz).

Dr. Alfred Büllesbach, Landesbeauftragter für den Datenschutz

Gliederung des 12. Jahresberichts Seite

1. **Einleitung** 5
1.1 **Wahrnehmung des Datenschutzes durch das Volk** 5
1.2 **Tendenz zur Überwachung?** 5
2. **Öffentlicher Bereich** 6
2.1 **Personalwesen** 6
2.1.1 Datenschutzregelungen für den Beihilfebereich 6
2.1.2 Weitergabe der Prüfungsakten von Lehramtsbewerbern 7
2.1.3 Betriebsärztlicher Dienst 8
2.2 **Inneres** 9
2.2.1 **Verfassungschutz** 9
2.2.1.1 Politische Veränderungen in der DDR und in Mittel- und Osteuropa 9
2.2.1.2 ADOS 9
2.2.1.3 Prüfung von Eingaben beim Landesamt für Verfassungsschutz 10
2.2.2 **Polizei** 10
2.2.2.1 Schengener Informationssystem (SIS) 10
2.2.2.2 Staatsschutzprüfung/APIS 11
2.2.2.3 Fortentwicklung der polizeilichen Datenverarbeitung in Bremerhaven und Bremen 12
2.2.2.4 Erkennungsdienst und Lichtbildervorzeigekartei 13
2.2.2.5 Funde polizeilicher Unterlagen in der Öffentlichkeit 17
2.2.3 **Meldewesen** 17
2.2.4 **Straßenverkehrsangelegenheiten** 19
2.2.4.1 Einführung des Verfahrens „Verkehrsordnungswidrigkeiten" bei der Ortspolizeibehörde Bremerhaven 19
2.2.4.2 Einführung des Verfahrens „Führerscheine" bei der Ortspolizeibehörde Bremerhaven 20
2.2.4.3 Aufbewahrungsfristen von Verkehrsordnungswidrigkeitsunterlagen 21

2.2.5	**Amtliche Statistik**	22
2.2.5.1	Landesstatistikgesetz	22
2.2.5.2	Bevölkerungsstatistik	22
2.2.5.3	Mikrozensus, Gebäude- und Wohnungsstichprobe	23
2.2.5.4	Hochschulstatistik	24
2.2.6	**Ausländerangelegenheiten**	27
2.2.6.1	Ausländerrecht und Datenverarbeitung	27
2.2.6.2	Zwangsweise ärztliche Untersuchung von Asylbewerbern	29
2.2.7	**Wahlen**	29
	Änderung des Bremischen Wahlgesetzes	29
2.3	**Justiz und Verfassung**	30
2.3.1	Novellierungsbedarf	30
2.3.2	Aufbau privater Schuldnerverzeichnisse	31
2.3.3	ADV-Einsatz bei Gerichten, Staatsanwaltschaften und im Strafvollzug	32
2.4	**Bildung, Wissenschaft und Kunst**	33
	Automatisierung von Aufgaben der Stadtbibliothek Bremen	33
2.5	**Arbeit**	34
	Rentenreformgesetz (Sozialgesetzbuch VI. Buch)	34
2.6	**Jugend und Soziales**	35
2.6.1	Schwerpunkte, Handlungsbedarfsfälle	35
2.6.1.1	Innerbehördlicher Datenschutz in den Sozialen Diensten	35
2.6.1.2	Empirische Untersuchungen zu den Ursachen der Sozialhilfeabhängigkeit	37
2.6.1.3	Dienstanweisung über die Pflicht zur Anzeige strafbarer Handlungen	38
2.6.2	Kurze Darstellung von Problemen und Beschwerden	39
2.6.2.1	Sachfremde Anmerkungen in der Sozialhilfeakte	39
2.6.2.2	Anforderungen von Gutachten des Hauptgesundheitsamtes bei Anträgen von HIV-positiven Sozialhilfeempfängern	39
2.7	**Gesundheit**	39
2.7.1	Schwerpunkte, Handlungsbedarfsfälle	39
2.7.1.1	Durchführung des Gesundheitsreformgesetzes (SGB V)	39
2.7.1.2	Datenschutz im öffentlichen Gesundheitsdienst	40
2.7.1.3	Wissenschaftliche Begleitung der Auflösung des Klosters Blankenburg	41
2.7.2	Auskünfte eines Krankenhauses an den Sozialleistungsträger	42
2.7.3	Humangenetik	42
2.8	**Umweltschutz und Stadtentwicklung**	43
	Altlastenkataster	43
2.9	**Bauwesen**	44
2.9.1	Novelle zum Bremischen Architektengesetz	44
2.9.2	Entwurf einer Verordnung über die Gutachterausschüsse nach dem Baugesetzbuch	44
2.9.3	Änderung der Bremischen Landesbauordnung (BremLBO)	45

2.10	**Wirtschaft, Technologie und Außenhandel**	46
	Auskunft gegenüber Dritten durch die Landeskartellbehörde	46
2.11	**Häfen, Schiffahrt und Verkehr**	46
	Gefahrgutbeauftragtenverordnung und 2. Straßengefahrgutänderungsverordnung	46
2.12	**Finanzen**	48
2.12.1	Kontrollmitteilungen an Finanzämter	48
2.12.2	Weiterleitung von Dozentendaten zur Überprfüung der Gemeinnützigkeit an das Finanzamt Bremen-Mitte	48
2.12.3	Anzeigepflicht der Notare nach dem Grunderwerbssteuergesetz	49
2.12.4	Kontrollbefugnisse der Datenschutzbeauftragten in der Steuerverwaltung	50
2.13	**Datenverarbeitung im Auftrag öffentlicher Stellen**	50
2.14	**Zugriff der Bremischen Bürgerschaft auf zentrale Datenspeicher der Verwaltung**	53
2.15	**Ausgewählte unerledigte Probleme aus früheren Jahresberichten**	54
3.	**Datenschutz in Europa**	54
4.	**Nicht-öffentlicher Bereich**	55
4.1	Vorbemerkungen	55
4.2	**Arbeitnehmerdatenschutz**	56
	Fragerecht des Arbeitgebers	56
4.3	**Patientendatenschutz**	56
4.3.1	Übergabe der Patientenkartei an den Käufer einer Arztpraxis	56
4.3.2	Laborbefunde im Park	57
4.4	**Aufbewahrung und Weiterleitung von Ladendiebstahlsanzeigen**	57
4.5	**Datenschutz in Fotolabors und Fotogeschäften**	58
4.6	**Forderung nach Regelungen des Datenschutzes bei Verbraucherkrediten**	58
4.7	**Auskunfteien**	60
4.7.1	Schufa	60
4.7.2	Creditreform	61
5.	**Informationstechnologie**	61
5.1	**Telekommunikation, Wirkungen der Digitalisierung**	61
5.2	**Datenschutz in Netzen**	63
5.2.1	Informationstechnologische Grundlagen	63
5.2.2	Datenschutzrechtliche Grundlagen	64
5.2.3	Technisch-organisatorische Schutzmaßnahmen in Netzen	66
5.3	**Datenschutz im ADV-Entwicklungsprozeß**	67
6.	**Deutsch-deutsche Entwicklung und Datenschutz**	69

7. Anlagen

1. Neuregelung des Bundesdatenschutzgesetzes (Konferenzbeschluß vom 05./06.04.1989) 70

2. Entwurf eines Rentenreformgesetzes (Konferenzbeschluß vom 05./06.04.1989) 71

3. Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (Konferenzbeschluß vom 05./06.04.1989) 71

4. Änderung des Gesetzes zur Art. 10 GG und der Strafprozeßordnung im Rahmen der Poststrukturreform (Konferenzbeschluß vom 05./06.04.1989) 73

5. Entwürfe Bundesverfassungsschutzgesetz, MAD-Gesetz und BND-Gesetz (Konferenzbeschluß vom 30.05.1989) 74

6. Datenschutz in der Europäischen Gemeinschaft (Konferenzbeschluß vom 26./27.10.1989) 76

7. Entwurf einer EG-Statistikverordnung (Konferenzbeschluß vom 26./27.10.1989) 77

8. Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen (Konferenzbeschluß vom 26./27.10.1989) 77

9. Genomanalyse und informationelle Selbstbestimmung (Konferenzbeschluß vom 26./27.10.1989) 79

10. Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten von 30.08.1989 80

11. Beschluß der Internationalen Konferenz der Datenschutzbeauftragten vom 30.08.1989 zu ISDN 81

12. Zusatzerklärung der Datenschutzbeauftragten der EG-Länder 82

1. Einleitung

1.1 Wahrnehmung des Datenschutzes durch das Volk

Internationale Beispiele, wie die Diskussion um den Staatsschutz in der Schweiz und neuerdings auch in Frankreich zeigen, wie elementar die Bevölkerung ihr Recht auf informationelle Selbstbestimmung versteht. Dort, wo es durch staatliche Organe nicht beachtet wird, nimmt das Volk es selbst wahr. Datenschutz wird nicht nur in der Bundesrepublik, sondern auch in anderen europäischen Staaten, ja international, als Persönlichkeitsschutz wie auch als Schutz demokratischer Rechte verstanden.

Die politische Entwicklung in der DDR zeigt diese Auffassung ebenfalls deutlich. Die Wahrnehmung des informationellen Selbstbestimmungsrechtes durch das Volk der DDR gegenüber den Aktensammelstellen und -speichern des Staatssicherheitsdienstes sprechen eine deutliche Sprache. Die historische Entwicklung der Selbstbestimmung als Menschenrecht und als Konstituens der Demokratie ist ohne informationelle Selbstbestimmung nicht vorstellbar. Freiheitliche und demokratische Entwicklungen basieren ganz wesentlich auf der Selbstbestimmung des Einzelnen wie des Volkes. Die Wahrnehmung der Selbstbestimmung hat zugleich etwas mit Macht- und Herrschaftsbeschränkung in Politik und Wirtschaft zu tun. Datenschutz ist so verstanden sowohl eine Reaktion auf die umfangreichen Informationsverarbeitungsmöglichkeiten, die die moderne Informationstechnik bietet, als auch ein wichtiges Gestaltungsgrundrecht im sozialen und gesellschaftlichen Lebensbereich.

Wie richtig diese Einschätzung ist, zeigen aber auch die Bemühungen der Menschen in Ost- und Mitteleuropa, z. B. in Polen, in Ungarn, ja auch in der UdSSR. So wird in Polen seit Jahren ein Recht auf Datenschutz rechtspolitisch diskutiert. In der UdSSR beschäftigen sich Rechtswissenschaftler wie Informationswissenschaftler mit der Gestaltung neuer Informationsbeziehungen und Informationsflüsse, auch unter dem Aspekt des Schutzes der Persönlichkeit. In Ungarn gibt es ernsthafte Diskussionen um den Beitritt zur Datenschutzkonvention des Europarates und um die Einfügung eines Rechts auf Datenschutz in die ungarische Verfassung.

Berücksichtigt man die Diskussion um den Datenschutz in Europa und nimmt man die Diskussion in der UNO hinzu, so zeigt sich ein weltweites Bedürfnis nach einem Recht auf Datenschutz.

1.2 Tendenz zur Überwachung?

Informationen über Personen sind nicht per se bedeutsam, sondern werden es erst durch das Interesse an ihrer Verarbeitung. Die Datenschutzdiskussion ist eng verbunden mit der Entwicklung der Informations- und Kommunikationstechnologien. Gleichwohl ist sie nicht nur darauf beschränkt. Die moderneren Entwicklungen der Informationstechnik einschließlich der weltweiten Vernetzungsstrukturen führen neben den bekannten Datenschutzrisiken zu weiteren neuartigen Problemstellungen. So kann durch die Vernetzung künftig ein an einer Informationsaustauschbeziehung nicht beteiligter Dritter oder gar Vierter an Informationen gelangen, die er bisher nicht besaß. Diese so erlangten Informationen können wiederum weitergegeben werden, ohne daß die Partner der eigentlichen Kommunikationsbeziehung dieses wissen. Dies hat nicht nur Rückwirkungen auf Urheber und Empfänger, sondern auch auf die Drittinteressierten. Alle Beteiligten können in Kenntnis dieser Sachlage und in dem Verständnis, selbst Netzbeteiligte zu sein, Informationen steuern, gezielt in das Netz senden, Intimfeinde bestimmten Informationen aussetzen etc., um so insgesamt Wirkungen auf die Struktur eines Gesellschaftsnetzes und damit auf dessen soziale Qualität auszuüben. Diese Probleme werden gegenwärtig erst anfänglich erörtert, sie sind auf Dauer in ihrer Informationstechnikwirkung wie in ihrer Sozialdimension noch auszuloten. Diese Probleme treten neben die schon bekannten Ausgangsprobleme der Datenschutzdiskussion wie

- Belästigungen, Beeinträchtigungen und Manipulationen des Individuums durch Eindringen in seine schutzwürdigen Bereiche
- Diskriminierung von Menschen durch Verbreitung kontextloser und damit multifunktionaler Informationen, Berücksichtigung unzureichender Informationen bei Entscheidungen, Fehlbeurteilungen durch mangelhafte Informationsbasis sowie unzulässige Informationsverarbeitung etc.

— Ausweitung der Mechanismen sozialer Kontrolle durch modernere Formen der Informationstechnik, z. B. durch Intensivierung der Überwachung des Verhaltens von Menschen, durch frühzeitiges Erkennen von Normverstössen, um die Sanktionsmöglichkeiten zu verbessern etc.

Der Datenschutz hat auf diese Risiken durch die Regelung von Informationsflüssen, die Bestimmung des Informationsumfanges, die Festlegung des Informationsverfahrens, Gewährleistung von Rechten Betroffener und schließlich durch technische und organisatorische Maßnahmen reagiert. Die Durchsetzung dieser Anforderungen war ohne Machtkonflikte, d. h. ohne Begrenzung von Macht- und Herrschaftsansprüchen über zu verarbeitende personenbezogene Informationen überwiegend nicht möglich. Auch in solchen Auseinandersetzungen wurde sichtbar, daß die Beschränkung von Informationsbegehrlichkeiten eine starke institutionelle Kontrolle voraussetzt. Datenschutz ist deshalb immer sowohl durch institutionell verankerte Kontrollen als auch auf dem Wege offener politischer Auseinandersetzung durchgesetzt worden. Je öfter die Datenschutzkontrolle unberücksichtigt bleibt, desto wichtiger ist die Kenntnis des Verhaltens der Macht, weil nur so ein offener Weg für die Realisierung des Datenschutzes gewährleistbar bleibt.

Öffentlichkeitsarbeit, institutionelle Datenschutzkontrolle und politische Kontrolle sind deshalb eng miteinander verzahnte Elemente.

Aus dieser Situation heraus erklären sich Konflikte zwischen Kontrollorgan und Kontrollierten. Es muß nicht vertieft dargestellt werden, daß der kontrollierte und ggf. auch beanstandete politische Machtträger solche Beanstandungen als unliebsamen Eingriff in seine Rechte versteht. Konflikte dieser Art sind — wenn der Datenschutz erfolgreich durchgesetzt werden soll — nicht vermeidbar. Kontrolltätigkeit versteht sich von ihrem Anspruch her als Gesetzmäßigkeits-, Richtigkeits-, Erforderlichkeits- und sehr häufig im Ergebnis als Informationsbeschränkungs- und damit als Machtkontrolle.

Diese Konfliktkonstellation ist auf Dauer auch von den Trägern der Kontrollorgane sozialpsychologisch nur durchhaltbar, wenn eine allgemeine Akzeptanz der Datenschutzberatungs- und Kontrolltätigkeit von allen politisch Verantwortlichen wie von der Verwaltung und, soweit es die Datenschutzbeauftragten in den privaten Betrieben angeht, von den Geschäftsleitungen akzeptiert wird.

Kontrollorgane, die in einem derartig sensiblen und konfliktträchtigen Feld tätig sind, müssen in ihrer Stellung stark und unabhängig sein, damit sie nicht zum Spielball unterschiedlicher Interessen gemacht und nicht diskriminiert werden können.

Objektiv bleibt festzuhalten, daß die Informatisierung der Verwaltung im Lande Bremen längst über die Anfangsschritte hinausgegangen ist, so daß die Frage der Datenschutzverträglichkeit und damit der Sozialverträglichkeit der Technik in allen Einzelschritten der Gestaltung von besonderem Gewicht ist. Es ist insgesamt zu lernen, wie mit der Informationstechnik umgegangen werden kann, wobei immer entscheidungsbedürftig ist, welche der denkbaren technischen Möglichkeiten aufgegriffen und welche Vorkehrungen gegen Mißbrauch der technischen Möglichkeiten getroffen werden müssen. Dies setzt — und dies sei noch einmal betont — eine starke Verankerung des Datenschutzes voraus. Deshalb müssen elementarer Datenschutz und Datensicherheit Bestandteil jeder Planung von Informationsvorhaben (z. B. ADV-Verfahren, Gesetze) sein.

2. Öffentlicher Bereich

2.1 Personalwesen

2.1.1 Datenschutzregelungen für den Beihilfebereich

Die Senatskommission für das Personalwesen (SKP) beabsichtigt, im Zuge der Einführung der zweiten Stufe des Abrechnungsverfahrens für Besoldung, Vergütung, Lohn- und Versorgung (PAADIS) zum Zwecke der Auszahlung der Beihilfebeträge ein Abrufverfahren einzurichten, das den Beihilfesachbearbeitern den Zugriff auf die für die Festsetzung von Beihilfe erforderlichen personenbezogenen Daten der Berechtigten aus PAADIS ermöglicht.

Ich habe dargelegt, daß die Einrichtung eines derartigen Abrufverfahrens nur dann zulässig ist, wenn sie nach Bundes- oder Landesrecht bestimmt ist. Es bestehen aber derzeit keine bereichsspezifischen gesetzlichen Bestimmungen, die die Datenverarbeitung im Rahmen des Beihilfeverfahrens erlauben.

Ich habe daher vorgeschlagen, gesetzlich zu regeln, unter welchen Voraussetzungen Beihilfedaten erhoben, gespeichert und übermittelt werden dürfen. Auch die Einrichtung eines automatisierten Abrufverfahrens bedarf hier einer Regelung.

Des weiteren bedarf es einer Regelung, aus der sich ergibt, wann die personenbezogenen Daten der Beihilfeberechtigten gelöscht werden. Außerdem halte ich es für erforderlich, bei der Regelung über technische und organisatorische Maßnahmen festzulegen, daß die Beihilfeakte getrennt von anderen Personalakten aufzubewahren ist und Beihilfesachbearbeiter nicht zugleich zuständig für die Bearbeitung sonstiger Personalangelegenheiten sein dürfen.

Schließlich habe ich auf die Bestimmung des § 22 Abs. 6 BrDSG hingewiesen, wonach medizinische und psychologische Befunde der Beihilfeberechtigten nicht automatisiert verarbeitet werden dürfen.

Eine Antwort der SKP steht noch aus.

2.1.2 Weitergabe der Prüfungsakten von Lehramtsbewerbern

Das Landesamt für Schulpraxis und Lehrerprüfungen hat mich gebeten zu prüfen, ob es zulässig ist, die Prüfungsakten an den Senator für Bildung, Wissenschaft und Kunst zur Verwendung innerhalb eines Bewerbungsverfahrens weiterzuleiten.

Die in den Prüfungsakten enthaltenen Unterlagen sind höchstpersönliche Dokumente der Lehramtskandidaten und unterliegen von daher der strikten Zweckbindung. Sie sind unter besonderen Bedingungen einer Prüfungssituation entstanden, die nicht mit einer Bewerbungslage zu vergleichen ist.

Die Verwendung der zum Zwecke der Ablegung der Prüfung erhobenen Daten im Rahmen eines Bewerbungsverfahrens stellt eine Zweckänderung und damit einen erneuten Eingriff in das informationelle Selbstbestimmungsrecht dar, für die es keine Rechtsgrundlage gibt.

Die Einsichtnahme in die Prüfungsakten kann auch nicht auf die Einwilligung der Betroffenen gestützt werden, da sie grundsätzlich im Rahmen eines Bewerbungsverfahrens nicht freiwillig erklärt werden und demnach nicht wirksam werden kann. Nach herrschender Rechtsauffassung fehlt diese Freiwilligkeit insbesondere dann, wenn faktische Zwänge wirksam werden, weil der Einzelne einer organisierten sozialen Macht gegenübersteht. Ein Hauptbeispiel dafür ist das Arbeitsverhältnis mit der charakteristischen Abhängigkeit des Arbeitnehmers bzw. Bewerbers, besonders in Zeiten hoher Arbeitslosigkeit. Willigt der Bewerber in die Akteneinsicht nicht ein, muß er damit rechnen, bei der Auswahl nicht berücksichtigt zu werden.

Darüber hinaus tritt die Einwilligung der Betroffenen dann zurück, wenn eine abschließende gesetzliche Regelung den Umfang der Datenverarbeitung festlegt. Dieses „Nachrangprinzip" gewährleistet ein ausbalanciertes Verhältnis von eigenständiger und fremder Verfügung über geschützte Daten. Dieses Verhältnis darf nicht dadurch aufgehoben werden, daß in das Instrument der Einwilligung eine globale Einwilligungsverpflichtung zugunsten der öffentliche Stelle hineingelesen wird. Dieser Grundsatz gilt gerade auch bei Bewerbungsverfahren, weil § 22 Abs. 1 BrDSG abschließend festlegt, unter welchen Voraussetzungen und in welchem Umfang die Verarbeitung personenbezogener Daten von Bewerbern zur Eingehung eines Dienst- oder Arbeitsverhältnisses zulässig ist.

Der Senator für Bildung, Wissenschaft und Kunst hat meiner Auffassung widersprochen, weil nach seiner Ansicht die Einwilligung auch gegenüber einer sozialen Macht, also gegenüber einem öffentlichen oder privaten Arbeitgeber, als freiwillig anzusehen ist. Nach seiner Ansicht ist die Einwilligung immer dann wirksam, wenn der Einwilligende die Bedeutung und die Folgen der Datenverarbeitung erkennen kann.

Demgegenüber vertrete ich nach wie vor die Auffassung, daß der Verarbeitungsspielraum der Behörden und der sonstigen öffentlichen Stellen von vornherein begrenzt ist, da ihre Aufgaben grundsätzlich gesetzlich definiert sind und damit zugleich die Verarbeitungsgrenze abgesteckt ist. Der Senator für Bildung, Wissenschaft und Kunst darf nur die Angaben verwenden, die für die Eingehung des Dienst- oder Arbeitsverhältnisses erforderlich sind. Ebenso wenig wie er deshalb das Recht hat, die eigenen Aufgaben jederzeit beliebig neu festzulegen, ist er berechtigt, mit Hilfe einer Einwilligung des Betroffenen mehr und andere Daten zu verarbeiten. Das Instrument der Einwilligung bleibt daher im öffentlichen Bereich auf wenige Ausnahmefälle beschränkt.

Es bleibt festzuhalten, daß die Kandidaten nach bestandener Prüfung ein Prüfungszeugnis erhalten, dessen Vorlage der Arbeitgeber zur Begründung eines Dienst- oder Arbeitsverhältnisses verlangen kann.

Auch durch neue organisatorische Zuordnung ändert sich nichts an der dargestellten Rechtslage. Gängige und rechtlich korrekte Praxis bei anderen Behörden ist, daß Prüfungsakten nicht zu anderen Zwecken verwendet werden.

2.1.3 Betriebsärztlicher Dienst

In dem Gebäude des Hauptgesundheitsamtes Bremen hat der dem Senator für Gesundheit angegliederte Betriebsärztliche Dienst der Stadtgemeinde Bremen seine Arbeit aufgenommen. Im Rahmen einer datenschutzrechtlichen Beratung zu unterschiedlichen Aspekten der Arbeit des Dienstes (PC-Einsatz, Formulare, Röntgenuntersuchungen, Mikroverfilmung, Statistik) stieß ich auf das Problem, daß der Dienst beabsichtigte, die Ergebnisse seiner arbeitsmedizinischen Untersuchungen an die Stadtgemeinde in ihrer Eigenschaft als Arbeitgeberin zu übermitteln. Dies ist einem allgemein gebräuchlichem Formblatt zu entnehmen, das der Gemeindeunfallversicherungsverband (GuV Bremen) herausgegeben hat. Mit ihm soll dem Arbeitgeber gemeldet werden, ob die Untersuchung

- keine gesundheitliche Bedenken,
- keine gesundheitliche Bedenken unter bestimmten Voraussetzungen oder
- gesundheitliche Bedenken

ergeben hat. In den beiden letzten Fällen sollen Empfehlungen an den Arbeitgeber in einer gesonderten Rubrik eingetragen werden. Ich bezweifle, daß es hierfür eine gesetzliche Grundlage gibt:

- § 22 Abs. 4 BrDSG erlaubt nur die Übermittlung des Ergebnisses einer Eignungsuntersuchung zum Zwecke der Eingehung eines Dienst- oder Arbeitsverhältnisses, nicht aber die Übermittlung des Ergebnisses einer Vorsorgeuntersuchung, die im Rahmen eines bereits bestehenden Beschäftigungsverhältnisses vorgenommen worden ist. Hinzukommt, daß die Zuständigkeit für Einstellungsuntersuchungen beim amtsärztlichen Dienst liegt.
- § 3 des Bundesgesetzes über Betriebsärzte vom 12. Dezember 1973 regelt abschließend die Befugnisse der Betriebsärzte zur Verarbeitung von arbeitsmedizinischen Daten von Arbeitnehmern. Nach Abs. 1 Nr. 2 hat der Betriebsarzt die Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten. Er hat also nur den Arbeitnehmer, nicht den Arbeitgeber im Zusammenhang mit Einzeluntersuchungen zu beraten. Die Beratung dem Arbeitgeber gegenüber, zu der der Betriebsarzt nach Abs. 1 Nr. 1 verpflichtet ist, kann nach Erfassung und Auswertung der Einzelbefunde auch ohne Übermittlung von Befunden über einzelne Arbeitnehmer erfolgen. Überdies wird sowohl in dieser Vorschrift als auch in § 8 Abs. 1 darauf hingewiesen, daß Betriebsärzte der ärztlichen Schweigepflicht unterliegen. Dies bestärkt den Schluß, daß der Betriebsarzt dem Arbeitgeber keine personenbezogenen Daten von Beschäftigten übermitteln darf, die er im Rahmen seiner Verpflichtungen untersucht hat.
- Die Berufsgenossenschaften, d. h. hier der GuV Bremen, haben in § 7 Abs. 2 der Unfallverhütungsvorschrift „Arbeitsmedizinische Vorsorge" (GuV 0.6) den Unternehmer verpflichtet, seinerseits den Betriebsarzt zu verpflichten, ihm über das Untersuchungsergebnis eine Bescheinigung zu erteilen. Als Rechtsgrundlage hierfür werden die §§ 708, 767 RVO angeführt. Dort ist aber von einer Unterrichtung des Arbeitgebers über ärztliche Untersuchungen nicht die Rede. Außerdem ist zu fragen, ob eine derartige Unfallverhütungsvorschrift überhaupt in der vorgesehenen Weise in Grundrechte von Beschäftigten, die selbst nicht Mitglieder der Berufsgenossenschaften sind, eingreifen dürfen.
- Dagegen dürfen Ärzte, die auf der Grundlage von § 19 Abs. 2 Nr. 9 Chemikaliengesetz (ChemG), §§ 28 ff. Gefahrstoffverordnung (GefStoffV), im Auftrag von Arbeitgebern Vorsorgeuntersuchungen von Arbeitnehmern vornehmen, die mit gefährlichen Stoffen in Berührung kommen, lt. §§ 31 Abs. 2, 34 GefStoffV das Untersuchungsergebnis dem Arbeitgeber übermitteln. Voraussetzung ist allerdings, daß der Arbeitnehmer in die Untersuchung eingewilligt hat und zwar in dem Wissen, daß der Arbeitgeber ihr Ergebnis erfährt. Überdies enthält § 19 Abs. 2 Nr. 9 b ChemG keine eindeutige Ermächtigung, durch Rechtsverordnung Regelungen zu treffen über die Unterrichtung nicht nur des untersuchten Arbeitnehmers, sondern auch des beauftragten Arbeitgebers

über das Untersuchungsergebnis. Zudem ist es nicht unproblematisch, wenn der Betriebsarzt auch mit Untersuchungen nach GefStoffV beauftragt wird, zieht man seine oben dargestellte Rechtsstellung und seine ärztliche Schweigepflicht in Betracht.

2.2 Inneres

2.2.1 Verfassungsschutz

2.2.1.1 Politische Veränderungen in der DDR und in Mittel- und Osteuropa

Die politischen Veränderungen in der DDR und in Mittel- und Osteuropa haben vor der Bundesrepublik nicht halt gemacht. So hat sich beispielsweise die Landesorganisation der DKP in Bremen aufgelöst, viele Mitglieder sind aus dieser Partei ausgetreten. Diese Entwicklung muß zu Konsequenzen bei der Verarbeitung personenbezogener Daten im Landesamt für Verfassungsschutz führen.

Ich erwarte eine intensive Überprüfung der einschlägigen Datenbestände. Insbesondere in Fällen, in denen dienstlich oder amtlich Kenntnis erlangt wird, daß sich Personen von der DKP losgesagt haben oder Zweifel bestehen, ob die gesammelten Unterlagen eine weitere Speicherung rechtfertigen, ist ein Verfahren zu entwickeln, das datenschutzrechtlichen Anforderungen genügt. In diesen Fällen bietet sich an, soweit eine Löschung zum jetzigen Zeitpunkt nicht in Betracht kommt, die Vergabe eines neutralen Aktenzeichens, das für andere Nutzer von NADIS nicht interpretierbar ist, um so Benachteiligungen für die Betroffenen auszuschließen. In all den Fällen, in denen eine weitere Speicherung aufrecht erhalten werden soll, sollte darüber hinaus durch die Vergabe einer kurzen Wiedervorlagefrist eine erneute Aussonderungs- und Löschungsprüfung nach drei, spätestens aber nach fünf Jahren vorgesehen werden.

Um rechtswidrige Mitteilungen anderer öffentlicher Stellen an das Landesamt für Verfassungsschutz zu vermeiden, sind generell die für diesen Bereich der Extremismusbeobachtung geltenden Richtlinien und Arbeitsanweisungen unter Berücksichtigung der politischen Entwicklung bundesweit zu überprüfen. Dies gilt etwa für Referenzbefragungen, Überprüfungen von Reisegruppen etc. Schließlich ist zu prüfen, in welchem Umfang diese Gesichtspunkte auch bei der Novellierung des Bundesverfassungsschutzgesetzes und der Geheimschutzgesetze durchschlagen.

2.2.1.2 ADOS

Wie aus den Medien bekannt, befindet sich beim Bundesamt für Verfassungsschutz (BfV) eine Datei im Aufbau, in die Daten von allen Aus- und Übersiedlern eingestellt werden sollen; benannt mit dem Namen ADOS (Adressen- und Objektdatei Ost). Dazu war beabsichtigt, auch die Länder mit der Erfassung und Speicherung der Daten zu beauftragen. Dagegen habe ich meine datenschutzrechtlichen Bedenken geltend gemacht.

Der Betrieb der Datei ADOS ist nach meiner Auffassung rechtlich unzulässig. Für die geplante Datenverarbeitung in ADOS fehlt es an einer gesetzlichen Grundlage. Weder die Übermittlung aus den Übergangslagern an die Verfassungsschutzämter noch der Datenumfang, die Zweckbindung und die Löschung der Daten sind geregelt. Den Aufbau und Betrieb der Datei halte ich aber auch unter verfassungsrechtlichen Gesichtspunkten für unzulässig. Angesichts der jetzt bekannten Zahlen ist davon auszugehen, daß eine riesige Datensammlung mit Daten von unverdächtigen Bürgern entstehen würde und anzunehmen ist, daß nur ein ganz geringer Teil für die Aufgaben der Spionageabwehr nutzbar gemacht werden könnte. Eine massenhafte Datensammlung über unverdächtige Bürger halte ich für unverhältnismäßig. Im übrigen ist ADOS aufgrund der politischen Veränderung in der DDR und in Mittel- und Osteuropa nicht mehr vermittelbar.

Das Landesamt für Verfassungsschutz hat mir gegenüber erklärt, daß das Land Bremen bisher keine Datensätze in das Informationssystem ADOS eingespeist hat und die Datei gegenwärtig bundesweit nicht fortgeführt wird. Gleichwohl lagern im Landesamt für Verfassungsschutz eine Vielzahl von Aufnahmeformularen über Aus- und Übersiedler mit dezidierten Angaben über Wohnungswechsel, beruflichen Werdegang und Verwandtschaftsverhältnisse (Lebenslauf) usw.

Ich bin der Auffassung, daß keine Daten aus dem Aufnahmeverfahren oder Formulare der Bundesaufnahmestelle mehr an das Landesamt für Verfassungsschutz übersandt werden dürfen. Deshalb habe ich gegenüber dem Landesamt für Verfassungschutzes verlangt, die in diesem Zusammenhang bereits dort gesammelten Unterlagen und Daten zu vernichten.

Wie ich nach Redaktionsschluß noch erfahren habe, hat der Arbeitskreis IV der Innenministerkonferenz am 5. März 1990 festgestellt, daß aufgrund der politischen Entwicklung in der DDR und in Osteuropa die Datei ADOS nicht mehr notwendig ist. Der Arbeitskreis IV beschloß weiterhin, die gespeicherten Daten zu löschen und die dazu noch vorhandenen Unterlagen zu vernichten.

2.2.1.3 Prüfung von Eingaben beim Landesamt für Verfassungsschutz

Im Berichtszeitraum habe ich wiederum eine Reihe von Eingaben und Beschwerden beim Landesamt für Verfassungsschutz überprüft. In vielen Fällen konnte aufgrund der Eingabe eine vorzeitige Löschung erreicht werden obwohl diese vom System noch nicht vorgesehen war. Zum Teil mußte ich dabei die Kooperation anderer Landesbeauftragter und des Bundesbeauftragten in Anspruch nehmen.

Ein Beschwerdeführer hatte im Jahre 1961 dem Verfassungsschutz über den Anwerbeversuch eines DDR-Agenten berichtet. Der Beschwerdeführer ging zu Recht von einer Speicherung dieses Vorganges im Informationssystem der Verfassungsschutzämter (NADIS) aus. Er litt sehr unter dieser Speicherung, so berichtete er von beruflichen Nachteilen, sowie von der Beeinträchtigung der Reisefreiheit seiner Tochter, die er auf die Speicherung zurückführte. Ob die Befürchtungen des Beschwerdeführers tatsächlich zutrafen, mag dahinstehen; meine Prüfung beim Landesamt für Verfassungsschutz hat ergeben, daß die Daten des Hinweisgebers in solchen Fällen erst gelöscht werden, wenn die Daten des Werbers gelöscht werden. Soweit der Agent weiterhin aktiv ist, bleiben alle Anwerbeversuche dieser Person dokumentiert. So erging es auch dem Beschwerdeführer, der bei meiner Prüfung noch gespeichert war. Aus Sicht des Verfassungsschutzes ist die Speicherung des Hinweisgebers kein negatives Datum, der Bürger hingegen empfand jede Speicherung durch die Sicherheitsbehörden als Eingriff in sein informationelles Selbstbestimmungsrecht. Fast 30 Jahre nach diesem Vorfall konnte erreicht werden, daß die personenbezogenen Daten des Hinweisgebers gelöscht wurden.

2.2.2 Polizei

2.2.2.1 Schengener Informationssystem (SIS)

Die Regierungen der BENELUX-Staaten, Frankreichs und der Bundesrepublik hatten 1985 ein Abkommen über den schrittweisen Abbau der Grenzen zwischen ihren Ländern vereinbart. Den darin vereinbarten Wegfall der Grenzkontrollen und die dadurch befürchteten Sicherheitsdefizite will man zum Anlaß nehmen eine Reihe von Ausgleichsmaßnahmen zu schaffen, die in einem Zusatzabkommen festgehalten werden sollen.

Hierzu gehört insbesondere die Errichtung eines gemeinsamen automatisierten Informationssystems (SIS) für den Bereich der Fahndung. Dieses System soll vor allem für die folgenden Bereiche praktiziert werden:

- Fahndungsersuchen nach Personen, die aus Gründen der Strafverfolgung oder der Strafvollstreckung zur Festnahme gesucht werden,
- Ausschreibung zur Zurückweisung von unerwünschten Ausländern aus Drittstaaten,
- Ausschreibung von Personen, die verdeckt registriert oder gezielt kontrolliert werden sollen,
- Fahndungsersuchen, die der Ermittlung des Aufenthalts der gesuchten Person zur Strafverfolgung oder Strafvollstreckung dienen,
- Ausschreibung zur Aufenthaltsermittlung,
- Fahndungsersuchen nach Sachen, die zur Sicherstellung oder Beweissicherung im Strafverfahren gesucht werden.

U. a. sind Regelungen zur Unterstützung des Informationsaustausches zur präventiven und repressiven Verbrechensbekämpfung vorgesehen (Art. 47); sollen Beamte der Vertragsparteien berechtigt, die Verfolgung auf dem Hoheitsgebiet einer anderen Vertragspartei ohne deren vorherige Zustimmung fortzusetzen (Art. 41) und soll die Polizei im Einzelfall der jeweils betroffenen anderen Vertragspartei Informationen mitteilen, die zur Unterstützung der Bekämpfung zukünftiger Straftaten, der Verhütung einer Straftat oder zur Abwehr von Gefahren für die öffentlicher Sicherheit und Ordnung von Bedeutung sind. Schließlich verpflichten sich die Vertragsparteien zur Zusammenarbeit der Sicherheitsdienste (Art. 48).

Die Entwürfe des Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen habe ich mit den anderen Datenschutzbeauftragten des Bundes und der Länder unter datenschutzrechtlichen Gesichtspunkten geprüft. Die wesentlichen Ergebnisse faßt die Entschließung der Konferenz der Datenschutzbeauftragten vom 26./27. Oktober 1989 zusammen (Anlage 8). Die ursprünglich für Ende des Jahres 1989 vorgesehene Unterzeichnung hat sich aufgrund von Differenzen über den Status der DDR-Bürger und die deutsch-deutsche Grenze verzögert.

Die Anwendung des Schengener Abkommens führt z. B. dazu, daß Personen aus Nordafrika, die bisher nach Frankreich nicht einreisen durften, nunmehr auch das Staatsgebiet der anderen Vertragsländer verschlossen ist. Mit SIS wird nach meiner Einschätzung der erste Schritt zu einem Aufbau eines polizeilichen Informationssystems der Gemeinschaft in die Wege geleitet, das mit einem zentralen Ausländerinformationssystem verbunden wird. Nach meiner Einschätzung wurden andere Möglichkeiten wie z. B. eine kleinere dezentrale Datenhaltung mit begrenztem Datenaustausch nicht untersucht.

Durch einzelne Regelungen im Schengener Abkommen wird die örtliche und sachliche Zuständigkeit der Strafverfolgungsbehörden erweitert. Es werden Möglichkeiten der Informationsverarbeitung über die Grenzen der BRD hinaus ermöglicht. Dabei erhalten die Strafverfolgungsbehörden nach ausländischem Strafprozeßrecht erhobene Daten. Dies kann ohne Harmonisierung der Rechtsordnungen dazu führen, daß Strafverfolgungsbehörden an Daten herankommen, die sie aufgrund eigener Kompetenzen nicht erhalten hätten.

Für den Bereich der Strafverfolgung und der Sicherheitsdienste fehlen bisher in der Bundesrepublik die notwendigen bereichsspezifischen Datenschutzregelungen. In anderen Vertragsländern, denen Daten zur Verfügung gestellt werden sollen, sind die Datenschutzstandards noch weniger ausgeprägt. Im übrigen sollte klargestellt werden, daß durch Ratifizierung des Zusatzabkommens der Polizei in der Bundesrepublik keine Befugnisse eröffnet werden, die für das Inland bisher nicht geregelt sind. So kennt etwa das Bremische Polizeigesetz den in Art. 46 des Abkommens vorgesehenen Begriff der öffentlichen Ordnung nicht.

Es ist weiterhin darauf zu achten, daß, solange ein Vertragsstaat seiner Verpflichtung aus dem Zusatzabkommen, ausreichende nationale Regelungen für Erheben und Nutzen von Daten zu erlassen, nicht nachgekommen ist (Art. 118), an ihn keine Daten auf der Grundlage des Abkommens übermittelt werden.

2.2.2.2 Staatsschutzprüfung/APIS

Im Anschluß an meine 1988 durchgeführte Prüfung des Staatsschutzes (vgl. meinen 11. Jahresbericht, Seite 57 ff.) hatte ich dem Senator für Inneres einen Prüfbericht zugeleitet und die darin festgestellten Mängel der Bearbeitung personenbezogener Daten in APIS gem. § 29 BrDSG beanstandet und zum Ausdruck gebracht, daß ich erwarte, daß unter Berücksichtigung meiner Empfehlungen ein DV-Konzept erarbeitet wird, das dann mit mir abgestimmt wird. Weil sich bis Dezember 1989 nichts bewegt hat, habe ich den Senator für Inneres noch einmal auf die folgenden Problembereiche hingewiesen:

- Erneut habe ich die Löschung der im Prüfbericht genau bezeichneten personenbezogenen Daten in APIS verlangt, denn solange mir eine Löschung nicht angezeigt wird, muß ich davon ausgehen, daß die rechtswidrigen Speicherungen in APIS aufrechterhalten werden.

