Staats- und Universitätsbibliothek Bremen
Staats-archiv Bremen
BREMISCHE BÜRGERSCHAFT

Kooperationsprojekt - Digitalisierung Drucksachen der Bremischen Bürgerschaft

Drucksache / Bremische Bürgerschaft, Landtag 11. Wahlperiode, 1983-84

27.03.1987 - Drucksache 11/915

Staats-und Universitätsbibliothek Bremen - Digitale Sammlungen

Visual Library

BREMISCHE BÜRGERSCHAFT
Landtag
11. Wahlperiode

Drucksache 11/915
27. 03. 87

Neunter Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag), dem Präsidenten des Senats den Neunten Bericht über das Ergebnis meiner Tätigkeit im Jahre 1986 zum 31. März 1987 (§ 26 Abs. 1 Bremisches Datenschutzgesetz).

Dr. Alfred Büllesbach, Landesbeauftragter für den Datenschutz

Inhaltsübersicht

1. Vorbemerkungen

1.1 Politischer Stellenwert des Datenschutzes

1.2 Zur Personalsituation

2. Rechts- und Informationstechnologie-Entwicklung

2.1 Rechtsentwicklung

2.1.1 Ubergangsbonus

2.1.2 Entwicklung der Gesetzgebung im Bund

2.1.2.1 Erlaß des Baugesetzbuches

2.1.2.2 Telekommunikationsordnung (TKO)

2.1.2.3 Bundesstatistikgesetz

2.2 Technologieentwicklung

2.2.1 Einsatz von Arbeitsplatzrechnern

2.2.2 Datensicherheit durch Chip-Karten

2.2.3 Uberregionale Informationsdatenbanken

3. Kooperationen

3.1 Kooperation mit dem Datenschutzausschuß der Bremischen Bürgerschaft (Landtag)

3.2 Mitarbeit im ADV-Ausschuß (AADV) Bremen

3.3 Kooperationen mit den Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz

3.4 Kooperation mit den Obersten Aufsichtsbehörden für den Datenschutz

3.5 Kooperation mit Kammern, Verbänden, sonstigen Institutionen

4. Eingaben und Beschwerden, Registerführung

4.1 Eingaben und Beschwerden

4.2 Register der meldepflichtigen Stellen

4.3 Dateienregister

5. Öffentlicher Bereich

5.0 Datenschutz beim Einsatz von Arbeitsplatzrechnern

5.1 Personalwesen

5.1.1 Schwerpunkte, Handlungsbedarfsfälle

5.1.1.1 PAADIS

5.2 Inneres

5.2.1 Innere Sicherheit

5.2.1.1 Schwerpunkte, Handlungsbedarfsfälle

— Anhörung des Innenausschusses zur Änderung des Bundesverfassungsschutzgesetzes und zum Entwurf eines Gesetzes über den Militärischen Abschirmdienst

— ISA-BK

— Speicherung eines Merkmals mit dem Hinweis auf AIDS-Ansteckungsgefahr in polizeilichen Auskunftssystemen

5.2.1.2 Kurze Darstellung von Problemen und Beschwerden

5.2.2 Meldewesen, Paß- und Ausweiswesen

5.2.2.1 Meldedatenübermittlungsverordnung des Landes

5.2.2.2 Paß- und Ausweisgesetz des Bundes, Landespersonalausweisgesetz

5.2.3 Kfz.-Zulassung/Führerschein

5.2.3.1 Führerschein auf Probe

5.2.3.2 Änderung des Straßenverkehrsgesetzes (Fahrzeugregister — ZEVIS)

5.2.3.3 Automatisierung der Kfz.-Zulassung in Bremen und Bremerhaven

5.2.4 Amtliche Statistik

5.2.4.1 Volkszählung 1987

5.2.4.2 Mikrozensus 1986

5.2.5 Ordnungswesen

5.2.5.1 Schwerpunkte, Handlungsbedarfsfälle

— Erlaß eines Gesetzes über die Ausstellung von Vertretungsbescheinigungen

— Erlaß von Wahlordnungen für die Bremischen Deichverbände

5.2.6 Ausländerangelegenheiten

5.2.6.1 Schwerpunkte, Handlungsbedarfsfälle

— Datenverarbeitung bei Ausländerbehörden und beim Ausländerzentralregister

5.3 Rechtspflege und Strafvollzug

5.3.1 Schwerpunkte, Handlungsbedarfsfälle

5.3.1.1 Fassung der Vordrucke für Zeugenladungen in Strafsachen

5.3.1.2 Einführung der elektronischen Datenverarbeitung in der Bremer Justiz

5.3.1.3 Akteneinsicht in Gerichtsakten zu Forschungszwecken

5.3.1.4 Justizmitteilungsgesetz (MiZi, MiStra)

5.3.1.5 Schuldnerverzeichnis nach § 915 ZPO

5.3.1.6 Informationsverarbeitungsregelungen im Strafverfahren

5.3.1.7 Staatsanwaltschaftliches Informationssystem (SISY)

5.3.1.8 Öffentliche Bekanntmachung der Entmündigung gem. § 687 ZPO

5.3.2 Kurze Darstellung von Problemen und Beschwerden

5.4 Bildung, Wissenschaft und Kunst

5.4.1 Änderung des Bremischen Schulverwaltungsgesetzes

5.4.2 Bremisches Weiterbildungsgesetz — Datenschutzbestimmungen

5.5 Jugend und Soziales

5.5.1 Schwerpunkte, Handlungsbedarfsfälle

5.5.1.1 Fragebogen für Pflegekindbewerber

5.5.1.2 Programmierte Sozialhilfe (PROSOZ)

5.5.2 Kurze Darstellung von Problemen und Beschwerden

5.6 Gesundheitswesen

5.6.1 Schwerpunkte, Handlungsbedarfsfälle

5.6.1.1 Datenschutz in den Krankenanstalten

5.6.1.2 Medizinische Dokumentation und statistische Auswertung (MEDUSA-K)

5.6.1.3 Teilprüfung des Zentralkrankenhauses Reinkenheide — ZKHR —

5.6.1.4 Befunddokumentation und Arztbriefschreibung im Krankenhaus (BAIK)

5.6.1.5 Übermittlung von Dialyse-Patientendaten

5.6.1.6 Fernsehgeräte-Verleih in den Krankenanstalten

5.6.2 Kurze Darstellung von Problemen und Beschwerden

5.7 Bauwesen

5.7.1 Schwerpunkte, Handlungsbedarfsfälle

5.7.1.1 Erlaß eines Entwässerungsortsgesetzes

5.7.1.2 Akteneinsicht durch die Kriminalpolizei beim Bauordnungsamt

5.7.2 Kurze Darstellung von Problemen und Beschwerden

5.8 Wirtschaft und Außenhandel

5.8.1 Schwerpunkte, Handlungsbedarfsfälle

5.8.1.1 Neufassung der Wahlordnung für die Wahlen zu den Arbeitnehmerkammern

5.8.1.2 Datenübermittlung durch Gewerbebehörden an Dritte

5.9 Finanzwesen

5.9.1 Steuern

5.9.1.1 Schwerpunkte, Handlungsbedarfsfälle

— Entwurf einer Kontrollmitteilungsverordnung nach § 93a der Abgabenordnung

— Erlaß einer Steuerdatenabrufverordnung nach § 30 Abs. 6 Satz 2 der Abgabenordnung