- Auch eine Überprüfung der übrigen, nicht von mir geprüften Speicherungen in APIS anhand der von mir genannten Kriterien und die Löschung bei vergleichbaren Fällen minderer Schwere hat bisher nicht stattgefunden. In Hamburg wurde ebenfalls eine APIS-Prüfung durchgeführt, mit dem Ergebnis, daß sämtliche Datenbestände in APIS von einer Arbeitsgruppe durchgeforstet wurden. Die Überprüfung in Hamburg ist fast abgeschlossen, ca. 2/3 der in APIS von Hamburg gespeicherten Datensätze sind gelöscht worden. Im Lande Bremen hingegen ist mit dieser Arbeit noch nicht einmal begonnen worden.

- Bisher wurde jedenfalls keine Änderungen eingeleitet, so daß APIS weiterhin als Nachweissystem für alle Fälle genutzt wird und somit auch die neuen Fälle uneingeschränkt in APIS eingespeichert werden. Abgesehen davon, daß eine anerkannt rechtswidrige Praxis damit perpetuiert wird, erhöht sich die Zahl der zu überprüfenden und umzusetzenden Fälle um ein Vielfaches.

— Die Frage der organisatorischen Trennung der Daten, die vom Landeskriminalamt verarbeitet werden dürfen und der Daten, die die Kommissariate benötigen, ist weiterhin offen.

Erst nachdem der Datenschutzausschuß in seinem Bericht zu meinem 11. Jahresbericht die Entflechtung von APIS-Verbunddateien und Aktennachweissystem für erforderlich gehalten hat und den Senat aufgefordert hat, die Verhältnismäßigkeit bei der Speicherung von verdächtigen und unverdächtigen Personen zu beachten, hat der Senator für Inneres sich bereiterklärt, im Februar 1990 über die Punkte ein Gespräch zu führen.

2.2.2.3 Fortentwicklung der polizeilichen Datenverarbeitung in Bremerhaven und Bremen

1984 wurde das Informationssystem Anzeigen (ISA) das vom Stadt- und Polizeiamt in Bremen und der Ortspolizeibehörde in Bremerhaven genutzt wird als zentrales Datenverarbeitungssystem errichtet. Dieses System soll modernisiert, erweitert und einer Vielzahl von Benutzern zugänglich gemacht sowie mit anderen Informationssystemen verknüpft werden.

In meinem letzten Jahresbericht (vgl. Punkt 5.2.1.1, Seite 54 ff.) habe ich über die Planungen der Ortspolizeibehörde Bremerhaven berichtet, durch die Einführung neuer Technologien eine integrierte Kommunikation polizeilicher und anderer Informationsysteme herzustellen und den dezentralen Zugriff auf verschiedene Informationssysteme zu ermöglichen. ISA soll Bestandteil dieser neuen Technologie sein. Nachdem ich datenschutzrechtliche Bedenken geäußert hatte, wurde sowohl von Seiten des Senators für Inneres als auch von der Ortspolizeibehörde Bremerhaven erklärt, daß diese neuen Technologien erst dann zum Einsatz kämen, wenn die rechtlichen Grundlagen hierfür geschaffen worden seien. Die Ortspolizeibehörde Bremerhaven hat nunmehr zur Umsetzung der Pläne die Geräte beschafft und befindet sich hinsichtlich des Telex-Fernschreibsystems in der Erprobung. Weitere polizeiliche Informationssysteme sind derzeit nicht Bestandteil des Systems.

In Bremen mußte ich bis zum Juni 1989 davon ausgehen, daß sämtliche Überlegungen zur Dezentralisierung von ISA zurückgestellt worden sind. Erst aufgrund eines ADV-Antrages des Stadt- und Polizeiamtes zur Umstellung von ISA auf eine relationale Datenbank wurde deutlich, daß ein Projekt ISA-Dezentral (ISA-D) bereits konkret ausgearbeitet war. Zur Begründung der Notwendigkeit der Umstellung wurde neben den verbesserten Zugriffsmöglichkeiten auch darauf hingewiesen, daß diese als Voraussetzung für die anstehende Dezentralisierung notwendig sei. Ich hatte zu der geplanten Umstellung datenschutzrechtliche Bedenken geäußert und um weitere Unterrichtung gebeten und ging davon aus, daß ich begleitend zu der dort genannten Projektphase (1990 bis 1992) die Möglichkeit habe, datenschutzrechtliche Anforderungen anzubringen.

Der Senat hat mit Beschluß vom 24. Oktober 1989 das geplante DV-Projekt ISA-D zustimmend zur Kenntnis genommen. Vor der Entscheidung des Senats wurde die Vorlage mit den Zenralressorts, der Senatskanzlei, dem Senator für Finanzen und der Senatskommission für das Personalwesen abgestimmt. Ich wurde nicht beteiligt, auch nicht in ausreichendem Maße von dem Vorhaben in Kenntnis gesetzt. Erst auf mehrfache Anforderung wurden mir Ende Januar 1990 Senatsvorlage und Beschluß zur Kenntnis gegeben, obwohl ich gem. § 27 Abs. 4 BrDSG „über Planungen zum Aufbau automatisierter Informationssysteme **rechtzeitig** zu unterrichten" bin. Dieser Unterrichtungspflicht wird nicht dadurch genügt, daß ich nach der Herbeiführung des Systementscheides in Überlegungen zu einem Datenschutzkonzept einbezogen werde. Gerade in einem so sensiblen Bereich wie der polizeilichen Datenverarbeitung erwarte ich eine rechtzeitige Unterrichtung über den jeweiligen Planungsstand.

Aus der Senatsvorlage wird folgende Entwicklung deutlich: Wie bereits bei dem in Bremerhaven geplanten Verfahren ist auch in Bremen die Integration der Informationssysteme ISA, DEMOS (Einwohnermeldedatei), FAZID (Kfz.-Halterdatei der Stadtgemeinde Bremen), INPOL (Fahndungsdatei des Bundes), ZEVIS (Zentrales Informationssystem des Kraftfahrtbundesamtes in Flensburg) sowie AZR (Ausländerzentralregister beim Bundesverwaltungsamt in Köln) vorgesehen. Geplant ist ausdrücklich der „flächendeckende Einsatz von PC's". In einer ersten Phase sollen alle Organisationseinheiten mit PC-Netzen ausgestattet werden. Die Zugriffe auf die Dateien sollen als „Standardauskünfte" erfolgen. Die Standardauskünfte sollen

nach Vorstellung des Innensenators selbst als integriertes System gestaltet werden, d. h. die aus den Datensammlungen bereitzustellenden Informationen sind in ein einheitliches Erscheinungsbild umzusetzen und sollen in einer einheitlichen Dialogstruktur zusammengefaßt werden. Dieses integrierte Auskunftssystem soll in ein Informationssystem eingebettet werden, das allen polizeilichen Ebenen bis hin zu den Polizeirevieren geöffnet werden soll.

Schon jetzt läßt sich hierzu sagen, daß der Senator für Inneres eine umfangreiche Erweiterung, Vernetzung und Integration der Datenverarbeitung vorsieht, obwohl die rechtlichen Grundlagen hierfür bisher nicht bestehen und zum Teil vom Landesgesetzgeber auch nicht erlassen werden können.

Grundlage für die Entwicklung soll eine Kommunikationsanalyse werden, die durch eine Fremdfirma beim Stadt- und Polizeiamt vorgenommen wird. Meinem Vorschlag, in die Ausschreibung zu dieser Kommunikationsanalyse auch datenschutzrechtliche Anforderungen einzubeziehen, wurde aus Kostengründen nicht entsprochen. Mittlerweile hat mir das Stadt- und Polizeiamt angeboten, bei der Erstellung eines Datenschutzkonzeptes mitzuwirken. Damit ist ein ganz wesentlicher Teil datenschutzgestaltender Möglichkeiten bereits ohne meine Beteiligung entschieden worden. Mir wird damit lediglich angeboten, unter von mir selbst nicht mehr zu beinflussenden Vorgaben, bei der Gestaltung eines kleinen Ausschnitts mitzuwirken. Diese Vorgehensweise wird der Intention des § 27 Abs. 4 BrDSG nicht gerecht. Das Ziel dieser Regelung ist, daß es nicht ausreicht, wenn ich eine bereits getroffene Entscheidung aus datenschutzrechtlichen Gründen beanstande, vielmehr war es Wunsch des Gesetzgebers, bereits in die Planungsphase von Datenverarbeitungssystemen die Datenschutzbelange mit einfließen zu lassen.

2.2.2.4 Erkennungsdienst und Lichtbildervorzeigekartei

Ein Beschwerdeführer trug vor, er sei von einer Bekannten angerufen worden mit der Bemerkung, was er denn für ein „Schwerverbrecher" sei, ihr sei aufgrund eines Handtaschenraubes als Zeugin das so wörtlich „Verbrecheralbum" vorgelegt worden und sie habe ihn dort erkannt. Der Beschwerdeführer war sehr empört, er sei bisher erst einmal „mit dem Gesetz in Berührung gekommen"; vor drei Jahren sei wegen schwerer Brandstiftung gegen ihn ermittelt worden, das Verfahren sei aber längst eingestellt worden.

Aufgrund dieser Eingabe habe ich mich entschlossen, das Verfahren der erkennungsdienstlichen Behandlung (ED) und die damit in Verbindung stehenden Datenverarbeitungsvorgänge zu überprüfen. Die Richtigkeit der Angaben des Beschwerdeführers fand ich bestätigt und habe die Entfernung des Lichtbildes aus der Vorzeigekartei verlangt.

Die Prüfung hat folgendes ergeben: Die erkennungsdienstliche Behandlung umfaßt in der Regel eine fotografische Aufnahme der Person von drei Seiten sowie die Abnahme eines Zehn-Finger-Abdrucks. Die erkennungsdienstliche Maßnahme kann zur Identitätsfeststellung gem. § 11 Abs. 2 Nr. 7 Bremisches Polizeigesetz, oder nach anderen spezialrechtlichen Vorschriften insbesondere aber nach § 81 b Strafprozeßordnung (StPO) für Maßnahmen der Strafverfolgung angeordnet werden. Die nach diesen Vorschriften gewonnenen Lichtbilder werden in die sogenannte „ED-Kartei" eingestellt.

Meine Prüfung hat ergeben, daß ganz überwiegend eine ED-Behandlung nach der Vorschrift des § 81 b StPO erfolgt. Soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist, erlaubt diese Vorschrift, Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufzunehmen und Messungen und ähnliche Maßnahmen an ihm vorzunehmen. Von den hergestellten ED-Unterlagen gehen jeweils ein Zehn-Finger-Abdruckbogen sowie ein Lichtbildabzug an das Bundeskriminalamt (BKA). Die restlichen Unterlagen werden in der ED-Kartei abgelegt, soweit nicht besondere Anforderungen eine Weitergabe insbesondere an andere Polizeidienststellen erforderlich machen.

In der ED-Stelle selbst werden die Daten in verschiedenen Datensammlungen katalogisiert und kategorisiert.

Die Hauptsammlung stellt die ED-Karteikartensammlung dar, die in männlich und weiblich unterteilt und alphabetisch sortiert ist. Zum Zeitpunkt der Prüfung umfaßte sie ca. 106.000 in Bremen (Stadt) erkennungsdienstlich behandelte Bürger. Weitere Datensammlungen existieren im Bereich der Daktyloskopie.

Eine der in der ED-Stelle geführten Dateien ist die Lichtbilder-Vorzeigekartei (LVK), gegen die sich wie eingangs dargestellt die Beschwerde gerichtet hat.

Diese habe ich beim Stadt- und Polizeiamt stichprobenartig überprüft und Fälle aus den folgenden Bereichen herausgezogen:

- Stadtstreicher
- Prostituierte
- Frauen, Allgemeine Straftaten
- Frauen, Taschen-, Trick- und Ladendiebe
- Einbrecher, Diebe (männlich)
- außerdem habe ich aus der zu der Lichtbilder-Vorzeigekartei gehörenden Namensdatei eine Stichprobe gezogen und die dort erkannten Auffälligkeiten überprüft.

Anhand der Eintragungen in dem polizeilichen Informationssystem ISA (Informationssystem Anzeigen) und der beim Stadt- und Polizeiamt geführten Kriminalakten habe ich dann geprüft, inwieweit die Aufnahme dieser Personen in die Lichtbilder-Vorzeigekartei berechtigt bzw. die weitere Aufbewahrung noch berechtigt war.

Bei der Prüfung ist offen geblieben, wer die im einzelnen festgestellten Mängel verursacht hat. Fest steht, daß viele Fehler nicht von der ED-Stelle zu verantworten sind, ein großer Teil ist strukturell bedingt. Die Prüfung hat im einzelnen u. a. zu folgenden Ergebnissen geführt:

— Gliederung der Lichtbilder-Vorzeigekartei

Viele der gebildeten Gruppen halte ich unter rechtlichen Gesichtspunkten für problematisch. Ich habe Zweifel, ob die gebildeten Gruppen gerade unter Berücksichtigung der Prüfergebnisse von ihrer Anlage her geeignet sind, dem Grundsatz der Verhältnismäßigkeit, der auch im Rahmen der Gefahrenabwehr und der Strafverfolgung zu wahren ist, Rechnung zu tragen. Auch die mir zur Verfügung gestellten Richtlinien über die Führung der Lichtbilder-Vorzeigekartei sehen vor, daß die Kartei lediglich nach verschiedenen Deliktsgruppen zu unterteilen ist. Anknüpfungspunkte außerhalb von Deliktsgruppen, etwa wie der soziale Status, halte ich für verfassungswidrig.

— Stadtstreicher

Die Einteilung „Stadtstreicher" bei der Lichtbilder-Vorzeigekartei stellt eine Kategorie dar, die dem von der Verfassung geprägten Begriff der Menschenwürde (Art. 1 Abs. 1 GG) nicht Rechnung trägt. Durch die Eingruppierung als Stadtstreicher werden diese Personen in besonderer Weise gebrandmarkt. Im übrigen mag der Begriff des Stadtstreichers im allgemeinen preußischen Landrecht seinen Platz gehabt haben, die moderne Rechtssprache kennt ihn nicht mehr.

Darüber hinaus legen die Ergebnisse meiner Prüfung nahe, die unter dieser Kategorie verwalteten Personen — soweit überhaupt — im Bereich der Deliktsgruppe „Diebstahl" einzuordnen, da ich überwiegend in ISA Speicherungen des Delikts Ladendiebstahl festgestellt habe.

Im einzelnen: Von sechs geprüften Fällen wurden drei aufgrund meiner Prüfung sofort gelöscht, eine weitere Person war bereits 1988 gestorben.

— Prostituierte

Aus der Lichtbilder-Vorzeigekartei habe ich zu dieser Personengruppe eine Stichprobe von sechs Vorgängen gezogen. Für alle Vorgänge habe ich die Aussonderung aus der Lichtbilder-Vorzeigekartei verlangt. So z. B. weil weder in ISA noch in der Kriminalakte ein Delikt im Zusammenhang mit Prostitution vermerkt war. In fünf Fällen habe ich darüber hinaus die Vernichtung der ED-Unterlagen verlangt, weil entweder die Person weder in ISA noch in einer Kriminalakte gespeichert war oder anläßlich meiner Prüfung festgestellt wurde, daß der Vorgang in ISA zu löschen war.

Im übrigen hatte ich erwartet, daß die geprüften Personen Delikte anläßlich der Ausübung der Prostitution begangen hätten. Bei den geprüften Vorgängen habe ich keinen Anhaltspunkt dafür gefunden, daß die in der Lichtbilder-Vorzeigekartei gespeicherten Personen solche Delikte begangen haben. Nur in einem einzigen Fall konnte ich feststellen, daß einer Person der Vorwurf der unerlaubten

Prostitution (§ 184 a StGB) gemacht wurde. Dieser Fall stammte aus dem Jahre 1982, der Ausgang des gerichtlichen Verfahrens war nicht bekannt. Auch wenn es sich bei der Stichprobe nur um eine kleine Auswahl handelt, habe ich mich des Eindrucks nicht erwehren können, daß es hier darum geht, Prostituierte soweit sie in irgendeiner Weise polizeilich auffällig werden, möglichst vollständig zu katalogisieren.

— Frauen, Allgemeine Straftaten

Die Stichprobe bezog sich auf 21 Frauen, die in den Jahren 1984 bis 1989 erkennungsdienstlich behandelt worden sind. Dabei bezog sich 2/3 der Stichprobe auf die Altersgruppe der bis 18jährigen, 1/3 auf die Altersgruppe der 1936 und früher geborenen Frauen. Acht der Vorgänge waren nicht zu beanstanden, einer ist aufklärungsbedürftig. In weiteren acht Fällen habe ich die Aussonderung aus der Lichtbilder-Vorzeigekartei verlangt, in zwei Fällen darüber hinaus die Löschung aus der ED-Datei, zwei Fälle wurden anläßlich der Prüfung in ISA gelöscht, so daß auch diese Fälle sowohl aus der Lichtbilder-Vorzeigekartei wie aus der ED-Datei zu löschen sind. Gravierende Fälle stellen die ED-Behandlung und Aufbewahrung in der Lichtbilder-Vorzeigekartei einer 13jährigen dar, die seit fünf Jahren nicht mehr in strafrechtlicher Weise in Erscheinung getreten ist und die Aufbewahrung des Bildes eines 1987 im Alter von 12 Jahren ED-behandelten Mädchens in der Lichtbilder-Vorzeigekartei, obwohl in ISA zu dieser Person kein Hinweis über irgendeine Straftat gespeichert war. In beiden Fällen handelt es sich um die erkennungsdienstliche Behandlung von Kindern. Kinder sind schuldunfähig (§ 19 StGB) und können nicht Beschuldigte sein. Eine erkennungsdienstliche Behandlung für die Zwecke der Durchführung eines Strafverfahrens scheidet aus. Im übrigen hat bei Kindern schon nach den KpS-Richtlinien „spätestens nach zwei Jahren" eine Aussonderungsprüfung stattzufinden.

Im übrigen habe ich die Aussonderung aus der Lichtbilder-Vorzeigekartei in den Fällen gefordert, in denen die Jugendlichen über einen langen Zeitraum strafrechtlich nicht mehr in Erscheinung getreten sind und somit eine Wiederholungsgefahr nicht angenommen werden kann. Gerade in diesem Bereich muß der besonderen Entwicklung von Jugendlichen Rechnung getragen werden. Außerdem ist zu erwarten, daß sich das Äußere der Betroffenen z. B. nach fünf Jahren soweit verändert haben dürfte, daß ein Wiedererkennen in vielen Fällen nicht mehr gegeben ist. Dies entspricht im übrigen auch den Richtlinien, wonach Jugendliche spätestens nach fünf Jahren auszusondern sind.

In einem weiteren Fall ist eine 60jährige aufgrund eines Mordfalles ED-behandelt worden. Laut ISA-Eintrag und Kriminalakte ist die Betroffene in diesem Fall lediglich als Zeugin vernommen worden. Es ist davon auszugehen, daß die Lichtbilder dieser Person seit fünf Jahren mit den Bildern anderer Straftäter zusammen mit der Lichtbilder-Vorzeigekartei wiederum Zeugen vorgelegt wird. Ich habe die Überprüfung der Fakten und ggf. die Löschung verlangt.

— Frauen, Taschen-, Trick- und Ladendiebstahl

Aus einer Stichprobe von sechs Personen habe ich die Überprüfung und Aussonderung aus der Lichtbilder-Vorzeigekartei von vier Personen empfohlen. U. a. habe ich die Aussonderung der Lichtbilder einer Frau empfohlen, die zwar 1985 mehrere Diebstähle begangen hat, danach aber nicht mehr in Erscheinung getreten ist und zu der vermerkt war, daß sie „nach Polen zurückgekehrt sei".

— Einbrecher, Diebe (männlich)

Aus einer Stichprobe von 11 Personen habe ich empfohlen sechs Personen aus der Lichtbilder-Vorzeigekartei auszusondern. In drei dieser Fälle habe ich darüber hinaus verlangt, auch die ED-Unterlagen zu vernichten, so konnte ich in einem Fall den Betroffenen nur als Geschädigten im ISA-Bestand feststellen. Er war also Opfer einer Straftat.

— LVK-Namenskartei

Zu der Lichtbilder-Vorzeigekartei gehört eine Namenskartei mit der sich die einzelnen Lichtbilder dem Personendatensatz zuordnen lassen. Die Namenskartei wird manuell geführt, die daraus gezogene Stichprobe wurde auf erkennbare Auffälligkeiten hin überprüft. So war dort vermerkt „Homosexuell", obwohl weder in ISA noch in der Kriminalakte sich deliktische homosexuelle Handlungen ergaben. In einem anderen Fall war laut Vermerk auf der LVK-Namenskartei der Betroffene im Jahre 1985 verstorben. Ein ISA-Eintrag konnte zu dem Betroffenen nicht fest-

gestellt werden. In einem Fall war auf der LVK-Namenskartei vermerkt „DDR-Straftäter". Zu dem Betroffenen konnte kein Eintrag in ISA festgestellt werden. Ich habe daher in allen Fällen die Löschung verlangt.

Im Zuge der Überprüfung der LVK-Namenskartei am ISA-Bestand bin ich auch auf andere Skurilitäten gestoßen, so fand ich zu einem 60jährigen die Deliktsbezeichnung „Jugendarrest" vermerkt. In einem anderen Fall war der Sondervermerk „Achtung Tageseinbrecher, polnische Zigeunerin" eingetragen. In beiden Fällen habe ich eine Überprüfung bzw. Löschung verlangt.

Zusammenfassendes Ergebnis

Allgemein ist zu begrüßen, daß meinen früher geäußerten Anregungen Rechnung getragen wurde und sowohl die Ausgabe als auch für den Verbleib von Lichtbildern ein geordnetes Verfahren eingeführt worden ist.

Neben der Aufbewahrung in der ED-Kartei (Hauptdatei) stellt die Aufbewahrung in der Lichtbilder-Vorzeigekartei einen weiteren schweren Eingriff in das Recht auf informationelle Selbstbestimmung dar, weil die Bilder im Laufe der Jahre vielen Zeugen und Geschädigten gezeigt werden. Eine Einordnung in die Lichtbilder-Vorzeigekartei kann daher nur in schwerwiegenden Fällen und bei „Wiederholungsgefahr" zulässig sein. Das Einordnungskriterium der Wiederholungsgefahr ist daher streng zu prüfen.

Die Prüfung hat bei einer Mehrzahl (38 von 55) der herangezogenen Fälle ergeben, daß die Aufbewahrung dieser Lichtbilder in der Lichtbilder-Vorzeigekartei datenschutzrechtlich sehr bedenklich oder gar unzulässig ist. Eine Durchforstung der Bestände der gesamten Lichtbilder-Vorzeigekartei ist dringend geboten. Eine Bereinigung hätte darüber hinaus den Effekt, daß die polizeiliche Arbeit effizienter gestaltet werden könnte.

Aufgrund der Prüfung komme ich weiter zu dem Ergebnis, daß die vom Senator für Inneres mit Wirkung vom 1. März 1984 erlassenen Richtlinien hinsichtlich der Löschungsprüfung der Lichtbilder-Vorzeigekartei nicht ausreichend sind. Hier sind kürzere Prüfroutinen und einschränkendere Kriterien zu formulieren. Der Verweis auf KpS-Fristen reicht nicht aus.

Bei der Einordnung des Lichtbildes in die Vorzeigekartei aufgrund des in den Richtlinien vorgesehenen Merkmals „dringender Tatverdacht" ist spätestens aufgrund des Verfahrensausganges die Entscheidung der Aufnahmen in die Lichtbilder-Vorzeigekartei zu überprüfen.

Zu Korrekturen sollte es auch bei der Speicherung jugendlicher Straftäter in der Lichtbilder-Vorzeigekartei kommen. Die vorgesehene Speicherdauer von fünf Jahren ohne Überprüfung der Entscheidung erscheint zu lang.

Die geprüften Fälle zeigen, daß die zur Einordnung bestimmten Kategorien zu unspezifisch sind. Insoweit sollte geprüft werden, ob nicht an die Einteilung des Strafgesetzbuches im besonderen Teil (28 Abschnitte) angeknüpft werden kann. Dabei ist insbesondere herauszuarbeiten, für welchen Deliktsbereich die Vorlage von Lichtbildern in Frage kommen kann.

Ein großer Teil der festgestellten Mängel ist strukturell bedingt. Insoweit bedarf es einer Umstellung des Verfahrens. Da die Realisierungsmöglichkeiten von den Gegebenheiten vor Ort abhängen, verzichte ich an dieser Stelle auf eine Darstellung von Lösungsmöglichkeiten.

Ich habe die bei der Prüfung festgestellten Mängel der Lichtbilder-Vorzeigekartei gegenüber dem Senator für Inneres gem. § 29 BrDSG beanstandet. Da bei einer Umstellung des Verfahrens aufgrund der geltenden KpS-Richtlinien frühestens in zehn Jahren mit einer auf rechtmäßiger Basis geführten Lichtbilder-Vorzeigekartei gerechnet werden könnte, gehe ich davon aus, daß meine Beanstandung zum Anlaß genommen wird, umgehend mit der systematischen Prüfung aller Speicherungen in der Lichtbilder-Vorzeigekartei zu beginnen.

Die große Anzahl der Personen, die in Bremen (Stadt) ED-behandelt und gespeichert sind (jeder fünfte Bürger), läßt mich zweifeln, ob die Maßnahme der ED-Behandlung unter Beachtung des Grundsatzes der Verhältnismäßigkeit und immer unter Beachtung der rechtlichen Voraussetzungen angeordnet und durchgeführt wurde. Die Prüfergebnisse bei der Lichtbilder-Vorzeigekartei geben mir Anlaß, in weiteren Bereichen der ED-Stelle die Prüfung fortzusetzen.

2.2.2.5 Funde polizeilicher Unterlagen in der Öffentlichkeit

1988 wurden in kurzen Abständen an verschiedenen Orten in Bremen polizeiliche Unterlagen von Privatpersonen gefunden, so z. B. eine Sammlung von rund 100 erkennungsdienstlichen Unterlagen. Die Vorgänge, die auch von den Medien aufgegriffen wurden, hatte ich bereits in meinem letzten Jahresbericht dargestellt und zum Anlaß genommen, Richtlinien über den Umgang mit geschützten Daten und deren Entsorgung (RiDat) (11. Jahresbericht, Seite 53 f.) zu verlangen. Das Stadt- und Polizeiamt Bremen hat daraufhin Richtlinien in Zusammenwirken mit meiner Dienststelle entworfen und dem Senator für Inneres zugeleitet. Bis heute, fast 1½ Jahre nach diesen Vorgängen, ist es dem Senator für Inneres nicht gelungen, diesen Bereich durch Richtlinien für Bremen und Bremerhaven einheitlich zu regeln.

2.2.3 Meldewesen

Das Meldewesen entwickelt sich immer mehr zu einem allgemeinen Informationssystem für die verschiedenen kommunalen und staatlichen Ämter und Behörden und für private Stellen und Personen. Vor allem die zunehmende Automatisierung der kommunalen Melderegister mit ihren neuartigen Abgleichs- und Verknüpfungsmöglichkeiten und den schnellen Aufbereitungs- und Übertragungsmöglichkeiten treibt diese Entwicklung voran. Standen früher im Melderecht die eigenständigen Ordnungs- und Nachweisaufgaben der Meldebehörden (Registrierung der Einwohner, Erteilung von Bescheinigungen und von Melderegisterauskünften im Einzelfall) im Vordergrund, so rücken heute die von den Meldebehörden der Einfachheit halber miterledigten Annexaufgaben (z. B. Ausstellen von Lohnsteuerkarten, Mitwirkung bei der Vorbereitung von Wahlen, Mitwirkung bei Paß- und Personalausweisangelegenheiten, bei der Wehr- oder Zivildienstüberwachung) und die Auskunfts- und Informationstätigkeit immer mehr ins Zentrum der meldebehördlichen Aufgabenstellung.

Vor dem Hintergrund dieser Entwicklung erlangen die im Melderecht verankerten Meldepflichten des Einwohners und eventuell Dritter eine neue Qualität. Ich bin der Auffassung, daß die Melde- und Nebenmeldepflichten als zwangsweise und bußgeldbewehrte Informationseingriffe einer öffentlichen Stelle grundlegend neu überdacht und hinsichtlich des überwiegenden Allgemeininteresses, des Verhältnismäßigkeitsprinzips und des rechtsstaatlichen Gebots der Normenklarheit neu gewichtet und inhaltlich präzisiert werden müssen. Ein Bürger muß wissen und überschauen können, daß er beispielsweise bei einer An- oder Ummeldung gleichzeitig (wegen der automatisch angestoßenen Mitteilungsdienste oder regelmäßig ablaufender Datenabgleiche oder der automatisierten Meldedatenabrufe) auch eine Vielzahl anderer Datenbestände von Behörden und — technisch denkbar — von privaten Stellen aktualisiert. Das, was der Rechtsausschuß des Deutschen Bundestages seinerzeit mit seinen verfassungsrechtlichen Bedenken hinsichtlich des individuellen Personenkennzeichens ausschließen wollte, nämlich ein bundesweit und mit vielen anderen Aufgaben — und Funktionsbereichen verzahntes integriertes Melderegister, schleicht sich jetzt durch die Hintertür der neuen informationstechnischen Entwicklung und des Bedeutungswandels der meldebehördlichen Aufgaben wieder ein.

Am Beispiel des Melderechtsrahmengesetzes und der Bremischen Meldedatenübermittlungsverordnung läßt sich dies deutlich machen:

Bereits im letzten Tätigkeitsbericht hatte ich über die anstehende **Novellierung des Melderechtsrahmengesetzes** (Punkt 5.2.2.1) berichtet. Inzwischen liegt dem Bundestag ein Gesetzentwurf zur Änderung des Melderechtsrahmengesetzes vor. Die erste Lesung dieses Gesetzentwurfs war Anfang Dezember 1989; es kann davon ausgegangen werden, daß dieser Gesetzentwurf noch in dieser Legislaturperiode des Deutschen Bundestages abschließend beraten und verabschiedet werden wird. Eine Änderung, die Aufgaben und Befugnisse der Meldebehörden betreffend, ist in diesem Zusammenhang von besonderer Bedeutung, macht sie doch den oben geschilderten Bedeutungswandel des Melderegisters und der Aufgaben der Meldebehörden besonders deutlich. § 1 Abs. 1 Melderechtsrahmengesetz, der die Aufgaben und Befugnisse der Meldebehörden regelt, soll einen zusätzlichen Satz erhalten: „Sie (die Meldebehörden) erteilen Melderegisterauskünfte, wirken bei der Durchführung von Aufgaben anderer Behörden oder sonstiger öffentlicher Stellen mit und übermitteln Daten".

Schon im letzten Tätigkeitsbericht hatte ich darauf hingewiesen, daß diese neue Regelung zwar deutlicher als bisher die tatsächlichen Tätigkeiten der Melde-

behörden beschreibt, daß aber dennoch Präzisierungen und Eingrenzungen dahingehend notwendig sind, für welche Aufgaben bzw. Behörden und öffentliche Stellen Mitwirkungspflichten bestehen, welcher Art diese Mitwirkung ist und wo die Grenze dieser Mitwirkung liegt. Es ist nach meiner Auffassung nicht hinnehmbar, daß der Meldebehörde ein allgemeines Mitwirkungsrecht bei der Erfüllung von Aufgaben anderer Behörden und sonstiger Stellen zugewiesen bzw. eingeräumt wird, ohne dies näher zu präzisieren. Wenn diese Regelung so Gesetzeskraft erlangt und von den Ländern — wie es bereits unisono im Bundesrat geäußert wurde — unverändert in die Landesmeldegesetze übernommen wird, dann gibt es von der Ausgestaltung des Melderechts her kaum noch Möglichkeiten, den technologischen Trend zur integrierten Informationsverarbeitung der Verwaltung mit dem Melderegister als zentralem und über die Meldepflicht des Bürgers stets auf dem neuesten Stand gehaltenen Einwohnerdatenbestand aufzuhalten. Die Verzahnung und Integrierung der automatisierten Verfahren der Verwaltung erhalten durch diese Regelung weiteren Auftrieb.

Schon jetzt erhalten neben den Meldebehörden eine Vielzahl anderer öffentlicher Stellen des Bundes (z. B. Kreiswehrersatzämter, Bundesanstalt für Arbeit, Rentendienst der Deutschen Bundespost, Datenstelle der Rentenversicherungsträger) sowie eine Vielzahl von Landes- und Kommunalbehörden (innerhalb des Landes Bremen z. B. Finanzämter, Landeshauptkasse und Stadtkasse Bremerhaven, Kfz.-Zulassungsstellen, Schutz- und Kriminalpolizei, Standesämter, Ausländerbehörden, Schulverwaltung, Versorgungsamt Bremen, Jugendamt Bremen, Gesundheitsämter, für Wohnungswesen und Bauförderung zuständige Ämter, statistische Ämter in Bremen und Bremerhaven, Bauordnungsamt Bremen, Senatskanzlei und Magistrat Bremerhaven) regelmäßig für bestimmte Zwecke Meldedaten übermittelt, wobei die Übermittlung dabei entweder in schriftlicher bzw. in listenmäßiger Form, in Form des Datenträgeraustausches (Austausch von Magnetbändern, Disketten oder Magnetbandkassetten), in Form des Direktabrufs/Online-Zugriffs oder in Form des Datenabgleichs erfolgt. Vor allem letztere (Direktabruf/Online-Zugriff und Datenabgleich) üben auf viele Verwaltungen einen großen Anreiz aus. Das zeigt besonders plastisch die Diskussion um die Änderung der Bremischen Meldedatenübermittlungsverordnung.

Im März des vergangenen Jahres erhielt ich vom Senator für Inneres den **Entwurf zur Änderung der Bremischen Meldedatenübermittlungsverordnung,** in dem neben einigen redaktionellen sowie weniger bedeutsamen inhaltlichen Änderungen vor allem die erhebliche Ausweitung der Stellen auffiel, die Online selbst an das Bremer bzw. Bremerhavener Melderegister angeschlossen werden wollten. Es handelte sich hierbei im wesentlichen um die Bußgeldstellen der beiden Stadtgemeinden, die Gewerbemeldestelle Bremen und die Staatsanwaltschaft Bremen. Diesen zusätzlichen Wünschen auf Einrichtung von Online-Anschlüssen an die bremischen Melderegister habe ich in meiner Stellungnahme entschieden widersprochen. Das tragende Argument in diesem Zusammenhang war der Hinweis, daß in den Fachgesetzen der jeweiligen Stellen bzw. Behörden spezifische Datenschutzregelungen fehlen und diese durch die Meldedatenübermittlungsverordnung selbst nicht geschaffen werden können. Dem Erfordernis des § 30 Abs. 4 Bremisches Meldegesetz (§ 18 Abs. 4 Melderechtsrahmengesetz) wird nicht Rechnung getragen, wonach regelmäßige Datenübermittlungen an andere Behörden oder öffentliche Stellen nur zulässig sind, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Im Verlauf der Diskussion wurden die neuen Tatbestände zur Einrichtung von Online-Anschlüssen an die Bremischen Melderegister zunächst aus dem Verordnungsentwurf herausgenommen. Der reduzierte Verordnungsentwurf wurde im September 1989 in der Innendeputation beraten; meinen verbliebenen Bedenken und Anregungen wurde dabei nur zum Teil entsprochen. Im Oktober 1989 trat die Änderungsverordnung der Meldedatenübermittlungsverordnung in Kraft.

Im November 1989 erhielt ich vom Senator für Inneres einen weiteren Entwurf zur Änderung der Meldedatenübermittlungsverordnung, der im wesentlichen die vorher ausgeklammerten bzw. zurückgestellten Online-Anschlüsse an die Melderegister zum Inhalt hat. Eine weitere Behörde, die Führerscheinstelle Bremerhaven, war als Interessent für den Online-Anschluß an das Melderegister Bremerhavens hinzugekommen. In meiner Stellungnahme zu diesem neuerlichen Änderungsentwurf habe ich Anfang Dezember 1989 unter anderem folgendes ausgeführt:

Die regelmäßige Übermittlung von Meldedaten an andere Behörden stellt eine Einschränkung des Rechts auf informationelle Selbstbestimmung dar. Ein solcher

Grundrechtseingriff ist nur auf einer verfassungsmäßigen gesetzlichen Grundlage zulässig, aus der sich die Voraussetzungen und der Umfang der Grundrechtsbeschränkung klar und für den Bürger deutlich erkennbar ergeben müssen. Neben dem Gebot der Normenklarheit hat der Gesetzgeber bei seinen Regelungen auch das Verhältnismäßigkeitsprinzip zu beachten. Zwar braucht er nicht jedes Detail selbst zu regeln, doch muß er alle wesentlichen Voraussetzungen eines solchen Eingriffs festlegen. Nur im Rahmen dieser Vorgaben können der Verordnungsgeber oder die Verwaltung weitere Regelungen treffen.

§ 30 Abs. 4 Bremisches Meldegesetz läßt regelmäßige Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen zu, soweit dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist. Die Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden nach dieser Rechtsbestimmung ist durch Rechtsverordnung näher zu regeln; der Innensenator kann in einer solchen Rechtsverordnung Anlaß und Zweck der Übermittlungen, die Datenempfänger, die zu übermittelnden Daten und ihre Form festlegen. Eine fehlende Rechtsgrundlage zur Datenverarbeitung kann durch eine solche Meldedatenübermittlungsverordnung jedoch nicht geschaffen werden.

Trotz verfassungsrechtlicher Bedenken (bezüglich der Normenklarheit und der Verhältnismäßigkeit) akzeptiere ich jedoch im Grundsatz die Auffassung des Innensenators, daß § 30 Abs. 4 Bremisches Meldegesetz und die auf § 36 Abs. 2 Nr. 2 gestützte Meldedatenübermittlungsverordnung als Konkretisierung dieser Melderechtsbestimmung eine ausreichende gesetzliche Grundlage für die Einrichtung von Direktabrufverfahren aus dem Melderegister darstellen. Hinsichtlich der Frage, ob das Bremische Datenschutzgesetz fehlendes spezifisches Datenschutzrecht beim Datenempfänger ersetzen kann, bleibe ich bei meiner Auffassung, daß dies bei dieser Art der Datenverarbeitung grundsätzlich nicht möglich ist. Auch der Datenempfänger muß für seine Datenverarbeitung präzise und normenklare spezifische Rechtsgrundlagen haben. Das Bremische Datenschutzgesetz als Auffangrecht, das auch die Datenerhebung in seinen Anwendungsbereich einbezieht, kann automatisierte Abrufe aus dem Melderegister nicht als regelmäßige Datenerhebungsvorgänge durch den jeweiligen Datenempfänger rechtfertigen. Vielmehr führt die konsequente Anwendung der Regelungen im Bremischen Datenschutzgesetz (vgl. § 10 Abs. 2 BrDSG) zu dem Ergebnis, daß ohne eine ausdrückliche gesetzliche Regelung keine der geplanten automatisierten Abrufverfahren zugelassen werden kann.

Nicht zuletzt wegen der fehlenden Abschottung der Datenverarbeitung zwischen Teilen der Verwaltung sowie fehlender Regelungen zum Schutz der erhobenen Daten gegen Zweckentfremdung durch ihre Weitergabe und Weiterverwertung hatte das Bundesverfassungsgericht seinerzeit das Volkszählungsgesetz 1983 in Teilen für verfassungswidrig erklärt. Ökonomische Gesichtspunkte allein können kein hinreichender Grund dafür sein, verfassungsrechtlich garantierte Grundrechte — und hierzu zählt auch das Recht auf informationelle Selbstbestimmung — einzuschränken.

Die Innendeputation wird im Frühjahr 1990 über den neuen Entwurf zur Änderung der Meldedatenübermittlungsverordnung beraten. Ich hoffe, daß meinen erheblichen datenschutzrechtlichen Bedenken dabei Rechnung getragen wird.

2.2.4 Straßenverkehrsangelegenheiten

2.2.4.1 Einführung des Verfahrens „Verkehrsordnungswidrigkeiten" bei der Ortspolizeibehörde Bremerhaven

Die Ortspolizeibehörde Bremerhaven plante im Berichtsjahr die Einführung des ADV-Verfahrens „Verkehrsordnungswidrigkeiten". Das Verfahren war so konzipiert, daß mit ihm sämtliche für die Bearbeitung einer Verkehrsordnungswidrigkeit von der Bußgeldstelle zu erfüllenden Aufgaben erledigt werden können.