— Übermittlung von Besteuerungsgrundlagen durch die Finanzämter an die Stadtgemeinden

— Kontrollmitteilungen bei der Besteuerung von Hunden

5.10 Sonstige öffentliche Stellen, Körperschaften, Kammern u. a.

5.10.1 Datenerhebung durch die Steuerberaterkammer bei der Zulassung zur Abschlußprüfung nach dem Berufsbildungsgesetz

5.10.2 Apothekerkammer

6. Nicht-öffentlicher Bereich

6.1 Vorbemerkungen

6.2 Kreditinformationssystem der SCHUFA

6.2.1 Verfahren vor dem Bundeskartellamt

6.2.2 Widerspruch gegen die SCHUFA-Klausel

6.2.3 Verfahren vor dem Bundesverfassungsgericht

6.3 Datenschutz im Versand- und Einzelhandel

6.3.1 Kein Datenschutzgespräch mit dem Versandhandel

6.3.2 Anzeige der Bankleitzahl und Kontonummer an der Kasse bei Zahlung mit Scheck

6.4 Prüfung einer großen Handelsauskunftei

6.5 Versicherungswirtschaft

6.5.1 Schweigepflichtentbindungsklausel

6.5.2 Datenverarbeitungs-Ermächtigungsklausel

6.5.3 Verwendung von Match-Codes in der Rechtsschutzversicherung

6.6 Mieterdatenschutz

6.6.1 Datenübermittlung durch Wohnungsvermittler

6.6.2 Bekanntgabe von Wasserverbrauchsdaten bei Wohnungseigentum

6.6.3 Datenübermittlung an Kleingärtnervereine

6.7 Arbeitnehmerdatenschutz

6.7.1 Bekanntgabe von Abmahnungen einzelner Arbeitnehmer durch den Arbeitgeber gegenüber dem Betriebsrat

6.7.2 Datenübermittlung zwischen zwei Arbeitgebern

6.7.3 Datensammlung durch Betriebsräte

6.7.4 Tonbandaufzeichnungen von Telefondaten

6.7.5 Weitergabe von Privatanschriften der Beschäftigten an einen Verlag

6.8 Gesundheitsbereich

6.8.1 Diavortrag über extrakorporale Befruchtung

6.8.2 Langzeitstudie eines Arzneimittelherstellers

6.8.3 Geltung der ärztlichen Schweigepflicht bei privatärztlichen Verrechnungsstellen sowie freien Rechenzentren

6.9 Bildschirmtext

6.10 Sonstige Fälle aus dem nicht-öffentlichen Bereich

6.10.1 Austausch von personenbezogenen Daten unter weiterbildenden Instituten

6.10.2 Tonbandaufzeichnungen von Telefondaten

6.10.3 Video-Aufzeichnungen im Sex-shop

6.10.4 Datenübermittlung eines Auktionshauses

6.11 Ordnungswidrigkeiten

7. Verwaltungsautomation ist Gestaltungsaufgabe

8. Anlagen

1. Datenschutz im Krankenhaus
(Konferenzbeschluß vom 14. März 1986)
2. Telekommunikationsordnung
(Konferenzbeschluß vom 18. April 1986)
3. Bundesverfassungsschutzgesetz und Entwurf MAD-Gesetz
(Stellungnahme des Landesbeauftragten für den Datenschutz für die öffentliche Anhörung am 28. April 1986)

4. Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren
(Stellungnahme vom 24./25. November 1986)

5. Neue SCHUFA-Klauseln

1. Vorbemerkungen

1.1 Politischer Stellenwert des Datenschutzes

In meinem letzten Jahresbericht verwies ich darauf, daß Datenschutz permanent um Ausgleich verschiedener Interessen bemüht ist. Doch ist Datenschutz keineswegs nur Interessenausgleich, sondern verfassungsrechtlich garantiertes informationelles Selbstbestimmungsrecht. Welchen Stellenwert Datenschutz für die Bevölkerung inzwischen eingenommen hat, zeigt die Diskussion um die Meldepflicht bei AIDS-Erkrankungen ebenso wie die Diskussion zur Volkszählung. Zentraler Aspekt ist die Frage der Glaubwürdigkeit staatlichen Handelns. Worauf es ankommt ist, daß der Bürger sich darauf verlassen kann, daß öffentliche Organe sich auch so verhalten wie sie es zusichern, und daß sie nicht durch verschleppte oder Persönlichkeitsrechte abbauende Datenschutzregelungen den errungenen Datenschutz wieder aufweichen (vgl. die Diskussion zu den sogenannten Sicherheitsgesetzen). So schreibt Theo Sommer im Leitartikel in „Die Zeit" vom 27. Februar 1987: „Ohne eine glaubwürdige Datenschutzpolitik kann es eine wirksame Seuchenpolitik nicht geben." Die Erwartungen an den Datenschutz sind in der Bevölkerung hoch gesteckt. Es wird erwartet, daß er vor den Gefahren einer unkontrollierten Verbreitung sowohl von Gesundheitsdaten als z. B. auch von Volkszählungsdaten sorgt und dies auch jederzeit gewährleisten kann. Der Gesetzgeber und die öffentliche Verwaltung müssen bei all ihren Überlegungen deshalb immer berücksichtigen, daß der Bürger sich auch insbesondere deshalb mißtrauisch z. B. einer Meldepflicht für AIDS-Erkrankungen oder anderen Zwangserhebungen gegenüber sieht, weil er den Gesamtrahmen möglicher Verarbeitung solcher Daten und damit die Auswirkungen nicht mehr erkennen kann. Verfassungsrechtlich gesicherter Datenschutz verlangt deshalb vom Gesetzgeber wie von der Verwaltung, daß sie die Auswirkungen auf die Betroffenen mitbedenken und unter Verhältnismäßigkeitsgesichtspunkten immer die geringste Belastung für den Betroffenen wählen. Wie z. B. mit Gesundheitsdaten umgegangen werden darf, muß dringend gesetzlich geregelt werden. Welche datenschutzrechtlichen Konsequenzen aus der Entwicklung der Bio- und Gentechnologie zu ziehen sind, muß weiter erörtert werden (vgl. dazu in meinem 8. Jahresbericht Pkt. 2.4, S. 22). Auch der Bericht der Enquete-Kommission wirft datenschutzrechtliche Fragen auf, die in nächster Zeit erörtert und geregelt werden müssen.