Datenschutzrechtliche Bedenken zu diesem DV-Verfahren ergaben sich für mich insbesondere daraus, daß das Konzept keine Datensicherungsmaßnahmen vorsah, wie sie nach § 6 BrDSG verlangt werden. Es fehlten insbesondere spezielle Zugriffssicherungsmaßnahmen gem. § 6 Abs. 2 Nr. 5 BrDSG. Nach dem mir vorgelegten Konzept sollte jeder Sachbearbeiter die Möglichkeit haben, von seinem Arbeitsplatz aus auf den gesamten OWI-Datenbestand zuzugreifen, somit auch auf Fälle und Daten, die er für die Erfüllung seiner Aufgaben gar nicht benötigt. Auch der generelle Zugriff auf frühere Ordnungswidrigkeiten eines Betroffenen sollte zugelassen sein, deren Kenntnis für den Sachbearbeiter nur dann notwendig ist,

wenn er diese für eine Ermessenentscheidung über die Höhe eines Bußgeldes benötigt. Aufgrund des Fehlens spezieller Zugriffsregelungen verlangte ich somit nach Sicherungsmaßnahmen im Rahmen des § 6 BrDSG. Nachdem ich mein Verlangen der Ortspolizeibehörde vorgetragen hatte, schloß sich diese meiner Auffassung an und traf entsprechde Maßnahmen.

Bedenken hatte ich auch hinsichtlich der im Verfahren „Verkehrsordnungswidrigkeiten" vorgesehenen Löschungsfristen. Nach § 20 Abs. 3 Nr. 2 BrDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernden Stelle zur rechtmäßigen Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Nach dem mir vorgelegten Konzept sollten die Auslagerungsfristen aber in Anlehnung an den Erlaß des Senators für Inneres zur Regelung der Aufbewahrungsfristen für Bußgeldakten vom 3. Februar 1986 generell 3 bzw. 5 Jahre betragen, je nach Höhe des verhängten Bußgeldes, was ich für viel zu lang halte. Ich meine, es ist nicht hinnehmbar, daß über Fälle, die bereits seit Jahren abgeschlossen sind, noch Daten gespeichert sind. Bleibt es bei der beabsichtigten Regelung, liegt für mich ein unverhältnismäßiger vom Gesetzgeber nicht geregelter Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen vor, der für mich so nicht hinnehmbar ist.

Wie sich die Ortspolizeibehörde in dieser Frage verhalten wird, hängt maßgeblich vom Ausgang einer Diskussion ab, die ich mit dem Senator für Inneres über die Änderung seines o. g. Erlasses führe (siehe hierzu auch Punkt 2.2.4.3 „Aufbewahrungsfristen von Verkehrsordnungswidrigkeiten-Unterlagen").

2.2.4.2 Einführung des Verfahrens „Führerscheine" bei der Ortspolizeibehörde Bremerhaven

Die Ortspolizeibehörde Bremerhaven beabsichtigt die Einführung eines Dialogsystems „Führerscheine", das ab April 1990 in Betrieb genommen werden soll. Beabsichtigt ist u. a. ein regelmäßiger Datenzugriff auf das Melderegister Bremerhaven und für Zeiten außerhalb der Arbeitszeit der Führerscheinstelle ein automatisierter direkter Zugriff der Vollzugspolizei auf die Daten der Führerscheinstelle. Datenschutzrechtliche Bedenken habe ich bei diesem Verfahren insbesondere wegen der geplanten Verknüpfung zu anderen DV-Verfahren und Stellen angemeldet.

Zu dem geplanten Datenzugriff auf das Melderegister habe ich der Ortspolizeibehörde mitgeteilt, daß ein solcher Zugriff unzulässig ist. Es gibt weder im Straßenverkehrsrecht noch derzeit im Bremischen Melderecht eine Rechtsgrundlage für einen Direktzugriff auf das Melderegister.

Nach den Bestimmungen des Straßenverkehrsrechts sind die für die Bearbeitung von Anträgen auf Erteilung einer Fahrerlaubnis zu erhebenden personenbezogenen Daten vielmehr direkt beim Betroffenen zu erheben. Der Antragsteller hat seine Identität nachzuweisen, was in der Regel durch die Vorlage eines gültigen Personalausweises geschieht. Sollte es in Einzelfällen dem Antragsteller nicht möglich sein, seine Identität nachzuweisen oder bestehen Zweifel an seinen Angaben, so kann die Führerscheinstelle jederzeit von der Möglichkeit § 30 Abs. 1 des Meldegesetzes Gebrauch machen und die Meldestelle um entsprechende Auskünfte bitten. Die Einrichtung eines Online-Zugriffs wäre für diese Fälle darüber hinaus weder erforderlich noch verhältnismäßig.

Wie bereits oben angeführt gibt es aber auch im Melderecht keine Grundlage für die Übermittlung von Meldedaten im Online-Verfahren an die Führerscheinstelle. Der Senator für Inneres beabsichtigt allerdings, durch Änderung der Meldedatenübermittlungsverordnung (MeldDÜV), eine Rechtsgrundlage zu schaffen. Gegen diese Erweiterung der MeldDÜV habe ich erhebliche Bedenken geltend gemacht; vgl. hierzu Punkt 2.2.3 dieses Berichts.

Auch für die geplante Zugriffsmöglichkeit der Vollzugspolizei zum automatisierten Führerscheinregister außerhalb der Dienstzeiten der Führerscheinstelle gibt es keine Rechtsgrundlage. Weder das StVG noch die StVZO, die hinsichtlich der Übermittlung von Daten der Fahrerlaubnisbehörden abschließende Regelungen treffen, sehen vor, daß die Führerscheinstelle der Vollzugspolizei Daten übermittelt. Das gilt auch für nicht automatisierte Verfahren.

Will die Vollzugspolizei überprüfen, ob der Fahrzeugführer eine Fahrerlaubnis besitzt, so kann sie dies für eine große Mehrheit der Fälle durch Nutzung der polizeilichen Informationssysteme (INPOL, ISA) und durch Anfrage beim zentralen Verkehrs-Informationssystem (ZEVIS) in Flensburg. In INPOL und ISA stehen der

Vollzugspolizei Informationen über gestohlene und verlorene Führerscheine, in ZEVIS über die Versagung und die Entziehung sowie den Verzicht auf eine Fahrerlaubnis während eines Entziehungsverfahren zur Verfügung.

Es verbleiben nur noch wenige Fälle, in denen die Vollzugspolizei die benötigten Informationen nicht aus diesen Informationssystemen erhalten kann, z. B., wenn der Fahrzeugführer eine Fahrerlaubnisprüfung nicht abgelegt hat. Für diesen kleinen Rest von Fällen hat die Vollzugspolizei immer die Möglichkeit, sich mit Einwilligung des Betroffenen an die Führerscheinstelle zu wenden. Die Einrichtung eines Online-Anschlusses zur Überprüfung dieser wenigen Fälle wäre unverhältnismäßig. Sie würde wegen der geringen Zahl auch dem haushaltsrechtlichen Grundsatz der Sparsamkeit der öffentlichen Verwaltung zuwiderlaufen. Ist die Führerscheinstelle außerhalb ihrer Dienstzeiten nicht erreichbar, so kann sich die Vollzugspolizei die Fahrerlaubnis nachträglich nachreichen lassen.

Bedenken habe ich auch gegen die geplanten bzw. getroffenen Datensicherungsmaßnahmen bei der Führerscheinstelle. Aus Platzgründen sollen zwei Räume im Dienstgebäude der Führerscheinstelle, in dem auch andere Organisationseinheiten der Ortspolizeibehörde untergebracht sind, als Aktenräume (Archiv) gemeinsam von der Führerschein- und Kfz.-Zulassungsstelle genutzt werden. Es mangelt nach meiner Auffassung hier an geeigneten Regelungen zur Vermeidung unberechtigter Zugriffe. Die Ortspolizeibehörde hat sich bereit erklärt, ihr Datensicherungskonzept zu überarbeiten.

Im übrigen fehlen im Grobkonzept Ausführungen zur Löschung.

2.2.4.3 Aufbewahrungsfristen von Verkehrsordnungswidrigkeitsunterlagen

Wie ich bereits zum Punkt 2.2.4.1 „Einführung des Verfahrens „Verkehrsordnungswidrigkeiten" bei der Ortspolizeibehörde Bremerhaven angeführt habe, betragen im Lande Bremen die Aufbewahrungsfristen für Bußgeldakten nach dem Erlaß des Senators für Inneres vom 3. Februar 1986 3 oder 5 Jahre, je nach Höhe des verhängten Bußgeldes. Ich halte dies aus datenschutzrechtlichen Gründen für viel zu lang. Gem. § 20 Abs. 3 Nr. 2 BrDSG, der hier anzuwenden ist, da es eine bereichsspezifische Rechtsgrundlage nicht gibt, dürfen personenbezogene Daten nur so lang gespeichert werden, wie dies für die speichernde Stelle zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Dies gilt gem. § 20 Abs. 4 BrDSG auch für Akten, soweit die Kenntnis des gesamten Akteninhalts zur Erfüllung der Aufgaben nicht mehr erforderlich ist. Bleiben personenbezogene Daten länger gespeichert bzw. werden Akten länger aufbewahrt, als dies nach den vorstehend genannten Rechtsvorschriften zulässig ist, so stellt dies einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar.

Der Senator für Inneres hält an der von ihm getroffenen Fristenregelung fest. Er begründet seine Auffassung gerade auch im Hinblick auf § 20 Abs. 3 Nr. 2 BrDSG damit, daß das für Widerspruchsentscheidungen bei Fahrerlaubnisentziehungen zuständige Referat seines Hauses die Bußgeldakten des Betroffenen zur Stützung seiner Widerspruchsentscheidungen benötige. Außerdem würde der Anhang zur Aktenordnung für die Behörden der Freien Hansestadt Bremen und Stadtgemeinde Bremen vom 12. August 1958 sowie die Verwaltungsvorschriften zur Landeshaushaltsordnung Nr. 21 Pkt. 1 zu § 79 der Landeshaushaltsordnung keine andere Fristenregelung zulassen.

Die Begründung des Senators für Inneres ist nicht überzeugend. Bußgeldakten sind zu vernichten, wenn die Widerspruchsentscheidung bestandskräftig geworden ist und der Betroffene gezahlt hat. Die Begründung, daß sich die Aufbewahrungsfristen nach dem Anhang zur Aktenordnung aus dem Jahre 1958 zu richten hätten, kann ebenfalls nicht dazu führen, daß die jetzigen Aufbewahrungsfristen beibehalten werden. Das aus der Rechtsprechung des Bundesverfassungsgericht hervorgegangene Grundrecht auf informationelle Selbstbestimmung verlangt nach einer bereichsspezifischen Regelung, die sich an den Vorgaben des Volkszählungsurteils aus dem Jahre 1983 zu orientieren hat. Die vor 32 Jahren erlassene Aktenordnung kann nicht mehr als Grundlage für die Regelung von Aufbewahrungsfristen für Akten mit personenbezogenem Inhalt herangezogen werden. Sie ist mit heutigem Recht nicht mehr vereinbar.

Dagegen, daß aus Rechnungsprüfungsgründen Rechnungsbelege für einen längeren Zeitraum aufbewahrt werden, habe ich keine Einwendungen. Für die Rechnungsprüfung reicht es aber in der Regel aus, wenn Belege über den Zahlungsgrund vorhanden sind. Diese Belege brauchen nicht in der Bußgeldakte, sondern

können von der für die Vereinnahmung des Bußgeldbetrages zuständigen Stelle gesondert aufbewahrt werden.

Ich habe meine Meinung zu der vom Senator für Inneres vorgebrachten Begründung für sein Festhalten an dem Erlaß zur Regelung der Aufbewahrungsfristen von Bußgeldakten mittlerweile diesem mitgeteilt. Eine Reaktion steht hier noch aus.

2.2.5 Amtliche Statistik

2.2.5.1 Landesstatistikgesetz

Im Berichtsjahr wurde der Entwurf eines neuen Landesstatistikgesetzes von der Bremischen Bürgerschaft (Landtag) beraten und beschlossen; im Juli 1989 wurde es verkündet, es trat am Tag nach seiner Verkündung in Kraft (am 21. Juli 1989).

Das Gesetz bringt neue und präzisere Regelungen für die Durchführung von Statistiken des Bundes, des Landes und der Kommunen sowie für die Durchführung sogenannter Geschäftsstatistiken öffentlicher Stellen und für das statistische Informationssystem des Landes (Statistische Datenbank). Ich war am Gesetzgebungsverfahren beteiligt, meine Anregungen wurden überwiegend aufgenommen. Lediglich der Punkt „Geschäftsstatistiken" muß noch durch Verwaltungsvorschriften ergänzt werden. Im Gesetzgebungsverfahren hatte ich hier die Auffassung vertreten, daß regelmäßig anfallende, möglicherweise noch bundesweit und bundeseinheitlich abgesprochene Geschäftsstatistiken der Ressorts eine eigenständige Rechtsgrundlage z. B. im jeweiligen Fachgesetz oder als spezielle Rechtsvorschrift benötigen und nicht durch allgemeine Bestimmungen im Landesstatistikgesetz über die Nutzung von Verwaltungsdaten für statistische Zwecke zugelassen werden können. Diesem Gedanken haben sich die Verwaltung und die Innendeputation angeschlossen. Durch Verwaltungsvorschrift des Senats soll eine Abgrenzung der amtlichen, durch besondere Rechtsvorschrift zu regelnden Statistik von dem Bereich Geschäftsstatistik, für den keine besondere Rechtsvorschrift notwendig ist, vorgenommen werden. Diese Verwaltungsvorschrift des Senats fehlt bisher; ich rege an, sie bald in Angriff zu nehmen.

2.2.5.2 Bevölkerungsstatistik

Im Berichtsjahr hat der Senator für Inneres mir verschiedene Entwürfe eines neuen Gesetzes über die Bevölkerungsstatistik zur Stellungnahme zugeschickt, mit dem das Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes vom 14. März 1980 abgelöst werden soll. Gerade dieses Gesetz entspricht mit seiner Verflechtung von Statistik und Verwaltungsvollzug schon lange nicht mehr den datenschutzrechtlichen Erfordernissen und muß dringend novelliert oder gänzlich aufgehoben werden. Dies habe ich mehrfach in meinen früheren Jahresberichten angemerkt. Der letzte mir bekannte und zwischen den Ländern und dem Bundesministerium des Innern offenbar abgestimmte Gesetzentwurf (Referentenentwurf) datiert vom 28. November 1989, den ich im Januar dieses Jahres in die Hand bekam. Nach meinen Informationen besteht in Bonn die Absicht, diesen Gesetzentwurf zeitgleich mit dem Entwurf zur Änderung des Mikrozensusgesetzes und dem Entwurf eines neuen Gebäude- und Wohnungsstichprobengesetzes in die Gesetzesberatungen einzubringen.

Mit dem neuen Gesetz über die Bevölkerungsstatistik soll die Statistik der natürlichen Bevölkerungsbewegung und Fortschreibung des Bevölkerungsstandes grundlegend neu gestaltet und ausgebaut werden. Zweck der Statistik soll es sein, die zahlenmäßigen und strukturellen Veränderungen der Bevölkerung festzustellen sowie Grundlagen für Bevölkerungsvorausschätzungen zu schaffen.

Die Statistik umfaßt Erhebungen über

- Geburten,
- Sterbefälle einschließlich Todesursachen,
- Eheschließungen,
- Zu- und Fortzüge einschließlich Änderungen der Haupt- und Nebenwohnung sowie
- rechtskräftige Urteile in Ehesachen

sowie darauf aufbauend die Fortschreibung des Bevölkerungsstandes nach Alter, Geschlecht, Familienstand, Deutschen und Ausländern.

Es besteht für alle Erhebungsteile und Erhebungsmerkmale Auskunftspflicht. Auskunftspflichtig sind je nach Erhebungsgegenstand die zuständigen Standesbeamten, Meldebehörden, Gesundheitsämter, die Urkundsbeamten der Geschäftsstellen der Familiengerichte oder die Betroffenen selbst, soweit die Erhebungsmerkmale im Verwaltungsvollzug der genannten Stellen nicht anfallen. In diesem Fall haben die auskunftspflichtigen Betroffenen den jeweiligen Stellen oder Behörden (z. B. Standesbeamten) gegenüber die Auskunft zu erteilen, die ihrerseits wiederum diese Angaben zusammen mit ihren Angaben aus dem Verwaltungsvollzug den statistischen Ämtern zuleiten. Es handelt sich dabei nicht um stichtagsbezogene einmalige Datenerhebungen, sondern um kontinuierliche, mit dem Verwaltungsvollzug weitgehend gleichlaufende Datenerhebungen (anlaßbezogene, monatlich nachträglich ablaufende statistische Datenerhebungen) in der Form einer Totalerhebung.

Dieser Gesetzentwurf wirft eine Vielzahl grundlegender Datenschutzfragen auf. So ist die grundsätzliche Frage nach der Erforderlichkeit dieser bevölkerungsstatistischen Datenerhebungen neben der Volkszählung, dem Mikrozensus und der neuen Gebäude- und Wohnungsstichprobe zu stellen. Das Gesamtsystem der bevölkungsstatistischen Datenerhebungen steht mit diesem Gesetzentwurf zur Disposition. Ich bin der Auffassung, daß eine funktionierende und im Sinne des Gesetzentwurfs ausgeweitete Bevölkerungsstatistik Volkszählungen überflüssig macht.

Auch die einzelnen Erhebungsteile und die jeweiligen Erhebungsmerkmale stehen hinsichtlich ihrer Erforderlichkeit und ihres Merkmalskataloges auf dem Prüfstand. So dringen einzelne Fragen wie etwa die nach der Religionszugehörigkeit, nach ehelicher, nicht-ehelicher Geburt, nach der Zahl der zuvor lebend- oder totgeborenen Kinder massiv in den absolut geschützten, auch für die amtliche Statistik nicht zugänglichen Intimbereich ein mit der Folge, daß derartige Fragen auf verfassungsrechtliche Bedenken stoßen. Gleiches gilt für die Regelung der Auskunftspflicht und die Art der Datenerhebung, die ebenfalls in Teilen wegen der Verflechtung von amtlicher Statistik und Verwaltungsvollzug nicht verfassungskonform ist. Sekundärstatistische Datenerhebungen müssen ihre Grenze am Bestand der Verwaltungsdaten finden. Daten, die für das Verwaltungshandeln selbst nicht benötigt werden, dürfen von der Verwaltung (z. B. dem Standesbeamten) für Zwecke der Bevölkerungsstatistik nicht beim Betroffenen — sogar mit Auskunftspflicht — erhoben werden.

Auch die Arbeitsweise der statistischen Ämter im Bereich der Bevölkerungsstatistik muß datenschutzrechtlich überprüft werden. Das Statistische Landesamt Bremen ist sowohl Landesamt als auch kommunalstatistisches Amt der Stadtgemeinde Bremen und erhält aufgrund melderechtlicher Regelungen (§ 15 Meld-DÜV) regelmäßig Meldedaten aus dem bremischen Melderegister, die mit den kontinuierlich zufließenden Daten aus der Bevölkerungsstatistik (Landesaufgabe) verknüpft und ausgewertet werden. § 13 Abs. 1 des Gesetzentwurfs, der die Übermittlung von Einzelangaben an die statistischen Ämter der Gemeinden regelt, läßt sich in Bremen so nicht gesetzeskonform vollziehen. Die Verknüpfung von Daten der Bevölkerungsstatistik mit Daten des Melderegisters im Statistischen Landesamt Bremen führt unter datenschutzrechtlichem Blickwinkel dazu, daß eine Art statistisches Melderegister entsteht, ohne daß die verfassungsrechtlich gebotene Trennung zwischen statistischen Landes- und Kommunalaufgaben gewährleistet wird.

2.2.5.3 Mikrozensus, Gebäude- und Wohnungsstichprobe

Im Berichtsjahr hat der Senator für Inneres mir verschiedene **Entwürfe zur Änderung des Mikrozensusgesetzes** vom 10. Juni 1985 zugeschickt. Der letzte Entwurf des Bundesministeriums des Innern datiert vom 25. Oktober 1989. Dieser Entwurf wurde im letzten Quartal des Berichtsjahres abschließend mit den zuständigen Länderressorts erörtert. Das Bundeskabinett hat den Gesetzentwurf jedoch bis jetzt noch nicht beschlossen; von den Innenpolitikern wurde zu dem Entwurf eine Reihe grundsätzlicher Fragen gestellt, deren Beantwortung noch offen ist.

Mit dem Änderungsgesetz zum Mikrozensusgesetz soll die Geltung des Gesetzes um vier Jahre bis einschließlich 1994 verlängert werden. Das geltende Mikrozensusgesetz läuft Ende 1990 aus. Das Erhebungsprogramm wird um den Punkt „Wohnverhältnisse" gekürzt; dieser Erhebungsteil war bereits durch Rechtsverordnung aufgehoben worden und nicht mehr im Fragenprogramm der Mikrozensuserhebung 1989 enthalten. Die Wohnverhältnisse der Bevölkerung und der

Wohnungsmarkt sollen durch eine eigenständige Stichprobenerhebung auf der Grundlage eines speziellen Gesetzes, dem Gebäude- und Wohnungsstichprobengesetz, weitergehend als bisher im Rahmen der Mikrozensuserhebungen statistisch erfaßt und aufbereitet werden. Das Erhebungsprogramm des Mikrozensus soll im übrigen im wesentlichen unverändert bleiben. An der Auskunftspflicht wird in dem Entwurf für ein geändertes Mikrozensusgesetz grundsätzlich festgehalten. Allerdings werden weitere Merkmale der freiwilligen Beantwortung überlassen. Beim **jährlichen Grundprogramm** des Mikrozensus (Angaben zur Wohnungsnutzung, zur Zahl der Haushalte und Personen in einer Wohnung, zur Wohnungs- und Haushaltszugehörigkeit, zum Geschlecht, Alter, Familienstand, Eheschließungsjahr, Staatsangehörigkeit, zur Erwerbstätigkeit, zur Art des überwiegenden Lebensunterhalts, zur Krankenversicherung) soll es im wesentlichen bei der allgemeinen Auskunftspflicht verbleiben, das Merkmal „zusätzlicher privater Krankenversicherungsschutz" wird jedoch zusätzlich von der Auskunftspflicht ausgenommen. Beim **Zusatzprogramm**, das in mehrjährigen Abständen zusätzlich zum Grundprogramm erhoben wird (alle zwei Jahre: Angaben zum ausgeübten Beruf und zum Arbeitsplatz, zur Stellung im Betrieb, Berufswechsel, Schulabschlußdaten, bei Ausländern Angaben zur Aufenthaltsdauer, Zahl und Alter der Kinder, zum Ehegatten und zu den Eltern im Ausland; alle drei Jahre: Angaben zu Arbeits- oder Ausbildungsstätte, zum benutzten Verkehrsmittel und zur Entfernung sowie zum Zeitaufwand bei Fahrten zwischen Wohnung und Arbeitsstätte, Angaben zur Dauer einer Erkrankung oder zu einem Unfall, zu einer evtl. Behinderung, zur Alterversorgung), sollen ebenfalls weitere Erhebungsmerkmale für die Beantwortung freigestellt werden, es handelt sich hier um die speziellen Fragen an die Ausländer (§ 5 Abs. 2 Nr. 3) und die besonderen Merkmale zur Arbeits- oder Ausbildungsstätte, zur Entfernung und zum benutzten Verkehrsmittel, zur Behinderteneigenschaft und zur Altersversorgung (§ 5 Abs. 3 Nrn. 1, 3, 4). In den Jahren 1991 und 1992 sollen schließlich vierteljährliche Testerhebungen „nach Maßgabe des § 9 Abs. 1 (also mit Auskunftspflicht) und Abs. 4 (freiwillige Beantwortung) im Rahmen der Erhebungsmerkmale des § 5 (sämtliche Erhebungsmerkmale) ermöglicht werden."

Der Gesetzentwurf zur Änderung des Mikrozensusgesetzes muß bei seiner Beurteilung im Zusammenhang mit den anderen bevölkerungsstatistischen Datenerhebungen gesehen werden. Dabei sind das Erhebungsprogramm (Grundprogramm, Zusatzprogramm) und der Umfang der Erhebungsmerkmale, die mit Auskunftspflicht erhoben werden, kritisch zu überprüfen. Die Regelung zu den vierteljährlichen Testerhebungen in den Jahren 1991 und 1992 erscheint mir nicht ausgereift (vorgesehen ist u. a. eine regelmäßige Übermittlung von Meldedaten!) und sollte in dieser Form nicht verabschiedet werden.

Im August 1989 hat das Bundeskabinett den **Entwurf eines Gebäude- und Wohnungsstichprobengesetzes** beschlossen und dem Bundesrat zugeleitet. Mit diesem Gesetz soll die aus dem Mikrozensus ausgegliederte Stichprobenerhebung über die Wohnverhältnisse der Bevölkerung und über den Wohnungsmarkt speziell geregelt und erheblich ausgebaut werden. Der Entwurf sieht vor, daß alle fünf Jahre eine Gebäude- und Wohnungsstichprobe als eigenständige Stichprobenerhebung durchgeführt wird. Das Erhebungsprogramm dieser Zählung wurde gegenüber dem Programm des Mikrozensus erheblich ausgeweitet. Statt bisher 14 Erhebungsmerkmalen sollen künftig weit über 50 Merkmale zu Gebäuden, zu Wohnungen, zu Haushalten und zu Wohnquartieren erhoben werden. Auch bei dieser Stichprobenerhebung soll an der bußgeldbewehrten Auskunftspflicht festgehalten werden. Dies ist insofern erstaunlich, als im Mikrozensusgesetz der Bereich der freiwilligen Beantwortung von Fragen ausgeweitet wurde. Die Gesetzesbegründung kann die Erforderlichkeit einer so umfangreichen zusätzlichen Stichprobenerhebung mit bußgeldbewehrter Auskunftspflicht nicht zureichend darlegen. Der Bundesrat hat auf der Basis kritischer Äußerungen von Datenschutzbeauftragten in seiner Stellungnahme Kritik an Umfang und Ausprägung der Erhebungsmerkmale geäußert. Es bleibt abzuwarten, ob den massiven Bedenken im weiteren Gesetzgebungsverfahren Rechnung getragen wird.

2.2.5.4 Hochschulstatistik

- **Individualerhebung des wissenschaftlichen und künstlerischen Personals an Hochschulen 1989**

Das Hochschulstatistikgesetz (HStatG) vom 21. April 1980 sieht vor, daß alle sechs Jahre eine individualisierte Erhebung des wissenschaftlichen und künstlerischen Personals an Hochschulen durchgeführt wird. Erhoben werden dabei Angaben

zur Person, Staatsangehörigkeit, Ausbildungsverlauf, berufliche Tätigkeit vor der Tätigkeit in der Hochschule, Lehrfächer, fachliche Schwerpunkte der wissenschaftlichen oder künstlerischen Tätigkeit, dienstrechtliche Stellung und Stellung in der Hochschule, Zahl und Art weiterer Beschäftigungsverhältnisse, Art der Finanzierung der Stelle. Erhebungsstichtag der letztjährigen Zählung war der 20. Oktober 1989.

Das Statistische Landesamt Bremen informierte mich Mitte Oktober über die bevorstehende Erhebung. Nach Durchsicht der Unterlagen mußte ich zum Erhebungsverfahren grundsätzliche Bedenken geltend machen. Vorgesehen war, daß die Hochschulen dem Statistischen Landesamt eine Reihe von Angaben über die auskunftspflichtigen Personen machen sollten. Diese Angaben sollten bis Anfang November dem Statistischen Landesamt übermittelt werden; Rechtsgrundlage sollte § 13 Abs. 3 HStatG i. V. m. § 26 Abs. 2 Bundesstatistikgesetz (BStatG) sein. Innerhalb des Durchführungskonzeptes dieser statistischen Datenerhebung sollten die Hochschulen lediglich Verteilfunktionen für diese statistische Datenerhebung übernehmen.

Ich habe das Statistische Landesamt darauf hingewiesen, daß die genannten Gesetzesbestimmungen die Übermittlung der erbetenen Merkmale durch die Hochschulen nicht rechtfertigen. Auch das Bremische Hochschulgesetz und das BrDSG können eine solche Datenübermittlung rechtlich nicht begründen. Ich habe dem Statistischen Landesamt stattdessen ein anderes Erhebungsverfahren vorgeschlagen. Die Hochschulen selbst sollten den Auskunftspflichtigen die Erhebungsbögen zusenden und darüber eine Liste führen, die dann später für ein evtl. Erinnerungs- und Mahnverfahren benutzt werden kann.

Das Statistische Landesamt hat auf meine Empfehlung hin nicht mehr reagiert. Von meinem Vorschlag hat allein die Universität Bremen Gebrauch gemacht; die übrigen Hochschulen des Landes sind so verfahren, wie das Statistische Landesamt es vorgeschlagen hat.

Nicht alle Auskunftspflichtigen waren bereit, die erbetenen Angaben zu machen, vor allem im Bereich der Universität Bremen nicht. Gegenwärtig läuft das Erinnerungs- und Mahnverfahren, das im Bereich der Universität Bremen noch hochschulintern abläuft (das Statistische Landesamt benennt die Ordnungsziffern, für die noch keine Erhebungsunterlagen eingegangen sind). Nach Abschluß dieses Erinnerungs- und Mahnverfahrens muß das Statistische Landesamt sich weitere Schritte zur Durchsetzung der Auskunftspflicht überlegen. Im Hinblick darauf, daß das HStatG, auf das diese Datenerhebung gestützt wird, schon lange nicht mehr den verfassungsrechtlichen Anforderungen an statistische Rechtsgrundlagen genügt, habe ich Zweifel, ob die Durchsetzung der Auskunftspflicht mit verwaltungsrechtlichen Mitteln und die evtl. Einleitung eines Ordnungswidrigkeitsverfahrens verfassungsrechtlich zulässig ist. Ob der sogenannte Übergangsbonus in diesem Fall noch einmal als Rechtsbegründung für diese statistische Datenerhebung herangezogen werden kann, erscheint mir ebenfalls sehr fraglich; nach weit überwiegender Meinung ist dieser Übergangsbonus bei diesem Gesetz längst abgelaufen. Es führt deshalb kein Weg an einer umgehenden Novellierung des HStatG vorbei.

● Novellierung des Hochschulstatistikgesetzes

Im Berichtsjahr hat die Bundesregierung den Entwurf eines Gesetzes über die Statistik für das Hochschulwesen (HStatG) beschlossen und das Gesetzgebungsverfahren eingeleitet. Nach Beschlußfassung im Bundesrat liegt der Gesetzentwurf inzwischen den Bundestag (erste Lesung Anfang Dezember 1989) vor. Ob es noch in dieser Legislaturperiode zur endgültigen Verabschiedung dieses Gesetzes kommt, bleibt abzuwarten.

Mit diesem Gesetzentwurf soll die Hochschulstatistik sowohl hinsichtlich ihres Erhebungsprogramms und hinsichtlich des Erhebungsverfahrens an die heutigen datenschutzrechtlichen Erfordernisse angepaßt werden. Das geltende Hochschulstatistikgesetz entspricht diesen Anforderungen schon lange nicht mehr. Folgende wesentliche Neuerungen sind geplant:

— Das geltende Hochschulstatistikgesetz stützt sich auf ein Erhebungsverfahren, bei dem die Statistik zugleich Grundlage für die Arbeit der Hochschulverwaltung ist. Die personenbezogenen Erhebungen zur Studenten-, Prüfungs- und Hochschulpersonalstatistik dienen gleichzeitig internen Verwaltungszwecken der Hochschulen. Das Bundesverfassungsgericht hält es im Hinblick auf das informationelle Selbstbestimmungsrecht für bedenklich, die für statistische

Zwecke erhobenen Daten gleichzeitig für Zwecke der Verwaltung zu verwenden. Dem trägt der Gesetzentwurf dadurch Rechnung, daß er die Auskunftspflicht ändert; während bisher die primär für statistische Zwecke vom Studenten erhobenen Daten in vollem Umfang auch der Verwaltung zur Verfügung standen, wird künftig von den Daten ausgegangen, die die Hochschulverwaltungen für ihre administrativen Zwecke benötigen (Umstellung auf Sekundärstatistik). Die im 6jährigen Rhythmus erfolgende Statistik des wissenschaftlichen und künstlerischen Personals der Hochschulen soll dagegen als reine Primärstatistik (Erhebung ausschließlich beim Betroffenen) weiterlaufen. Diese Neuregelung soll verhindern, daß die Hochschulverwaltungen Einblick in die Erhebungsunterlagen erhalten oder Kontrollbefugnisse im Erhebungsverfahren ausüben können.

- Auch die im bisherigen Hochschulstatistikgesetz enthaltene Studienverlaufsstatistik in Form einer halbjährlichen Verknüpfung von Einzeldaten der Studentenbestandsdateien miteinander und mit der jährlichen Prüfungsteilnehmerdatei — unter Verwendung von sogenannten Identifikationsmerkmalen, die aus personenbezogenen Daten entwickelt werden und reidentifizierbar sind — soll künftig verzichtet werden.

Ich habe zu diesem Gesetzentwurf gegenüber dem Senator für Bildung, Wissenschaft und Kunst Stellung genommen.

Dabei habe ich darauf hingewiesen, daß der Gesetzentwurf eine Reihe von Verbesserungen enthält, die ich aus datenschutzrechtlicher Sicht positiv bewerte. Einzelne Gesetzesbestimmungen entsprechen jedoch nicht der von der Bundesregierung gesetzten Zielsetzung.

So wird in § 1 Abs. 1 des Entwurfs lediglich geregelt, daß eine Bundesstatistik zur Erfüllung der Aufgaben des Bundes im Hochschulbereich durchgeführt werden soll. Angaben darüber, welche Aufgaben konkret gemeint sind, fehlen. Es wird somit dem Konkretisierungsgebot, das nicht zuletzt nach dem Volkszählungsurteil des Bundesverfassungsgerichts auch für den Bereich der amtlichen Statistik gilt, nicht ausreichend Rechnung getragen.

Gem. § 3 Abs. 1 Nr. 1 des Entwurfs soll die Studentenstatistik weiterhin semesterweise durchgeführt werden. Es ist hierbei zu berücksichtigen, daß es sich bei der Studentenstatistik weiterhin um eine Totalerhebung handelt, die alle Studenten jedes Semesters betrifft und die einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Studenten darstellt. Ob die Ergebnisse der Statistik wesentlich schlechter sind, wenn die Zählung nur einmal jährlich vorgenommen wird, könnte im Hinblick auf die Intensität des Eingriffs und den Verhältnismäßigkeitsgrundsatz zumindest geprüft werden.

Die Absicht des Gesetzgebers, auf die Studienverlaufsstatitik zu verzichten, wird von mir ausdrücklich begrüßt. Überlegungen, eine derartige Statistik doch wieder einzuführen, sollte wegen der damit verbundenen datenschutzrechtlichen Probleme nicht gefolgt werden. Allerdings ist der Entwurf in diesem Punkt nicht konsequent, da er eine Reihe bisher nicht erhobener Angaben über Studenten, wie z. B. die Bezeichnung der im vorangehenden Semester besuchten Hochschule, die Studiengänge im vorangehenden Semester, den Prüfungserfolg und die Gesamtnote abgelegter Prüfungen oder Studienunterbrechungen nach Art und Dauer vorsieht. Neben bestandsstatistischen Aufbereitungen werden damit auch verlaufsstatistische Auswertungen möglich. Der Gesetzgeber begründet die von ihm beabsichtigte zusätzliche Erhebung von Angaben dann auch damit, daß man bestimmte verlaufsanalytische Feststellungen treffen wolle. Offen bleibt, auch in der Begründung, welche Feststellungen konkret gemeint sind und ob diese Feststellungen für die Erreichung der mit der Hochschulstatistik beabsichtigten Zwecke erforderlich sind. Fraglich ist auch, ob die Erhebung bestimmter Daten wie z. B. Geburtsmonat oder die Staatsangehörigkeit der Studenten für den Zweck dieser Statistik überhaupt erforderlich ist.

Für die Hochschulstatistik besteht Auskunftspflicht. Auskunftspflichtig sind nach § 5 des Gesetzentwurfs die Leiter der jeweiligen Hochschuleinrichtung oder die Betroffenen (bei der Statistik des wissenschaftlichen und künstlerischen Personals). Die Auskunftspflicht kann sich bei den sekundärstatistischen Erhebungen nur auf das Datenmaterial beziehen, das den Auskunftspflichtigen für ihre Aufgabenerfüllung zur Verfügung steht. Das Hochschulstatistikgesetz kann diesen durch Landesrecht abgesteckten Rahmen nicht erweitern.

Nach § 6 des Entwurfs sollen vom Statistischen Bundesamt Zusatzaufbereitungen für Bundeszwecke und Sonderaufbereitungen, soweit nicht von den statistischen Ämtern der Länder vorgenommen, durchgeführt werden. Offen bleibt im Entwurf, welche Daten dem Statistischen Bundesamt für diese Zusatz- und Sonderaufbereitungen von den statistischen Landesämtern zur Verfügung gestellt werden sollen.

Ich hoffe, daß meine Anregungen bei der laufenden Gesetzesberatung noch berücksichtigt werden können.

2.2.6 Ausländerangelegenheiten

2.2.6.1 Ausländerrecht und Datenverarbeitung

In meinem 11. Jahresbericht habe ich unter Pkt. 5.2.6.1 ausführlich über den Entwurf des Bundesministers des Innern eines Gesetzes über das Ausländerzentralregister berichtet und aus datenschutzrechtlicher Sicht kritisch bewertet. Die Bundesregierung hat nunmehr einen Gesetzentwurf zum Ausländerzentralregister beschlossen und in den Deutschen Bundestag (Drs. 11/5828) eingebracht. Dieser Gesetzentwurf hat zwar einige meiner wesentlichen Kritikpunkte berücksichtigt, ein großer Teil der datenschutzrechtlich und verfassungsrechtlich bedenklichen Bestimmungen ist jedoch unverändert geblieben.

Ich habe dargelegt, daß das Ausländerzentralregistergesetz nur die Datenverarbeitung im Zusammenhang mit der Führung des Ausländerzentralregistergesetzes regeln kann, daß aber die Einschränkungen des informationellen Selbstbestimmungsrechts der Ausländer nur durch entsprechende Regelungen in den die Ausländer betreffenden Gesetzen legitimiert werden können. Es bedarf dabei präziser Vorschriften

- darüber, welche Daten für welchen Zweck erhoben werden dürfen. Dabei ist zu unterscheiden nach dem aufenthaltsrechtlichen Status des Betroffenen und der im Einzelfall zu treffenden ausländerrechtlichen Entscheidung. Der Grundsatz, daß personenbezogene Daten beim Betroffenen mit dessen Kenntnis zu erheben sind, ist zu wahren und die Erhebung bei Dritten nur ausnahmsweise zuzulassen,
- welche Daten unter welchen Voraussetzungen an öffentliche Stellen, an natürliche und juristische Personen des privaten Rechts, an öffentliche Stellen anderer Staaten oder an zwischenstaatliche Organisationen übermittelt werden dürfen.
- über die Berichtigung, Sperrung und Löschung von Daten und
- Auskunftsrechte der Betroffenen.

Der Bundesminister des Innern hat am 28. September 1989 einen Entwurf für ein Gesetz zur Neuregelung des Ausländerrechts vorgelegt. Am 10. November 1989 hat auch die SPD-Bundestagsfraktion einen Entwurf eines Bundesausländergesetzes in den Deutschen Bundestag (Drs. 11/5637) eingebracht.

Während letzterer keinen wesentlichen datenschutzrechtlichen Bedenken begegnet, weil er die vorher genannten Anforderungen erfüllt, habe ich zum Entwurf des Bundesinnenministers insbesondere folgende Kritik vorgebracht:

Der Gesetzentwurf berücksichtigt nicht die vorher genannten Anforderungen, die an eine das auch Ausländern zustehende Recht auf informationelle Selbstbestimmung einschränkende Norm zu stellen sind.

Er enthält nur einige wenige Datenverarbeitungsregelungen, insbesondere über die Zulässigkeit erkennungsdienstlicher Maßnahmen, die Verpflichtung zur Aufenthaltsanzeige, die Verpflichtung zur Beibringung von Nachweisen und Mitteilungspflichten anderer Behörden sowie die Durchbrechung des Sozialgeheimnisses.

Der Entwurf enthält keine präzisen Bestimmungen über Art und Umfang der Daten, deren Verarbeitung erlaubt ist, und über den Zweck, für den sie verarbeitet werden dürfen. Die Durchführung der materiell-rechtlichen Regelungen des Gesetzentwurfs setzt jedoch die Verarbeitung einer Fülle personenbezogener Daten der Betroffenen voraus. Der Gesetzentwurf vernachlässigt insoweit den Grundsatz der Normenklarheit eklatant.