Die Diskussion um die Meldedatenübermittlungsverordnung und den Entwurf zum Bremischen Schulverwaltungsgesetz hat gezeigt, daß durch beharrliche und fundierte Argumentation und durch die öffentliche Unterstützung, z. B. betroffener Eltern, datenschutzrechtlicher Fortschritt errungen werden kann.

Diese Beispiele mögen genügen, um zu demonstrieren, daß der Bürger mehr Erwartungen an den Datenschutz hat, als dies manchen Verantwortlichen in Politik und Verwaltung bewußt zu sein scheint. Ohne den Datenschutz zu gewährleisten, würde die Volkszählung 1987 nicht durchgeführt werden können. Die Erwartung in den Datenschutz ist jedoch nicht auf spektakuläre Ereignisse beschränkt. Die gegenwärtige Phase der Computerisierung vieler öffentlicher Aufgaben durch Arbeitsplatzrechner, Personal-Computer und Bürokommunikationssysteme steht ebenfalls unter der Erwartung datenschutzrechtlich konformer Gestaltung. Die Erwartung ist sowohl von seiten der Bürger als auch von seiten der betroffenen Mitarbeiter in den Verwaltungen, die z. B. durch Protokollierungen abgebildet werden, so hoch gesteckt, daß sie zunehmend fragen, ob der Landesbeauftragte die hierfür notwendige Bedeutung und Ausstattung hat, um den Datenschutz tatsächlich durchsetzen zu können. Betrachtet man hingegen die gegenwärtige Praxis, so hat z. B. keine Beteiligung meines Hauses bei der Planung von Bürokommunikationssystemen in der bremischen Verwaltung stattgefunden. Integrierte Netze der Bürokommunikation in der gesamten bremischen öffentlichen Verwaltung werfen derartig grundsätzliche Datenschutzfragen auf, daß es nicht ausreicht, mich in späteren Phasen zu beteiligen oder darauf hinzuweisen, daß der Datenschutz nach dem Bremischen Datenschutzgesetz beachtet wird. Wer sich einmal die Mühe

gemacht hat, in Details der Gestaltung und der Planung auch zum Thema Datenschutz vorzudringen, der hat sehr schnell erkannt, wie kompliziert und detailorienriert die Realisierung datenschutzrechtlicher Anforderungen ist.

Es ist eine gute Uberlegung, daß der Senat in neueren Projekten, die teilweise durch Drittmittel gefördert werden, gleichzeitig auch externe Aufträge zur Erarbeitung von Datenschutzkonzepten, so z. B. bei PROSOZ und ISA-BK erteilt. Meine Erfahrung mit diesen beiden Projekten zeigt aber, daß sowohl die Zusammenarbeit nicht in dem Umfang gegeben ist, wie es erforderlich wäre, als auch Bremenspezifische Rechtsbelange nicht ausreichend berücksichtigt werden. Schließlich kommt hinzu, daß die Auslagerung solcher Datenschutzarbeit mich nicht der Notwendigkeit enthebt, das Konzept auf datenschutzrechtliche Konsequenzen zu prüfen, so daß die beabsichtigte Entlastung tatsächlich nicht oder nur in sehr geringem Maße eintritt. Ich halte es deshalb für zweckmäßiger, statt Auslagerung der Datenschutzarbeit an dritte Institutionen, die Beratungskapazität in meinem Hause zu erhöhen.

Die bevorstehende Novellierung des Bremischen Datenschutzgesetzes greift einerseits die dringenden Erfordernisse der Rechtsfortentwicklung aufgrund der Rechtsprechung des Bundesverfassungsgerichtes und andererseits die permanente Technikfortentwicklung auf. Die dauernde Ausweitung der Datenschutzaufgaben und die hohe Erwartung der Bürger an der Durchsetzung und Beachtung des Datenschutzes sind unter dem Aspekt der Glaubwürdigkeit nur aufrecht zu erhalten, wenn gleichzeitig mit gesetzgeberischen Maßnahmen auch darüber befunden wird, mit welchen personellen und sachlichen Mitteln diese Aufgabe durchgeführt werden soll. Wenn im Laufe des Jahres 1986 zu hören war, daß Datenschutz im Moment kein aktuelles Thema mehr sei, so ist nicht auszuschließen, daß Datenschutz leicht zum Spielball unterschiedlicher Interessen werden könnte. Die Öffentlichkeit erwartet jedoch, daß Datenschutz glaubwürdig in allen Anwendungsbereichen berücksichtigt wird.

Datenschutz ist keine Eintagsfliege, deren man sich je nach Opportunität bedienen kann. Der Bürger muß dauerhaft die Gewährleistung des Datenschutzes erleben. Ist dieses Erlebnis positiv, wird auch sein Verhältnis zur staatlichen Informationsverarbeitung davon geprägt sein. Ist dieses Erlebnis überwiegend Vertrauen zerstörend, dann verbindet sich hiermit auch die Grundeinstellung zum Staat. Dies hat grundsätzliche politische Bedeutung.

Es muß deutlich bleiben, Informationen und Daten über Menschen sind nun einmal in einer menschlichen Gesellschaft wichtige Voraussetzungen für Kommuniktion, für Planung, für staatliches und privates Handeln schlechthin. Der Bürger ist nur bereit mitzuwirken, wenn ihm auf Dauer glaubhaft zugesichert wird, daß diese Daten geschützt, gesetzeskonform verarbeitet und seinem ursprünglichen Zweck entsprechend verwendet werden. Dies zu gewährleisten und durch Kontrolle zu überprüfen, ist Aufgabe des Datenschutzes.

Ich möchte es nicht versäumen, allen meinen Mitarbeitern für ihren unermüdlichen Einsatz, der weit über die normale Arbeitszeit hinausgeht und für die ich keinen Ausgleich anbieten kann, auch an dieser Stelle einmal öffentlich zu danken.

1.2 Zur Personalsituation

Die personelle Situation ist aufgrund der permanenten Aufgabenausweitung nicht mehr nur durch einzelne Stellenanträge jährlich neu zu diskutieren, sondern es bedarf eines grundsätzlichen Konzeptes, wie sich der Senat die Gewährleistung des Datenschutzes auch personell vorstellt. Ich habe hierzu ein Personalentwicklungskonzept für die nächsten Jahre vorgelegt und erwarte, daß der Senat und die Bürgerschaft prinzipiell erklären, wie sie die sich ständig ausweitende Datenschutzberatungs- und Kontrolltätigkeit auch unter dem Aspekt der Glaubwürdigkeit gewährleisten wollen. Es ist unverzichtbar, wenn Datenschutz gewollt wird, sich mit dieser Frage zu beschäftigen und dafür Sorge zu tragen, daß mehr qualifizierte Mitarbeiter in meine Dienststelle gelangen. Hinhaltende Erklärungen und Verweise auf die permanente Haushaltssituation können auf die Dauer nicht befriedigen. Strukturveränderungen der öffentlichen Verwaltung müssen auch zu personellen Versetzungen führen. Meine Behörde, die aufgrund der strukturellen Veränderungen zusätzliche und umfangreiche Aufgaben übernehmen muß, bedarf hierfür der entsprechenden Ausstattung. Aufgrund des Dienstsitzes Bremerhaven