Die wenigen Datenverarbeitungsregelungen wahren auch nicht den Verhältnismäßigkeitsgrundsatz. So hat sich ein Ausländer erkennungsdienstlichen Maßnahmen zu unterwerfen, wenn Zweifel über seine Person oder seine Staatsangehörigkeit bestehen. Nach der Formulierung dieser Vorschrift reichen subjektive

Zweifel eines bearbeitenden Beamten aus, um die Rechtsfolge eintreten zu lassen. Der mit der Durchführung erkennungsdienstlicher Maßnahmen verbundene Eingriff in das informationelle Selbstbestimmungsrecht kann jedoch nur gerechtfertigt werden, wenn objektive Zweifel dieses verlangen. Die Vorschrift sollte deshalb so gefaßt werden, daß eine erkennungsdienstliche Maßnahme nur angeordnet werden kann, wenn Tatsachen vorliegen, die Zweifel rechtfertigen.

Behörden und andere öffentlichen Stellen werden verpflichtet, auf Anforderung den mit der Durchführung des Ausländergesetzes betrauten Behörden ihnen bekanntgewordene „Umstände" mitzuteilen, welche für die nach dem Gesetz zu treffenden Entscheidungen von Bedeutung sein können. Die Beurteilung, ob die Kenntnis der mitzuteilenden „Umstände" für die Durchführung des Gesetzes erforderlich ist, soll allein den mit der Durchführung des Ausländergesetzes betrauten Behörden obliegen. Daraus folgt, daß die verpflichteten Stellen auch solche Daten übermitteln müssen, welche die mit der Durchführung des Ausländergesetzes betrauten Stellen für die Erfüllung ihrer Aufgaben nicht benötigen.

Die Mitteilungspflicht wird auch nicht auf solche „Umstände" begrenzt, die den genannten Stellen bei der Durchführung der ihnen übertragenen Aufgaben bekanntgeworden sind. Das bedeutet, daß jedwede Behörde oder andere öffentliche Stelle zu einem Instrument der Ausforschung der Betroffenen gemacht werden kann.

Darüber hinaus sieht der Entwurf vor, daß Behörden auch ohne Anforderungen der Ausländerbehörden personenbezogene Daten von Ausländern mitzuteilen haben. Welche Behörden mitteilungspflichtig sein sollen und welche personenbezogenen Daten zu übermitteln sind, wird nicht geregelt. Dieses soll durch Rechtsverordnung bestimmt werden. Diese Regelung verstößt gegen Art. 80 Abs. 1 Satz 2 Grundgesetz (GG), wonach der Gesetzgeber wesentliche Regelungen selbst treffen muß und dieses nicht dem Verordnungsgeber überlassen darf.

Sonst bestehende Schweigepflichten werden in „Fällen strafbarer Handlungen" und einer „Gefährdung der öffentlichen Gesundheit durch Ausländer" aufgehoben.Nach dem jetzt geltenden Ausländergesetz wird die besondere Schweigepflicht nur in besonderen Fällen aufgehoben, z. B. bei Verstößen gegen das Steuerrecht, das Außenwirtschaftsrecht oder soweit er die öffentliche Gesundheit oder Sittlichkeit gefährdet.

Abgesehen davon, daß die gewählte Formulierung „in den Fällen strafbarer Handlungen" nicht normenklar ist, ergibt sich eine Verletzung des Verhältnismäßigkeitsprinzips bei dieser Vorschrift allein schon daraus, daß nach materiellrechtlichen Vorschriften nicht jedwede strafbare Handlung ausländerrechtliche Entscheidungen nach sich zieht.

Der Grundsatz der Verhältnismäßigkeit wird auch dadurch verletzt, daß alle vorgesehenen Mitteilungspflichten für alle Ausländer ohne Rücksicht auf ihren Status gleichermaßen geregelt sind, obwohl die so erhobenen Daten für die Erfüllung der Aufgaben der mit der Durchführung des Gesetzes betrauten Behörden nicht erforderlich sind, weil viele Informationen für viele Gruppen von Ausländern ausländerrechtlich nicht relevant sind. Der Umfang der normierten Mitteilungspflichten verstößt auch gegen das Prinzip der Zweckbindung von beim Betroffenen zwangsweise erhobenen Daten. Viele der Daten, die durch eine Mitteilungspflicht erhoben werden sollen, könnten auch ohne erheblichen Aufwand bei den Betroffenen selbst erhoben werden.

Eine Reihe materiell-rechtlicher Regelungen des Entwurfes verstößt gegen den Grundsatz der Verhältnismäßigkeit, weil der damit verfolgte Zweck in keinem Verhältnis zu der Schwere des damit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung steht. Eingriffstatbestände, die einen sehr weiten Rahmen bieten, haben notgedrungen auch umfangreiche und schwer begrenzbare Datenverarbeitung zur Folge.

Außerdem enthält der Entwurf keinerlei Schutz-, Verfahrens- sowie Löschungs- und Sperrungsvorschriften. Auch sind keine Betroffenenrechte normiert.

Die Zulässigkeit von Datenübermittlungen durch die mit der Durchführung des Gesetzes betrauten Stellen an Dritte ist nicht geregelt, obwohl nach bisheriger Praxis und der sich aus dem Gesetzentwurf ergebenden Zielsetzung vermutet werden muß, daß solche vorgesehen sind.

Insgesamt gesehen drängt sich der Eindruck auf, daß mit dem Gesetzentwurf das Recht auf informationelle Selbstbestimmung von Ausländern de facto ad absurdum geführt wird. Das kann auch Auswirkungen auf die Verarbeitung personen-

bezogener Daten von Deutschen haben, die in Beziehung zu ausländischen Staaten treten. Das ergibt sich durch das auch in der EG geübte „Prinzip der Gegenseitigkeit". Das kann schon deshalb nicht außer acht bleiben, weil noch nicht einmal alle EG-Staaten das informationelle Selbstbestimmungsrecht schützende Datenschutzvorschriften haben.

2.2.6.2 Zwangsweise ärztliche Untersuchung von Asylbewerbern

Die Arbeitsgemeinschaft der leitenden Medizinalbeamten hat der Gesundheitsministerkonferenz empfohlen, die Bundesregierung zu bitten, das Gesetzgebungsverfahren zur Schaffung einer Rechtsgrundlage für die obligatorische zwangsweise ärztliche Untersuchung aller Asylbewerber einzuleiten. Die Gesundheitsuntersuchung aller Asylbewerber diene der öffentlichen Sicherheit und Ordnung zum Schutz der öffentlichen Gesundheit und sei im übrigen aus solchen rechtlichen Aspekten notwendig.

Ich habe dem Senator für Inneres und dem Senator für Gesundheit dargelegt, daß eine zwangsweise Untersuchung aller Asylbewerber nur dann als verhältnismäßig angesehen werden kann, wenn dadurch Gefahren für die öffentliche Gesundheit abgewehrt werden. Dies setze jedoch einen hohen Durchseuchungsgrad, insbesondere mit schwer behandelbaren oder unbehandelbaren übertragbaren Krankheiten aller Asylbewerber voraus.

Aus den Stellungnahmen des Senators für Inneres und des Senators für Gesundheit geht hervor, daß die Gruppe der Asylbewerber keine Gefahr für die öffentliche Gesundheit darstellt und Untersuchungen bisher lediglich auf freiwilliger Basis erfolgt sind.

Inzwischen hat die Arbeitsgemeinschaft der leitenden Medizinalbeamten festgestellt, daß die Untersuchungen aus seuchenhygienischen und fürsorgerischen Gründen auf freiwilliger Basis sinnvoll und geboten erscheinen. Im Hinblick auf die erforderliche Einwilligung sollte der Asylbewerber mit der Aufforderung zur Untersuchung in geeigneter Form über Zweck, Umfang und Freiwilligkeit der Untersuchungen informiert werden, falls die Untersuchung nicht vom Gesundheitsamt oder der Ausländerbehörde angeordnet wird. Die Einwilligung ist zu dokumentieren und der Asylbewerber darauf hinzuweisen, daß die Ergebnisse der Untersuchungen keinen Einfluß auf das Asylverfahren haben. Eine Verpflichtung zur Untersuchung besteht nur im Einzelfall, wenn die Gesundheitsbehörde auf der Grundlage der Bestimmungen des Bundesseuchengesetzes oder die Ausländerbehörde auf der Grundlage des Asylverfahrensgesetzes Untersuchungen anordnen.

In der freiwilligen Untersuchung wird ein Mittel gesehen, das geboten aber auch ausreichend ist, der Gesundheitsfürsorge zu genügen und der Abwehr übertragbarer Krankheiten nachzukommen. Notwendige Maßnahmen zur Verhütung und Bekämpfung einer übertragbaren Krankheit hat das Gesundheitsamt nach eigener Beurteilung zu treffen. Untersuchungsbefunde von Asylbewerbern werden an andere Stellen nur weitergeleitet, soweit hierzu gesetzliche Grundlagen vorliegen oder die Einwilligung des Asylbewerbers gegeben ist.

Das Hauptgesundheitsamt Bremen bereitet nun ein freiwilliges Beratungs- und Untersuchungsangebot vor und hat mich um Beteiligung gebeten.

2.2.7 Wahlen

Änderung des Bremischen Wahlgesetzes

Anläßlich einer aus anderen Gründen beabsichtigten Änderung des Bremischen Wahlgesetzes habe ich auf die Notwendigkeit hingewiesen, gesetzliche Regelungen für die mit der Durchführung von Wahlen, Volksbegehren und Volksentscheiden verbundene Verarbeitung personenbezogener Daten festzulegen.

Das Gesetz regelt nunmehr im einzelnen, welche personenbezogenen Daten der Wahlberechtigten das bei der Gemeindebehörde für jeden Wahlbezirk zu führende Verzeichnis enthält, und daß diese Daten im automatisierten Abrufverfahren bei der Meldebehörde erhoben werden dürfen.

Diese Regelung schafft die notwendige Erhebungsgrundlage für das automatisierte Verbundwahlverfahren Bürgerschaft/Beiräte/Ausländer. Die erforderliche Übermittlungsvorschrift für die Meldebehörde ist noch in der Meldedatenübermittlungsverordnung zu schaffen.

Der Senator für Inneres hat mir dazu einen entsprechenden Änderungsvorschlag übersandt. Ich habe dazu vorgeschlagen, daß die Übermittlungen auf einen Zeitraum vom 60. Tag vor der Wahl bis einschließlich zum Wahltag beschränkt bleiben. Der Senator für Inneres hat mir mitgeteilt, daß er diesen Vorschlag übernehmen werde. Wegen solcher Übermittlungen bei Volksbegehren und Volksentscheiden soll die Zeitspanne noch geprüft werden.

Parteien und Wählervereinigungen, die noch nicht in der Bremischen Bürgerschaft oder im Bundestag vertreten sind, benötigen für die Gültigkeit eines Wahlvorschlages die Unterschriften von einem pro Tausend der Wahlberechtigten des Wahlbereichs. In das Wahlgesetz ist eine Vorschrift aufgenommen worden, wonach der Nachweis der Wahlberechtigung der Unterschreibenden von der Partei oder Wählervereinigung künftig nur noch mit Einwilligung der Betroffenen von der das Verzeichnis der Wahlberechtigten führenden Gemeindebehörde direkt eingeholt werden kann. Der Nachweis der Wahlberechtigung kann auch durch eine vom Unterschreibenden beigebrachte Bescheinigung der Gemeindebehörde erbracht werden.

2.3 Justiz und Verfassung

2.3.1 Novellierungsbedarf

— Justizmitteilungsgesetz

Die Datenschutzbeauftragten des Bundes und der Länder haben u. a. in ihren Beschlüssen vom 6./7. Juni 1984 (MiStra) und vom 13. September 1985 (MiZi) darauf hingewiesen, daß die Mitteilungen aus dem Straf- (MiStra) und Zivilverfahren (MiZi) an andere Stellen einer gesetzlichen Grundlage bedürfen. Die seinerzeit vorgenommene kursorische Überarbeitung der Richtlinien wurde von den Datenschutzbeauftragten des Bundes und der Länder nur deshalb hingenommen, weil erklärt wurde, ein Justizmitteilungsgesetz werde schon bald vorliegen. Seit dieser Zeit sind viele Jahre ins Land gegangen, ohne daß greifbare Ergebnisse vorliegen. Ich weise noch einmal darauf hin, daß mit Ablauf dieser Legislaturperiode auch nach dem Urteil verschiedener Gerichte in der Bundesrepublik der Übergangsbonus verbraucht ist. Daraus folgt, daß schon jetzt nur noch in ganz eingeschränktem Maße unter Beschränkung auf das unabdingbar Erforderliche von den Mitteilungen Gebrauch gemacht werden kann. Offenbar besteht kein dringender Bedarf an der Fortsetzung der Mitteilungspraxis, auf die Datenübermittlung kann scheinbar verzichtet werden. Nur so ist zu verstehen, warum der Gesetzgeber bisher sich nicht hinreichend um eine gesetzliche Regelung bemüht hat, obwohl mit Ablauf der Legislaturperiode ohne eine gesetzliche Grundlage die Mitteilungen gänzlich einzustellen sind.

— Strafprozeßordnung

Im Berichtszeitraum sind erneut Referentenentwürfe zur Änderung und Ergänzung des Strafverfahrensrechts vorgelegt worden. Über den Entwurf mit Stand vom 3. November 1988, ergänzt durch den Entwurf mit Stand vom 22. Dezember 1988, habe ich bereits im letzten Jahresbericht (vgl. 11. Jahresbericht, Seite 77) berichtet. Hierauf bezog sich auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vgl. 11. Jahresbericht, Seite 137 f.). Inzwischen ist mir ein weiterer Referentenentwurf des Strafverfahrensänderungsgesetzes (StVÄG) mit Stand vom 26. Juni 1989 zugeleitet worden.

Neben einigen geringfügigen Verbesserungen gegenüber dem Entwurf von 1988 enthält die neue Vorlage auch eine Reihe von materiellen Verschlechterungen des Datenschutzes. So werden durch Herabsetzen der Eingriffsschwelle und durch Verlängerung von Fristen die Eingriffsmöglichkeiten in Rechte betroffener Bürger ausgeweitet. In meiner Stellungnahme gegenüber dem Senator für Justiz und Verfassung habe ich darauf hingewiesen, daß auch diese datenschutzrechtlichen Verschlechterungen der Stellung der vom Strafverfahren Betroffenen nicht hinnehmbar sind.

Die §§ 98 a bis c des Entwurfs zum StVÄG regeln die sog. Rasterfahndung. Das Verfahren umfaßt sowohl den Datenabgleich mehrerer Bestände wie auch die Selektion einer Datei. Unterschieden wird dabei zwischen der sogenannten positiven (es werden Personen ermittelt, bei denen sich z. B. tätertypische Merkmale kummulieren) und der negativen Rasterfahndung (aus einem Datenbestand werden gewiß unschuldige Personen ausgeschlossen). Meine prinzipiellen datenschutzrechtlichen Bedenken hiergegen hatte ich bereits im letzten Jahr gegen den Senator für Justiz und Verfassung geltend gemacht.

Der neue Arbeitsentwurf enthält nun in § 98 c StVÄG eine weitere erhebliche Verschlechterung. Die vorgesehene Erweiterung der Rasterfahndung auf Daten der Polizei, die sie zur Gefahrenabwehr gespeichert hat, bedeutet eine prinzipielle Zweckdurchbrechung, die völlig unverhältnismäßig den Eingriff in Rechte auch am Strafverfahren nicht beteiligter Dritter zuläßt. Meine prinzipiellen Bedenken gegenüber der Rasterfahndung habe ich bereits in früheren Jahresberichten hinlänglich deutlich gemacht. Nunmehr soll die Rasterfahndung auch auf von der Polizei zu präventiven Zwecken erhobene Daten zugelassen werden, die Daten, die aus Anlässen gewonnen wurden, die nicht im Zusammenhang mit der Durchführung eines Strafverfahrens liegen.

Diese Regelung würde in der Praxis dazu führen, daß viele teils von Bürgern im Vertrauen auf das Schlagwort „Die Polizei, Dein Freund und Helfer" abgegebenen Daten mit in die Rasterfahndung einbezogen werden können. Hilfebedürftige und vermißte Personen können ebenso in die Verdachtschöpfungsmaschinerie der Rasterfahndung geraten, wie z. B. der Familienzwist oder Schüler, die wegen Ruhe störenden Lärms auffällig geworden sind.

Gleiches gilt für den im Entwurf vorgesehenen Abgleich des Fahndungsbestandes mit jedwedem anderen Datenbestand öffentlicher Stellen. Spätestens hier wird der schrankenlose Ansatz der Regelung in § 98 c StVÄG deutlich. Eine derart uferlose Regelung ist mit dem Grundgesetz nicht mehr vereinbar.

Auch die in § 481 StVÄG vorgesehene Regelung hat meine Kritik hervorgerufen. Mit dieser Vorschrift sollen die Strafverfolgungsbehörden berechtigt werden, die im Zuge des Strafverfahrens gewonnenen Daten den im Bundesverfassungsschutzgesetz vorgesehenen Stellen und den Bundesnachrichtendiensten zur Verfügung zu stellen. Bereits in meiner Stellungnahme zum Entwurf des Bundesverfassungsschutzgesetzes (vgl. 9. Jahresbericht, Seite 98 f.) habe ich aufgrund der historischen Erfahrung die strikte Trennung von Polizei und Nachrichtendiensten als verfassungsrechtlich unverzichtbar dargestellt. In diesem Zusammenhang habe ich darauf hingewiesen, daß sich das Trennungsgebot nicht in einer bloßen organisatorischen Trennung zwischen Nachrichtendiensten und Polizei erschöpfen kann. Gerade wegen der automatisierten Datenverarbeitung ist eine strikte Trennung der Informationsbestände ebenso wichtig. Das Trennungsgebot darf daher nicht durch einen umfassenden Informationsaustausch unterlaufen werden. Die im Entwurf des Bundesverfassungsschutzgesetzes vorgesehenen Regelungen sollen nun eine Entsprechung in der Strafprozeßordnung finden. Nahezu schrankenlos soll es möglich sein, Informationen, die mit spezifischen, nur den Strafverfolgungsbehörden zur Verfügung stehenden Methoden gewonnen wurden, den Verfassungsschutzbehörden und den Nachrichtendiensten zu übermitteln.

In meiner Stellungnahme gegenüber dem Senator für Justiz und Verfassung bin ich abschließend zu dem Ergebnis gekommen, daß auch der 1989 vorgelegte Arbeitsentwurf zur Strafprozeßordnung noch einer weitgehenden Überarbeitung bedarf und keinesfalls datenschutzrechtlichen Anforderungen entspricht. Interessierte können meine Stellungnahmen zu den Arbeitsentwürfen zum Strafverfahrensänderungesetz bei mir anfordern.

2.3.2 Aufbau privater Schuldnerverzeichnisse

Die Notwendigkeit einer Novellierung der Vorschrift zum Schuldnerverzeichnis ist seit Jahren bekannt. Die geltenden Vorschriften sind zu wenig präzise, teilweise fehlt ihnen die Rechtsnormqualität und außerdem berücksichtigen sie nicht die neuere Rechtsprechung zum Grundrecht auf informationelle Selbstbestimmung. Das Hauptproblem der Weitergabe von Schuldnerlisten an eine Vielzahl öffentlicher Stellen und privater Firmen ist weiterhin nicht befriedigend gelöst. Die Risiken der heutigen Praxis liegen u. a.

- in der zum Teil nicht ausreichenden Identifizierung der Eingetragenen und der damit verbundenen Gefahr einer Verwechslung,
- in der breiten Streuung der Daten, welche die Einhaltung der gesetzlichen Berichtigungs- und Löschungsregelungen stark erschwert sowie
- in der nicht ausreichenden Möglichkeit der Datenschutzkontrolle bei privaten Stellen.

Diese Situation wird noch verschärft, soweit die Absicht durchschlagen sollte, daß private Firmen eigene bundesweite Schulderverzeichnisse aufbauen.

Gegen die Einführung eines bundesweiten privaten Schuldnerverzeichnisses spricht, daß die Daten der Betroffenen mit staatlichen Zwangsmaßnahmen erhoben werden. Die Verarbeitung dieser Daten muß daher öffentlichen Stellen vorbehalten bleiben. Nach geltendem Recht sind Schuldnerverzeichnisse regional bei den Amtsgerichten zu führen. Auch dies stellt eine Form des Datenschutzes dar, weil selbst im Falle unvollständiger Identifizierungsdaten bei regionalem Bezug eine Verwechslung leichter vermeidbar werden kann. Eine bundesweite Zusammenführung der Schuldnerdaten von privater Seite erhöht dem gegenüber das Risikopotential und die Mißbrauchsmöglichkeiten erheblich und unverhältnismäßig. Die Schuldnerverzeichnisse sollten deshalb ausschließlich bei den Justizbehörden geführt werden, nur dann ist gewährleistet, daß die gesetzlichen Löschungs- und Berichtigungspflichten eingehalten und Auskünfte nur im Rahmen der gesetzlich vorgeschriebenen Zwecke erteilt werden.

Die Zulassung privater zentraler Schuldnerverzeichnisse birgt die Gefahr in sich, daß die mit der Löschung aus dem Schuldnerverzeichnis verbundene Rehabilitation (Recht auf Vergessen) gefährdet wird. Auch die Sicherung der Zweckbindung der Daten erscheint gefährdet, der Abgleich verschiedenster Datenbestände mit Daten aus dem Schuldnerverzeichnis wird dadurch erleichtert werden.

Ich habe den Senator für Justiz und Verfassung gebeten, diese Rechtsauffassung bei der Erteilung von Auskünften und Abschriften aus dem Schuldnerverzeichnis zu berücksichtigen.

2.3.3 ADV-Einsatz bei Gerichten, Staatsanwaltschaften und im Strafvollzug

Im Bereich der DV-unterstützten Führung des Schuldnerverzeichnisses und des Vollstreckungsregisters sind die Untersuchungen nunmehr abgeschlossen; die Realisierung des Verfahrens **SIJUS-Zwangsvollstreckung** steht unmittelbar bevor. Dieses Verfahren löst das bisher eingesetzte Verfahren AVUS (Automatisiertes Vollstreckungsregister und Schulderverzeichnis) ab, wobei Erweiterungsmöglichkeiten durch die Einbeziehung des ADV-Verfahrens ADAM (Andere M-Sachen = übrige Mobiliar-Zwangsvollstreckungsverfahren) und der Textverarbeitungskomponente verwirklicht werden. Noch nicht realisiert ist die Automatisierung des Handelsregisters, die bei Ausweitung der Hardware-Konfiguration in dieses Verfahren einbezogen werden könnte.

Bei meiner datenschutzrechtlichen Stellungnahme habe ich zunächst die Forderungen aufgenommen, die ich bereits zu dem ADV-Projekt AVUS im Jahre 1986 gestellt habe. In Verbindung mit dem Schuldnerverzeichnis hatte ich seinerzeit auf die Notwendigkeit der grundsätzlichen Überarbeitung der Vorschriften nach § 915 Abs. 4 ZPO, insbesondere die Eingrenzung der Weitergabe der Schuldnerverzeichnisdaten an dritte Stellen, wie auch die Einhaltung der Löschungsvorschriften durch dritte Stellen, hingewiesen (vgl. Punkt 2.3.2). Da die gesetzliche Überarbeitung noch aussteht, gehe ich weiter davon aus, daß im Zuge einer Novellierung dieser Vorschrift auch das neu eingesetzte Verfahren den neuen gesetzliche Anforderungen umgehend angepaßt werden wird. Neben diesen grundsätzlichen Aussagen bin ich auf die erweiterten Funktionsmöglichkeiten eingegangen, die mit dem SIJUS-Zwangsvollstreckungsverfahren geboten werden. Dieses System bietet die Möglichkeit, den Zugriffsschutz durch eine Kennwortvergabe herzustellen und darüber hinaus die Möglichkeit der Definitionen von Anwenderprofilen, um dem jeweiligen Anwender jeweils nur Zugang zu den Funktionen zu ermöglichen, die dieser für seine Aufgabenerfüllung braucht. Ich habe gefordert, diese Möglichkeiten zu nutzen. Es bestehen darüber hinaus vielfältige Suchfunktionen, wobei nicht ohne weiteres auszuschließen ist, daß dabei Daten nicht nur für Zwecke verarbeitet werden, für die sie erhoben worden sind. Ich habe daher gefordert, technische und organisatorische Maßnahmen zu treffen, um die Zweckbindung sicherzustellen. Weiterhin werden vielfältige Statistikfunktionen angeboten, die die Möglichkeit zulassen, Aussagen über Tätigkeitsbereiche der eingesetzten Mitarbeiter zu treffen. Es ist daher sicherzustellen, daß diese Statistiken nicht arbeitsplatz- oder arbeitnehmerbezogen ausgewertet werden; das gleiche gilt für Fehler- und Änderungsprotokolle. Soweit die Funktion der Anlage von Hilfsdateien genutzt wird, sind diese unmittelbar nach Erreichen der gewünschten Information zu löschen; bzw. bei längerer Speicherung in das Dateienverzeichnis aufzunehmen.

Hinsichtlich der Erweiterung um Textverarbeitungskomponenten habe ich schließlich gefordert, sicherzustellen, daß in diesem Zusammenhang nur Daten genutzt werden, deren Speicherung im Zusammenhang mit der Verarbeitung von

Zwangsvollstreckungsvorgängen erforderlich ist. Darüber hinausgehende personenbezogene Daten anderer Personen sind nach Absenden des Schreibens zu löschen.

Ich gehe davon aus, daß bei der Realisierung des Verfahrens SIJUS-Zwangsvollstreckung meine Anforderungen berücksichtigt werden.

Weitere ADV-Verfahren im Bereich der Zivilsachen, der Familiensachen, der Automatisierung des Grundbuches sowie der Gerichtskosten- und Geldstrafenvollstreckung befinden sich im Stadium der Voruntersuchung bzw. der Vorüberlegung.

Weiterhin habe ich auch in diesem Berichtszeitraum zu vielfältigen **PC-Einsätzen** in den Geschäftsstellen, Präsidialabteilungen, Schreibdiensten der Gerichte und Staatsanwaltschaften Stellung genommen und dabei datenschutzrechtliche Anforderungen — z. B. im Bereich des Arbeitnehmerdatenschutzes — durchgesetzt.

2.4 Bildung, Wissenschaft und Kunst

Automatisierung von Aufgaben der Stadtbibliothek Bremen

Zur Rationalisierung verschiedener bisher manuell erledigter Aufgaben beabsichtigt die Stadtbibliothek Bremen die Einführung eines ADV-Verfahrens. Eine Entscheidung darüber, welches von zwei getesteten Bibliotheksverwaltungssystemen eingeführt werden soll, steht noch aus. Ich hatte im Berichtsjahr Gelegenheit, die beiden Systeme im Test kennenzulernen und datenschutzrechtliche Probleme zu erörtern.

Da es für die Verarbeitung personenbezogener Daten durch die öffentlichen Bibliotheken im Lande Bremen keine spezifischen Erlaubnisvorschriften gibt, kann die Zulässigkeit der von der Stadtbibliothek Bremen beabsichtigten Datenverarbeitung nur aus den Bestimmungen des BrDSG abgeleitet werden. Nach § 3 Abs. 1 BrDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das BrDSG oder eine andere Rechtsvorschrift sie erlaubt oder zwingend voraussetzt bzw. alternativ, wenn der Betroffene in die Verarbeitung seiner Daten eingewilligt hat. Als gesetzliche Erlaubnisvorschriften zur Datenverarbeitung kommen mangels spezifischer Regelungen die §§ 10 ff. BrDSG in Frage. Nach den §§ 10 und 11 BrDSG dürfte die Stadtbibliothek Bremen personenbezogene Daten erheben, speichern und nutzen, wenn dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist.

„Rechtmäßige Aufgabenerfüllung" wird im Sinne von „durch Rechtsnorm zugewiesene Aufgabe" interpretiert. Die Stadtbibliothek Bremen arbeitet jedoch nicht auf der Grundlage einer Rechtsvorschrift, also einer durch Rechtsnorm zugewiesenen Aufgabe im Sinne vom § 3 Abs. 1 Nr. 1 BrDSG; es gibt lediglich eine von der Stadtbibliothek erlassene Benutzungsordnung sowie eine vom Senator für Bildung, Wissenschaft und Kunst erlassene Entgeltordnung. Zwar hängt in jeder Zweigstelle der Stadtbibliothek Bremen die Benutzungsordnung aus, diese hat aber keinen rechtsverbindlichen Charakter im Sinne einer Rechtsvorschrift. In der Benutzungsordnung wird die Stadtbibliothek Bremen als eine öffentliche Einrichtung ausgewiesen, in der jedermann berechtigt ist, auf privatrechtlicher Grundlage u. a. Bücher auszuleihen. Trotz der privatrechtlichen Ausgestaltung des Benutzungsverhältnisses ist die Stadtbibliothek Bremen als öffentliche Einrichtung zu betrachten, weil sie eine auf der Landesverfassung beruhende Kulturaufgabe erfüllt.

In Bremerhaven hat der Magistrat am 26. Juni 1966 nach Beschlußfassung durch die Stadtverordnetenversammlung eine Benutzungs- und Gebührenordnung verkündet. Bei dieser Ordnung handelt es sich um ein Ortsgesetz, das die Verfassung des Landes Bremen und die Stadtverfassung Bremerhaven ortsgesetzlich konkretisiert. Diesem Beispiel folgend sollte die Stadtgemeinde Bremen für ihre Stadtbibliothek adäquates Ortsrecht schaffen, mit der Folge, daß die Zulässigkeitsnormen des BrDSG zur Datenverarbeitung, speziell die §§ 10 - 13, 17 anwendbar wären.

Die Verarbeitung von Benutzerdaten wäre dann im erforderlichen Umfang auch ohne spezielle Einwilligung der Betroffenen erlaubt. Die Nutzung dieser Daten für geschäftsstatistische Aufbereitungen wie z. B. Benutzerstatistik, Ausleihstatistik, Erwerbungsstatistik etc. wäre im Rahmen des § 11 Landesstatistikgesetz möglich. Als Grundsatz für diese Geschäftsstatistiken muß gelten, daß Benutzerprofile, Leserprofile, d. h. personenbezogene Geschäftsstatistiken, nicht erstellt werden

und im übrigen statistische Ergebnisse nur weitergegeben oder veröffentlicht werden, wenn sie keine Angaben enthalten, die einen Bezug auf Betroffene zulassen.

Neben Überlegungen zur Zulässigkeit der personenbezogenen Datenverarbeitung hat die Stadtbibliothek Bremen auch angemessene Datensicherungsmaßnahmen zu ergreifen und die Betroffenenrechte sowie die sonstigen Pflichten des Bremischen Datenschutzgesetzes (z. B. § 7, § 28) zu beachten. In diesem Sinne werde ich die Stadtbibliothek Bremen weiter beraten.

2.5 Arbeit

Rentenreformgesetz (Sozialgesetzbuch VI. Buch)

Im 11. Jahresbericht habe ich auf den Seiten 14 bis 16 die Stellungnahme wiedergegeben, die ich dem Senator für Arbeit gegenüber zu dem seinerzeit vorliegenden Gesetzentwurf abgegeben hatte. Inzwischen ist das Gesetz in Kraft getreten, nachdem der Gesetzgeber einige der datenschutzrechtlichen Anforderungen, die übereinstimmend von den Datenschutzbeauftragten des Bundes und der Länder aufgestellt worden waren, in einem neu eingefügten Abschnitt „Datenschutz" aufgegriffen hatte. Es fehlen aber weiterhin Löschungsregelungen sowie ausreichende Regelungen zum Schutz der besonders schutzbedürftigen medizinischen Daten, vor allem im Bereich der Rehabilitationsmaßnahmen und der ärztlichen Untersuchungen wegen Erwerbs- und Berufsunfähigkeit.

Vor allem aber kann es künftig allen übrigen Trägern der Rentenversicherung, den gesetzlichen Krankenkassen, den Arbeitsämtern, der Bundespost und dem Verband deutscher Rentenversicherungsträger gestattet werden, bei einem Träger der Rentenversicherung die Daten von dessen Versicherten direkt abzurufen (§§ 148 Abs. 3 und 150 Abs. 4 Rentenreformgesetz). Darüber hinaus wird der Direktabruf von diesen Daten auch aus dem Ausland zugelassen. Damit wird es der speichernden Stelle unmöglich gemacht, ihrer im Sozialgesetzbuch geregelten Pflicht nachzukommen, für die Wahrung des Sozialgeheimnisses der bei ihr Versicherten Sorge zu tragen. Wer einen solchen Direkt- oder Online-Anschluß benutzen darf, braucht nämlich weder die speichernde Stelle um Erlaubnis zu fragen noch sein Auskunftsersuchen zu begründen. Auf Knopfdruck werden ihm alle Versichertendaten zur Verfügung gestellt. Dies birgt die akute Gefahr in sich, daß Versichertendaten über den gesetzlich zulässigen Rahmen hinaus zu fremden Zwecken verarbeitet werden. Und dies, obgleich Rentenversicherungen auch höchst sensible gesundheitliche und psychologische Daten ihrer Versicherten speichern. Die Eröffnung des Direktabrufs aus dem Ausland auf alle bei den deutschen Rentenversicherungsträgern gespeicherten Versichertendaten gefährdet in besonders hohem Maße das Persönlichkeitsrecht der davon betroffenen, zumal längst nicht alle Staaten — selbst nicht innerhalb der EG — ein Datenschutzgesetz oder einen entsprechenden Sozialdatenschutz geschaffen haben. Die Regelung genügt nicht den Anforderungen, die das Bundesverfassungsgericht an einen Eingriff in das Recht auf informationelle Selbstbestimmung aufgestellt hat.

Sie ist kurz vor der abschließenden Lesung im Deutschen Bundestag in das Rentenreformgesetz eingefügt worden, ohne daß Notwendigkeit und Auswirkung politisch und fachlich hätten erörtert werden können. Allein der Einfluß von interessierter Seite scheint den Ausschlag gegeben zu haben. Die Datenschutzbeauftragten der Länder hatten vor der Verabschiedung durch den Deutschen Bundestag keine Gelegenheit, ihre Bedenken vorzutragen. Ich konnte lediglich vor der abschließenden Behandlung des Gesetzentwurfs im Bundesrat dem Senator für Arbeit und dem Senator für Bundesangelegenheiten gegenüber meine Bedenken vortragen. Meine Bedenken wurden geteilt, es sei dem Bundesrat jedoch nur möglich, über eine Anrufung des Vermittlungsausschusses noch eine Gesetzesänderung zu erreichen, dies aber sei angesichts des politischen Stellenwertes des dem Gesetz zugrundeliegenden Rentenkompromisses nicht realisierbar. Ähnliche Antworten haben die Datenschutzbeauftragten anderer Länder von ihren Landesregierungen erhalten. Es bleibt jetzt nur zu hoffen, daß der Präsident des Senats seine Ankündigung, die Angelegenheit bei nächstgeeigneter Gelegenheit aufzugreifen, um die aufgezeigten Mängel auszuräumen, in absehbarer Zeit umsetzen kann. Andernfalls bliebe nur die Hoffnung, daß das Bundesverfassungsgericht angerufen wird und die kritisierten Regelungen des Rentenreformgesetzes für nichtig erklärt werden.

2.6 Jugend und Soziales

2.6.1 Schwerpunkte, Handlungsbedarfsfälle

2.6.1.1 Innerbehördlicher Datenschutz in den sozialen Diensten

Den Schwerpunkt meiner Tätigkeit in diesem Bereich — sei es im Zusammenhang mit Einzelbeschwerden, sei es bei der Beteiligung an der Ausgestaltung von Verfahrensregelungen, sei es bei Fortbildungsveranstaltungen oder Behördenkonferenzen — bildete das Bemühen, auf den Schutz des Sozialgeheimnisses (§ 35 Sozialgesetzbuch I —SGB I —) und die Respektierung beruflicher Schweigepflichten (§ 203 Strafgesetzbuch — StGB —) in der Praxis des Amtes für Soziale Dienste hinzuwirken. Dabei zeigte sich immer wieder, daß die Sozialarbeiter/innen, Sozialpädagog/innen sowie Sachbearbeiter/innen durchweg sich ihrer einschlägigen Rechte und Pflichten bewußt sind, während — jedenfalls in der Vergangenheit — mit zunehmender Distanz zu den Klient/innen auf Kontroll-, Koordinierungs- und Planungsebene Datenschutz bzw. der Schutz des Sozialgeheimnisses all zu oft gar nicht ins Blickfeld geraten ist bzw. als Restaufgabe verkannt worden ist. Dies ist vor allem auch deshalb beklagenswert, weil

- mit der Neuorganisation der Sozialen Dienste (Zusammenfassung verschiedener Ämter im Amt für Soziale Dienste, Konferenzsystem, Kooperation zwischen verschiedenen Sachgebieten im Einzelfall),
- mit dem Bemühen, interne Kontrollen, Sozialplanung und praxisbegleitende Forschung zu intensivieren,
- mit der Entwicklung inhaltlich anspruchsvoller und differenzierter Konzeptionen für Hilfen und Angebote

die Quantität der Datenerhebung und der Datenfluß innerhalb des Ressorts Jugend und Soziales erheblich zugenommen haben. Leider ist die Einbeziehung des Datenschutzbeauftragten bereits in der Phase der Konzeptionierung, wie es bei PROSOZ praktiziert wurde, bislang die Ausnahme geblieben.

Rechtliche Grundlagen des Schutzes des Sozialgeheimnisses

- Die Erhebung eines Sozialdatums beim Betroffenen ist nur zulässig,
  - soweit dieser eine Sozialleistung beantragt und deshalb die entsprechende Tatsache anzugeben hat,
  - weil sie für die Entscheidung über die Gewährung der Leistung erheblich ist (§ 60 Abs. 1 Nr. 1, 1. Alternative SGB I),
  - im übrigen nur, wenn der Betroffene die Tatsache angibt, nachdem er über den Zweck der Erhebung sowie darüber aufgeklärt ist, daß er zur Angabe dieser Tatsache nicht verpflichtet ist und seine Weigerung zur Mitwirkung für ihn keine nachteiligen Folgen hätte. Letzteres gilt z. B. für die Erhebung von Daten zum Zwecke des Forschungsprojekts „Empirische Untersuchungen zu den Ursachen der Sozialhilfeabhängigkeit" (vgl. Pkt. 2.6.1.2).
- Zur Bearbeitung eines Antrages darf der Sozialleistungsträger Auskünfte bzw. Gutachten von Dritten nur einholen, nachdem der Antragsteller dem zugestimmt hat, vgl. §§ 60 Abs. 1 Nr. 1, 2. Alternative, 62 SGB I. Ggf. ist zusätzlich erforderlich, daß der Dritte von seiner Schweigepflicht nach § 203 StGB vom Antragsteller entbunden wird. Jedenfalls ist es unzulässig, die Auskunft oder das Gutachten über den Kopf des Antragstellers hinweg einzuholen. Es besteht Anlaß zu der Annahme, daß aus Gründen der Arbeitseffektivität in der alltäglichen Praxis dieser Grundsatz nicht immer eingehalten wird. Ein Anruf „auf dem kurzen Dienstweg" eröffnet oft leichter den Weg zur erwünschten bzw. auch erforderlichen Information als die Auseinandersetzung mit dem Antragsteller/Klienten.
- Davon zu unterscheiden ist die Frage, ob und inwieweit die Stelle oder Person, die zuständig ist für die Erhebung von Sozialdaten, zu deren Geheimhaltung verpflichtet ist oder ob sie berechtigt ist, sie an andere Stellen bzw. Personen zu offenbaren bzw. zu übermitteln. Dies ist im Bereich der Sozialleistungsträger in §§ 35 SGB I, 67 - 79 SGB X, aber auch im § 203 StGB geregelt. Aus dem Recht zur Erhebung von Daten ergibt sich nicht das Recht zu ihrer Offenbarung. Anders gesagt: Aus der Verpflichtung des Antragstellers, im Rahmen seiner für die Entscheidung erforderlichen Mitwirkung Daten preiszugeben bzw. der Preisgabe von Daten zuzustimmen, folgt nicht, daß er verpflichtet ist, der Weiterleitung von Daten zuzustimmen. Andernfalls liefen die Vorschriften zum Schutz des Sozialgeheimnisses neben denen zur Mitwirkungspflicht leer. Dies verkennt die Stellungnahme des Senats zu meinem 11. Jahresbericht (vgl. Seite 9 der Bürgerschaftsdrucksache — Landtag — 12/604).

- Das Sozialgeheimnis ist auch innerhalb eines Sozialleistungsträgers zu wahren. Sozialdaten dürfen zwischen Arbeitseinheiten, die nach der Geschäftsverteilung unterschiedliche Aufgaben wahrnehmen, nur offenbart werden,
  - soweit dies zur Erfüllung derjenigen im Sozialgesetzbuch geregelten Aufgabe, für die die Sozialdaten erheblich sind und deshalb erhoben werden durften, erforderlich ist (§ 69 Abs. 1 Nr. 1 SGB X) oder
  - soweit es für den Fall, daß mit der Offenbarung eine Änderung des Verwendungszwecks der Daten verbunden ist, eine aufgabenspezifische Übermittlungsnorm in einem Spezialgesetz gibt oder die Offenbarung durch die §§ 70—77 SGB X gedeckt ist oder
  - soweit der Antragsteller/Leistungsempfänger/Klient wirksam eingewilligt hat.
- Beratungsgeheimnisse, die durch § 203 StGB geschützt sind, dürfen auch intern grundsätzlich nur mit Einwilligung des Klienten offenbart werden. Voraussetzung für die Wirksamkeit der Einwilligung sind
  - Erheblichkeit der geschützten Daten für die Entscheidung über eine beantragte Leistung (analog § 60 SGB I); hierüber und über evtl. nachteilige Folgen bei verweigerter Einwilligung ist der Klient aufzuklären; oder
  - Aufklärung über die Freiwilligkeit der Einwilligung und das Ausbleiben nachteiliger Folgen bei verweigerter Einwilligung.
- Sozialdaten, die ein Arzt oder eine andere in § 203 Abs. 1, 3 SGB genannte Person einer Stelle innerhalb des Sozialleistungsträgers im Zusammenhang mit einer Begutachtung zwecks Entscheidung über eine beantragte Sozialleistung zugänglich gemacht hat (vgl. § 62 SGB I, 76 SGB X), dürfen an eine andere Stelle innerhalb des Sozialleistungsträgers nur unter den oben genannten Voraussetzungen weiterübermittelt werden.
- Um die rechtlich gebotene Differenzierung zu gewährleisten, sind
  - vertrauliche Beratung,
  - Begutachtung,
  - Entscheidung über den Antrag auf eine Sozialleistung
  - sowie Forschung und Sozialplanung

eindeutig voneinander abzugrenzen.

- In jedem Falle ist die Offenbarung von Daten auf das für das Verfahren, in dessen Zusammenhang sie erhoben wurden, unumgängliche Maß zu beschränken. Es sind organisatorische Maßnahmen zu treffen, um darüber hinausgehende Erhebungen und Offenbarungen zu verhindern. Dies bedeutet z. B. im einzelnen:
  - An Fallbesprechungen (Konferenzen) dürfen nur solche Personen teilnehmen, deren Teilnahme für die Entscheidung über den gestellten Antrag erforderlich ist. Personenbezogene Daten in Einladungen, Besprechungsunterlagen, Ergebnisvermerken, Protokollen o. ä. dürfen nur diesem Personenkreis zugänglich gemacht werden.
  - Kooperieren mehrere Stellen innerhalb des Sozialleistungsträgers mit unterschiedlichen Aufgabenstellungen in einem arbeitsteiligen Verfahren, so dürfen jeder dieser Stellen nur die Daten zugänglich gemacht werden, die sie für ihren jeweiligen Arbeitsanteil benötigen (abgestufter Informationsfluß).
  - Ärztliche/Psychologische Gutachten dürfen nur der öffentlichen Stelle zugänglich gemacht werden, zu deren fachlicher Entscheidung/Stellungnahme ihre Übermittlung erheblich ist.
  - Die Antragsteller sind zu Beginn umfassend über das Verfahren und den Zweck einzelner vorgesehener Erhebungen bzw. Offenbarungen aufzuklären.
  - Vor Stellung eines Antrages handelt es sich in der Regel um vertrauliche Beratung, so daß Schweigepflicht besteht und jede Offenbarung unzulässig ist.
  - Es sollten möglichst Informationsblätter und Vordrucke benutzt werden (vgl. § 60 Abs. 2 SGB I).
  - Den Antragstellern sind über sie eingeholte Auskünfte und Gutachten zugänglich zu machen.

- Die Sozialdaten sind zu löschen, sobald sie für die Entscheidung, zu deren Vorbereitung sie erhoben wurden, nicht mehr benötigt werden und kein Grund für die Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden (vgl. § 84 SGB X).

Anwendungsfälle: Aufnahmeverfahren für die heilpädagogische Erziehung in Kindertagesheimen und für das Betreute Wohnen

Im Zusammenhang mit den Verfahren auf Aufnahme/Verlängerung/Finanzierung von

— heilpädagogischer Erziehung in Kindertagesheimen und

— der Unterbringung in Einrichtungen des Betreuten Wohnens

(vgl. meine Kritik im 11. Jahresbericht unter Pkt. 5.5.1.3/4) ist inzwischen mit Vertretern der senatorischen Dienststelle und des Amtes für Soziale Dienste ein Konsens erzielt worden, der den oben genannten Anforderungen Rechnung trägt und der bereits für das Aufnahmeverfahren für das Kindergartenjahr 1990/91 Anwendung finden soll. Als Hauptproblem im Rahmen des „Betreuten Wohnens" hatte sich herausgestellt, daß das Sachgebiet „Wirtschaftliche Hilfen" des Amtes für Soziale Dienste, das über die Übernahme der Betreuungskosten zu entscheiden hat, sämtliche von den Antragstellern erhobene Daten und über sie erstellte ärztliche und psychologische Gutachten übermittelt hat und in seinen Akten speichern wollte, obwohl für die fachliche Beurteilung des Hilfebedarfs und der Eignung der beantragten Maßnahme einer der altersbezogenen Sozialdienste zuständig ist.

Schließlich sind aber einverständlich datenschutz-rechtlich akzeptable Lösungen gefunden worden. Ärztliche bzw. psychologische Gutachten werden nur dem Sozialpsychiatrischen Dienst zur Erstellung von dessen Stellungnahme zum Gesamtplan (vgl. § 46 BSHG) zugänglich gemacht. Dieser übermittelt seine Stellungnahme auf einem Formblatt dem altersgruppenbezogenen Sozialdienst, der seinerseits fachlich zu beurteilen hat, ob die beantragte Maßnahme erforderlich bwz. geeignet ist. Der letztere Dienst wiederum trennt vor der Weiterleitung der Stellungnahme die Seite des Formblatts ab, die Aussagen zur Krankheitsvorgeschichte sowie zur Sozialen Anamnese, zur Selbständigkeit und zur sozialen Situation des Klienten enthält. Dagegen werden eine kurze Begründung für die Befürwortung des Antrags sowie die Daten an die Abteilung „Wirtschaftliche Hilfen" übermittelt, die diese für die ihr obliegenden Entscheidungen benötigen wird. Nachteil dieses Verfahrens ist es sicherlich, daß im Einzelfall auch nicht erforderliche Daten übermittelt werden können. Es ist jedoch zu bedenken, daß insgesamt eine Praxis gewährleistet wird, die den bisherigen Datenfluß erheblich einschränken wird. Vor allem Daten, die der Schweigepflicht nach § 203 StGB unterliegen, werden künftig erstmals einen garantierten innerbehördlichen Schutz genießen.

Die gilt vorerst nur für die Bereiche

— der heilpädagogischen Erziehung in den Kindertagesheimen und

— des Betreuten Wohnens.

Vergleichbare Probleme der innerbehördlichen Übermittlung bzw. Offenbarung von Daten, die den Schutz des Sozialgeheimnisses genießen, treten aber auch z. B. im Zusammenhang mit

— dem Aufnahmeverfahren für Kindertagesheime,

— der Hilfe in Heimen,

— dem Einsatz von Familienhelfern und

— den Stellungnahmen der Jugendgerichtshilfe

auf. Ich erwarte, daß der für die erstgenannten Verfahren erzielte Standard des Datenschutzes für die Ausgestaltung der vergleichbaren Verfahren durchgesetzt wird.

2.6.1.2 Empirische Untersuchungen zu den Ursachen der Sozialhilfeabhängigkeit

In meinem letzten Jahresbericht habe ich unter Pkt. 5.1.2 über einen Forschungsauftrag berichtet, den der Senator für Jugend und Soziales dem Zentrum für Sozialpolitik der Universität Bremen erteilt hat.

Anläßlich einer Prüfung beim Zentrum für Sozialpolitik wurde ich darüber in Kenntnis gesetzt, daß zwei Mitarbeiter dieses Sonderforschungsbereichs an das Amt für Soziale Dienste abgeordnet seien und dort Sozialhilfeakten für dieses Forschungsprojekt auswerteten.

Ich habe gegenüber der senatorischen Dienststelle dargelegt, daß durch diese Personenidentität die Verpflichtung des Sozialleistungsträgers in Frage gestellt wird, das Sozialgeheimnis gegenüber dem Forschungsbereich wirksam zu schützen. Entsprechend war es bisher das gemeinsame Bestreben zu gewährleisten, daß Mitarbeiter des Forschungsprojektes lediglich anonymisierte Sozialdaten ohne Möglichkeit der Reidentifizierung zur Kenntnis erhalten sollten, es sei denn, daß für die weitere Auswertung vorher Einwilligungen eingeholt werden.

Das nunmehr praktizierte Verfahren steht im Widerspruch zu § 75 SGB X. Danach ist eine Offenbarung von Sozialdaten zu Forschungszwecken dann nicht zulässig, soweit es zumutbar ist, die Einwilligung des Betroffenen einzuholen oder den Zweck der Forschung auf andere Weise zu erreichen. Da das Forschungsprojekt — zumindest bei der Groberhebung — von einer Einwilligung unabhängig verfahren will, kommt es wie wiederholt auch ausführlich erörtert, in diesem Zusammenhang darauf an, die Daten wirkungsvoll zu anonymisieren, bevor sie an das Forschungsprojekt übermittelt werden. Dies haben sowohl der Senator für Jugend und Soziales als auch das Amt für Soziale Dienst ausdrücklich anerkannt.

So heißt es in der Genehmigung des Senators für Jugend und Soziales als oberste Landesbehörde nach § 75 Abs. 2 SGB X, daß durch geeignete organisatorische Maßnahmen sicherzustellen ist, daß die Deanonymisierung zum Zwecke der weiteren Feinauswertung und zum Zwecke der Befragung der Hilfeempfänger nur durch die dafür zuständigen Mitarbeiter des Amtes für Soziale Dienste in den Räumen des Amtes stattfindet.

Darüber hinaus ist anläßlich einer Besprechung festgelegt worden, daß bei der Auswertung der Akten mit Hilfe des Groberhebungsbogens nur Mitarbeiter des Amtes für Soziale Dienste tätig werden sollen. Es sollte genau festgelegt werden, welche Mitarbeiter eine Zugriffsberechtigung für diese Arbeit haben sollen. Ebenso bestand Einvernehmen darüber, daß genau festgelegt werden muß, wie die Stichprobenakten vor unbefugtem Zugriff gesichert werden sollen. Es wurde ausdrücklich abgesprochen, daß an das Zentrum für Sozialpolitik ausschließlich anonymisierte Daten weitergegeben werden. Umgekehrt werden vom Zentrum für Sozialpolitik ausschließlich aggregierte, ausgewertete Daten an das Amt für Soziale Dienste weitergegeben.

Ich hatte den Senator für Jugend und Soziales sowie das Amt für Soziale Dienste um unverzügliche Stellungnahme gebeten und mir vorbehalten, den Verstoß gegen Datenschutzbestimmungen entsprechend § 29 BrDSG zu beanstanden. Da nach Ablauf von zwei Monaten noch keine Reaktion erfolgt war, habe ich inzwischen die Beanstandung ausgesprochen.

2.6.1.3 Dienstanweisung über die Pflicht zur Anzeige strafbarer Handlungen

Das Amt für Soziale Dienste hat seine Mitarbeiter/innen in einer Dienstanweisung darüber informiert, inwieweit sie verpflichtet sind, strafbare Handlungen anzuzeigen, von denen sie dienstlich Kenntnis erhalten. Die nunmehr bekanntgegebene Fassung hat die von mir bereits an einem Entwurf geübte Kritik in wesentlichen Teilen nicht aufgenommen, ohne daß dafür eine Begründung gegeben worden wäre. Die Anweisung bezieht sich als Grundlage auf eine Anweisung der Senatskommission für das Personalwesen aus dem Jahre 1959, in der — allerdings vor Ausweitung der durch § 203 Strafgesetzbuch (StGB) sanktionierten beruflichen Schweigepflichten und vor der gesetzlichen Regelung des Sozialgeheimnisses im Sozialgesetzbuch — eine unterschiedslose Anzeigepflicht behauptet wurde. Anschließend wurden die Regelungen des Sozialgesetzbuches daneben gestellt. Die strafrechtliche Schweigepflicht wird überhaupt nicht erwähnt. Die ihm obliegende Fürsorgepflicht gegenüber dem Arbeitnehmer gebietet es aber, daß der Arbeitgeber dafür Sorge trägt, daß der Arbeitnehmer vor strafbaren Handlungen bewahrt wird.

Ich habe das Amt für Soziale Dienste erneut darauf hingewiesen, daß auch die Anweisung in der neuen Fassung verwirre, statt zutreffend über Anzeige- bzw. Schweigepflichten aufzuklären, und daher aufzuheben sei. Eine entsprechende Anweisung müsse völlig neu erarbeitet werden. Nachdem das Amt auch hierauf nicht reagiert hatte, habe ich mich an den Senator für Jugend und Soziales und an

die Senatskommission für das Personalwesen gewandt mit der Bitte, tätig zu werden, das Sozialgeheimnis zu schützen bzw. die Fürsorgepflicht des Arbeitgebers wahrzunehmen. Antworten stehen noch aus.

2.6.2 Kurze Darstellung von Problemen und Beschwerden

2.6.2.1 Sachfremde Anmerkungen in der Sozialhilfeakte

Anläßlich einer Eingabe habe ich in einem Ortsamt die Sozialhilfeakte des Betroffenen durchgesehen und dabei festgestellt, daß sich in ihr Unterlagen und Hinweise befinden, die nicht im Zusammenhang mit dem Sozialhilfeantrag stehen.

So enthielt die Akte einen Zeitungsartikel, der über den Betroffenen in einem anderen Zusammenhang berichtete. Darüber hinaus enthielt die Sozialhilfeakte Vermerke, die persönliche Bewertungen und subjektive Eindrücke der jeweiligen Sachbearbeiter wiedergeben, obwohl sie ebenfalls für die Gewährung der beantragten Leistung nicht erheblich waren, z. B. Hinweise darauf, der Betroffene sei Querulant usw.

Inzwischen sind die entsprechenden Unterlagen aus der Akte entfernt worden.

Grundsätzlich stimmt der Senator für Jugend und Soziales mit mir überein, daß die Aufnahme von Vermerken in die Akte, die ein persönliches Verhalten des Klienten bewerten, nur dann als zulässig angesehen werden kann, wenn sie für die Bearbeitung des Falles im Sinne einer umfassenden Hilfegewährung erforderlich sind. Er hat mir zugesichert, bei Fortbildungs- oder ähnlichen Veranstaltungen diesem Gesichtspunkt besondere Aufmerksamkeit zu widmen.

2.6.2.2 Anforderungen von Gutachten des Hauptgesundheitsamtes bei Anträgen von HIV-positiven Sozialhilfeempfängern

Veranlaßt durch eine Einzelbeschwerde habe ich das Amt für Soziale Dienste und das Hauptgesundheitsamt Bremen darum gebeten, mir darzulegen, warum bei Anträgen von HIV-positiven Sozialhilfeempfängern auf Gewährung von Mehrbedarf (Krankenkostzulage) in jedem Fall die Einholung eines amtsärztliche Attests verlangt werde. Die Frage sei, ob diese Untersuchung erheblich bzw. erforderlich im Sinne der §§ 60, 62 SGB I sei.

Das Hauptgesundheitsamt hat einen Widerspruch zwischen der garantierten Anonymität und Vertraulichkeit seiner Beratungsangebote für HIV-positive Klienten und der Verarbeitung personenbezogener Daten im Rahmen des hier in Rede stehenden Begutachtungsverfahrens anerkannt. Inzwischen hat das Amt für Soziale Dienste bei Mehrbedarfsanträgen von HIV-positiven Sozialhilfeempfängern im Einverständnis mit dem Hauptgesundheitsamt auf die Einholung eines amtsärztlichen Gutachtens verzichtet, wenn ein ärztliches Attest vorgelegt worden ist.

2.7 Gesundheit

2.7.1 Schwerpunkte, Handlungsbedarfsfälle

2.7.1.1 Durchführung des Gesundheitsreformgesetzes (SGB V)

Das „Gesundheitsreformgesetz" ist mit Wirkung vom 1. Januar 1989 als Sozialgesetzbuch V (SGB V) in Kraft getreten. Die zum Teil umfangreichen Neuerungen machen es erforderlich, daß die bisher praktizierte Datenverarbeitung sowohl der Leistungserbringer als auch der Kostenträger den neuen Bestimmungen angepaßt wird. Einige nachstehend dargelegte Beispiele verdeutlichen dies:

— Vereinbarung über die Durchführung der klinischen Arbeitstherapie im Zentralkrankenhaus Bremen-Ost mit den Krankenkassen

Mit Wirkung vom 1. Januar 1989 gilt eine Vereinbarung zwischen dem Zentralkrankenhaus Bremen-Ost und den Krankenkassen, die Aufnahme, Umfang, Dauer und verwaltungsmäßigen Ablauf sowie Kosten der Belastungserprobung für psychiatrische Patientinnen und Patienten im Rahmen der klinischen Arbeitstherapie regelt. Die im Erhebungsbogen aufgeführten personenbezogenen Daten der Patienten sind Leistungsdaten, die über den in § 301 Abs. 1 SGB V genannten Datenumfang hinausgehen.

Ich habe den Senator für Gesundheit gebeten, als Aufsichtsbehörde gegenüber dem Zentralkrankenhaus Bremen-Ost darauf hinzuwirken, daß die Vereinbarung

über die Durchführung der klinischen Arbeitstherapie entsprechend den Bestimmungen des SGB V geändert wird. Eine Antwort des Senators für Gesundheit steht noch aus.

— Maschineller Datenträgeraustausch zwischen den Krankenhausbetrieben und interessierten Kostenträgern

Um das bisherige stationäre Abrechnungsverfahren abzukürzen und die Arbeiten im Krankenhaus sowie beim jeweiligen Kostenträger zu reduzieren, beabsichtigt der Senator für Gesundheit mit interessierten Kostenträgern einen maschinellen Datenträgeraustausch dahingehend durchzuführen, daß bei jeder Rechnungsschreibung pro Kostenträger ein maschineller Datenträger erstellt wird. Da den Krankenhäusern nicht in jedem Fall die Krankenversichertennummer vorliegt, beabsichtigte der Senator für Gesundheit, ersatzweise den Patientennamen und das Geburtsdatum des Patienten sowie die entsprechenden Angaben des Stammversicherten zu übermitteln.

Ich habe dem Senator für Gesundheit dargelegt, daß grundsätzlich gegen einen derartigen maschinellen Datenträgeraustausch keine Bedenken bestehen, jedoch die nach dem SGB V abzuschließende Vereinbarung mit den Kostenträgern keine Übermittlung von Daten vorsehen darf, die über den in § 301 Abs. 1 SGB V genannten Umfang hinausgeht. Inwieweit die abzuschließende Vereinbarung den Bestimmungen des SGB V entspricht, bleibt abzuwarten.

— Prüfung ungewöhnlich langer Verweildauern durch die Krankenkasse

Nach Angaben des Senators für Gesundheit erfolgt derzeit eine Berichterstattung von Seiten der Krankenhäuser an Kostenträger für den Fall, daß Patienten länger als zwei Wochen im Krankenhaus behandelt werden (ärztlicher Bericht), im übrigen auf Einzelanforderung der jeweiligen Krankenkasse.

Ich habe den Senator für Gesundheit darauf hingewiesen, daß der Umfang der an die Kostenträger zu übermittelnden personenbezogenen Daten abschließend in § 301 Abs. 1 SGB V geregelt ist. Lediglich in Einzelfällen kann die zuständige Krankenkasse nach § 275 SGB V eine gutachterliche Stellungnahme des Medizinischen Dienstes einholen. Darüber hinaus bedarf es zur Überprüfung der Notwendigkeit und Dauer der Krankenhausbehandlung einer Vereinbarung nach § 112 Abs. 2 Nr. 2 SGB V. Die Vereinbarung kann jedoch ergänzende Datenübermittlungen über § 301 Abs. 1 SGB V hinaus nicht rechtfertigen.

Der Senator für Gesundheit wird diese Problematik mit den Krankenhäusern erörtern und mich über das Ergebnis unterrichten.

2.7.1.2 Datenschutz im öffentlichen Gesundheitsdienst

Die Gesundheitsämter verarbeiten im Rahmen unterschiedlicher Zuständigkeiten auf der Grundlage der verschiedensten Rechtsvorschriften und in vielfältiger Form personenbezogene Daten. Ihre Aufgaben reichen von der Beratung über die Erstellung von Gutachten bis zu ordnungsrechtlichen Zuständigkeiten. Als Sozialleistungsträger (etwa im Rahmen der Eingliederungshilfe für Behinderte nach §§ 127 f. BSHG) sind sie zum Schutz des Sozialgeheimnisses im Rahmen des Sozialgesetzbuchs (SGB) und des BDSG verpflichtet. Im übrigen haben sie als kommunale Behörden im Lande Bremen die Vorschriften des BrDSG zu beachten. Die Mitarbeiter der Gesundheitsämter unterliegen darüber hinaus als Ärzte, Psychologen, Berater, Sozialarbeiter, Sozialpädagogen sowie als Amtsträger bzw. als Gehilfen der genannten Berufsgruppen der Pflicht zur Wahrung des Berufsgeheimnisses nach § 203 StGB. Eine bereichsspezifische Rechtsgrundlage für die Datenverarbeitung im öffentlichen Gesundheitsdienst im Lande Bremen fehlt. Wie dringend sie ist, wird aus folgenden Zusammenhängen klar:

— Überprüfungen von Gesundheitsämtern in anderen Bundesländern haben eine ganze Reihe von datenschutzrechtlichen Mängeln ergeben.

— An Verfahren im Ressort für Jugend und Soziales, die Gegenstand datenschutzrechtlicher Überprüfung waren (vgl. Punkt 2.2.1.1), sind auch Mitarbeiter/innen des Hauptgesundheitsamts Bremen als Gutachter beteiligt. Sie selbst beklagten wiederholt das Fehlen einer Regelung, die festlegt, welche Daten sie an die Sozialen Dienste übermitteln dürfen und welche nicht.

— Vor allem haben aber auch Überprüfungen und Gespräche im Hauptgesundheitsamt Bremen und im Gesundheitsamt Bremerhaven die Notwendigkeit bereichsspezifischer Regelungen gezeigt.

Stichprobenartige Prüfungen in der Zentralkartei des Amtsärztlichen Dienstes im **Hauptgesundheitsamt Bremen** haben ergeben, daß dort Daten entweder frühestens nach 30 Jahren (Bremische Aktenordnung von 1959), nach der Mitteilung der Meldebehörde über den Tod eines Betroffenen (soweit er zuletzt in Bremen seinen Wohnsitz hatte) oder 100 Jahre nach Geburt des Betroffenen gelöscht werden. Auf diese Weise wird eine Unmenge unnötiger Daten weitergespeichert, weil eine bereichsspezifische Rechtsgrundlage für ihre Löschung und die Kapazität zur Überprüfung der Unterlagen fehlen.

Mit dem Gesundheitsamt Bremerhaven haben bereits mehrere Gespräche, zum Teil verbunden mit Überprüfungen, stattgefunden. Anschließend habe ich dem Gesundheitsamt gegenüber deutlich gemacht, daß

- inhaltliche Aufzeichnungen über Beratungsgespräche nur dem Berater selbst zugänglich sein dürfen, es sei denn, der Klient hat in eine Weiterleitung wirksam eingewilligt,
- ein Vermerk in der Zentraldatei des Amtsärztlichen Dienstes über die Inanspruchnahme eines Beratungsangebotes — etwa des Sozialpsychiatrischen Dienstes — unzulässig ist,
- der Amtsarzt Kenntnisse über eine Klientin, die er zuvor als ärztlicher Berater z. B. im Sozialpsychiatrischen Dienst gewonnen hat, nicht ohne wirksame Einwilligung verwerten darf,
- ich es für zweifelhaft halte, ob der Amtsarzt ohne weiteres Kenntnisse verarbeiten darf, die er über die zu untersuchende Person bereits zuvor im Rahmen vorhergegangener amtsärztlicher Untersuchungen zu anderen Zwecken erhoben hat.

Das Gesundheitsamt Bremerhaven hat sich bislang nicht dazu geäußert. Unabhängig davon halte ich es für erforderlich, daß in dem nunmehr vom Senator für Gesundheit in Angriff genommenen **Gesetz über den öffentlichen Gesundheitsdienst** folgende Datenschutzregelungen getroffen werden:

- Es bedarf einer klaren Definition und Abgrenzung der unterschiedlichen Tätigkeitsformen der Gesundheitsämter dem Bürger gegenüber sowie darauf aufbauend Regelungen zur Übermittlung personenbezogener Daten an andere Stellen.
- Es muß bereichsspezifisch klargestellt werden, daß Berufsgeheimnisse nach § 203 StGB sowohl im innerbehördlichen Bereich als auch gegenüber anderen Stellen gelten.
- Es bedarf der Klärung, inwieweit Daten entgegen dem Zweckbindungsprinzip verarbeitet werden dürfen, die von einem anderen Dienst und/oder in einem anderen Zusammenhang erhoben worden sind.
- Es muß sichergestellt werden, daß personenbezogene Daten gelöscht werden, sobald sie für die Tätigkeit der Gesundheitsämter voraussichtlich nicht mehr erforderlich sind (§ 20 Abs. 3, 4 BrDSG).

2.7.1.3 Wissenschaftliche Begleitung der Auflösung des Klosters Blankenburg

In der Verantwortung des Studiengangs „Psychologie" der Universität Bremen und des Zentralkrankenhauses Bremen-Ost wird eine "Wissenschaftliche Evaluationsstudie zur Auflösung der psychiatrischen Langzeitklinik Kloster Blankenburg und ihrer Umwandlung in dezentrale gemeindenahe Versorgungseinrichtungen im Stadtgebiet Bremen" vorbereitet mit dem Ziel, eine Längsschnittuntersuchung ehemals langzeithospitalisierter geistig und mehrfach behinderter bzw. chronisch seelisch behinderter Erwachsener mit einer Systemanalyse der regionalen psychiatrischen Versorgung zu verbinden. Im Verlauf dieses Projekts wird seinen Mitarbeitern mit Hilfe der Methode der teilnehmenden Beobachtung über einen längeren Zeitraum der gesamte private Bereich der Betroffenen offengelegt werden. Hinzu kommt die Verarbeitung personenbezogener Daten mit Hilfe von Dokumentenanalysen sowie von Befragungen der Betroffenen selbst, ihrer Familien, ihrer Betreuer sowie verschiedener öffentlicher Stellen.

Auf der Grundlage der von den Projektbetreibern vorgelegten Unterlagen sind einverständlich ein Datenschutzkonzept, ein Informationspapier sowie Formulierungen für Einverständniserklärungen und Schweigepflichtsentbindungen durch

die Betroffenen bzw. ihre gesetzlichen Vertreter entwickelt worden. Dabei wurde besonderer Wert darauf gelegt, daß

- die Information sowie die Formulare für Erklärungen der Betroffenen bzw. ihrer Vertreter konkret und verständlich gefaßt sind,
- die Datenverarbeitung an das fortdauernde Einverständnis der Betroffenen gebunden ist,
- der Zugang zu gespeicherten personenbezogenen Daten eng begrenzt und strikt zu protokollieren ist,
- Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, nur solange gespeichert werden dürfen, als es für das Forschungsprojekt erforderlich ist, sie also zum frühestmöglichen Zeitpunkt anonymisiert/gelöscht werden.

2.7.2 Auskünfte eines Krankenhauses an den Sozialleistungsträger

Im Zentralkrankenhaus Bremen-Ost richtet die Zahlstelle bei Bedarf für Patienten ein Eigengeldkonto ein. Überschreitet das Guthaben den Betrag von DM 4.500,—, soll — so eine Richtlinie der Direktion — die Zahlstelle zwecks Information des Sozialhilfeträgers das Sachgebiet Rechnungswesen unterrichten. Hintergrund ist die Regelung, daß Sozialhilfeempfänger kleinere Barbeträge — bei Hilfe in besonderen Lebenslagen von bis zu DM4.500,— — nicht einsetzen müssen, Rechtsverordnung zu § 88 Abs. 2 Nr. 8 Bundessozialhilfegesetz (BSHG). Ich habe das Krankenhaus und das Amt für Soziale Dienste darauf hingewiesen, daß nach § 60 Sozialgesetzbuch I (SGB I) es Sache des Antragstellers auf Sozialhilfe selbst ist, die erheblichen Tatsachen anzugeben. Auskünfte von anderen Stellen darf der Sozialleistungsträger nicht ohne Zustimmung des Antragstellers einholen.

Das Krankenhaus weigert sich, die Richtlinie zu ändern und beruft sich auf das Amt für Soziale Dienste. Dieses erkennt zwar an, daß der Heimträger nicht verpflichtet sei, dem Sozialhilfeträger den Vermögensstand des bei ihm untergebrachten Sozialhilfeempfängers zu melden. Jedoch sei nach § 4 Abs. 1 Nr. 8 Bremisches Krankenhausdatenschutzgesetz (BremKHDSG) das Krankenhaus verpflichtet, Patientendaten dem Kostenträger zu übermitteln, soweit dies zur Feststellung von dessen Leistungspflicht erforderlich sei. Letzteres aber sei hier der Fall, weil nach dem Bundessozialhilfegesetz der Einsatz des angesparten Barbetrags als Vermögen zu verlangen sei, soweit der auf DM 4.500,— festgesetzte Freibetrag überschritten sei.

Ich kann dem nicht folgen. Wenn das Krankenhaus dem Amt für Soziale Dienste über den angesparten Eigenbetrag eines Patienten berichtet, so rechnet es nicht mit dem Kostenträger über die medizinische Versorgung ab, die es erbracht hat. Vielmehr erteilt es eine Auskunft über die Vermögensverhältnisse eines Sozialhilfeempfängers. Nicht das Bremische Krankenhausdatenschutzgesetz, sondern das Sozialgesetzbuch ist anwendbar. Die Auskünfte sind unzulässig, sofern nicht der Betroffene im Einzelfall wirksam eingewilligt hat. Die Richtlinie ist zu ändern.

2.7.3 Humangenetik

Im 11. Jahresbericht habe ich unter dem Stichwort „Gentechnologie" unter Pkt. 2.4 auf Seiten 30 bis 37 ausführlich die Probleme der Anwendung gentechnischer Verfahren auf den Menschen in Gestalt der Genomanalyse — insbesondere der DNA-Analyse — dargestellt. Inzwischen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die als Anlage 9 beigefügte Entschließung verabschiedet. Die Forderungen aus datenschutzrechtlicher Sicht fasse ich so zusammen:

- Die Genomanalyse sowie die Verarbeitung ihrer Ergebnisse setzt eine fortdauernde, nach umfassender Aufklärung erklärte Einwilligung des Betroffenen voraus. Die Ergebnisse dürfen nur im Rahmen der zuvor wirksam festgelegten Zweckbindung verarbeitet werden.
- Die Genomanalyse setzt in allen Anwendungsbereichen eine gesetzliche Regelung voraus.
- Die Genomanalyse im Strafverfahren bedarf zwar nicht der Einwilligung des Betroffenen, ist aber auf die reine Identitätsfeststellung zu beschränken; Verfahren, die darüber hinaus Informationen zur Person liefern, dürfen nicht angewandt werden.
- Innerhalb arbeitsvertraglicher Beziehungen und im Versicherungswesen sind Genomanalysen zu verbieten.

— In der pränatalen Diagnostik und beim Neugeborenen-Screening ist durch eine präzise Begrenzung der Methoden und Erkenntnisziele sicherzustellen, daß Tendenzen in Richtung auf eine pränatale Selektion oder die gesellschaftliche Diskriminierung Behinderter ausgeschlossen werden.

In der rechtspolitischen Diskussion hat sich im Berichtszeitraum in erfreulicher Weise die Forderung verstärkt, den Gefahren der Humangenetik mit strikten Verboten und Einschränkungen zu begegnen. Dies spiegelt sich auch wieder

— in der Entschließung des europäischen Parlaments vom 13. April 1989 zu den ethischen und rechtlichen Problemen der Genmanipulation (Bundestags-Drucksache 11/4341),

— im Bericht des Bundestagsausschusses für Forschung und Technologie vom 4. Oktober 1989 zum Bericht der Enquete-Kommission zur Gentechnologie (Bundestags-Drucksache 11/5320).

Bedauerlicherweise aber sprechen sich beide Papiere unter bestimmten Umständen für die Anwendung der Genomanalyse an Arbeitnehmern in Bezug auf die gegenwärtige gesundheitliche Eignung für einen Arbeitsplatz aus. Lediglich Untersuchungen auf Krankheitsanlagen und zukünftige Krankheiten sollen ausgeschlossen werden. Ich hatte bereits im 11. Jahresbericht auf Seite 35 dargelegt, daß eine derartige Differenzierung vielleicht gut gemeint, in der Praxis aber kaum überprüfbar ist und überdies verkennt, daß die spezifischen Erkenntnismöglichkeiten der Genomanalyse gerade auf Krankheitsanlagen und zukünftige Krankheiten gerichtet sind. Die SPD-Bundestagsfraktion dagegen hat in ihrem Änderungsantrag zu dem oben genannten Ausschußbericht (Bundestags-Drucksache 11/5468) das notwendige umfassende Verbot der Genomanalyse im Rahmen arbeitsvertraglicher Beziehungen gefordert. Dies ist auch die Position des Senators für Arbeit.

Im Berichtszeitraum haben verschiedene Strafgerichte die DNA-Analyse als Beweismittel zwecks Identifizierung oder Ausschluß einer Person als Täter zugelassen. Das Bundeskriminalamt und verschiedene Landeskriminalämter bereiten die baldige Durchführung von DNA-Analysen vor. Zugleich sind aber in der Öffentlichkeit zunehmend Zweifel an der Zuverlässigkeit der Verfahren geäußert worden. Dies bestätigt die Forderung der Konferenz der Datenschutzbeauftragten, ein staatliches Zulassungsverfahren für DNA-Sonden einzuführen. Der Bundesminister für Justiz hat inzwischen angekündigt, er werde noch in diesem Jahr den Entwurf einer Regelung über den Einsatz von DNA-Analysen im Strafverfahren vorlegen. Eine Beteiligung der Datenschutzbeauftragten ist sichergestellt. Es wird dabei darauf zu achten sein, daß die bereits formulierten Datenschutzanforderungen Eingang in die gesetzliche Regelung finden.

Den mir zugegangenen Reaktionen von Senatoren, denen ich die dargestellten Positionen der Datenschutzbeauftragten übermittelt hatte, entnehme ich, daß die Bereitschaft besteht, sie bei bremischen Stellungnahmen und Vorhaben im Bereich der Humangenetik zu berücksichtigen.

2.8 Umweltschutz und Stadtentwicklung

Altlastenkataster

Der Senator für Umweltschutz und Stadtentwicklung hält für die Vorbereitung von Bebauungsplänen, Baugenehmigungen, den Verkauf städtischer Grundstücke sowie die Bewertung, Sanierung und Überwachung von Altlasten, die Erarbeitung einer vollständigen Übersicht über die Identifizierung und grundlegende Beschreibung der stadtbremischen kontaminierten Altstandorte (Altlastenkataster) für dringend erforderlich. Mit der Erfassung von Informationen und dem Eintragen in Datenstammblätter für Verdachtsflächen hat er ein Ingenieurbüro beauftragt. Zu diesem Zweck sollte das Ingenieurbüro die von der Verwaltung zur Verfügung gestellten Informationen (genauer Standort, Größe und Eigentümer des Grundstücks sowie Lagekarten) sichten und ggf. ergänzen. Des weiteren soll die Erfassung der Nutzungsgeschichten (frühere und heutige Nutzung auf der Fläche und die jeweiligen Nutzer) möglichst differenziert ermittelt und dargestellt werden, damit aus der Beschreibung heraus eine Ableitung möglich ist, mit welchen Kontaminationen zu rechnen ist. Die Arbeiten für die Einzelfälle umfassen sowohl Ortstermine als auch je nach Notwendigkeit Gespräche mit Mitgliedern der Verwaltung sowie Akteneinsicht bei verschiedenen Behörden (Liegenschaftsamt, Bauordnungsamt, Gewerbeaufsichtsamt, Wasserwirtschaftsamt und Stadt- und Polizeiamt).

Da durch die Auskünfte und die ggf. gewährte Akteneinsicht durch die genannten Behörden personenbezogene Daten an den Auftragnehmer übermittelt werden, habe ich dem Senator für Umweltschutz und Stadtentwicklung gegenüber dargelegt, daß für eine derartige Einschränkung des informationellen Selbstbestimmungsrechts ohne Einwilligung der Betroffenen die dafür erforderliche gesetzliche Grundlage fehlt und insoweit Auskünfte und Einsichtnahmen in Akten unzulässig sind.

Mit dem Senator für Umweltschutz und Stadtentwicklung bin ich daher übereingekommen, daß die genannten Behörden lediglich anonymisierte Informationen übermitteln und damit gewährleisten, daß das Altlastenkataster keine personenbezogenen Daten enthält. Nach Erstellung des Altlastenkatasters ist die Verarbeitung personenbezogener Daten lediglich der belasteten Grundstücke zulässig, soweit dadurch die aufgrund dieser Belastungen bestehenden erheblichen Nachteile für das Gemeinwohl oder schwerwiegende Beeinträchtigungen der Rechte Einzelner verhindert und beseitigt werden sollen.

2.9 Bauwesen

2.9.1 Novelle zum Bremischen Architektengesetz

Wegen der notwendigen Anpassung der Rechtsvorschriften an europäische Richtlinien war eine Novellierung des Bremischen Architektengesetzes erforderlich. Die Änderung gab Gelegenheit, notwendige Regelungen zur Verarbeitung personenbezogener Daten durch die Architektenkammer zu entwickeln.

Die inzwischen in Kraft getretene Gesetzesänderung sieht vor, daß die Architektenkammer personenbezogene Daten verarbeiten darf, soweit dies zur rechtmäßigen Erfüllung der Kammeraufgaben nach dem Bremischen Architektengesetz erforderlich ist. Die im einzelnen aufgeführten personenbezogenen Daten dürfen grundsätzlich nur beim Betroffenen erhoben werden.

Das Recht auf Einsichtnahme in die Architektenliste, die Stadtplanerliste und das Verzeichnis der auswärtigen Architekten und Stadtplaner besteht nur dann, wenn ein berechtigtes Interesse dargelegt wird.

Darüber hinaus ist die Architektenkammer berechtigt, in allen die Tätigkeit der Architekten und Stadtplaner betreffenden Angelegenheiten den Baubehörden, den Architektenkammern und deren Aufsichtsbehörden Auskünfte zu erteilen oder von derartigen Stellen einzuholen, soweit es zur rechtmäßigen Erfüllung der Aufgaben der Architektenkammer oder der auskunftsersuchenden Stelle erforderlich ist. Darüber hinaus ist die Architektenkammer verpflichtet, notwendige Auskünfte zu erteilen, soweit ein Auskunftsersuchen der Durchführung von EWG-Richtlinien dient. Festgelegt worden ist eindeutig, daß über Rügen des Vorstandes keine Auskünfte erteilt werden dürfen.

Mit den Datenverarbeitungsregelungen erfüllt des Bremische Architektengesetz die Anforderungen des Volkszählungsurteils zur Einschränkung des informationellen Selbstbestimmungsrechts der Betroffenen.

2.9.2 Entwurf einer Verordnung über die Gutachterausschüsse nach dem Baugesetzbuch

Nach dem Baugesetzbuch werden zur Ermittlung von Grundstückswerten und für sonstige Wertermittlungen selbständige, unabhängige Gutachterausschüsse gebildet. Die Landesregierungen werden ermächtigt, durch Rechtsverordnung u. a. die Führung und Auswertung der Kaufpreissammlung, die Ermittlung sowie Veröffentlichung der Bodenrichtwerte und sonstiger Daten der Wertermittlung und die Erteilung von Auskünften aus der Kaufpreissammlung zu regeln.

Hierzu hat mir der Senator für das Bauwesen den Entwurf einer Rechtsverordnung vorgelegt.

Insbesondere habe ich angeregt, die beabsichtigten bzw. von interessierten Kreisen geforderten Regelungen zur Auskunftserteilung einzugrenzen. Ich halte es für unverhältnismäßig, den freien Sachverständigen Daten und Informationen aus den Urkunden sowie sonstige für die Wertermittlung erforderliche Daten und Informationen zu erteilen. Grundsätzlich ist davon auszugehen, daß alle personenbezogenen Daten, die nicht in die Kaufpreissammlung aufgenommen werden, zwangsläufig Einzelheiten beinhalten, die nur unmittelbar für die Beteiligten bestimmt sind. Abgesehen davon hat der Bundesgesetzgeber zum Erlaß landesrechtlicher Vorschriften nur insoweit ermächtigt, als es sich ausschließlich um

Auskünfte aus der Kaufpreissammlung und nicht um darüber hinausgehende Informationen handelt.