bedeutet dies selbstverständlich auch, daß die konsumtiven Ausgaben (z. B. mehr Telefonkosten, mehr Fahrtkosten etc.) erhöht werden müssen. Es ist an der Zeit, sich einmal grundsätzlich politisch zu bekennen, welchen Stellenwert der Datenschutz im Lande Bremen haben soll, welche Mittel man dafür bereitstellen möchte und wieviel Personal politisch verantwortlich zur Verfügung gestellt werden soll. Einzelne Beschlüsse auf Stellenbereitstellung, wie etwa die eines Mitarbeiters im gehobenen Dienst, die dann noch nicht einmal realisiert werden, reichen hierfür nicht mehr aus.

2. Rechts- und Informationstechnologie-Entwicklung

2.1 Rechtsentwicklung

2.1.1 Übergangsbonus

Das Bundesverfassungsgericht hat in seinem Urteil zum Volkszählungsgesetz 1983 darauf hingewiesen, daß die zwangsweise Datenerhebung beim Bürger nur im überwiegenden Allgemeininteresse zulässig sei, und daß der Umfang der Datenverarbeitung (Zwecke und Nutzung) gesetzlich zu regeln sei. Damit stellt sich die Frage, wie lange der Gesetzgeber sich Zeit nehmen kann, dieser Forderung in den einzelnen Rechtsgebieten Rechnung zu tragen.

Grundsätzlich sind Maßnahmen der Verwaltung, die in das informationelle Selbstbestimmungsrecht eingreifen und die einer verfassungsrechtlich gebotenen Grundlage entbehren, auch wenn es bisher geübte Praxis sein sollte, verboten. Das Bundesverfassungsgericht hat jedoch in einer Reihe von Fällen, in welchen eine verfassungsrechtlich ursprünglich unbedenkliche Maßnahme aufgrund einer gewandelten Rechtsauffassung oder völlig veränderter tatsächlicher Umstände, die der bisherigen gesetzlichen Regelung zugrunde lagen und verfassungsrechtlich bedenklich geworden sind, die Notwendigkeit von Übergangsfristen in den Fällen anerkannt, in denen dem Gesetzgeber die Gelegenheit gegeben wird, eine verfassungsgemäße Regelung zu schaffen.

Solche Übergangsfristen (Übergangsbonus) werden nur dann für verfassungsrechtlich zulässig gehalten, wenn sonst die Funktionsfähigkeit staatlichen Handelns erheblich beeinträchtigt würde, die Aufgabe der bisherigen Praxis gravierende Nachteile für das Allgemeinwohl mit sich bringt oder durch Unterlassung der Maßnahme ein Zustand erreicht würde, der der verfassungsmäßigen Ordnung noch ferner liegen würde als der bisherige Zustand. Bei der Zubilligung von Übergangsfristen ist die Schwere des Eingriffs zu berücksichtigen, denn je tiefer eine Verwaltungsmaßnahme die Grundrechte des Betroffenen tangiert, desto strengere Anforderungen sind an die Einräumung von Übergangsfristen zu stellen. Für die Dauer derartiger Übergangsfristen gibt es keine allgemeinen Maßstäbe, das Bundesverfassungsgericht hat aber verschiedentlich darauf gedrungen, daß eine gesetzliche Regelung bis zum Ende einer laufenden Legislaturperiode des Parlaments verabschiedet wird. Eine Übergangsfrist kann im übrigen in den Fällen nicht länger zugebilligt werden, in denen der Gesetzgeber eine Neuregelung ungebührlich verzögert hat oder aber in denen er andere verfassungsrechtlich nicht gebotene Regelungen schafft, gleichzeitig aber die verfassungsrechtlich gebotene Regelung eines Sachverhaltes unterläßt (so ein Zustand könnte etwa bei § 163 d StPO angenommen werden).

Schließlich ist die Verwaltungspraxis darauf zu begrenzen, die Eingriffe in die verfassungsrechtlich geschützte Position auf das zu beschränken, was im konkreten Fall für die geordnete Weiterführung und die Funktionsfähigkeit des Staates unerläßlich ist. Die Verwaltung ist daher gehalten zu prüfen, inwieweit sie etwa auf Informationsverarbeitungen zu verzichten hat, solange ihr die ausreichenden gesetzlichen Regelungen zum Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen nicht zur Verfügung stehen.

Der Bremische Senat hat in seiner Stellungnahme zu meinem 8. Jahresbericht erklärt, daß nach seiner Auffassung der durch das Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983 den Ländern eingeräumte „Übergangsbonus" über die Legislaturperiode der Bürgerschaft hinaus nicht zu vertreten ist.

Diese Auffassung des Senats bedeutet, daß nicht nur eine allgemeine Datenschutzgesetzgebung erforderlich ist, sondern auch bereichsspezifische Regelungen in dieser Zeit geschaffen werden müssen.

Als Beispiele für bereichsspezifische Regelungen seien besonders hervorgehoben:

— Schulverwaltungsgesetz,

— Landeshochschulgesetz,

— Archivgesetz,

— Datenschutzregelungen für Gesundheitsverwaltung und Krankenhäuser,

— Arbeitnehmer-Datenschutz für den bremischen öffentlichen Dienst.

Zu Anforderungen des Datenschutzes im Krankenhaus hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 eine Entschließung gefaßt, die als Anlage 1 abgedruckt ist.

2.1.2 Entwicklung der Gesetzgebung im Bund

2.1.2.1 Erlaß des Baugesetzbuches

Am 1. Juli 1987 wird das am 8. Dezember 1986 vom Bundestag beschlossene Baugesetzbuch (BauGB) in Kraft treten. Mit dem Baugesetzbuch werden das bisher geltende Bundesbaugesetz und das Städtebauförderungsgesetz bei gleichzeitiger Änderung materiellrechtlicher und verfahrensrechtlicher Vorschriften zu einem Gesetz zusammengefaßt.

Es soll nicht verkannt werden, daß der Gesetzgeber versucht hat, die im Gesetz vorhandenen datenschutzrechtlich relevanten Vorschriften den vom Bundesverfassungsgericht insbesondere in seinem Urteil zum Volkszählungsgesetz 1983 festgelegten Anforderungen anzupassen. Es bleibt jedoch erhebliche Kritik an den gefundenen Regelungen anzumelden. Das gilt besonders für die Vorschriften des § 138 BauGB, welche die Datenerhebung und -verarbeitung für die Durchführung von Sanierungsmaßnahmen regeln, und des § 195 BauGB, in denen die Führung der Kaufpreissammlung und die damit verbundene Datenverarbeitung geregelt werden.