Eine Antwort des Senators für das Bauwesen, ob und inwieweit meine Anregung aufgegriffen wird, steht noch aus.

2.9.3 Änderung der Bremischen Landesbauordnung (BremLBO)

Die BremLBO weist den Bauordnungsbehörden eine Vielzahl von Aufgaben zu, die im Zusammenhang mit der Nutzung und Bebauung von Grundstücken steht. Beispielhaft führe ich an: das Baugenehmigungsverfahren, die Prüfung und Zulassung von Baustoffen, die Überwachung der Einhaltung baurechtlicher Vorschriften, die Führung des Baulastenverzeichnisses und die Verfolgung von Ordnungswidrigkeiten. Dabei werden personenbezogene Daten von Bauherren, Grundstückseigentümern, Nachbarn, Planverfassern, Bauleitern, Baustoffproduzenten und -händlern zwangsweise erhoben und verarbeitet.

Am Beispiel des Baugenehmigungsverfahrens wird deutlich, daß die Art der erhobenen Daten einen umfassenden Einblick in die Lebensverhältnisse und die wirtschaftlichen Verhältnisse des Bauherrn geben. Er macht Angaben über die Höhe der Baukosten, die Ausstattung der Wohnung mit sanitären Einrichtungen, die Größe und Anzahl und den Verwendungszweck der Räume, das Vorhandensein von Garage, Schwimmbad, Sauna usw. Diese Daten werden an eine Vielzahl von am Verfahren beteiligte öffentliche Stellen und an private Dritte wie an Nachbarn übermittelt.

Bei dem zu führenden Baulastenverzeichnis handelt es sich um ein öffentliches Register, welches jedermann einsehen kann, der ein berechtigtes Interesse darlegt.

Ich habe wiederholt darauf hingewiesen, daß es wegen der Art, des Umfangs und der Verwendung der verarbeiteten Daten einer bereichsspezifischen Datenverarbeitungsregelung in der BremLBO bedarf.

Anfang Februar 1990 hat der Senator für das Bauwesen mir den Entwurf eines Gesetzes zur Änderung der BremLBO vorgelegt. Dieser sieht eine Ermächtigung des Senators für das Bauwesen vor, durch Rechtsverordnung die Erhebung und Verarbeitung personenbezogener Daten zum Zwecke der Erfüllung der bauaufsichtlichen Aufgaben durch die Bauaufsichtsbehörden zu regeln. Er soll dabei die Übermittlung von Daten an Dritte bestimmen. Ihm wird dabei ein Ermessen eingeräumt festzulegen, daß für verschiedene Arten von Vorhaben unterschiedliche Anforderungen an die Übermittlung und das Verfahren zu stellen sind.

In einer ersten vorläufigen Stellungnahme habe ich erhebliche datenschutzrechtliche Bedenken gegen diese Regelung geltend gemacht. Die Normierung von Eingriffen in das mit Grundrechtscharakter ausgestattete Recht auf informationelle Selbstbestimmung muß der Gesetzgeber selbst treffen. Er darf dieses nicht dem Verordnungsgeber überlassen. Die Vorschrift entspricht auch nicht dem Verfassungsprinzip der Normenklarheit, weil der Bürger aus ihr das Ausmaß der Einschränkung seines Grundrechts nicht klar erkennen kann. Der von ihr betroffene Personenkreis muß präsize beschrieben sein. Der Zweck der Datenverarbeitung, Art und Umfang der zu verarbeitenden Daten und deren Verwendung muß aus der Ermächtigungsnorm ersichtlich sein. Wegen des erheblichen Eingriffscharakters der Datenverarbeitung hat der Gesetzgeber Schutzvorkehrungen und Regelungen über die Löschung von Daten und über Betroffenenrechte zu treffen.

Der Gesetzentwurf regelt nur die Datenverarbeitung, die mit der Durchführung der Aufgabe Bauaufsicht verbunden ist, nicht aber die mit den übrigen Aufgaben verbundene Verarbeitung personenbezogener Daten. Beispielhaft erwähne ich hier die Führung des Baulastenverzeichnisses.

Er berücksichtigt auch nicht, daß die Landesbauordnung bereits Datenverarbeitungsregelungen enthält, die nach dem veränderten Verfassungsverständnis zum Recht auf informationelle Selbstbestimmung verfassungsrechtlich bedenklich sind. Das gilt z. B. für eine Vorschrift, nach der personenbezogene Daten durch ein öffentliches Auslegungsverfahren bekannt gegeben werden müssen, wenn eine Befreiung von baurechtlichen Bestimmungen erteilt werden soll und zu vermuten ist, daß öffentlich-rechtlich geschützte Belange von Nachbarn, die nicht Angrenzer sind, beeinträchtigt werden könnten.

2.10 Wirtschaft, Technologie und Außenhandel

Auskunft gegenüber Dritten durch die Landeskartellbehörde

Das Hauptquartier der Kriminalpolizei der US-Landstreitkräfte hat die Landeskartellbehörde beim Senator für Wirtschaft, Technologie und Außenhandel aufgefordert, ihr eine Liste von Firmen zu übersenden, die wegen wettbewerbsrechtlicher Verstöße mit Bußgeld belegt worden sind. Die Anfrage der Landeskartellbehörde, ob derartige listenmäßige Auskünfte zulässig sind, habe ich verneint.

Nach den Vorschriften des Gesetzes über die internationale Rechtshilfe in Strafsachen kann auf Ersuchen einer zuständigen Stelle eines ausländischen Staates Rechtshilfe in einer strafrechtlichen Angelegenheit geleistet werden. Sie darf jedoch nur geleistet werden, wenn die Voraussetzungen vorliegen, unter denen deutsche Gerichte oder Behörden einander Rechtshilfe leisten könnten.

Diese Voraussetzung ergibt sich aus der Gewerbeordnung, wonach Auskünfte aus dem Gewerbezentralregister den kriminaldienstverrichtenden Dienststellen der Polizei für Zwecke der Verhütung und Verfolgung von Straftaten nach dem Gesetz gegen den unlauteren Wettbewerb erteilt werden. Demnach ist die Landeskartellbehörde befugt, der Kriminalpolizei der US-Landstreitkräfte als zuständiger Stelle eines ausländischen Staates Rechtshilfe zu leisten.

Rechtshilfe ist nach dem Gesetz über die internationale Rechtshilfe in Strafsachen jede Unterstützung, die für ein ausländisches Verfahren in einer strafrechtlichen Angelegenheit gewährt wird. Daraus ergibt sich zweifelsfrei, daß Rechtshilfe lediglich im Einzelfall geleistet werden darf. Das Auskunftsersuchen der Kriminalpolizei der US-Landstreitkräfte stellt jedoch nicht auf einen Einzelfall ab, sondern läßt die Vermutung zu, daß bei der auskunftsersuchenden Stelle eine Datenvorratsspeicherung vorgenommen werden soll, die nach dem Volkszählungsurteil ausdrücklich eine unzulässige Einschränkung des informationellen Selbstbestimmungsrechts bedeutet.

Ich gehe davon aus, daß die Landeskartellbehörde beim Senator für Wirtschaft, Technologie und Außenhandel entsprechend meiner Rechtsauffassung verfährt.

2.11 Häfen, Schiffahrt und Verkehr

Gefahrgutbeauftragtenverordnung und 2. Straßengefahrgutänderungsverordnung

Der Entwurf der **Gefahrgutbeauftragtenverordnung** sieht die Einführung von Gefahrgutbeauftragten in Unternehmen und Betrieben vor, die eine Mindestmenge an gefährlichen Gütern absenden, befördern oder zur Beförderung verpacken oder übergeben. Des weiteren legt der Entwurf die Voraussetzungen für die Bestellung von Gefahrgutbeauftragten, die an sie zu stellenden Anforderungen sowie ihre Rechte und Pflichten fest.

Die im Entwurf festgelegten Pflichten schränken in mehrfacher Hinsicht das informationelle Selbstbestimmungsrecht der Betroffenen ein:

- Der Betriebsinhaber wird verpflichtet, gegenüber der Überwachungsbehörde bekanntzugeben, wer Gefahrgutbeauftragter ist.
- Der Gefahrgutbeauftragte wird verpflichtet, die Fahrzeugführer und Schiffsführer nach den Vorschriften über die Beförderung gefährlicher Güter im Unternehmen oder Betrieb zu überwachen sowie Aufzeichnungen darüber anzufertigen, drei Jahre lang aufzubewahren und diese Unterlagen der Überwachungsbehörde auf Verlangen zur Prüfung vorzuzeigen oder auszuhändigen.
- Die Bescheinigungen über die Schulung der beauftragten Personen, aus der der Zeitpunkt, die Dauer und der Inhalt der Schulung hervorgeht, sind der Überwachungsbehörde auf Verlangen zur Prüfung vorzuzeigen oder auszuhändigen.

Diese in der Rechtsverordnung vorgesehenen Einschränkungen des informationellen Selbstbestimmungsrechts sind unter Beachtung des Volkszählungsurteils des Bundesverfassungsgerichts nur dann zulässig, wenn sie auf einer ausreichenden gesetzlichen Norm nach Art. 80 Abs. 1 Satz 2 Grundgesetz (GG) beruhen.

Die einschlägige Ermächtigungsnorm im Gesetz über die Beförderung gefährlicher Güter, wonach der Verordnungsgeber ermächtigt wird, zur Durchführung der Überwachungsaufgaben nach diesem Gesetz Auskunfts-, Aufzeichnungs- und Anzeigepflichten sowie Befähigungsnachweise festzulegen, ist unter Beachtung der Kriterien des Art. 80 Abs. 1 Satz 2 GG nicht ausreichend.

Nach dem Gesetz über die Beförderung gefährlicher Güter ist ausschließlich der Unternehmer oder der Inhaber eines Betriebes Verantwortlicher für die Beförderung gefährlicher Güter. Daraus folgt, daß aus der Ermächtigungsnorm dieses Gesetzes die Einschränkung des informationellen Selbstbestimmungsrechts ausschließlich des Unternehmers oder des Inhabers eines Betriebes abgeleitet werden kann, nicht jedoch des Gefahrgutbeauftragten bzw. der sonstigen verantwortlichen Personen (z. B. Fahrzeugführer, Schiffsführer). Auch sind weder Art, Zweck noch Ausmaß der Einschränkung des informationellen Selbstbestimmungsrechts in der gesetzlichen Norm erkennbar oder vorhersehbar.

Weil also das Wesentliche, die Einschränkung des Rechts auf informationelle Selbstbestimmung, nicht geregelt ist, stellt die Ermächtigungsnorm zum Erlaß der beabsichtigten Rechtsverordnung keine ausreichende Rechtsgrundlage dar.

Ich habe daher den Senator für Häfen, Schiffahrt und Verkehr gebeten, sich auf Bundesebene dafür einzusetzen, daß die in der Rechtsverordnung enthaltenen Einschränkungen im Gesetz über die Beförderung gefährlicher Güter geregelt werden.

Abgesehen davon ist es nach dem Volkszählungsurteil des Bundesverfassungsgerichts auch erforderlich, die in der Rechtsverordnung vorgesehenen Einschränkungen des Persönlichkeitsrechts normenklar zu regeln. Aus dem Verordnungsentwurf sind keine Regelungen ersichtlich, die die Verpflichtung der Unternehmen zur Übermittlung bestimmter personenbezogener Daten an die zuständigen Überwachungsbehörden sowie Art und Umfang der Verarbeitung dieser Daten (einschließlich der Übermittlung an Dritte) durch die zuständigen Behörden festlegen. Ebenso ist der Umfang der Speicherung und die Art der Verarbeitung personenbezogener Daten durch die Gefahrgutbeauftragten nicht normenklar geregelt. In Anlehnung an die Regelungen zum Personaldatenschutz sollte eine besondere Geheimhaltungspflicht für Gefahrgutbeauftragten vorgesehen werden. Außerdem bedarf es einer Regelung, die die Nutzung der Arbeitnehmerdaten zur Verhaltens- und Leistungskontrolle durch den Arbeitgeber ausschließt.

Des weiteren gehe ich davon aus, daß der Nachweis über durchgeführte Schulungen des Gefahrgutbeauftragten oder der beauftragten Personen lediglich zur Kontrolle der Sachkunde benötigt wird und daher die Vorlagepflicht gegenüber der Überwachungsbehörde durchaus genügen dürfte.

Ich habe den Senator für Häfen, Schiffahrt und Verkehr gebeten, meine datenschutzrechtlichen Bedenken und Anregungen in die weiteren Beratungen auf Bundesebene einzubringen und mich über das Ergebnis seiner Bemühungen zu unterrichten.

Ähnliche Probleme ergeben sich bei der **2. Straßengefahrgutänderungsverordnung.** Diese Rechtsverordnung sieht die Einschränkung des informationellen Selbstbestimmungsrechts des Beförderers, Absenders, Verladers oder Empfängers von gefährlichen Gütern vor. Die Betroffenen sind verpflichtet, bei der zuständigen Straßenverkehrsbehörde die Fahrwegbestimmung zu beantragen und darüber hinaus durch eine Bescheinigung einer Wasser- und Schiffahrtsdirektion bestimmte Nachweise zu beantragen und zu erbringen. Ebenso wird das Persönlichkeitsrecht des Fahrzeugführers eingeschränkt, in dem dieser z. B. die Bescheinigung über Tankwagenführerschulungen bei der Beförderung mitzuführen und nachzuweisen hat.

Auch hier ergibt sich aus der angegebenen Ermächtigungsnorm zum Gesetz über den Transport gefährlicher Güter, daß diese Norm unter Beachtung der Kriterien des Art. 80 Abs. 1 Satz 2 GG nicht als ausreichend zur Einschränkung des informationellen Selbstbestimmungsrechts angesehen werden kann.

Ich habe daher gegenüber dem Senator für Häfen, Schiffahrt und Verkehr angeregt, die vorgesehenen Einschränkungen auf eine gesetzliche Grundlage bzw. eine ausreichende gesetzliche Ermächtigungsnorm zu stellen.

Darüber hinaus enthält der Verordnungsinhalt nicht, welche personenbezogenen Daten von verschiedenen Straßenverkehrsbehörden erhoben und auch an andere Stellen übermittelt werden sollen, evtl. so gar ins Ausland. Im übrigen habe ich auch Bedenken dagegen, daß die Deutsche Bundesbahn im Rahmen ihrer Einbindung in eine verwaltungsbehördliche Entscheidung vom Antragsteller zwangsweise erhobene Daten zu wirtschaftlichen Zwecken nutzen darf, wie es die Begründung zu dem Verordnungsentwurf vorsieht.

Nachdem der Senator für Häfen, Schiffahrt und Verkehr meine Anregungen und Bedenken in die bundesweiten Erörterungen eingebracht hatte, hat der Bundesminister für Verkehr die Auffassung vertreten, mit beiden Verordnungen würden zur Umsetzung der im Gesetz über die Beförderung gefährlicher Güter enthaltenen Schutzziele Vorschriften für die öffentliche Sicherheit in Kraft gesetzt. Sowohl bei den Beratungen mit den Bundesressorts als auch mit den Fachressorts der Bundesländer hätten daher datenschutzrechtliche Fragen keine Rolle gespielt. Selbst bei den Beratungen der Ausschüsse des Bundesrates zu den beiden Verordnungen habe sich gezeigt, daß datenschutzrechtliche Erwägungen nicht anzustellen seien.

Im Falle der 2. Straßengefahrgutänderungsverordnung komme hinzu, daß einige Regelungen bereits seit mehr als 15 Jahren rechtsgültig seien und daß bisher die aufgezeigten Probleme datenschutzrechtlicher Art bei der Umsetzung dieser Bestimmungen nicht aufgetreten seien.

Dies würde in gleicher Weise von den Bundesressorts und den Fachressorts der Bundesländer hinsichtlich der jetzt anstehenden Neufassung der Vorschriften in diesem Bereich gesehen. Zusammenfassend gelangte der Bundesminister für Verkehr zu der Auffassung, daß die beiden genannten Verordnungsentwürfe keinen Anlaß zu datenschutzrechtlichen Bedenken geben.

Zusammenfassend muß trotz der Ablehnung durch den Bundesverkehrsminister gesagt werden, daß über die Betroffenen derartig detaillierte Tagesablaufdaten erhoben und gespeichert werden, daß dies der Erstellung eines Persönlichkeitsprofils — auf jeden Fall aber eines Bewegungsprofils — insbesondere der Fahrzeugführer und Schiffsführer sehr nahe kommt. Der Schutz derartig umfangreicher Arbeitnehmerdaten ist unverzichtbar.

Inzwischen hat der Bundesminister für Verkehr beide Rechtsverordnungen erlassen.

2.12 Finanzen

2.12.1 Kontrollmitteilungen an Finanzämter

Aufgrund von zahlreichen Beschwerden hatte ich mich dagegen gewandt, daß die Senatskommission für das Personalwesen die Honorarabrechnungen von nebenamtlichen Dozenten der Volkshochschule an das jeweilige Finanzamt übermittelt (vgl. Ziffer 5.8.2 meines 11. Jahresberichts). Zur Begründung hatte ich angeführt, daß die Bundesregierung von der ihr durch § 93 a der Abgabenordnung (AO) eingeräumten Ermächtigung, Mitteilungspflichten von Behörden durch Rechtsverordnung zu bestimmen, noch nicht Gebrauch gemacht habe. Daraufhin hat der Senator für Finanzen vorerst auf derartige Mitteilungen verzichtet. Ich gehe dabei davon aus, daß dies auch für Mitteilungen aus anderen Behörden und in anderen Zusammenhängen als dem beanstandeten Fall gilt. Außerdem hat der Senator für Finanzen mir seine Auffassung mitgeteilt, daß § 93 a AO eine gesetzliche Grundlage dafür, auch nicht-öffentliche Stellen zu entsprechenden Mitteilungen zu verpflichten, nicht enthalte.

Inzwischen hat der Hessische Minister für Finanzen per Erlaß die hessischen Behörden gebeten, Kontrollmitteilungen an die Finanzbehörden vorerst nicht mehr zu übersenden, soweit nicht eine spezielle Rechtsnorm dazu verpflichtet. Andere Länder werden voraussichtlich in Kürze folgen.

Auch nach Verabschiedung der Rechtsverordnung nach § 93 a AO, womit nach Auskunft des Bundesbeauftragten für den Datenschutz voraussichtlich im Sommer dieses Jahres zu rechnen ist, wird es aber — darauf weise ich vorsorglich hin — nicht zulässig sein, die Höhe von Zuwendungen etwa in Form von Honorarabrechnungen mitzuteilen. § 93 a Abs. 1 Satz 2 AO ermächtigt lediglich zu einer Regelung über die Mitteilung der Zahlungsempfänger, des Rechtsgrundes und des Zeitpunktes, nicht aber der Höhe der Zahlung.

2.12.2 Weiterleitung von Dozentendaten zur Überprüfung der Gemeinnützigkeit an das Finanzamt Bremen-Mitte

Verschiedene nicht-öffentliche Stellen haben sich an mich gewandt und moniert, daß das Finanzamt Bremen-Mitte zur Überprüfung der Gemeinnützigkeit Auflistungen der Honorarempfänger (Name, Anschrift, Höhe des Honorars) verlange. Ich bin gebeten worden zu prüfen, ob sie verpflichtet sind, derartige Auflistungen an das Finanzamt zu übermitteln und dadurch in das informationelle Selbstbestimmungsrecht einzugreifen.

Den Einrichtungen ist eine Steuervergünstigung nach § 51 Abgabenordnung (AO) gewährt worden, weil sie als Körperschaften ausschließlich und unmittelbar gemeinnützige, mildtätige oder kirchliche Zwecke (steuerbegünstigte Zwecke) verfolgen.

Sie halten es für problematisch, wenn sie anläßlich eines Verwaltungsverfahrens zur Überprüfung der Gemeinnützigkeit Auskünfte über die Steuerverhältnisse ihrer Honorarkräfte erteilen sollen, obwohl nach den Bestimmungen der Abgabenordnung andere Personen als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht. Die Körperschaften sind bisher davon ausgegangen, daß die Honorarkräfte die Höhe der Honorarzahlungen im Rahmen ihrer eigenen Einkommensteuererklärung angeben.

Die Überprüfung der Gemeinnützigkeit umfaßt auch die Frage, ob die Körperschaften andere Personen durch Ausgaben, die dem Zweck der Körperschaft fremd sind, oder durch unverhältnismäßig hohe Vergütungen begünstigt haben. Zur Ermittlung des Sachverhalts bedient sich die Finanzbehörde der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Zu diesem Zweck kann das Finanzamt durchaus eine Liste aller Ausgaben verlangen, aus der sich der Zweck dieser Ausgaben ergibt. Das Finanzamt kann dann feststellen, ob die Ausgabezwecke dem Zweck der Körperschaft fremd sind oder nicht. Soweit die Körperschaft Vergütungen zahlt, z. B. Gehälter oder Honorare, ist es erforderlich und ausreichend, Angaben zur Vergütung und die damit zusammenhängende Aufgabenstellung der Beschäftigten ohne Namensnennung zu verlangen. Werden Honorare ausgezahlt, ist das Auskunftsverlangen der Finanzbehörde zulässig, soweit es sich auf die Angaben der Honorarleistungen, den Zweck der Honorarleistungen, den Honorarsatz pro Stunde sowie die Anzahl der Honorarkräfte erstreckt. Darüber hinausgehende Auskunftsverlangen, insbesondere nach den Namen und Anschriften von Honorarkräften, sind nicht erforderlich, und damit auch nicht zulässig.

Ebenso verhält es sich mit den Mitwirkungspflichten der Körperschaften. Soweit die Finanzbehörden Auskünfte verlangen, erstreckt sich die Auskunftspflicht lediglich auf die Auskünfte, die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes erforderlich sind. Da weder Namen noch Anschriften der Honorarempfänger zur Prüfung der Gemeinnützigkeit erforderlich sind, haben die Mitwirkungspflichten der Körperschaften hier ihre Grenzen, zumal Kontrollmitteilungen in diesen Fällen durch die Abgabenordnung nicht vorgesehen sind.

Ich habe dem Finanzamt Bremen-Mitte gegenüber erklärt, daß die beschwerdeführenden Einrichtungen nicht befugt seien, die Namen und Anschriften ihrer Honorarempfänger zu übermitteln.

Ich habe verlangt, daß auf dem dafür verwendeten Erklärungsformular auf die Angaben der Namen und Anschriften der Honorarempfänger verzichtet wird. Eine Antwort des Finanzamtes Bremen-Mitte steht noch aus.

2.12.3 Anzeigepflicht der Notare nach dem Grunderwerbssteuergesetz

Im 11. Jahresbericht hatte ich unter Punkt 5.8.3 ausführlich meine Bedenken dagegen wiedergegeben, daß in Bremen — wie übrigens bundesweit — der einen Grundstückkauf beurkundende Notar per Formblatt nicht nur dem für die Erhebung der Grunderwerbssteuer zuständigen Finanzamt, sondern auch an andere Stellen der Finanzverwaltung den Vorgang anzuzeigen hat. Ich hatte kritisiert, daß abgesehen von § 18 Grunderwerbssteuergesetz für die erstgenannte Anzeige im übrigen Rechtsgrundlagen hierfür fehlten. Einer der beschwerdeführenden Notare hat inzwischen in einer gegen die Anzeigepflichten gerichteten Klage vor dem Finanzgericht Bremen obsiegt. Allerdings hat das Gericht sich in der Begründung darauf beschränkt, das Verlangen des Finanzamts, der Notar habe drei weitere Kopien der Veräußerungsanzeige einzureichen, für unverhältnismäßig zu erklären: „Der Erlaß und das anschließende Gerichtsverfahren wären nämlich überflüssig gewesen, wenn das Finanzamt nach Eingang der Veräußerungsanzeige selbst drei Kopien angefertigt hätte". Auf eine Entscheidung über die eigentlich strittige Frage, ob der mit der Anzeige verbundene Eingriff in das informationelle Selbstbestimmungsrecht des Steuerpflichtigen bzw. in das Auskunftsverweigerungsrecht des Notars zulässig sei, hat das Gericht verzichtet. Ebenso wie andere Datenschutzbeauftragte erwarte ich, daß die Finanzverwaltungen ihre rechtlich und verfassungsrechtlich umstrittene Praxis aufgeben, die den Bürger

zum der Steuerhinterziehung verdächtigen Objekt degradiert. Da auch das Finanzgericht Bremen die materiellrechtlichen Probleme nicht entschieden hat, bleibt der Senator für Finanzen aufgefordert, Stellung zu nehmen.

2.12.4 Kontrollbefugnisse der Datenschutzbeauftragen in der Steuerverwaltung

Ein Mitarbeiter eines bremischen Finanzamtes hat es abgelehnt, mir eine Auskunft über einen konkreten Steuervorgang zu erteilen. Er hat sich darauf berufen, es heiße in einer Kommentierung zu § 30 Abgabenordnung (AO), daß der Datenschutzbeauftragte kein Recht zur Einsichtnahme in den vom Steuergeheimnis geschützten Bereich habe. Diese Auffassung ist falsch. Das Steuergeheimnis steht ebensowenig wie andere Amts- oder Berufsgeheimnisse (etwa das Sozial- oder das Arztgeheimnis) einer Prüfung personenbezogener Vorgänge durch die Datenschutzbeauftragten entgegen, sondern soll ja gerade durch eben diese Prüfung geschützt werden. Das Bundesverfassungsgericht hat im Flick-Urteil (BVerfGE 67, 100, 142 ff.) das Recht auf Wahrung des Steuergeheimnisses mit dem Recht auf informationelle Selbstbestimmung in Zusammenhang gestellt. Zu dessen Wahrung wiederum hatte es das Bundesverfassungsgericht im Volkszählungsurteil dem Gesetzgeber zur Pflicht gemacht, organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegen wirken. Dabei ist — so das Gericht — „die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung".

2.13 Datenverarbeitung im Auftrag öffentlicher Stellen

Im Berichtsjahr führte ich aufgrund von Presseveröffentlichungen über „unseriöse" Datenerfassungsbetriebe bei den bremischen Behörden eine Umfrage zur Feststellung des Umfangs und der Art der Fremdvergaben durch bremische Behörden durch. Gemeldet wurden mir daraufhin von den einzelnen senatorischen Dienststellen für ihre Bereiche 81 Datenfremdverarbeitungsaufträge, von denen 45 über das Rechenzentrum der bremischen Verwaltung vergeben wurden.

Im einzelnen teilen sich die Fremdverarbeitungsverträge auf die einzelnen Bereiche wie folgt auf:

Senatorischer Bereich	Vergebene Aufträge	davon über das RbV
Senatskanzlei	—	—
Senatskommission für das Personalwesen	12	8
Senator für Inneres	6	3
Senator für Justiz und Verfassung	7	—
Senator für Sport	—	—
Senator für Bildung, Wissenschaft und Kunst	5	1
Senator für Arbeit	3	—
Senator für Jugend und Soziales	4	4
Senator für Gesundheit	7	—
Senator für Umweltschutz und Stadtentwicklung	3	1
Senator für das Bauwesen	6	6
Senator für Wirtschaft, Technologie und Außenhandel	1	—
Senator für Häfen, Schiffahrt und Verkehr	—	—
Senator für Finanzen	27	22
Senator für Bundesangelegenheiten	—	—
Gesamtsumme	81	45

Hinsichtlich der Art der Aufträge ergab sich, daß insgesamt

43 Mikroverfilmungsaufträge

18 Datenvernichtungsaufträge

15 Datenerfassungsaufträge

5 Sonstige Aufträge

vergeben wurden.

Getrennt nach der Verarbeitungsart ergibt sich folgendes Bild:

Senatorischer Bereich	Mikro-verfilmung	Daten-erfassung	Datenver-nichtung	Sonstiges
Senatskanzlei	—	—	—	—
Senatskommission für das Personalwesen	10	—	1	1
Senator für Inneres	3	1	2	—
Senator für Justiz und Verfassung	—	—	7	—
Senator für Sport	—	—	—	—
Senator für Bildung, Wissenschaft und Kunst	—	4	—	1
Senator für Arbeit	—	—	3	—
Senator für Jugend und Soziales	1	3	—	—
Senator für Gesundheit	1	—	5	1
Senator für Umweltschutz und Stadtentwicklung	2	1	—	—
Senator für das Bauwesen	4	2	—	—
Senator für Wirtschaft, Technologie und Außenhandel	—	1	—	—
Senator für Häfen, Schiffahrt und Verkehr	—	—	—	—
Senator für Finanzen	22	3	—	2
Senator für Bundesangelegenheiten	—	—	—	—

Die Fremdverarbeitungsaufträge stellen sich mir dabei oft so dar, daß sie den Bestimmungen des Bremischen Datenschutzgesetzes (BrDSG) bzw. den Allgemeinen Verwaltungsvorschriften (AVV) zum Bremischen Datenschutzgesetz nicht voll entsprechen. Die auftraggebende Stelle ist gem. § 8 Abs. 1 BrDSG verpflichtet, vor der Vergabe eines DV-Auftrages den Auftragnehmer unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Bei Durchsicht der Umfrageergebnisse habe ich den Eindruck, als habe der Auftraggeber die erforderliche Sorgfalt nicht walten lassen und sich mit der allgemeinen Zusage, daß von der auftragnehmenden Stelle Sicherungsmaßnahmen ergriffen worden seien, begnügt. Nr. 8.1.1 der AVV zu § 8 BrDSG besagt dazu ausdrücklich, daß der Auftraggeber verpflichtet ist, auf die Einhaltung der Datensicherungsmaßnahmen, die nach § 6 BrDSG zu treffen sind, hinzuwirken. § 8 Abs. 1 BrDSG schreibt vor, daß sich der Auftragnehmer den Bestimmungen des BrDSG zu unterwerfen hat. Entsprechende Regelungen darüber fehlten in den mir vorgelegten Verträgen oft.

Nicht selten fehlten auch Vertragsbestimmungen darüber, daß, wie nach Nr. 8.1.3 der AVV verlangt, der Auftragnehmer nur im Rahmen der ihm vom Auftraggeber erteilten Weisungen tätig werden darf. Vertragliche Regelungen bzgl. einer Herausgabe- oder Löschungspflicht für im Auftrag gespeicherte und verarbeitete Daten fehlen in vielen mir vorgelegten Verträgen ebenso wie Festlegungen von Vertragsstrafen oder die Einräumung eines fristlosen Kündigungsrechts des Auftraggebers bei Verletzungen von Datenschutzbestimmungen.

Dem Umfrageergebnis kann auch entnommen werden, daß Ordnungswidrigkeitsdaten, Daten aus dem Polizeibereich, aus Gerichtsakten, Sozialdaten, Patientendaten sowie Steuerdaten durch Servicebetriebe bzw. Auftragsdatenverarbeiter verarbeitet werden. Bei diesen Daten handelt es sich um Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die deshalb gem. Nr. 8.1.2 der AVV nicht an nicht-öffentliche Servicebetriebe zur Verarbeitung vergeben werden sollen.

Zur Verbesserung der dargestellten, mit den Bestimmungen des BrDSG und den AVV zum BrDSG nicht immer vereinbaren Situation bei der Fremdvergabe von Aufträgen zur Verarbeitung personenbezogener Daten habe ich gegenüber den Ressorts u. a. folgende Empfehlungen und Hinweise gegeben:

- Um dem Landesbeauftragten für den Datenschutz die Möglichkeit einzuräumen, die Vergabe von Fremdverarbeitungsaufträgen besser als bisher zu kontrollieren und schon frühzeitig auf eine evtl. mangelhafte Berücksichtigung datenschutzrechtlicher Bestimmungen hinzuweisen, wird beim Landesbeauftragten für den Datenschutz ein Register der Aufträge gem. § 8 BrDSG eingerichtet werden, das alle Aufträge enthält, die von öffentlichen Stellen an insbesondere nicht-öffentliche Stellen vergeben werden. Die Allgemeinen Verwaltungsvorschriften zu § 8 BrDSG (Nr. 8.1.4) verpflichten die öffentlichen Stellen, den Landesbeauftragten für den Datenschutz von der ersten Auftragserteilung in Kenntnis zu setzen.

- Die Auftraggeber prüfen vor einer Auftragserteilung sorgfältig, ob der Auftragnehmer in hinreichendem Umfang technisch-organisatorische Sicherungsmaßnahmen gem. § 6 BrDSG getroffen hat und insoweit geeignet ist, und läßt sich nicht auf allgemeine Aussagen, Zusagen oder Erläuterungen ein. Dies könnte auch durch das Rechenzentrum der bremischen Verwaltung oder durch einen sonstigen Sachverständigen geprüft werden.

- Verarbeitungsaufträge über Daten, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen, werden nicht mehr fremd vergeben, so wie es die AVV in Nr. 8.1.2 empfehlen.

- Das Auftragsverfahren sollte nach Möglichkeit standardisiert werden. Dies könnte z. B. durch vorgefertigte Vertragstexte und ein zentrales Vergabeverfahren z. B. durch das Rechenzentrum der bremischen Verwaltung geschehen, das ohnehin schon über die Hälfte der Fremdverarbeitungsaufträge vergibt.

In zwei Fällen habe ich die Fremdverarbeitung von Sozialdaten durch nicht-öffentliche Stellen überprüft. Rechtsgrundlage für die Fremdvergabe ist in diesen Fällen nicht § 8 Bremisches Datenschutzgesetz (BrDSG), sondern § 80 Sozialgesetzbuch X (SGB X) i. V. m. § 8 Abs. 1, 3 Bundesdatenschutzgesetz (BDSG). Damit finden auch die AVV zum BrDSG keine direkte Anwendung. Es ist allerdings geregelt, daß

- der Auftragnehmer sorgfältig auszuwählen ist und regelmäßig kontrolliert werden muß,

- der Auftragnehmer eine Erklärung unterschreiben muß, in der er sich zur Einhaltung des Datenschutzes und der speziellen Weisungen des Auftraggebers verpflichtet und sich außerdem den gesetzlich vorgesehenen Kontrollen unterwirft,

- die Verantwortung für den Schutz des Sozialgeheimnisses beim Sozialleistungsträger verbleibt und dieser Weisungen zur Verarbeitung zu erteilen hat,

- der Auftraggeber eine Anzeigepflicht gegenüber seiner Aufsichtsbehörde hat und

- soweit personenbezogene Daten betroffen sind, die Fremdvergabe nur erfolgen darf, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der ADV hierdurch kostengünstiger besorgt werden können.

In einem Falle hatte das Rechenzentrum der bremischen Verwaltung (RbV) im Auftrag des Senators für Jugend und Soziales die adv-mäßige Erfassung von Sozialhilfedaten im Rahmen von HESSIAS an eine nicht-öffentliche Stelle vergeben, ohne daß die Verteilung der Verantwortung zwischen Sozialleistungsträger und RbV schriftlich festgelegt worden wäre. Die Erklärung des nicht-öffentlichen Auftragnehmers entsprach nicht den gesetzlichen Anforderungen. Es bestanden auch Zweifel darüber, ob — von wem auch immer — die gesetzlichen Kontrollbefugnisse wahrgenommen worden waren.

Im anderen Falle hatte das Studentenwerk Bremen zunächst die Erfassung von Daten aus seiner Finanzbuchhaltung, später auch die Erfassung von Daten ausländischer Studenten, die aus einem Hilfsfond für notleidende Studenten aus der Dritten Welt unterstützt werden, selbst an eine nicht-öffentliche Stelle vergeben. Hierzu existierte lediglich ein Auftragsschreiben aus dem Jahre 1977, in dem von Datenschutz nicht die Rede war; damals ging es auch noch nicht um die oben genannten personenbezogenen Daten. Eine Kontrolle auf Einhaltung des Datenschutzes hatte praktisch nie stattgefunden.

Inzwischen ist auf mein Betreiben hin in beiden Fällen — im letzteren Falle im Wege einer Neuvergabe des Auftrags — sichergestellt, daß die gesetzlichen Vorschriften eingehalten werden.

Zu überlegen ist in diesen Fällen, ob nicht entsprechend Nr. 8.1.2 der AVV zum BrDSG die Verarbeitung von Sozialdaten, die dem besonderen Amtsgeheimnis des § 35 SGB I unterliegen, künftig von der Vergabe an nicht-öffentliche Stellen ausgenommen werden.

2.14 Zugriff der Bremischen Bürgerschaft auf zentrale Datenspeicher der Verwaltung

Gemäß § 27 Abs. 2 BrDSG habe ich den Auftrag, die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der bremischen Verwaltung darauf zu beobachten, ob sie zu einer Verschiebung der Gewaltenteilung zwischen den Verfassungsorganen des Landes führen, und ggf. Maßnahmen anzuregen, die mir geeignet erscheinen, derartige Auswirkungen zu verhindern. Bereits in meinem ersten Bericht für das Jahr 1978 hatte ich unter Pkt. 5.9/10 auf die Gefahr hingewiesen, daß durch die ADV die Gewichte zugunsten der Exekutive verschoben werden könnten. Dem könne die Legislative aber u. a. dadurch begegnen, daß sie von ihren Auskunftsrechten wirkungsvoll Gebrauch mache.

Die Senatskanzlei hat mich gebeten zu prüfen und dem Senat zu berichten, ob es rechtlich zulässig sei, daß die Bremische Bürgerschaft bzw. einzelne ihrer Abgeordneten direkten Zugriff auf die zentralen Datenspeicher der bremischen Verwaltung erhalten und wenn ja, auf welche Datenbestände.

In meiner Stellungnahme bin ich davon ausgegangen, daß

- § 16 BrDSG in Abs. 1 Satz 1 den Senat verpflichtet, der Bürgerschaft bzw. einer Fraktion Auskünfte über den Inhalt von automatisierten Dateien zu geben, die das Rechenzentrum der bremischen Verwaltung im Auftrag der Verwaltung führt, soweit Auswertungsprogramme vorhanden sind,
- Abs. 1 Satz 2 personenbezogene Daten aus dem genannten Auskunftsanspruch ausklammert,
- lt. Abs. 4 der Antrag einer Fraktion über den Präsidenten der Bürgerschaft zu leiten ist.

Anschließend habe ich festgestellt, daß ein weitergehender Auskunftsanspruch nicht besteht, daß aber aus meiner Sicht es dem Senat unbenommen bleibt, darüber hinauszugehen, sofern personenbezogene Daten ausgeklammert bleiben. Ich habe aber zugleich zu bedenken gegeben, ob nicht die zunehmende Informatisierung der Verwaltung zu einem Machtzuwachs von Senat und Verwaltung gegenüber dem Parlament führt, der auch Auswirkungen auf die Gewaltenteilung hat. Ich habe angeregt, § 16 BrDSG in diesem Licht neu zu überdenken.

Der Senat ist meiner Anregung dadurch gefolgt, daß er sich über seine gesetzliche Verpflichtung hinaus mit dem unmittelbaren Zugriff des Parlaments und einzelner Abgeordneter auf zentrale Datenspeicher der Verwaltung einverstanden erklärt hat, sofern es sich um Datenbanken handelt, in denen lediglich anonyme Basisdaten enthalten sind, oder um Datenbanken, in denen Verwaltungsdaten nach Aufbereitung durch Dritte abrufbar sind. Er hat lediglich den Zugriff auf personenbezogene Daten sowie auf Daten der laufenden Verwaltung hiervon ausgenommen. Ich begrüße diesen Senatsbeschluß als einen Schritt zur Stärkung der Rechte der Bremischen Bürgerschaft und ihrer Abgeordneten gegenüber einer Verwaltung, die durch die Entwicklung der ADV neue Instrumente der Planung und Aufgabenerfüllung, aber auch für Eingriffe in die Rechte der Bürger erhalten hat.

2.15 Ausgewählte unerledigte Probleme aus früheren Jahresberichten

Neben den in diesem Kapitel genannten Anforderungen, die sich an den Gesetzgeber, den Senat und die Verwaltung im Lande Bremen richten, stelle ich fest, daß weitere Datenschutzprobleme, die ich in zurückliegenden Jahresberichten aufgezeigt habe und zu denen der Datenschutzausschuß der Bremischen Bürgerschaft Stellung genommen hat, noch immer nicht hinreichend gelöst sind. Beispielhaft möchte ich hierzu folgende drei Punkte benennen:

- Entsprechend den Anforderungen in meinem 8. und 10. Jahresbericht hat auch der Datenschutzausschuß in seiner Sitzung vom 25. Oktober 1988 die Novellierung des **Bremischen Archivgesetzes** angemahnt. Der Novellierungsbedarf wird auch vom Senat anerkannt, ein Gesetzentwurf wurde mir noch nicht zugeleitet.