Im § 138 Abs. 1 BauGB heißt es, daß an personenbezogenen Daten insbesondere Angaben über die persönlichen Lebensumstände im wirtschaftlichen und sozialen Bereich, namentlich über die Berufs-, Erwerbs- und Familienverhältnisse, das Lebensalter, die Wohnbedürfnisse, die sozialen Verflechtungen sowie über die örtlichen Bindungen der Mieter, Eigentümer, Pächter usw. erhoben werden dürfen. Ich habe erhebliche Zweifel, ob eine so weitgehende Erlaubnis für eine Datenerhebung und -verarbeitung für die Durchführung der Sanierung erforderlich ist. Keinesfalls ist dieser Umfang von Daten für die Vorbereitung der Sanierung erforderlich. Es besteht insoweit sicherlich ein erheblicher Unterschied, ob aus stadtplanerischer Sicht zu beurteilen ist, ob eine Sanierungsbedürftigkeit eines Stadtteiles oder eines Quartieres gegeben ist, oder ob eine Sanierung durchzuführen ist. Die Art der Daten, die erhoben werden dürfen, ist weder abschließend noch hinreichend präzise geregelt. Durch die im Gesetzestext verwendeten Formulierungen „insbesondere" und „namentlich" wird eine erhebliche Ausdehnung des Umfanges der Daten, die erhoben werden dürfen, zugelassen. Auch die Verwendung von Begriffen wie „Erwerbs- und Familienverhältnisse", persönliche Lebensumstände im sozialen und wirtschaftlichen Bereich usw. beschreiben Art und Umfang der Daten, deren Verarbeitung zulässig sein soll, nicht ausreichend genau. Damit sind den das Gesetz durchführenden Stellen uferlose Ermessens- und Beurteilungsspielräume gegeben.

Die Vorschriften genügen somit nicht den Grundsätzen der Verhältnismäßigkeit und der Normenklarheit.

Zu begrüßen ist, daß im § 138 Abs. 2 BauGB festgelegt worden ist, daß die erhobenen Daten nur für Zwecke der Sanierung verwendet werden dürfen. Die Vorschrift enthält jedoch eine kritikwürdige Ausnahme von diesem Grundsatz. Die erhobenen Daten dürfen an die Finanzbehörden weitergegeben werden, soweit sie für die Besteuerung erforderlich sind. Ich bezweifle, ob eine solche Datenübermittlung überhaupt erforderlich ist. Zumindest hätte eine Formulierung gefunden werden müssen, die klargestellt hätte, für welchen Besteuerungszweck welche Datenarten aus welchem Anlaß übermittelt werden dürfen. Die jetzige Formulierung verstößt gegen den Grundsatz der Normenklarheit. Zu bemängeln ist auch die Vorschrift, nach der die erhobenen Daten nach der Aufhebung der förmlichen Festlegung des Sanierungsgebietes zu löschen sind. Sie berücksichtigt nicht, daß Daten aus Bereichen, die zwar in die Vorbereitung der Sanierung, nicht aber in die förm-

liche Festlegung als Sanierungsgebiet einbezogen waren, oder Daten von Betroffenen, die aus dem Sanierungsgebiet ausgezogen sind, nicht bis zur Aufhebung der förmlichen Festlegung erforderlich sind.

Nach § 195 BauGB sind die beurkundenden Stellen verpflichtet, Verträge über die Eigentumsübertragung an Grundstücken abschriftlich dem Gutachterausschuß für die Führung der Kaufpreissammlung zu übersenden. In solchen Verträgen sind personenbezogene Daten über Verkäufer, Käufer und evtl. auch über Dritte in erheblichem Umfange vorhanden, die auf diese Weise dem Gutachterausschuß übermittelt werden. Nur ein geringer Teil dieser Daten wird von dem Gutachterausschuß für seine gesetzlichen Aufgaben benötigt. So sind sämtliche Daten über den Verkäufer oder über Dritte entbehrlich. Das gilt auch für eine Reihe von Informationen, die über den Käufer im Vertrag enthalten sind. Das angegebene Ziel hätte auch mit anderen Mitteln, die nicht einen so weitgehenden Eingriff in das Recht auf informationelle Selbstbestimmung zur Folge gehabt hätten, erreicht werden können. Denkbar wäre z. B., daß die beurkundenden Stellen verpflichtet worden wären, die wirklich erforderlichen Vertragsmerkmale an den Gutachterausschuß zu übersenden. Die Vorschrift verstößt damit gegen den Grundsatz der Verhältnismäßigkeit.

Sie ermächtigt außerdem die Länder, durch landesrechtliche Vorschriften zu regeln, wer neben dem zuständigen Finanzamt einen Anspruch auf Auskunft aus der Kaufpreissammlung erhalten soll.

Es bleibt zu hoffen, daß für das Land Bremen eine Regelung gefunden wird, die den datenschutzrechtlichen Belangen der Betroffenen gerecht wird.

2.1.2.2 Telekommunikationsordnung (TKO)

Der Verwaltungsrat der Deutschen Bundespost hat im Juni 1986 dem vom Bundesminister für das Post- und Fernmeldewesen vorgelegten Entwurf einer „Verordnung über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Fernmeldewesens (Telekommunikationsordnung — TKO)" zugestimmt. Im November 1986 wurde diese Verordnung im Bundesgesetzblatt veröffentlicht; sie tritt am 1. Januar 1988 in Kraft.

Mit dieser Verordnung wird versucht, die wichtigsten fernmelderechtlichen Bestimmungen für die verschiedenen alten und neuen Dienste der Deutschen Bundespost wie z. B. Telefon, Telex, Teletex, Telefax, Bildschirmtext, Datel-Dienste, Funkdienste etc. zusammenzufassen, neu zu strukturieren und inhaltlich zu ergänzen (vgl. zu dieser Thematik auch meine Ausführungen im 8. Jahresbericht unter Pkt. 2.1.3.3, S. 17 f.). Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Berichtsjahr mit diesem umfangreichen Regelungspaket beschäftigt und eine gemeinsame Entschließung zum Entwurf der Telekommunikationsordnung verabschiedet (vgl. Anlage 2). In dieser Entschließung wird auf einige datenschutzrechtliche Probleme im TKO-Entwurf hingewiesen und werden Änderungen und Ergänzungen vorgeschlagen. Ziel dabei war es, dem Recht auf informationelle Selbstbestimmung und den Anforderungen des Volkszählungsurteils auch im Bereich der Postdienste eine größere Geltung zu verschaffen.

Wesentliche Anregungen der Datenschutzbeauftragten wurden nicht berücksichtigt. Zum Beispiel:

— Die Verpflichtung der Deutschen Bundespost zur Aufklärung über nicht vermeidbare Risiken bei der Datensicherung.

— Eine präzise Umschreibung der öffentlichen Telekommunikationsdienste einschließlich Definition des jeweils erforderlichen Datenprofils.

— Eine angemessene Regelung über die Zulassung einer Benutzung des öffentlichen Netzes für sonstige Telekommunikationszwecke.

— Eine übersichtliche Definition der für den Datenschutz relevanten Grundbegriffe.

— Eine genaue Umschreibung der vom Teilnehmer beantragbaren „anderen Art der Verarbeitung" von Verbindungsdaten.

— Bestimmungen zum Datenschutz bei der Entstehung von Gebührendaten.

— Die Nutzungsbeschränkung der gespeicherten personenbezogenen Daten für die Zwecke der jeweils in Anspruch genommenen Dienste statt allgemein zu „Telekommunikationszwecken".

— Den Ausschluß der Verbindungsdaten von jeglicher Übermittlung.

— Die Beseitigung des „Zwangseintrags" in Teilnehmerverzeichnisse.

— Das Angebot eines Dienstes zur Verschlüsselung von Nachrichten.

— Die Möglichkeit der Gebührenzählung beim Teilnehmer.

Neben diesen Detailforderungen sind die Datenschutzbeauftragten der Länder der Auffassung, daß auch die Länder Initiativen entwickeln müssen, um im Rahmen ihrer Zuständigkeit möglichst einheitliche Regelungen für die Nutzung der über den Datentransport hinausgehenden Dienste zu schaffen. Dies beginnt bereits mit der Frage, in welchem Umfang die Länder bei der Einführung neuer Dienste beteiligt werden müssen (Diensteinführungsentscheidung). Ist die Entscheidung für einen bestimmten Dienst gefallen, sind die Länder aufgerufen, im erforderlichen Umfang den Nutzungsbereich zu strukturieren. Beispiele hierfür sind der Btx-Staatsvertrag und die in verschiedenen Ländern eingeführten Nutzungsregelungen zur Einführung von Fernwirkdiensten.

2.1.2.3 Bundesstatistikgesetz

Der Deutsche Bundestag hat am 4. Dezember 1986 — kurz vor dem Ende der Legislaturperiode — das Gesetz über die Statistik für Bundeszwecke in völlig neuer Fassung verabschiedet. Der Bundesrat hat in seiner Sitzung vor Weihnachten 1986 dem neugefaßten Bundesstatistikgesetz ebenfalls zugestimmt. Ende Januar 1987 wurde es im Bundesgesetzblatt verkündet; einen Tag nach seiner Verkündung trat es in Kraft.

Mit dieser Novelle des Bundesstatistikgesetzes hat der Bundesgesetzgeber die Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts für diese Gesetzesmaterie gezogen. Er ist damit auch einer dringenden Empfehlung der Datenschutzbeauftragten nachgekommen, die eine Novellierung dieses Gesetzes für dringend geboten gehalten haben. Im 8. Jahresbericht habe ich bereits unter Pkt. 5.2.4.1, S. 36 f. zu diesem Gesetzesvorhaben Stellung genommen.

Diese Stellungnahme bezog sich nicht auf den Gesetzentwurf, den die Bundesregierung nach Beteiligung des Bundesrates im April 1986 dem Bundestag zugeleitet hat, sondern auf den Kabinettsentwurf von Ende 1985. Die beschlossene und verkündete Fassung des neuen Bundesstatistikgesetzes unterscheidet sich vom alten Bundesstatistikgesetz und von der seinerzeitigen Entwurfsfassung erheblich. Zu dem dort von mir beschriebenen Regierungsentwurf konnten im Laufe der weiteren Gesetzesberatungen einige datenschutzrechtliche Verbesserungen erreicht werden. Sah der Regierungsentwurf eine grundsätzliche Auskunftspflicht vor, von der nur durch besondere gesetzliche Regelung abgewichen werden sollte, normiert die beschlossene Fassung eine Auskunftspflicht nur dann, wenn die eine Bundesstatistik anordnende Rechtsvorschrift diese ausdrücklich festlegt.

Nach dem Regierungsentwurf war für die Durchführung einer Bundesstatistik eine pauschale Ermächtigung für solche Fälle gegeben, in denen die Angaben ausschließlich aus allgemein zugänglichen Quellen oder aus öffentlichen Registern, zu denen das statistische Bundesamt oder die statistischen Landesämter Zugang haben, verwendet werden. Das beschlossene Gesetz läßt eine Verwendung von Daten aus öffentlichen Registern nur zu, wenn dem statistischen Bundesamt oder den statistischen Ämtern der Länder in einer Rechtsvorschrift ein besonderes Zugangsrecht zu diesen Registern gewährt wird. Wenn die beschlossene Fassung insoweit auch eine Verbesserung darstellt, bleiben jedoch Zweifel, ob damit die verfassungsrechtliche Notwendigkeit der Normenklarheit der entsprechenden Vorschrift erfüllt wird.

Erhebliche verfassungsrechtliche Bedenken bleiben wegen der Zulässigkeit der Verarbeitung von Daten aus allgemein zugänglichen Quellen. Denn durch Verknüpfung frei zugänglicher, normalerweise nicht verknüpfter Daten aus unterschiedlichen Lebensbereichen, können neue sensible schützenswerte Informationen entstehen. Gerade wegen solcher Gefahren hat das Bundesverfassungsgericht für die Verarbeitung von Informationen für statistische Zwecke klare, den Zweck bestimmende gesetzliche Regelungen gefordert.

Mit dem Gesetz wird die Bundesregierung ermächtigt, unter bestimmten Voraussetzungen Wirtschafts- und Umweltstatistiken durch Rechtsverordnung anzuordnen.

Wenn auch eine im Laufe der Gesetzesberatung eingefügte periodische Berichtspflicht der Bundesregierung über so angeordnete Statistiken die Kontrollmöglichkeiten erhöht, halte ich eine so weitgehende Ermächtigung aber nach wie vor nur unter der Voraussetzung für zulässig, daß die Auskünfte in solchen Fällen freiwillig gegeben werden können.

Schwerwiegende Bedenken gegen das Bundesstatistikgesetz bleiben insoweit bestehen, als es die Übermittlung im Verwaltungsvollzug von Verwaltungsstellen des Bundes erhobener oder sonstwie angefallener Daten an das Statistische Bundesamt auch hinsichtlich personenbezogener Daten zuläßt, da sie eine Änderung des Verwendungszwecks der vom Betroffenen gemachten Angaben bedeutet. Ich halte eine solche Übermittlung personenbezogener Daten nur in anonymisierter Form für zulässig.

Die mit der Durchführung dieses Gesetzes betrauten Stellen bleiben aufgerufen, bei der Handhabung des Gesetzes die datenschutzrechtlichen Belange der Betroffenen zu wahren. Das liegt auch im Interesse des Aussagewertes der beabsichtigten Statistiken.