- Trotz eines umfassenden PC-Einsatzes in allen Bereichen der bremischen Verwaltung fehlt weiterhin ein abgestimmtes **PC-Konzept,** obwohl dieses nach Auffassung des Datenschutzausschusses (Sitzung vom 23. September 1988) bereits vor der Systementscheidung unter meiner Beteiligung zu erstellen gewesen wäre. Hierfür müssen die Verwaltungskonzeption, die Verwaltungsorganisation und die Rechtsorganisation berücksichtigt werden. Den Anwendern ist ein Leitfaden an die Hand zu geben, um die Organisation und Gestaltung des PC-Einsatzes unter Berücksichtigung der Datenschutz- und Datensicherungsanforderungen leisten zu können; dieses würde auch meine Kontroll- und Beratungstätigkeit erleichtern.

- Die **Datenregisterverordnung** ist den Anforderungen des novellierten BrDSG noch immer nicht angepaßt worden. Das von mir geführte Dateienregister weist nicht den aktuellen Stand auf. Es ist dringend erforderlich, daß die Datenregisterverordnung aktualisiert wird. Infolgedessen konnte das auf der alten Verordnung basierende Datenverarbeitungs-Verfahren noch nicht weiterentwickelt werden.

3. Datenschutz in Europa

Die Europäische Gemeinschaft verwirklicht bis zum 31. Dezember 1992 schrittweise den europäischen Binnenmarkt. Dabei wird konsequenterweise zugleich eine europäische Informationsgemeinschaft geschaffen, etwa durch

- die Entwicklung des grenzüberschreitenden Datenverkehrs im öffentlichen Bereich (vgl. der im Rentenreformgesetz verankerte grenzüberschreitende Direktabruf von Versichertendaten) und im nicht-öffentlichen Bereich (Beispiele sind der internationale Zahlungsverkehr, Kreditkarten, internationale Auskunfteien),

- eine Fülle von Aktivitäten der EG zur Förderung von Forschung und Entwicklung der Informationstechnologie (vgl. den neuen Titel VI des EWG-Vertrages),

- Datenbanken und sonstige Datenverarbeitung durch die EG-Organe selbst.

Diese Entwicklung birgt deshalb besondere Gefahren, weil,

- die EG einseitig von wirtschaftlichen Interessen geprägt ist,

- ein europäischer Grundrechtskatalog, folglich auch ein europäisches Grundrecht auf informationelle Selbstbestimmung, fehlt

- und es deshalb nahe liegt, daß die Institutionen der EG den Datenschutz eher als Wettbewerbshindernis denn als politische Aufgabe begreifen.

Dem Datenschutz droht selbst dann Vernachlässigung, wenn die EG sich der Rechte ihrer Bürger annimmt. So wurde offensichtlich schlicht vergessen, in den Entwurf einer Gemeinschaftscharta der sozialen Grundrechte den Arbeitnehmerdatenschutz aufzunehmen. Der Versuch der Datenschutzbeauftragten, dies für die Stellungnahme des Bundesrats zu korrigieren, blieb ohne Erfolg. Inzwischen aber haben auf Vorschlag Bremens die Arbeits- und Sozialminister des Bundes und der Länder die Datenschutzinitiative aufgegriffen. Der Bundesarbeitsminister hat zugesagt, auf europäischer Ebene tätig zu werden.

Die Europäische Gemeinschaft hat Anfang 1989 den Entwurf einer Verordnung über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an ihr statistisches Amt vorgelegt. Danach soll das nationale Statistikgeheimnis für solche Übermittlungen weitgehend aufgehoben werden, ohne daß gleichzeitig auch nur in etwa vergleichbare Datenschutzvorkehrungen bei dem

statistischen Amt der Europäischen Gemeinschaft geschaffen werden. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Konferenz vom 26./27. Oktober 1989 dazu eine kritische Entschließung gefaßt (siehe Anlage 7).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine vorbereitende Arbeitsgruppe zum Datenschutz in der EG eingesetzt. Parallel dazu haben für den nicht-öffentlichen Bereich eine Arbeitsgruppe „Internationaler Datenverkehr" der Obersten Datenschutzaufsichtsbehörden der Länder und ein Bund-Länder-Gesprächskreis „Grenzüberschreitender Datenverkehr" beim Bundesminister des Innern ihre Arbeit aufgenommen. Angesichts der europäischen Entwicklung gewinnt auch die internationale Konferenz der Datenschutzbeauftragten, die ihre 11. Tagung im August 1989 in Berlin abhielt, eine besondere Bedeutung. Sie verabschiedete dort die als Anlagen 10 und 11 beigefügten Beschlüsse zur Telekommunikation und zu den Medien. Die nächste Konferenz wird im September 1990 in Paris tagen. Von deutscher Seite ist bislang Interesse an den Themen „Regulierung grenzüberschreitender Datenflüsse" und „Genomanalyse im Arbeitsverhältnis" angemeldet worden.

Auf der Berliner Konferenz verabschiedeten die Datenschutzbeauftragten der EG-Länder eine Zusatzerklärung (Anlage 12). Übereinstimmend mit dieser Zusatzerklärung sehe ich es als erforderlich an, daß die Europäische Gemeinschaft

- einen einheitlichen datenschutzrechtlichen Mindeststandard in der Gemeinschaft schafft, indem sie durch Rechtsakte die Datenschutzkonvention des Europarates vom 28. Januar 1981 zu unmittelbar bindendem Recht sowohl für die Datenverarbeitung der EG-Institutionen als auch in den Mitgliedstaaten erklärt,

- darauf aufbauend das europäische Datenschutzrecht weiterentwickelt, damit es mit den Anforderungen einer europäischen Informationsgesellschaft Schritt halten kann,

- bei jedem Vorhaben und jeder Regelung zugleich das erforderliche bereichsspezifische datenschutzrechtliche Instrumentarium festlegt und bereitstellt,

- eine unabhängige Datenschutzkontrollinstanz einrichtet.

4. Nicht-öffentlicher Bereich

4.1 Vorbemerkungen

Im November 1987, also fast vier Jahre nach der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsurteil, wurde vom Bundesminister des Innern der Entwurf für ein Artikelgesetz zur Neufassung des Bundesdatenschutzgesetz sowie zur Änderung des Verwaltungsverfahrensgesetzes (VwVfG) zunächst als Referentenentwurf vorgelegt. Die darin vorgesehenen Regelungen entsprachen in großen Teilen den alten Entwürfen der Koalitionsparteien und der Bundesregierung aus der 10. Wahlperiode. Nach dem Verständnis der Datenschutzbeauftragten entspricht der Gesetzentwurf in wesentlichen Teilen nicht den Anforderungen des Bundesverfassungsgerichts. Die Beratungen im Bundesrat am 10. Februar 1989 zu dem Gesetzentwurf der Bundesregierung brachten eine Vielzahl von Änderungsvorschlägen. Die Beschlüsse des Bundesrates insgesamt wurden von der Konferenz der Datenschutzbeauftragten in ihrer Entschließung vom 05./06. April 1989 als Bestätigung ihrer bisher vertretenen Auffassung begrüßt (vgl. Anlage 1). Es ist nicht abzusehen, wann ein neues Bundesdatenschutzgesetz in Kraft treten wird.

Es bleibt deshalb nach wie vor dabei, daß bei den privaten Stellen, die Datenverarbeitung für eigene Zwecke betreiben, die Datenschutzaufsichtsbehörde nur aufgrund von Beschwerden tätig werden kann. Da auf der geltenden Rechtsgrundlage Systemprüfungen nur fallbezogen möglich sind, sind die Aufsichtsbehörden bei Verhandlungen — z. B. mit dem Versandhandel, der Kreditwirtschaft oder der Versicherungswirtschaft — auf deren Angaben angewiesen. Auch im Bereich der Datenverarbeitung für fremde Zwecke fehlen substantielle Regelungen, z. B. für die Werbewirtschaft und den Adreßhandel. Wegen der nur sehr eingeschränkten Prüfmöglichkeiten können die nachfolgend aufgeführten Fälle nur partielle Datenschutzprobleme deutlich machen.

4.2 Arbeitnehmerdatenschutz

Fragerecht des Arbeitgebers

Die Zentralstelle für Recht und Schutz der Kriegsdienstverweigerer aus Gewissensgründen mit Sitz in Bremen bat mich, dazu Stellung zu nehmen, ob es zulässig sei, daß Arbeitgeber Arbeitsplatzbewerber danach fragten, ob sie den Kriegsdienst verweigert bzw. den Zivildienst abgeleistet hätten. In der Presse war darüber berichtet worden, daß die Firma Messerschmidt-Bölkow-Blohm keine Bewerber einstelle, die als Kriegsdienstverweigerer anerkannt seien oder einen entsprechenden Antrag gestellt hätten. Gemeinsam mit dem Bundesbeauftragten für den Datenschutz, den Bundesministern des Inneren sowie für Arbeit und Sozialordnung sowie anderen obersten Aufsichtsbehörden der Länder für den Datenschutz halte ich eine derartige Frage und die anschließende Datenverarbeitung der Antworten für unzulässig, weil mit ihr der Arbeitgeber tiefer in die Privatssphäre des Bewerbers eindringt, als es der Zweck des Arbeitsverhältnisses erfordert (vgl. BAG NJW 87, 2459).

Die Vereinigung der Arbeitgeberverbände im Lande Bremen teilt die Auffassung, daß die differenzierte Frage eines Personalfragebogens nach Wehr- oder Ersatzdienst grundsätzlich nicht arbeitsplatzrelevant sei. Anderes müsse aber gelten für Unternehmen, die in nicht unerheblichem Maße in der Rüstungsproduktion engagiert seien. Da Arbeitnehmer nicht nur für einen bestimmten Arbeitsplatz eingestellt würden, sondern Versetzungen von einem Arbeitsplatz zum anderen — auch von der Zivil- in die Rüstungsproduktion — üblich seien, hätten solche Unternehmen ein Interesse daran, zu wissen, ob ein Arbeitnehmer auch in der Rüstungsproduktion beschäftigt werden könne oder ausschließlich in der Zivilproduktion.

Ursprünglich hatte ich danach differenzieren wollen, ob eine Beschäftigung in der Zivil- oder in der Rüstungsproduktion beabsichtigt ist. Ich schließe mich der Argumentation an, daß eine solche Differenzierung der unternehmerischen Praxis nicht gerecht wird, ziehe daraus aber den Schluß, daß in keinem Fall — auch in Unternehmen, die ausschließlich oder anteilig Rüstungsgüter produzieren, nicht — eine differenzierte Frage nach dem Wehr- oder dem Ersatzdienst zulässig ist. Andernfalls würde in weiten Bereichen der Wirtschaft die Wahrnehmung des Rechts auf Kriegsdienstverweigerung zur Einschränkung der Arbeitsplatzfreiheit führen.

4.3 Patientendatenschutz

4.3.1 Übergabe der Patientenkartei an den Käufer einer Arztpraxis

In der Presse war unter dem Stichwort „Handel mit Patientenkarteien" kritisch darüber berichtet worden, daß es üblich sei, daß Ärzte ihre Praxen zusammen mit den Patientenunterlagen verkauften, ohne ihre Patienten zuvor um Einwilligung gebeten zu haben, ja oft, ohne daß die Patienten überhaupt darüber informiert würden. Auf Fragen eines Bremer Journalisten habe ich meine Position bekräftigt, daß jeder Patient nicht nur zu informieren sei, sondern auch schriftlich einwilligen müsse, daß seine Daten in die Obhut des anderen Arztes übergingen, und eine vorherige Einwilligung des einzelnen Patienten in die Übergabe seiner Unterlagen verlangt. In Folge des darauf basierenden Presseartikels ist es zu einem Gedankenaustausch mit Vertretern der bremischen Ärzteschaft gekommen. Das Problem ist außerdem unter den obersten Aufsichtsbehörden der Länder für den Datenschutz erörtert worden. Es liegen ein juristisches Gutachten sowie Stellungnahmen verschiedener Fachministerien der Länder vor.

Nach geltendem Recht — und dies ist die einhellig geäußerte Meinung — bedarf die Übergabe von Patientenunterlagen, die der ärztlichen Schweigepflicht unterliegen, an den Praxisnachfolger der ausdrücklichen Einwilligung des Patienten (§ 203 StGB, §§ 3, 24 BDSG). Ohne Prüfung des Einzelfalles kann eine konkludente Einwilligung nicht unterstellt werden, denn zunehmend suchen Patienten einen bestimmten Arzt als Person ihres Vertrauens auf. Eine mutmaßliche Einwilligung scheidet in der Regel schon aus rechtlichen Gründen aus. Die in den Berufsordnungen für Ärzte begründete Verpflichtung des Arztes, dafür Sorge zu tragen, daß die Patientenunterlagen „nach Aufgabe der Praxis in gehörige Obhut gegeben werden", widerspricht dem nicht.

Die praktischen Schwierigkeiten bei der Umsetzung der rechtlichen Anforderungen verkenne ich nicht. Sie rechtfertigen jedoch nicht eine Praxis, die die ärztliche Schweigepflicht schlicht außer Kraft setzt.

Ich habe den Senator für Gesundheit gebeten darauf hinzuwirken, daß die Berufsordnung für Ärzte im Lande Bremen vom 28. Mai 1979 so ergänzt bzw. präzisiert wird, daß sie auf der Grundlage des geltenden Rechts die Interessen der Patienten an freier Arztwahl und Wahrung des Arztgeheimnisses wirksam schützt. Zugleich sollte auch für den Schutz der Patientendaten nach Auflösung der Praxis bzw. nach Tod eines Arztes die erforderliche Regelung getroffen werden (vgl. meinen 7. und 8. Jahresbericht unter Pkt. 5.11.1.2 bzw. 5.12.2).

Andere in diesem Zusammenhang erörterte Probleme können auf der Grundlage der geltenden Regelungen gelöst werden:

- Bei Praxisvertretungen ist die Einsichtnahme des Vertreters in Patientenakten grundsätzlich zulässig, wenn der jeweilige Patient die Behandlung durch den Vertreter wünscht; insoweit ist dann von einer konkludenten Einwilligung des Patienten des zu vertretenden Arztes auszugehen.
- In Gemeinschaftspraxen und Praxen, in denen Ärzte im Praktikum tätig sind, ist der Patient auf diese besondere Konstellation hinzuweisen. Soweit das Praxisschild die Besonderheit bereits ausweist, ist der Informationspflicht Genüge getan.

Ich habe die Bremische Ärztekammer entsprechend angeschrieben.

4.3.2 Laborbefunde im Park

In Bremerhaven wurden in einer öffentlichen Anlage ärztliche Unterlagen mit Laborbefunden über Blutuntersuchungen aufgefunden. Die Untersuchungsergebnisse waren mit Namen und Geburtsdaten der Betroffenen versehen.

Bei meinen Nachforschungen stellte sich heraus, daß bei der ärztlichen Stelle, die den Verlust noch nicht bemerkt hatte, die Unterlagen aus einem Blechbriefkasten entwendet worden waren. Der Briefkasten war an der Außentür angebracht und öffentlich zugänglich.

Auch wenn das Entwenden und unbefugte Öffnen von Briefen strafbar ist, macht dieser Vorgang deutlich, daß der Datensicherung ein eigener Rang eingeräumt werden muß. Ich habe der ärztlichen Stelle empfohlen, den Briefkasten entweder in den kontrollierbaren Innenbereich zu verlegen oder ein Schließfach bei der Bundespost einzurichten. Um völlig sicherzugehen und das Arztgeheimnis zu wahren, hat sich die Stelle entschlossen, ein Postschließfach einzurichten.

4.4 Aufbewahrung und Weiterleitung von Ladendiebstahlsanzeigen

Aufgrund von Eingaben habe ich in verschiedenen Verbrauchermärkten geprüft, wie dort mit Anzeigen über Ladendiebstähle verfahren wird. In allen Fällen stellte sich das gleiche Bild dar:

Von der Ladendiebstahlsanzeige werden drei Ausfertigungen erstellt, eine geht an die Polizei, eine an die Unternehmenszentrale und eine verbleibt in der Filiale, in der der Diebstahl beobachtet wurde. Gleichzeitig wird eine Vertragsstrafe auf einem Formular erfaßt, das in der Filiale sowie in Kopie in der Zentralstelle des Unternehmens aufbewahrt wird. In den Filialen habe ich festgestellt, daß die Anzeigeformulare dort bis zu vier Jahren in Aktenordnern aufbewahrt werden, zum Teil gemeinsam mit Mitteilungen der Staatsanwaltschaft über den Ausgang des Verfahrens.

Da ich für die jeweiligen Zentralstellen nicht zuständig bin, habe ich die Vorgänge zur weiteren Prüfung an die zuständige Aufsichtsbehörde weitergeleitet. Von dort wurde mitgeteilt, daß die Anzeige zu statistischen Zwecken und zur Prüfung über zu treffende Maßnahmen zur Eindämmung von Ladendiebstählen ausgewertet und anschließend vernichtet werden. Das Formular zur Vertragsstrafe wird zur Abrechnung der „Fangprämie" in der Abrechnungsstelle der Zentralstelle und bei den Hausdetektiven aufbewahrt.

Hinsichtlich der Verarbeitung bei der Zentralstelle habe ich die zuständige Aufsichtsbehörde gebeten, darauf hinzuwirken, hierfür ein anonymisiertes Verfahren einzuführen, da für die genannten Zwecke die Kenntnis der personenbezogenen Daten nicht erforderlich ist.

Die Speicherung in der Filiale ist nur zulässig, soweit es um die zivilrechtlichen Ansprüche aus der Vertragsstrafe und um die Durchsetzung des ausgesprochenen Hausverbots geht oder das Strafverfahren noch nicht abgeschlossen ist. Die Aufbewahrung der Unterlagen von bis zu vier Jahren halte ich nicht für erforderlich;

der Grund für die Speicherung ist nach Zahlung der Vertragsstrafe und nach Ablauf des Hausverbots (das in der Regel nicht über ein Jahr hinausgeht) nicht mehr gegeben.

Nach § 27 Abs. 3 Satz 3 BDSG sind Daten über strafbare Handlungen zu löschen, wenn ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann. Dieses gilt auch für Verfahren, die gemäß § 170 Abs. 2 StPO eingestellt werden. In den anderen Fällen, in denen die Kenntnis nicht mehr erforderlich ist, sieht § 27 Abs. 2 Satz 2 BDSG nur die Sperrung der Daten vor; eine Maßnahme, die die Interessenlage der Betroffenen nicht ausreichend berücksichtigt. Die Löschung ist dagegen nicht zwingend geboten, es sei denn, der Betroffene beantragt dieses. Diese Regelung des BDSG ist derart ungenügend, daß ich Betroffenen derzeit nur empfehlen kann, von ihrem Recht auf Löschung durch entsprechende Anträge Gebrauch zu machen. Dieses ist nur möglich, wenn bereits bei der Aufnahme der Daten in die Formulare dem Betroffenen die weitere Datenverarbeitung transparent gemacht wird.

4.5 Datenschutz in Fotolabors und Fotogeschäften

Ein Bürger hatte unter einer Parkbank einen Plastikbeutel mit einer Vielzahl von Fotos gefunden. Auf den Fotos erkannte er auch einen Alleinunterhalter. Diesen rief er an und informierte ihn über seinen Fund. Die Recherchen der beiden haben ergeben, daß ein Fotolabor Fehlentwicklungen, d. h. Bilder mit schlechter Qualität gesammelt und in einen Container geworfen hatte. Dieser Container war öffentlich zugänglich. Es ist daher nicht auszuschließen, daß die Fotos auf diesem Wege in die Öffentlichkeit gelangt sind.

Mit der Weitergabe des Fotomaterials an Fotogeschäfte und Labors entäußert sich der Kunde seiner zum Teil intimsten Lebenssphäre. Konkludente Vertragsbedingung ist dabei, daß der Kunde selbst darüber entscheidet, wem er das Fotomaterial zugänglich machen will (Recht am eigenen Bild). Die andere Vertragspartei trifft daher die vertragliche Nebenpflicht, die Privat- und Intimsphäre des Kunden weitmöglichst zu schützen. Sie hat deshalb technische und organisatorische Vorkehrungen zu treffen, die die Privat- und Intimsphäre des Kunden sicherstellen. Ich habe die Geschäftsleitung des Fotolabors aufgefordert sicherzustellen, daß sämtliches personenbeziehbares Fotomaterial, das nicht an den Kunden ausgeliefert wird, im Betrieb vernichtet wird. Ich habe empfohlen, die Beschäftigten hierauf hinzuweisen, um die private Mitnahme von Fotomaterial auszuschließen.

Dieser Fall macht deutlich, daß die Regelungen des geltenden BDSG nicht ausreichen, Verstöße gegen das informationelle Selbstbestimmungsrecht seitens der Aufsichtsbehörden zu verfolgen.

4.6 Forderung nach Regelungen des Datenschutzes bei Verbraucherkrediten

Gemeinsam mit Vertretern anderer Aufsichtsbehörden habe ich mich darum bemüht, daß der Bundesminister der Justiz datenschützende Regelungen in den Entwurf des Verbraucherkreditgesetzes einfügt. Die Notwendigkeit hierfür ergibt sich aus folgenden Überlegungen: In der Kreditwirtschaft werden vielfältige Informationen über die Kreditwürdigkeit nahezu aller am Waren- und Geldverkehr Beteiligten gesammelt und weitergegeben. Nicht nur Kreditaufnahmen, sondern bereits die Einrichtung eines Giro-Kontos oder die Ausgabe einer Kreditkarte ziehen eine ständig automationsgestützte Bonitätsbeobachtung der Verbraucher nach sich. Den generalklauselartigen Erlaubnisnormen im geltenden und künftigen BDSG sind präzise Vorgaben zum Schutz der Verbraucher beim Umgang mit Kreditdaten, wie etwa Zahlungsverzug und Zwangsvollstreckungsmaßnahmen, nicht zu entnehmen.

Nach dem Vorbild anderer europäischer Länder sollten deshalb im Zusammenhang mit gesetzlichen Bestimmungen über Verbraucherkredite spezielle Regelungen geschaffen werden, die einen besonderen Datenschutz bei Verbraucherkrediten gewährleisten. Datenschutzabsprachen mit den speichernden Stellen konnten bisher nur in Teilbereichen getroffen werden. Es ist es noch nicht gelungen, bestimmte Nutzer von Kreditinformationen wie z. B. Handel und Versandhandel dazu zu bewegen, die Nutzung der Datenbestände der Auskunfteien auch gegenüber dem Verbraucher offenzulegen.

Angesichts wachsender internationaler Verflechtungen im Waren- und Kreditverkehr, nicht zuletzt wegen des bevorstehenden EG-Binnenmarktes, ist eine starke Zunahme grenzüberschreitender Datenflüsse über Kreditnehmer zu

erwarten. Da im Ausland vielfach ausreichende Datenschutzregelungen noch fehlen, muß eine bereichsspezifische Regelung des Datenschutzes bei Verbraucherkrediten auch diesem Aspekt besondere Aufmerksamkeit widmen. Über nationale Initiativen hinaus, sollte daher auf Richtlinien der Europäischen Gemeinschaft hingewirkt werden, die einen einheitlichen Mindestdatenschutz bei Verbraucherkrediten in allen Mitgliedstaaten sicherstellen.

Zum Schutze der Verbraucher bei der Gewährung und Abwicklung von Krediten erscheinen insbesondere folgende Datenschutzregelungen erforderlich:

- Kreditinformationsdienste (Auskunfteien müssen einer strikten Zweckbindung unterliegen. Daten von Kreditnehmern dürfen sie nur erfassen und nutzen, soweit dies zu Beurteilung der Kreditwürdikgeit und zur Bonitätskontrolle erforderlich ist. Eine Verwendung für andere Zwecke, etwa zur Personaleinstellung, zum Abschluß von Mietverträgen oder zu Werbezwecken, ist unzulässig, Die Empfänger von Kreditinformationen dürfen die Daten ebenfalls nur im Rahmen der Zweckbindung verwenden.
- Durch Rechtsvorschrift ist abschließend festzulegen, welche Merkmale über nicht vertragsgemäßes Verhalten und welche sonstigen Angaben über Zahlungsfähigkeit oder -unwilligkeit (Negativmerkmale) in Kreditinformationssystemen verarbeitet werden dürfen.
- Vor der Übermittlung bestimmter Negativmerkmale, bei denen Fehlentscheidungen über die Zahlungsunfähigkeit oder -unwilligkeit nicht auszuschließen sind (z. B. Verdacht des Scheckkartenmißbrauchs), ist dem Kreditnehmer Gelegenheit zur Stellungnahme zu geben.
- Durch Verpflichtung zu fortwährender Aktualisierung ist sicherzustellen, daß der Datenbestand des Kreditinformationsdienstes zu jeder Zeit ein zutreffendes Bild über die Bonität der Kreditnehmer vermittelt. Zu melden sind auch Umstände, die für den Kreditnehmer sprechen (etwa Ausgleich von Zahlungsrückständen) bzw. Zweifel an seiner Zahlungsunfähigkeit oder -unwilligkeit begründen können (z. B. Widerspruch gegen Mahnbescheid).
- Mit Einwilligung der Kreditnehmer dürfen auch Mermale über die Beantragung, Aufnahme und vereinbarungsgemäße Abwicklung von Verbraucherkrediten (Positivmerkmale) von Kreditinformationsdiensten verarbeitet werden. In einem Katalog sind die Daten aufzuführen, die nicht verarbeitet werden dürfen (z. B. Daten über die rassische Herkunft, politische oder religiöse Anschauungen, Gesundheit und Sexualleben).
- Personenverwechselungen, die in der Praxis häufig auftreten und zu schwerwiegenden Nachteilen für die Betroffenen führen, sind wirksam auszuschließen.
- Es sind Löschungsfristen festzulegen, die der besonderen Sensitivität der Kreditdaten Rechnung tragen.
- Kreditnehmer sind schon dann zu benachrichten, wenn erstmals im Kreditinformationssystem zu ihrer Person Daten gespeichert werden, sofern nicht feststeht, daß sie auf andere Weise hiervon Kenntnis erlangt haben.
- Das Auskunftsrecht der Kreditnehmer muß sich auch auf die Herkunft und die Empfänger der Daten erstrecken.
- Von Kreditnehmern darf nicht verlangt werden, eine Auskunft über ihre im Kreditinformationssystem gespeicherten Daten einzuholen, damit die Zweckbindung der Kreditdaten nicht unterlaufen wird.
- Auch die Teilnehmer am Kreditinformationsverfahren sind der regelmäßigen Überwachung durch die Auskunftsbehörden nach § 40 BDSG zu unterstellen.
- Eine Verwendung von Kreditdaten für nichtkreditorische Zwecke in anderen Geschäftssparten innerhalb des kreditgewährenden Unternehmens ist von der Einwilligung des Betroffenen abhängig zu machen.
- Bei statistisch-mathematischen Verfahren zur Bewertung der Bonität von Verbrauchern (Kreditscoring) ist dem Kreditnehmer über die Bewertungsgrundlagen und -kriterien sowie über errechnete Teil- und Gesamtwerte auf Antrag kostenlos Auskunft zu erteilen.
- Es ist zu prüfen, ob für den grenzüberschreitenden Austausch von Verbraucherkreditdaten besondere Datenschutzregelungen erforderlich sind.

4.7 Auskunfteien

4.7.1 Schufa

Mehrfach, zuletzt im 11. Jahresbericht, habe ich über das Problem der **Schufa-Nachmeldungen** berichtet. Auslöser waren Bürgereingaben, die sich darüber wunderten, daß ihre Hausbank Informationen über neue Kreditverhältnisse erhielt, die sie bei einer anderen Bank eingegangen sind. Auch im Berichtsjahr erhielt ich wieder Eingaben zu diesem Problem. Da ich die Praxis der „automatischen" Schufa-Nachmeldungen über neue Kreditverhältnisse an die alten Kreditgeber für nicht vereinbar mit der bestehenden Rechtslage halte, habe ich dieses Thema in den „Düsseldorfer Kreis" eingebracht. Der entsprechende Arbeitskreis will sich im Laufe dieses Jahres mit diesem Thema beschäftigen.

Wiederholt erhielt ich auch Bürgereingaben zum Problem des sogenannten **„Versandhauskontos".** Versandhäuser sind in der Regel, wenn sie Kredit gewähren (z. B. Lieferungen gegen Rechnung; bei Einräumung eines Kundenkredits für Lieferungen und Leistungen), Anschlußkunde des Schufa-Systems. Manche Versandhäuser richten generell — auch wenn der Kunde es gar nicht will — ein Kundenkonto ein und melden diesen Tatbestand an die zuständige Schufa-Gesellschaft. Die Schufa speichert in diesen Fällen zum jeweiligen Betroffenen die Information „Name, Anschrift des Versandhauses, Versandhauskonto, Beginn-Ende-Datum".

Ich halte diese Datenverarbeitungspraxis, vor allem in den Fällen, in denen der Versandhauskunde einen Versandhauskredit nicht haben will, datenschutzrechtlich für unzulässig. Die Zulässigkeit der Datenübermittlung vom Versandhaus an das Schufa-System bestimmt sich nach den §§ 3, 24 BDSG (Einwilligung in Kaufvertrag oder gesetzliche Erlaubnis nach § 24 BDSG). Ohne ausdrückliche Einwilligung des Betroffenen halte ich die Übermittlung einer nicht-kreditorischen Versandhausbestellung — auch wenn vom Versandhaus ein Konto eingerichtet wird — an das Schufa-System für unzulässig und mit der Zweckbestimmung dieses Systems nicht für vereinbar. Ein gesetzlicher Erlaubnistatbestand zur Übermittlung (§ 24 BDSG) läge nur vor, wenn tatsächlich ein Versandhauskredit vereinbart ist und hierbei negative Tatbestände objektiver Art auftreten. Die Speicherung derartiger Daten im Schufa-System wäre nur im letztgenannten Fall zulässig, d. h. wenn die Daten zulässigerweise an das Schufa-System gelangt sind und wenn die Daten richtig sind.

Aber auch in den Fällen, in denen der Versandhauskunde per Rechnung/auf Zahlungsziel hin Waren bestellt, erscheint mir die Speicherung der Information „Versandhauskonto" im Schufa-System rechtlich zweifelhaft. Aus der Sicht der Versandhäuser besagt die Information „Versandhauskonto" nämlich nur, daß bei Bedarf dort Ware bestellt werden kann; sie besagt jedoch nicht, daß Kreditverpflichtungen gegenüber dem Versandhaus bestehen. Als Schufa-Information besagt die Auskunft „Versandhauskonto" jedoch — entsprechend der Zweckbestimmung des Schufa-Systems — daß ein Versandhauskredit eingeräumt wurde. Da Versandhäuser in der Regel von der Schufa nur sogenannte B-Verträge (d. h. Meldung/Übermittlung sogenannter Negativdaten zu Kreditverhältnissen = Daten über nicht vertragsgemäßes Kundenverhalten) erhalten, ist die scheinbar neutrale Schufa-Eintragung „Versandhauskonto" mißbräuchlich.

Aufgrund einer Eingabe hatte ich mich im Berichtsjahr mit der Zulässigkeit der Speicherung und Verwendung von Kreditdaten zu beschäftigen, die die Schufa Bremen über eine **ausländische Kreditschutzorganisation** erhalten hatte. Im konkreten Fall waren die Kreditdaten des Betroffenen (Name der Bank, Art des Kredits, Höhe des Betrages, Ratenzahl, Fälligkeit, Name/Anschrift/Geburtsdatum des Betroffenen) von einer österreichischen Bank an den österreichischen Kreditschutzverband in Wien übermittelt und von dort über die Bundesschufa e. V. in Wiesbaden (als Dachverband der Schufa-Gesellschaften) zur Schufa Bremen weiterübermittelt worden. In Frage standen bei dieser Eingabe die Übermittlungsvorgänge aus Österreich zur Bundesschufa e. V., die Übermittlungsvorgänge von der Bundesschufa e. V. zur örtlichen Schufa-Gesellschaft in Bremen und die Speicherung und Verwendung der übermittelten Daten durch die örtliche Schufa-Gesellschaft.

Die Speicherung und Verwendung der Daten bei der örtlichen Schufa ist nur zulässig, wenn die Daten rechtmäßig übermittelt wurden. Die Datenübermittlungsvorgänge in Österreich regeln sich nach dem österreichischen Datenschutzgesetz, das für diese Fälle im Grundsatz dem Bundesdatenschutzgesetz ähnliche Regelungen enthält. Ob die österreichische Bank zulässigerweise Kreditdaten des Betrof-

fenen (Positivdaten) an den österreichischen Kreditschutzverband in Wien übermitteln durfte, hängt davon ab, ob der Betroffene sich mit dieser Datenübermittlung einverstanden erklärt, eine wirksame Einwilligungserklärung gegenüber der Bank abgegeben hat. Im konkreten Fall konnte dies nicht mehr überprüft werden, da der Petent den österreichischen Kreditvertrag nicht vorlegte. Aus anderen Sachzusammenhängen ist mir aber bekannt, daß bis dato in den österreichischen Kreditverträgen keine Einwilligungserklärungen enthalten sind mit der Folge, daß schon die Datenübermittlung in Österreich von der Bank zum Kreditschutzverband in Wien fragwürdig ist. Gleiches gilt für die Weiterübermittlung zur Bundesschufa e. V. in Wiesbaden und weiter zur örtlichen Schufa-Gesellschaft. Die Speicherung im Datenbestand der örtlichen Schufa-Gesellschaft, im konkreten Fall also bei der Schufa in Bremen, wäre damit ebenfalls in Zweifel zu ziehen.

Im Hinblick auf die Tatsache, daß das Schufa-System mit anderen inländischen Informationssystemen (z. B. KSV) und mit ausländischen Kreditschutzsystemen (z. B. Österreich, Niederlande) vertraglich und zum Teil auch systemtechnisch verflochten und dieser Trend im Zuge der technischen Entwicklung und der europäischen Einigung zunehmen wird, beschäftigen sich zur Zeit die Datenschutzaufsichtsbehörden mit dieser system- und grenzüberschreitenden Thematik.

4.7.2 Creditreform

Bei vielen Eingaben, die Auskunftei Creditreform betreffend, stellt sich — auch in diesem Berichtsjahr wieder — das Problem der **Nutzung der Inkassodaten für Zwecke der Auskunftstätigkeit.** Die örtlichen Vereine Creditreform betreiben neben ihrer Tätigkeit als Auskunftei auch eine Tätigkeit als Inkassobüro. Beide Bereiche sind innerbetrieblich zwar getrennt (getrennte Abteilungen), systemtechnisch und informationsmäßig sind beide Bereiche jedoch nicht getrennt. Häufig kommt es sogar vor, daß säumigen Schuldnern im Rahmen des Inkassos damit „gedroht" wird, daß ihre Inkassodaten im Rahmen der Auskunfteitätigkeit weiterverwendet, sprich weiter übermittelt werden. Die Vereine Creditreform betrachten das Inkassogeschäft und die darin liegenden Informationsmöglichkeiten als sinnvolle und rechtlich zugelassene Informationsquelle für den Bereich Auskunftei. Entsprechend ist auch das automatisierte Informationssystem der Vereine Creditreform angelegt.

Die Datenschutzaufsichtsbehörden bestreiten die Auffassung der Vereine Creditreform und sind gemeinschaftlich der Auffassung, daß beide Bereiche getrennt zu sehen und zu behandeln sind. Die systemtechnische und informationsmäßige „Verquickung" beider Bereiche durch die Vereine Creditreform wird datenschutzrechtlich als unzulässig angesehen.

In meinem 11. Jahresbericht (Pkt. 6.3.1) hatte ich hierüber bereits berichtet. Der Sachverhalt besteht — leider — fort.

Das Informationssystem der Vereine Creditreform wirft eine Reihe **weiterer Datenschutzprobleme** auf, die zwischen den Datenschutzaufsichtsbehörden und den Vereinen Creditreform streitig diskutiert werden. Vor allem die zentrale Speicherung der Daten der örtlichen Vereine Creditreform beim Verband der Vereine Creditreform e. V. in Neuss sowie die dortige Datenverarbeitung und extensive Vermarktung der gespeicherten Daten stehen im Mittelpunkt dieser Auseinandersetzungen. Der zentrale Datenbestand in Neuss wird zunehmend für online-Anschlüsse von Mitgliedsfirmen der Vereine Creditreform geöffnet; die Bereitstellung des gesamten Datenbestandes der Vereine Creditreform ohne speziellen Nachweis des berechtigten Interesses halte ich datenschutzrechtlich für unzulässig. Der zentrale Datenbestand ist als Teildatenbank über verschiedene Wirtschaftsdatenbanken, Mailbox-Dienste oder Wirtschaftsinformationsdienste erreichbar und für Nutzer derartiger Dienste verfügbar; auch dies ist mit § 32 Abs. 2 BDSG nicht vereinbar. Neuartige Aufbereitungs- und Auswertungsmöglichkeiten werden genutzt und angeboten (z. B. bonitätsgeprüfte Adressen; Errechnung von Bonitätsindices für Kreditmanagement und Marketing); diese Datenverarbeitung ist ebenfalls nicht mit den Bestimmungen des Bundesdatenschutzgesetzes zu vereinbaren.

5. Informationstechnologien

5.1 Telekommunikation — Wirkungen der Digitalisierung

Wie bereits im 11. Jahresbericht beschäftige ich mich mit dem Thema ISDN; jetzt mit den Wirkungen, die durch die Umstellung des Telefonnetzes im Zusammenhang mit dem Aufbau des ISDN-Netzes entstehen.

Die Wirkungen lassen sich aus Datenschutzsicht in fünf Bereiche einteilen.

- **Digitalisierung von Sprache**

Durch die Digitalisierung von Sprachsignalen besteht die Möglichkeit, während des Abhörens eines Telefonates den Gesprächsinhalt programmgesteuert nach bestimmten „Stichworten" zu durchsuchen und Folgeaktionen anzustoßen (Protokollierung, Meldung, etc.).

Die Möglichkeiten für systematische, permanente Überwachung von Kommunikationsinhalten steigen, weil insbesondere Kontroll- und Überwachungsinstitutionen sich dieser Möglichkeiten bedienen werden wollen. Dadurch entstehen für den Bürger neue Risiken.

- **Digitalisierung der Vermittlung**

Die Möglichkeiten der analogen Vermittlung von Gesprächen werden auf Kosten der Anonymität der Teilnehmer zur digitalen Vermittlung erweitert. Die begrenzte Anzahl von Befehlen, die zum Aufbau und Abbau einer Verbindung zwischen zwei Vermittlungsstellen ausgetauscht werden, ist stark erweitert worden. Die technischen Steuerungsgrenzen der Analogtechnik sind aufgehoben und der Umfang der Befehle ist flexibel erweiterbar. Ausgetauscht werden diese Befehle nicht mehr vor und nach einem Gespräch über den gleichen Kanal, sondern parallel in einem Steuerkanal (D-Kanal).

Aufgebaut wird die Verbindung nicht mehr durch schrittweise Auswertung der Wählinformationen und Schaltung einer Leitung bis zum Zielpunkt, sondern durch die Mitteilung der Telefonnummer von End- und Zielteilnehmer an potentielle Vermittlungsstellen, Prüfung der Verbindungsmöglichkeit und Schaltung einer Leitung.

Dies eröffnet nicht nur die Möglichkeit, bei Engpässen laufende Gespräche ohne Unterbrechung auf eine andere Leitung zu schalten, um dadurch den Gesamtdurchsatz des Netzes zu optimieren, sondern führt auch zu einer Erweiterung der Funktionalität von Endgeräten, neuen Dienstmerkmalen wie zum Beispiel der Nutzung mehrerer Dienste und Endgeräte parallel über einen Anschluß, das Anklopfen und die der Anzeige des anrufenden Teilnehmers auf dem Zeilendisplay.

- **Flächendeckende Kommunikationsinfrastruktur für Computer**

Die Anzahl der „Computer-Steckdosen" von heute ca. 300.000 wird durch ISDN mittelfristig erhöht auf fast 30 Millionen. Aufgrund der freien Gestaltbarkeit der Steuerbefehle in ISDN ist es möglich, das Telefonnetz den Computernetzen anzugleichen und somit den Telefonanschluß, der bisher überwiegend nur der Sprach-Kommunikation zwischen Menschen gedient hat, zu einem Anschluß für die programmgesteuerte Daten-Kommunikation zwischen Computern umzugestalten. Da Computer sich nicht wie Menschen an der Sprache erkennen können, wenn diese Daten von Programm zu Programm austauschen, ist es für sie zwingend notwendig, die Rufnummern auszutauschen.

Der Anteil der Sprachkommunikation im Verhältnis zur Datenkommunikation wird sich, speziell bei der Abwicklung von Vorgängen in den Bereichen Produktion, Handel und Dienstleistung, stärker und zugunsten der Datenkommunikation schneller verschieben.

- **Verarbeitung der Kommunikationsbeziehungen von fast 30 Millionen Telefonteilnehmern**

Die Integration von Kommunikation zwischen Menschen und von Computern untereinander eröffnet einerseits neue Möglichkeiten der Optimierung durch Netzwerk-Management und eine feinere Differenzierung von Gebührenstrukturen und -abrechnungen durch differenziertere Basisdaten. **Andererseits** werden die Kommunikationsbeziehungen der Teilnehmer an Telefon und Computer durch diese Basisdaten auch auswertbar.