2.2 Technologieentwicklung

2.2.1 Einsatz von Arbeitsplatzrechnern

Durch die Entwicklung der Arbeitsplatzrechner gewinnt die autonome und dezentrale Datenverarbeitung am Arbeitsplatz große Bedeutung sowohl in Unternehmen der Wirtschaft wie in den Behörden und öffentlichen Stellen. Diese Form der individuellen Datenverarbeitung verbreitet sich zunehmend durch den Einsatz von Mikrocomputern, Textverarbeitungssystemen etc., kurz durch PC's, immer mehr aus. Die Leistungsfähigkeit dieser Geräte hat heute bereits die der früheren Großrechner erreicht. Die Anwendungsmöglichkeiten sind nahezu unbegrenzt, die Anschaffungskosten immer niedriger und ergeben ein äußerst günstiges Preis-/Leistungsverhältnis. Hinzu kommt, daß der Umgang mit PC's keine besonderen EDV-Kenntnisse voraussetzt, so daß in naher Zukunft jedermann mit einem PC umgehen kann.

Arbeitsplatzrechner lassen sich prinzipiell in drei verschiedenen Formen einsetzen, nämlich als Stand-alone-Installation, d. h. als einzelner isolierter PC, als untereinander verbundene PC's und schließlich können die PC's mit einem zentralen Rechner verbunden werden.

Die neuen Möglichkeiten, die der Arbeitsplatzrechner mit sich bringt, wie die unabhängige und dezentrale Verarbeitung und damit die entsprechende Ausstattung an Sachbearbeiterplätzen und in Fachabteilungen, bringen nicht nur arbeitsorganisatorische und Rationalisierungsvorteile, sondern bergen für Behörden und Unternehmen Gefahren in sich, denen von vornherein durch eindeutige Regelungen und Konzepte für Datenschutz und Datensicherung begegnet werden muß.

Aus meiner Kontrollpraxis kann ich bereits jetzt folgende Gefahren darstellen:

— Es werden eigenmächtig Hard- und Software beschafft, so daß damit die Gefahr des Wildwuchses in unterschiedlicher Hardware, verschiedenen Installationsmöglichkeiten, verschiedene Software und nicht bekannte und unkontrollierbare Anwendungen entsteht.

— Durch dezentrale Verarbeitung entstehen Inseln, die Datenbestände aufbauen und führen, die weder mit den zentral gespeicherten Daten identisch sind noch deren Kontrollfähigkeit gegeben ist.

— Es ist gar nicht oder nur mangelhaft sichergestellt, daß die gesetzlichen Vorschriften eingehalten werden, die Datenverarbeitung ordnungsgemäß organisiert ist, Datenschutz und Datensicherung betrachtet werden und Wirtschaftlichkeitskriterien mitunter zu kurz kommen.

— Dienstliche PC's mißbräuchlich für private Zwecke bzw. private PC's für dienstliche Zwecke genutzt werden.

Neben diesen verschiedenen Gefahren muß beim Einsatz von PC's im Rahmen von Bürokommunikationskonzepten zusätzlich berücksichtigt werden, daß dieser Einsatz nicht nur Rationalisierungserfolge mit sich bringt, sondern auch neue Risiken für Persönlichkeitsrechte schafft. So verfügen Bürokommunikationssysteme über sogenannte Multifunktionsterminals, mit denen

— auf Großrechnern interne und externe Informationssysteme genutzt,

— Telefongespräche geführt und aufgezeichnet,

— Btx-Angebote abgegeben und abgerufen,

— auf Dateien zugegriffen, Dateien angelegt und verfügbar gemacht,

— Graphiken, z. B. im medizinischen Bereich, mit personenbezogenen Daten erstellt sowie

— Texte erstellt, verknüpft, versandt und archiviert

werden können.

Neben diese vielfältigten Anwendungsformen tritt die Entwicklung der Nachrichtentechnik und der Telekommunikation. Die Integration der verschiedenen Postdienste, wie z. B. Telefon, Telefax, Telex, Teletex etc. hin zu einem universalen Netz, eröffnet umfangreiche Formen der telekommunikativen Übertragung. Mit dieser Entwicklung tritt ein in der Öffentlichkeit bereits diskutiertes Phänomen der vernetzten Strukturen und der technischen Vernetzung auf. Die Entwicklung hat nicht nur datenschutzrechtliche Bedeutung, sondern wirft für die künftige gesellschaftliche Gestaltung neue Fragen der gesellschaftspolitischen Verantwortung auf. Hierauf erwarten die Bürger zu Recht Antwort.

Der Einsatz von PC's in Bürokommuniktionssystemen hat Vorteile, wie sie sich ergeben etwa aus der klaren Definition von Verantwortlichkeit, durch die automatisierte Speicherung das jederzeitige Auffinden von Akten und Dokumenten (es wird das häufig umfangreiche Suchen nicht auffindbarer Akten vermeidbar), Vorgänge werden schnell aufgefunden, und schließlich werden Umlaufzeiten verkürzt. Neben solchen Vorteilen entstehen allerdings auch Risiken, weil eine große Zahl bisher manuell bearbeiteter Vorgänge jetzt über Bürokommunikation direkt zugreifbar verarbeitet werden, so daß die mit der manuellen Verarbeitung bisher zwangsläufig auftretenden Nutzungsbeschränkungen wegfallen. Hinzu kommt, daß die Datensicherungsmaßnahmen für PC-Einsätze, die sowohl im Hardware- wie im Softwarebereich angeboten werden, bisher unzureichend sind.

Abgesehen von nicht ausreichenden technischen und organisatorischen Maßnahmen beim Einsatz von Bürokommunikationssystemen bestehen im Datenschutzrecht nicht ausreichende Regelungen zur Nutzung personenbezogener Daten. Im einzelnen seien hier folgende Risiken benannt:

— Verwendung von Archivdaten

In Bürokommunikationssystemen (BKS) sollen künftig Inhalte von Akten und Dokumenten aufbewahrt werden, die nach beliebigen Kriterien sortierbar und inhaltlich auswertbar sind. Die Datenverarbeitung bekommt eine sehr viel höhere Qualität. Akten waren bisher je Einzelperson bzw. Einzelfall aufbewahrt und bearbeitbar. Eine Verbindung von verschiedenen Informationen aus unterschiedlichen Akten war zwar möglich, aber äußerst schwierig manuell durchzuführen. Bei der Speicherung auf direkt zugreifbaren Datenträgern ist derartiges verhältnismäßig problemlos.

— Möglichkeit der Leistungskontrolle

Die herkömmliche Gegenzeichnung nach der Bearbeitung von Vorgängen, die für den Nachweis von Verantwortlichkeit verwendbar war, wird im BKS erweitert durch die Möglichkeit, daß Arbeits- und Leistungsdaten der BKS-Sachbearbeiter einfach, schnell und so oft wie gewünscht festgestellt werden können. Ergänzt mit einer Vielzahl gemessener Werte kann auch eine Leistungsbeurteilung vorgenommen werden. Eine lückenlose Speicherung des Arbeitsverhaltens eines Arbeitnehmers stellt die freie Entfaltung seiner Persönlichkeit in Frage, auf die er auch am Arbeitsplatz Anspruch hat. Bei der Regelung des Arbeitnehmerdatenschutzes ist dem besondere Bedeutung beizumessen.