Die Folgen treffen nicht nur Teilnehmer im öffentlichen ISDN, sondern auch Benutzer lokaler Netze, wie z. B. LANs, ISDN-Nebenstellenanlagen und Spezialnetzen wie MAP (zu diesen Begriffen vgl. Pkt. 5.2), da nicht nur der Datentransport- und die Datenverarbeitungsfunktionen in Netzen dem gleichen internationalen Standard (ISO/OSI-Referenzmodell, s. Pkt. 5.2) für offene Kommunikation in

Netzen entsprechen, sondern auch der netzübergreifende Austausch von Management- und Accounting-Daten (Verwaltungs- und Abrechnungsdaten), den Basisdaten, Gegenstand der internationalen Normung ist.

Besonders problematisch ist der Austausch von personenbezogenen Verwaltungs- und Abrechnungsdaten zwischen staatlichen und privaten Dienstleistungsanbietern. Einerseits werden staatliche Kontrollmöglichkeiten tief in den privaten Sektor (PC-Anwender in privat betriebenen lokalen Netzen, z.B. ISDN-Nebenstellenanlagen) hineinreichen und andererseits werden große Teile bisher ausschließlich staatlicher Dienstleistungen in die Leistungen privater Dienstanbieter integriert (z. B. der Betrieb eines „netzübergreifenden" privaten Netzwerkes auf der Basis von angemieteten öffentlichen Standleitungen für den Fernbereich, öffentliche Netze im Nahbereich und private lokale Netze im „inhouse"-Bereich bis zu den End-Teilnehmern) und für den Dienstanbieter und den Leistungsnehmer transparent.

- **Integrierte und vernetzte Organisation**

Die Umstellung der Kommunikation mittels Sprache auf eine flächendeckende Datenkommunikation von Programm-zu-Programm beinhaltet neue Formen der Aufbau- und Ablauforganisation mit neuen Risiken. Personenbezogene Daten werden dem Schutz des Fernmeldegeheimnisses entzogen.

Markante Meilensteine dieses Entwicklungsprozesses sind

- „electronic mailing", d. h. der elektronische Nachrichtenaustausch mit Hilfe von Datenkommunikation und elektronischen Briefkästen, eines noch relativ unstrukturierten Austauschs, analog zum Austausch von Zetteln unterschiedlicher Form, Größe und Inhalt,
- EDI (Electronic Data Interchange), der Austausch von digitalen Briefen in digitalen Umschlägen im Standardformat zwischen Computern und anderen Datenendgeräten wie z. B. BTX-, TELEX-, TELETEXT- und TELEFAX-Geräten und
- EDIFACT (EDI for Administration, Commerce and Transport), der Normung von bereichsspezifischen Formularen (z. B. Rechnungen, Bestellungen und Verträge), bis hin zu Zollerklärungen und Frachtpapieren. Zur Zeit existieren ca. 40 Formulare, die Gegenstand internationaler Standardisierung sind. Ein Teil der Standardformulare liegt schon vor, andere sind noch in Arbeit. Zur Zeit wird EDIFACT in 110 bundesrepublikanischen Projekten und 520 EG-weiten Projekten erprobt.

Diese Entwicklungen begünstigen die Optimierungsansätze für organisationsübergreifende Abläufe wie „just-in-time", die zusätzlich zu den allgemeinen Wirkungen von Vernetzung als Katalysator für Systemintegration zu immer längeren Wertekettensystemen (die Verkettung der einzelbetrieblichen Wertschöpfung durch Systeme) führen und die Erbringung von Verwaltungsdienstleistungen immer stärker beinflussen werden (z. B. der „digitale" Zollstempel bei Ein- oder Ausfuhr, den Enden der Kette).

Elektronischer Datenaustausch wird vor Verwaltungshandeln nicht Halt machen. Die Integration und Vernetzung in der Organisationsform „just in time" bestimmen das Handeln der öffentlichen Verwaltung dadurch, daß private, technische Prozesse in das Verwaltungshandeln hineinreichen. Es besteht die Gefahr, daß sich der Gestaltungsrahmen der Verfassungsorgane schleichend vermindert.

5.2 Datenschutz in Netzen

5.2.1 Informationstechnologische Grundlagen

Rechnernetze wurden von den Herstellern der EDV-Anlagen entwickelt, um die Verarbeitungsfunktionen eines EDV-Systems den Anwendern und Benutzern näher zu bringen. Anfangs hatten Rechnernetze eine strikt hierarchische und zentralistische Grundstruktur und konnten quasi nur mit den Geräten des Netz-Herstellers betrieben werden, da nur diese problemlos angeschlossen werden konnten. Mit der Anzahl der Netze stieg der Bedarf an netzübergreifender Datenkommunikation. Der Aufwand für die Schaffung und den Betrieb von Netzübergängen stieg. Es folgte die Forderung nach offenen Systemen. Die wesentlichen Impulse gehen hier von der ISO (International Organisation for Standardization) aus. Ihr Ziel ist es, Verhaltensregeln (Protokolle) für eine offene Kommunikation zwischen unterschiedlichen Systemen und Endgeräten zu entwickeln und allgemein verbindlich festzulegen.

Da bei Datenkommunikation, im Unterschied zu menschlicher Kommunikation, eine Verständigung nur streng formal ablaufen kann, mußte die Problemstellung entsprechend komplex gestaltet werden. Um einfacher zu abgestimmten Ergebnissen zu kommen, hat man Datenkommunikation in 7 Funktionsbereiche, den 7 Schichten, aufgeteilt und das Zusammenspiel strikt hierarchisch gestaltet. Jede Schicht kann für die Erledigung ihrer Aufgabe ausschließlich nur auf die Dienstleistung der direkt darunterliegenden Schicht zugreifen. Dieses funktionale Modell von Datenkommunikation, das OSI(Open System Interconnection)-Referenzmodell, ist die Grundlage internationaler Standardisierung.

Die Schichten lassen sich grob in die Bereiche Nachrichtentechnik und DV-Technik aufteilen: Einerseits die Schichten 1-4 mit den Verhaltensregeln für den Transport von Bits zwischen den Endgeräten, andererseits die Schichten 5-7 mit Verhaltensregeln für die Verarbeitung dieser Bits zu Daten und deren Interpretation in bestimmten Anwendungszusammenhängen, wie z. B. dem Austausch von Bestellungen und Rechnungen im EDIFACT-Standard (vgl. Pkt. 5.1).

In Analogie zur Einteilung von Telefonnetzen in Ortsnetz, Fernnetz und weltweites Netz werden Datenkommunikationsnetzwerke in folgende Entfernungsklassen aufgeteilt:

- GAN (Global Area Networks), die Datenkommunikation mittels Satelliten, ohne praktische räumliche Begrenzung, mit Übertragungsraten von ca. 100 Textseiten pro Sekunde bei einer geringen Anzahl von Teilnehmern;
- WAN (Wide Area Networks), die Datenkommunikation mittels Telefonleitungen mit einer räumlichen Grenze bei etwa 1000 km und einer Übertragungsrate von weniger als einer Textseite pro Sekunde bei gleichzeitig mehreren 1.000 Teilnehmern;
- MAN (Metropolitan Area Networks), Datenkommunikation mittels Spezialleitungen für Ballungsräume bis ca. 20 km Ausdehnung und mit Übertragungsraten von ca. 20 Textseiten pro Sekunde bei gleichzeitig 200 Teilnehmern;
- LAN (Local Area Networks), die Datenkommunikation mittels Telefonleitungen oder Spezialleitungen bis ca. 10 km und 3 Übertragungsklassen:

  „low cost" LANs bis ca. 20 Texts./Sek. bei 10 Teilnehmern,

  „backbone" LANs bis ca. 20 Texts./Sek. bei 100 Teilnehmern und

  „high speed" LANs für mehr als 1000 Texts./Sek. bei 10 Teilnehmern.

In all diesen Netzwerken werden — mehr oder weniger ausgeprägt — die Verhaltensregeln für die Datenkommunikation nach dem ISO/OSI-Referenzmodell angewendet. Der netzübergreifende Datenaustausch ist dadurch möglich.

Mögliche Arten des Einsatzes von LANs in der öffentlichen Verwaltung sind:

- zentrale Druckerverwaltung (Printer Server),
- zentrale Dateiverwaltung (File-Server),
- verteilte Transaktionsverarbeitung (Client/Server-Konzept in Datenbankverwaltungssystemen),
- Fernstart von PCs ohne Festplatte und Diskettenlaufwerk,
- zentrale Stapelverarbeitung,
- zentrale Kommunikationsdienste (Gateways),
- verteilte Verarbeitung mittels Standardsoftware.

Auf eine differenzierte Darstellung konkreter Anwendungsfälle der bremischen öffentlichen Verwaltung (z. B. Senatskanzlei, Statistisches Landesamt, Hochbauamt, der Senator für Häfen, Schiffahrt und Verkehr und Standesamt) wird an dieser Stelle verzichtet. Für eine Bewertung nach datenschutzrechtlichen Gesichtspunkten werden grundsätzliche Aspekte von Netzen in den Vordergrund gestellt. Ausreichende Regelungen für den Datenschutz liegen noch nicht vor.

5.2.2 Datenschutzrechtliche Grundlagen

Wenn man den Datenaustausch über Netze beurteilen will, kann man zweckmäßigerweise vom datenschutzrechtlichen Verarbeitungsbegriff ausgehen.

Das BrDSG regelt insbesondere die Datenverarbeitung bremischer Behörden (§ 1 Abs. 2 BrDSG).

Behörden im Sinne dieses Gesetzes sind alle Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen. Die Abgrenzung einer Aufgabe, Aufgabenstellung oder Funktion ergibt sich aus einem Gesetz oder einer anderen Rechtsnorm. Insofern eine Behörde mehrere abgegrenzte, durch Rechtsnorm oder Gesetz zugewiesene Aufgaben erfüllt, besteht sie je Aufgabe aus einer datenverarbeitenden Stelle (vgl. AVV zu § 2 BrDSG und § 13 Abs. 5 BrDSG).

Dritte im Zusammenhang mit Datenkommunikation und im engeren Sinne des Gesetzes (§ 2 Abs. 3 Nr.3, § 13 Abs. 5 BrDSG) sind Personen oder Stellen außerhalb einer datenverarbeitenden Stelle. Eine Ausnahme bilden die Betroffenen und die Stellen, die im Auftrage Daten speichern. Sie zählen nicht zu den Dritten im Sinne diese Gesetzes.

Eine Übermittlung nach BrDSG liegt dann vor, wenn Daten durch eine datenverarbeitende Stelle an einen Dritten bekanntgegeben werden, d.h. Daten weitergegeben oder abgerufen werden. Dazu gehört auch die Datenkommunikation zwischen zwei Stellen mit unterschiedlichen Aufgaben innerhalb einer Behörde (z. B. Stadt- und Polizeiamt Bremen).

Aus informationstechnischer Sicht betrachtet gibt es Netze, die so aufgebaut sind, daß auf sie das Konzept des Referenzmonitors (z. B. das ISO/OSI-Referenzmodell) zutrifft. Beispiele für solche Netze sind lokale Netze, digitale Nebenstellenanlagen und private Fernmeldenetze. Diese Netze haben eine einzige Rechnerbasis (Server im LAN), die physisch und logisch zwischen den Komponenten des Netzes aufgeteilt ist, und ermöglichen so den Aufbau einheitlicher technisch/organisatorischer Schutzmaßnahmen. Sie können als ein einziges DV-System angesehen werden. Soweit sie nicht die Grenzen einer Aufgabenstellung einer Behörde überschreiten, können sie auch eindeutig einer datenverarbeitenden Stelle zugeordnet werden und unterliegen nicht den besonderen rechtlichen Bedingungen an eine Übermittlung.

Für Netze, die nicht auf diese Weise eingeordnet werden können, weil sie z. B. aus Komponenten oder Teilnetzen bestehen, die unabhängig voneinander aufgebaut, betrieben und verantwortet werden, die über keine einheitlichen technisch/organisatorischen Schutzmaßnahmen verfügen oder unterschiedlichen abgegrenzten Aufgabenstellungen innerhalb einer Behörde zuzuordnen sind, kann ein anderer Ansatz gewählt werden.

Solche Netze können als zusammengeschaltete DV-Systeme, d. h. DV-Systeme, die über eine Schnittstelle miteinander verbunden, jedoch einzeln für die Verarbeitung von schutzwürdigen Daten verantwortlich sind, aufgefaßt werden.

Während für DV-Systeme im obigem Sinne die Verarbeitung innerhalb der Systemgrenzen Gegenstand eines Datenschutzkonzeptes ist, erweitert sich dies bei zusammengeschalteten DV-Systemen auf die Übermittlung, wofür in den Datenschutzkonzepten der beteiligten DV-Systeme (auch beim Fernmeldetechnischen Amt, bei der Bundespost und beim Rechenzentrum der bremischen Verwaltung) besondere technisch/organisatorische Schutzmaßnahmen enthalten sein müssen.

Die Maßnahmen sind auf die einzelnen Zwecke und DV-Systeme insgesamt und deren Komponenten im einzelnen zu beziehen.

Zwei Sonderfälle bleiben noch zu regeln. Wenn innerhalb einer datenverarbeitenden Stelle zwei lokale Netze miteinander verbunden werden und technisch/organisatorische Maßnahmen nur netzbezogen zu realisieren sind, so sind auch hier spezielle Maßnahmen für den Schutz der Datenkommunikation vorzusehen. Obwohl rechtlich keine Übermittlung vorliegt, handelt es sich technisch um zwei Systeme, die nur zusammenschaltbar sind.

Der zweite Fall bezieht sich auf Stellen, die im Auftrag für datenverarbeitende Stellen die Verarbeitung von Daten durchführen (z. B. Diensteanbieter wie etwa die Bundespost, das Fernmeldetechnische Amt oder das Rechenzentrum der bremischen Verwaltung). Obwohl übergreifende technisch/organisatorische Maßnahmen realisierbar sind, handelt es sich hier nicht um ein einziges DV-System im obigen Sinne, da verschiedene datenverarbeitende Stellen Aufgaben wahrnehmen lassen, die rechtlich gegeneinander abgegrenzt sind. Dies bedarf besonderer Maßnahmen, die auch in die Architektur der Verarbeitung eingreifen müssen und im Datenschutzkonzept der datenverarbeitenden Stelle und der beauftragten Stelle zu berücksichtigen sind.

5.2.3 Technisch/organisatorische Schutzmaßnahmen in Netzen

Obwohl lokale Netze nach der rechtlichen Einordnung vergleichbar sind mit einem Arbeitsplatzcomputer, bestehen hinsichtlich Sicherheit und Datenschutz doch erhebliche zusätzliche Probleme. Bei der Festlegung technisch/organisatorischer Maßnahmen sind zusätzlich die Schwachstellen lokaler Netze zu berücksichtigen. Dies gilt im gleichen Maße auch für Nebenstellenanlagen, da sie sich funktional (ISO/OSI-Referenzmodell) ähnlich verhalten wie lokale Netze.

Die zusätzlichen Komponenten eines vernetzten PCs sind

— die Netzwerkkarte (LAN-Controller), über die auf

— das Übertragungsmedium (Datenkabel) und

— die daran angeschlossenen PCs zugegriffen werden kann.

Geht man davon aus, daß für alle PCs die gleichen Sicherungs- und Schutzmaßnahmen realisiert sind, so entstehen beim Zugriff über die Tastatur keine zusätzlichen Gefahren.

Bei Datenkabeln besteht die Gefahr, daß entweder über eine vorhandene oder eine während des Betriebs problemlos anschließbare Daten-Steckdose ein zusätzlicher PC unbemerkt angeschlossen werden kann. Lichtwellenleiter bieten einen gewissen Schutz, da die Daten-Steckdosen sehr komplex sind und das unbemerkte Anzapfen während des Betriebs noch größeren technischen Aufwand erfordert.

Je nach Netzwerktechnik wird ein netzfremder PC überhaupt nicht oder nur, wenn er sich aktiv in das Netz einschaltet, erkannt. Das passive Mithören ist nur mit großem zusätzlichem technischen Aufwand, wie z. B. bei der Einpeilung von „Schwarz"-Hörern, zu erkennen. Da in einem LAN, ähnlich wie auf einem Funkkanal, alle Daten die gesendet werden, auch von allen empfangen werden, kann der gesamte Datenverkehr eines Netzes über einen Anschluß mitgehört werden.

Die zweite zusätzliche Komponente ist die Schnittstelle oder Verbindung zwischen PC und Datenkabel, die Netzwerkkarte. Auf ihr wird bei der Installation eine eindeutige Netz-Adresse eingetragen. Erst wenn diese Netz-Adressen gegenseitig bekannt und die betreffenden PCs in Betrieb sind, können zwischen ihnen Daten über das Netz ausgetauscht werden.

Prinzipiell sind Netz-Adressen frei einstellbar, so daß ein PC durch Änderung der eigenen Adresse die Daten für einen anderen PC mitempfangen kann. Bei einigen Netzwerkkarten muß nicht einmal die eigene Empfangsadresse geändert werden. In einem speziellen Verfahren kann der Netzwerkkarte eine ganze Liste von Netz-Adressen übergeben werden.

Die quasi unvermeidbare Gefahr des Abhörens mit Hilfe von manipulierten oder zusätzlich angeschlossenen PCs birgt weiterreichende Gefahren in sich.

Neben dem Informationsgehalt der Daten allgemein können speziell Passwörter, Netzadressen und Schlüssel erkannt und für die Aneignung der Verarbeitungsrechte eines legalen Netzbenutzers genutzt werden. Auch wenn diese Zugriffsinformationen verschlüsselt werden, besteht die Gefahr, daß sie abgehört, gespeichert und zum Zwecke der Aneignung von Verarbeitungsrechten wieder ausgesandt werden.

Um dieses Gefährdungsrisiko zu verringern, ist es notwendig, nicht nur die Identität, sondern auch die Authentizität von Empfängern und Absendern in Netzen zu prüfen. Die Forderung nach Authenzität bedeutet, daß Nachrichten nachweisbar authentisch sind, d.h. daß ein Absender gegenüber Dritten beweisen kann, daß ein von ihm adressierter Empfänger gegenüber Dritten beweisen kann, daß er Nachrichten eines behaupteten Inhalts von einem behaupteten Sender erhalten hat. Authentizität bedeutet weiterhin den Schutz von Nachrichten und Kontrollnachrichten gegen Verfälschung (sowohl durch unbefugte Dritte als auch durch Sender oder Empfänger) sowie eine sichere und nachvollziehbare Verknüpfung zwischen Nachrichten und ihren Urhebern. Weitere Sicherheitsforderungen sind die nach Schutz gegen Nachrichtenwiederholungen und Einhaltung von Nachrichtenreihenfolgen. Möglich ist dies mit Hilfe kryptographischer Verfahren durch Schlüsselmanagementprotokolle und Handshakeprotokolle mit zusätzlichen Zeitstempeln, Zufallszahlen, o. ä., um sich auch vor den Folgen von Wiedereinspielungen alter abgehörter Authentizitätsprüfvorgänge schützen zu können. In größeren Netzen wird hierfür ein PC als Authentifikations-Server eingesetzt, der die Netz-Teilnehmer auf Anfrage mit den nötigen, authentischen Informationen versorgt, mit Hilfe derer ein Netz-Teilnehmer die Authentizität eines anderen Teilnehmers überprüfen kann. Sie sind eine zwingende Voraussetzung für sichere Kommunikationssysteme auf der Grundlage sicherer Authentikationspfade.

Eine zusätzlich mögliche Maßnahme ist der Nachweis von Kommunikationsbeziehungen. Mittels eines sogenannten Notariats-Servers können Kommuniaktionsabläufe technisch beglaubigt, d. h. auf einem nicht-löschbaren Speicher, z. B. einer nur einmal beschreibbaren optischen Platte, aufgezeichnet und somit nachgewiesen werden.

Unter der Voraussetzung, daß die Beteiligten dieses Verfahren anerkennen, können so auch rechtskräftige Vereinbarungen über lokale Netze abgewickelt werden.

Will man auch den Boykott des Kommunikationssystems, z. B. durch Blockieren von Teilnehmern mittels permanentem Verbindungsaufbauversuch oder durch Blockieren des Netzes insgesamt mittels Blindverkehr mit nutzlosen Massendaten, verhindern, so erfordert dies ein umfangreiches Sicherheits- und Netzwerkmanagement. Mit Hilfe spezieller Leitungsmonitore und LAN-Analysegeräte sind permanente Kontrolldatenerfassungen durchzuführen, Verkehrsstatistiken zu erstellen und auszuwerten um ggf. sofort Gegenmaßnahmen von zentraler Stelle ergreifen zu können. Die hierfür notwendigen Daten sind natürlich nicht nur personenbezogen, sondern auch besonders schutzwürdig, da sie sehr differenziert die Leistung und das Verhalten von einzelnen Mitarbeitern/innen dokumentieren.

Zusammenfassend kann man feststellen, daß eine Vernetzung, d. h. der Einsatz von zwei zusätzlichen Komponenten an einem PC-Arbeitsplatz mit erheblichen zusätzlichen Gefahren verbunden ist. Um diesen Gefahren überhaupt angemessen begegnen zu können, ist es notwendig, alle Komponenten im einzelnen im gesamten Wirkzusammenhang innerhalb eines DV-Systems einer datenverarbeitenden Stelle und im Wirkzusammenhang der Übermittlung von einem DV-System zu einem anderen zu analysieren, die Risiken zu bewerten, Maßnahmen abzuleiten und diese Ergebnisse übersichtlich, z. B. programmunterstützt, zu dokumentieren.

Die Rechte für die Verarbeitung sind enger zu fassen als bei unvernetzten PCs, da nicht nur die legalen, sondern auch illegalen Verarbeitungsmöglichkeiten und damit auch die Mißbrauchsmöglichkeiten gerade durch berechtigte Benutzer größer sind. Viele praktische Fälle von Vernetzung in der öffentlichen Verwaltung können von der Aufgabenstellung genauso wie ein DV-System, quasi wie ein PC mit vielen Komponenten, bewertet werden und implizieren die Beherrschbarkeit der Gefährdung von Bürgerrechten. Es handelt sich hier jedoch um eine neue Qualität, der Potenzierung von Gefahren, die vom Einsatz von PCs für die Verarbeitung von Bürgerdaten ausgehen.

Aufgrund der Tatsache, daß die Maßnahmen gegen die Gefahren des unvernetzten PC-Einsatzes in der öffentlichen Verwaltung noch nicht greifen, teilweise noch nicht einmal umgesetzt werden können, da die notwendigen Richtlinien und Handlungsanweisungen immer noch fehlen, obwohl

- die für solche Maßnahmen vorgesehene Datenschutz- und Datensicherungssoftware (z. Z. Safeguard) vorhanden und vielerorts beschafft ist,
- die für die Realisierung von Maßnahmen mittels Datenschutz- und Datensicherungssoftware notwendige Definition und Dokumentation in Datenschutz- und Datensicherungskonzepten, Dateianmeldungen und Geräteverzeichnissen erst in Arbeit sind und
- daher der Schutz von Bürgerrechten bei der Datenverarbeitung noch nicht einmal beim Einsatz von unvernetzten Arbeitsplatz-PCs in der Praxis erprobt ist,

sehe ich die Gefahr, daß aufgrund einer zu frühen, ungeplanten, unabgestimmten Vernetzung der Datenschutz im Lande Bremen nicht mehr zu gewährleisten ist.

5.3 Datenschutz im ADV-Entwicklungsprozeß

Das Bundesverfassungsgericht hat in seinem grundlegenden Urteil zum Volkszählungsgesetz sich nicht auf das Recht auf informationelle Selbstbestimmung begrenzt.

Daher beschränkt sich das Datenschutzrecht nicht allein darauf, den einzelnen vor dem Mißbrauch seiner Daten zu schützen. Es hat vielmehr die Erhebung, Speicherung, Verwendung, Weitergabe und sonstige Nutzung personenbezogener Daten ohne Rücksicht darauf zu regeln, ob ein Mißbrauch zu befürchten ist. Gegenstand des Datenschutzes ist auch nach der Rechtsprechung des Bundesverfassungsgerichts **der rechtmäßige Umgang mit personenbezogenen Daten** und nicht nur die Verhinderung vorwerfbaren Fehlverhaltens.

Die Aufgabe ist damit definiert, was fehlt, ist der Weg für die wirkungsvolle Umstellung.

Die Planung von Datenschutz unterliegt dem grundsätzlichen Dilemma, eingebunden in einen Prozeß zu gestalten, der nicht determiniert abläuft. Entwicklung verläuft selten nach Plan. Nicht allein Pläne bestimmen Entwicklungen, sondern Datenschutz ist auch dem freien Spiel der Kräfte ausgesetzt.

Die Planung von Datenschutz erfolgt meist für Anwendungen, die noch unbekannt sind. Systeme werden quasi von unten nach oben, z. B. im Bereich der Telekommunikation von den ISO/OSI-Schichten über die Dienste (ISDN, VANS, BTX, Mailbox, EDI, etc.) zu den Anwendungsmöglichkeiten im Rahmen neuer Organisationskonzepte, einzuschätzen versucht.

Die Ziele von Datenschutz stehen im Spannungsfeld mit verschiedenen Interessen. Zum Beispiel:

- Die Protokollierung von Verarbeitung als Grundlage für Wiederanlaufverfahren, für Revisionszwecke und als Maßnahme zur Ausfüllung von Bereichen des § 6 BrDSG steht im Konflikt zum Datenschutz von Arbeitnehmern vor Leistungs- und Verhaltenskontrollen durch Technik, d. h. zum Arbeitnehmerdatenschutz.
- Das Gebot zur Durchführung von Maßnahmen zum Datenschutz steht im vermeintlichen Konflikt zum Gebot der Wirtschaftlichkeit von Verwaltungshandeln. Viele Risiken der automatisierten Datenverarbeitung sind auch wirtschaftliche Risiken. Die Wirtschaftlichkeit von Maßnahmen kann erst in diesem erweiterten Kontext angemessen beurteilt werden. Datenschutz, der zu umfangreiche Datenbestände reduziert, erhöht die Effizienz und verbessert damit deutlich die Wirtschaftlichkeit des Verwaltungshandelns.

Eine pragmatische Lösung des Planungsdilemmas ist die Schaffung von Instrumentarien zur Lenkung von Datenschutz, z. B.

- durch die Berücksichtigung des Datenschutzes schon bei der Analyse von Arbeitsabläufen im Vorfeld der Automatisierung oder Umorganisation,
- durch die Beteiligung an der Planung von technisch/organisatorischen Rahmenentscheidungen mit dem Ziel, Gefahren vorbeugen zu können,
- durch die Einflußnahme auf die Anforderungen an den Inhalt und die Informationsdarstellung in Analyseergebnissen, Problemdarstellungen, Verfahrensdokumentationen etc., um überhaupt dafür Sorge tragen zu können, daß Gefahren erkannt und Maßnahmen definiert werden.

Der rechtmäßige Umgang mit personenebezogenen Daten muß ein zentrales Ziel jeder ADV-Entwicklung sein. Die Entwicklungsdokumentation muß daher mindestens auch die Anforderungen an ein Datenschutz- und Datensicherungskonzept befriedigen (vgl. Beschluß AADV, TOP 12, 27. September 1989).

Vorraussetzungen eines so ausgestalteten Datenschutz-/Datensicherungs-Konzeptes sind eine differenzierte Analyse und ein vollständiger, konsistenter Entwurf im Vorfeld eines jeden AADV-Antrags. Angesprochen sind hier keine Programmablaufpläne, sonder eher das „WAS" von Datenverarbeitung, das organisatorische Umfeld, die Aufgabenstellung und die geplanten DV-Komponenten zur Unterstützung einer Aufgabe im Kontext ihrer Wirkzusammenhänge.

Insbesondere sollten folgende Informationen erarbeitet werden:

- Gesetzlicher Auftrag der Verwaltungseinheit,
- Aufgaben nach Geschäftsverteilung,
- Umfang der dafür notwendigen Daten und Kreis der Betroffenen,
- Zwecke und Rechtsgrundlagen der Verarbeitung von der Erhebung bis zur Löschung oder der sonstigen Nutzung,
- an der Verarbeitung beteiligte Mitarbeiter/innen und andere datenverarbeitende Stellen,
- Komponenten der automatisierten Verarbeitung (Hardware, systemnahe Software, Standard-Software, eigenentwickelte Software, etc.),
- Folgen von Datenverlusten und Systemausfällen,
- Maßnahmen zur Verringerung der Risiken von automatisierter Datenverarbeitung,

- Möglichkeiten von Informationsmißbrauch für die Persönlichkeitsrechte des Bürgers,
- Maßnahmen zur Gewährleistung der Datenschutzrechte des Bürgers, der Ordnungsmäßigkeit und der Rechtmäßigkeit allgemein bei der Informationsverarbeitung.

Ein so ausgestalteter AADV-Antrag ist dann eine brauchbare Grundlage für alle weiteren Dokumentationen des Systems im Kontext von Rechtsnormen und Organisationsstrukturen. Er enthält dann wesentliche Informationen

- für das **Verzeichnis der automatischen DV-Anlagen und Bildschirmgeräte** (§ 17 Dienstvereinbarung über den Einsatz von DV-Anlagen),
- für das **Geräteverzeichnis** und die **Dateibeschreibung** hier speziell die technisch/organisatorische Maßnahmen, insbesondere die Gestaltung der Organisation, d. h. auch Dienstanweisungen (§§ 6, 7 BrDSG).

6. Deutsch-Deutsche Entwicklung und Datenschutz

Die politische Entwicklung vom Deutsch-Deutschen Verhältnis und der zunehmend und begleitend hierzu stattfindende Datentransfer hat erhebliche Auswirkungen auf den Datenschutz. Unabhängig davon, wie dieses Verhältnis künftig konkret ausgestaltet sein wird, kann bereits heute festgestellt werden, daß mehr personenbezogene Daten als früher ausgetauscht werden. Dieser Datentransfer wird noch zunehmen. Aktuelle Anlässe, wie der Austausch von Daten bei Verkehrsunfällen sowie im Rahmen der polizeilichen Gefahrenabwehr und der Strafverfolgung haben in der Öffentlichkeit besondere Aufmerksamkeit gefunden.

Der Prozeß der sozialen, wirtschaftlichen und politischen Einigung führt zu verstärktem grenzüberschreitenden Datenverkehr, z. B. im Sozialrecht, im Melderecht, im Versicherungs- und Kreditrecht. Dies wirft Fragen des Datenschutzes auf. Für die Bundesrepublik gelten das allgemeine Datenschutzrecht und besondere Vereinbarungen und Gesetze, wie z. B. das Gesetz über die innerdeutsche Rechts- und Amtshilfe in Strafsachen vom 2. Mai 1953. Für das Land Bremen regelt § 18 des Bremischen Datenschutzgesetzes (BrDSG) die Datenübermittlung an Stellen der Deutschen Demokratischen Republik. Hiernach ist eine Übermittlung personenbezogener Daten zulässig, soweit die Übermittlungen einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaft oder einer zwischenstaatlichen Vereinbarung ausdrücklich geregelt ist. Unter diesen Voraussetzungen kann eine Datenübermittlung auch erfolgen, wenn für den Empfänger gleichwertige Datenschutzregelungen gelten. Dies trifft für die DDR gegenwärtig nicht zu. Eine Übermittlung hat zu unterbleiben, wenn sie gegen das Bremischen Datenschutzgesetz oder eine andere Rechtsvorschrift verstossen würde oder, soweit Grund zu der Annahme besteht, daß sie schutzwürdige Belange des Betroffenen verletzt. Schließlich ist der Empfänger durch die übermittelnde Stelle darauf hinzuweisen, daß die Daten einer strikten Zweckbindung unterliegen.

Bevor also bundesdeutsche Stellen personenbezogene Daten in die DDR übermitteln, muß sichergestellt sein, daß wichtige Datenschutzprinzipien, wie

- Erforderlichkeit
- Zweckbindung
- Wahrung der Auskunftsrechte der Betroffenen
- Einhaltung der Datensicherung
- Gewährleistung des Löschungsanspruches

beachtet werden. Die Einhaltung dieser datenschutzrechtlichen Mindeststandards muß auch kontrollierbar sein.

Bei den vielfältigen deutsch-deutschen Gesprächen, den städtepartnerschaftlichen Beziehungen, den Facherörterungen ist deshalb auf allen Ebenen der Schutz personenbezogener Daten zu berücksichtigen. Der Ausbau der Telekommunikationsdienste und die Verbreitung der automatisierten Datenverarbeitung müssen datenschutzgerecht erfolgen.

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

Die politischen Veränderungen in der DDR und im übrigen Mittel- und Osteuropa müssen aber zwangsläufig auch Konsequenzen bei der personenbezogenen Datenverarbeitung der verschiedenen Sicherheitsbehörden in der Bundesrepublik Deutschland und in Bremen zur Folge haben. Instrumente, die im Zeichen der Ost-West-Konfrontation geschaffen worden sind, müssen kritisch überprüft und ggf. beseitigt werden. Die Notwendigkeit zu einer solchen Einschränkung der Datenverarbeitung sehe ich z. B. auf folgenden Gebieten:

- Bei der Überprüfung von Mitarbeitern im öffentlichen Dienst und in der privaten Wirtschaft.

- Die Datenerhebung und die Datenübermittlung des Bundesgrenzschutzes (im Land Bremen die Wasserschutzpolizei, die Aufgaben des Bundesgrenzschutzes wahrnimmt) anläßlich von Grenzkontrollen an die Geheimdienste muß gesetzlich geregelt und auf die Bereiche Terrorismus und Spionageabwehr begrenzt werden. Die Beobachtung von Reisen extremismusverdächtiger Personen ist einzustellen.

- Die Beobachtung von DDR-beeinflußten extremistischen Organisationen in der Bundesrepublik Deutschland ist einzuschränken im Verlaufe der Entwicklung später einzustellen.

Die Forderung der Datenschutzbeauftragten, die Sammlung personenbezogener Daten über Aus- und Übersiedler in der Datei ADOS einzustellen und die Datenbestände zu vernichten, ist inzwischen aufgegriffen worden. Der Arbeitskreis IV der Innenministerkonferenz hat am 5. März 1990 folgenden Beschluß gefaßt:

„Der Arbeitskreis IV stellt fest, daß angesichts der politischen Entwicklung in der DDR und in Ost-Europa die Notwendigkeit der Datei ADOS jetzt nicht mehr gegeben ist. Er beschließt, die gespeicherten Daten zu löschen und die dazu noch vorhandenen Unterlagen zu vernichten."

Dr. Alfred Büllesbach
Landesbeauftragter für den Datenschutz

Bremerhaven, 29. März 1990

Anlage 1

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 Entschließung gefaßt:

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

Anlage 2

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 Löschungsfristen 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 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (Strafverfahrensänderungsgesetz vom 3. November 1988)

Die Konferenz begrüßt, daß ein Entwurf zur Regelung des Datenschutzes im Strafverfahrensgesetz vorgelegt worden ist und daß darin für die besonderen Ermittlungs- und Fahndungsmethoden eigenständige Befugnisnormen vorgesehen sind sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht in die Strafprozeßordnung aufgenommen werden sollen.

Die im Entwurf vorgesehenen Datenschutzregelungen sind an den verfassungsrechtlichen Grundsätzen der Verhältnismäßigkeit und Normenklarheit zu messen. Weil im Bereich der Grundrechtsausübung nach der Rechtsprechung des Bundesverfassungsgerichts alle wesentlichen Entscheidungen vom Gesetzgeber selbst zu treffen sind, ist die gesamte Informationsverarbeitung wegen ihres Eingriffscharakters in der Strafprozeßordnung präzise und umfassend gesetzlich zu regeln.

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

1. Zu den Regelungen über die Ermittlungs- und Fahndungsmethoden

   — Die Erhebung und Weiterverarbeitung personenbezogener Daten durch Strafvollzugsorgane 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 erheblicher 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 Entschädigungen 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.

Anlage 4

Entschließung 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 Strafprozeßordnung im Rahmen der Poststrukturreform

Der im Rahmen der Ausschußberatungen zur Poststrukturreform aus den Reihen des Bundestages eingebrachte Entwurf zur Änderung des Gesetzes zu Art. 10 GG (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) soll die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst u. a. dazu ermächtigen, den Fernmeldeverkehr zu überwachen und aufzuzeichnen. Bisher war den Diensten nach dem Gesetz zu Art. 10 GG nur gestattet, „den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf Tonträger aufzunehmen". Auch die Überwachungsvorschriften der Strafprozeßordnung (§§ 100a, 100b) sollen entsprechend verändert werden.

Während in der Vergangenheit neben dem Briefverkehr nur Telefongespräche und Fernschreiben kontrolliert und ausgewertet werden durften, soll dies nach dem Entwurf in Zukunft für den gesamten Fernmeldeverkehr (z. B. Btx, Temex, Telefax, Datel-Dienste, ISDN) zulässig sein. Daraus ließe sich ableiten, daß auch Abrechnungs-, Verbindungs- und Nutzungsdaten sowie im Rahmen elektronischer Dienste gespeicherte Inhaltsdaten (z. B. bei Mailboxen, Btx usw.) kontrolliert werden dürfen. Damit würde jedenfalls für den Bereich der Strafprozeßordnung auch eine rückwirkende Kontrolle legalisiert. Nicht auszuschließen ist außerdem, daß Dienstbetreiber dazu verpflichtet werden, für Überwachungszwecke in größerem Umfang Daten zu speichern, als für 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 Telekommunikationdienste in die Regelungen, die bislang nur für die Post gelten.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zu den Entwürfen eines Bundesverfassungsschutzgesetzes (BVerfSchG), eines MAD-Gesetzes (MADG) und eines BND-Gesetzes (BNDG) vom 30. Mai 1989

I.

Mit den von der Bundesregierung vorgelegten Entwürfen sollen die nach der Rechtsprechung des Bundesverfassungsgerichts erforderlichen bereichspezifischen Rechtsgrundlagen für die Informationsverarbeitung der Verfassungsschutzbehörden und Nachrichtendienste geschaffen werden. So dringend die Beseitigung der bestehenden Regelungsdefizite auch ist, müssen sich neue Gesetze gerade in diesem Bereich in besonderem Maße daran messen lassen, daß in die Freiheitsrechte der Bürger nicht unverhältnismäßig eingegriffen wird. Dieser Vorgabe werden auch die nunmehr vorgelegten Entwürfe in vielerlei Hinsicht nicht gerecht.

II.

1. Da sich der zulässige Umfang der Informationsverarbeitung nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Für den Einzelnen muß erkennbar sein, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Die in § 3 Abs. 1 verwendeten Begriffe, wie etwa „Bestrebungen gegen die freiheitliche demokratische Grundordnung" oder „Gefährdung auswärtiger 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 die Grundordnung gerichteten Bestrebungen mitwirken;

   - ob und ggf. in welchem Umfang Informationen über nicht extremistische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung (-sversuche) 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 unverdächtige 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 Löschungsregelungen. 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 Aufgabenbereichen 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.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 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 Datenschutzinstanz 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 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 1989 zum Entwurf einer EG-Statistikverordnung

Die Kommission der Europäischen Gemeinschaft 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 vorgehaltene 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 Gemeinschaftebene 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 8

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 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 intensivierte 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. März 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 schwerwiegenden 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.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 1989 über Genomanalyse und informationelle Selbstbestimmung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat den Abschlußbericht der Enquête-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" (Drucksache 10/6775) zum Anlaß genommen, die Risiken für die informationelle Selbstbestimmung jedes Betroffenen abzuwägen gegenüber den Chancen, die die Genomanalyse bringt. Durch die Offenlegung genetischer Daten eines Menschen kann dieser in seinem Persönlichkeitsrecht und sonstigen schutzwürdigen Belangen nachhaltig beeinträchtigt werden. Informationen aus dem Kernbereich der Privatsphäre, die dem Betroffenen selbst bisher unbekannt waren, können ihn zu einem an sich ungewollten Verhalten in seiner Lebens- oder Berufsgestaltung veranlassen; ihre Kenntnis kann zu einer psychischen und sozialen Zwangslage für den Betroffenen führen. Wegen der genetischen Bedingtheit solcher Informationen können 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 möglichen Folge gesellschaftlicher Ausgrenzung.

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

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 Erbanlangen 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.

Anlage 10

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 Nr. 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. Datenübermittlung 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, damit die Beachtung der Rechte der Betroffenen tatsächlich sichergestellt wird.

Das Ziel dieser Maßnahmen 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 seiner Daten zu bestimmen, müssen durch internationale Zusammenarbeit der Datenschutzbeauftragten ausgeglichen werden.

Beschluß der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 zu ISDN 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 Dienstanbieter 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 vielmehr 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 Vereinfachung 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 kommerzieler 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 Telekommunikationsgeräten 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.

Zusatzerklärung 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 Datenschutzes 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.

Druck: Anker-Druck Bremen