— Unkontrollierbare Datenverarbeitung

Eine Vielzahl von miteinander verbundenen Datensammlungen kann auch dazu führen, daß die Ordnungsmäßigkeit der Datenverarbeitung nicht mehr gewährleistet ist. So haben immer mehr Bedienstete Gelegenheit, auf ihnen bisher nicht zugängliche Dateien zuzugreifen und diese auch zu verändern. Diese Möglichkeiten werden beim flächendeckenden Einsatz nicht mehr kontrollierbar sein, zumal auch technische Maßnahmen bei der Prüfung der Zugriffsberechtigung häufig versagen, wenn die intelligenten Arbeitsplatzrechner kenntnisreich gehandhabt werden.

— Nicht ausreichender Zugriffsschutz

Wie oben schon erwähnt, gibt es derzeit kein System auf dem Hardware- und Softwaremarkt, mit dem eine flexibel abgestufte und individuell gestaltbare Zugriffssicherung zu realisieren wäre. Ergänzende organisatorische Maßnahmen sind häufig nur mangelhaft geeignet, die vielen BKS-Möglichkeiten, wie z. B. das Archiv zu durchsuchen, interne und externe Informationssysteme zu nutzen, Dateien anzulegen, zu empfangen, zu versenden, zu sichern oder zu bearbeiten usw. zu kontrollieren.

— Protokollierung

Wie Bearbeitungsvorgänge und Zugriffe auf Daten über ein BKS für Datenschutzzwecke protokolliert werden können, ist noch nicht geklärt. Ich verweise beispielhaft auf die Problematik der Eingabe-, der Zugriffs-, der Transport- und der Übermittlungskontrolle. Es ist unverzichtbar, für Datenschutzzwecke automatisierte Kontrollen zu ermöglichen.

— Technische Manipulationsmöglichkeiten

Je nach Netz-Topologie ist es zwar schwierig, aber immerhin doch möglich, Datenübertragungen „abzuhören", indem z. B. die elektrische Induktion gemessen wird. Ebenso können Datenstationen auf dem Weg der Übertragung zwischengeschaltet werden und die digitalisierten Informationen aufgezeichnet und verwertet werden. Derartige unbefugte Eingriffe, die auch zur Manipulation führen können, kann man zwar durch komplizierte Übergabeprotokolle zu und von den einzelnen Stationen stark erschweren, verhindern kann man sie jedoch nicht.

BKS erlauben auch die Verbindung zu zentralen Teilhabersystemen, wie z. B. im öffentlichen Bereich das automatische Melderegister, INPOL etc. Über einen sogenannten Server können diese Verbindungen angefordert werden, wenn die Multifunktionsterminals nicht entsprechend zugriffsgeschützt sind. Da eventuell vorhandene Zugriffsschutzvorkehrungen durch geschickte Manipulation des Betriebssystems eines Arbeitsplatzrechners umgangen werden können, ist diese Kontrolle nur im zentralen System durchzuführen.

Bei dieser Darstellung muß beachtet werden, daß keineswegs alle Möglichkeiten der Verbindung von Arbeitsplatzrechnern untereinander und mit Zentralrechnern in „breiten" Netzen bisher ausgeschöpft wurden bzw. bereits bekannt sind.

Die Bewältigung der datenschutzrechtlichen Anforderungen beim Einsatz von Arbeitsplatzrechnern und Bürokommunikationssystemen setzt die Analyse von Risiken bei allen beteiligten Gruppen, wie Hersteller von Hard- und Software, Anwender, Datenschutzkontrollinstanzen, Wissenschaftlern und dem Gesetzgeber voraus. Die Lösung datenschutzrechtlicher Fragen wird gegenwärtig in der Literatur erörtert, deshalb wird auf diese Diskussion verwiesen, ohne hier im einzelnen Literaturhinweise zu geben.

2.2.2 Datensicherheit durch Chip-Karten

Die Sicherheit eines Datenverarbeitungssystems ist so gut wie deren Sicherheitssoftware einerseits und technische Sicherungen (Hardware) andererseits. Dabei kommt dem Individualschutz eine besondere Bedeutung zu. Insbesondere bei Einsatz von Arbeitsplatzsystemen, die räumlich leicht zugänglich sind und in der Regel nicht im „Closed-shop-Betrieb" gefahren werden, spielt der Zugangs- und Zugriffsschutz eine wesentliche Rolle. Wie oben erwähnt, sind sowohl Hardware als auch Software für eine optimale Sicherung der Datenbestände heute noch nicht geeignet. Zwar gibt es Ansätze, diese sind jedoch mit erheblichen Schwächen verbunden. Die Chip-Karten-Technologie gehört zu diesen Ansätzen, bei denen die Authentitätsfeststellung eines Benutzers besondere Beachtung finden soll.

Die Miniaturisierung der Speicherchips hat die Möglichkeit geschaffen, Mini-Computer in Scheckkartengröße und -abmessung unterzubringen. Das hat zu der Entwicklung der sogenannten Chip-Karte geführt. Diese Karte beinhaltet neben einem Mikroprozessor-Chip auch einen oder mehrere Speicherchips. Die Kraft- und Datenübertragung geschieht durch Kontakte, die an Lese- und Schreibstationen (sogenannte Chip-Karten-Leser an PC, Bankautomaten) anschließbar sind. Der Inhalt der Chip-Karte läßt sich im Speicherteil sowohl über eine Kontakttastatur auf der Karte selbst als auch über einen „erschlossenen" Computer verarbeiten.

Mit der Chip-Karte ist eine Möglichkeit geschaffen, mittels eines Schlüssels in Verbindung mit einer „elektronischen Unterschrift" die Authentifizierung eines

Benutzers feststellen zu lassen. Die elektronische Unterschrift besteht aus einer Zeichenkombination, die in Verbindung mit dem vergebenen und im Speicherteil der Chip-Karte gespeicherten Identifikationsschlüssel kombiniert wird und somit für Prüfzwecke verwendet werden kann. Dabei entstehen drei Sicherheitsbereiche:

Der „geheime Bereich" beinhaltet Angaben wie die persönliche Identifikationsnummer (PIN), kryptographische Schlüssel (RSA) und Teile von Sicherheitsprogrammen. Der Zugriff zu diesem Bereich erfolgt ausschließlich über den integrierten Mikroprocessor.

Im „geschützten Bereich" (Speicherbereich) sind Eigentümerdaten, Berechtigungen und Informationen über die mit dieser Karte möglichen Transaktionen festgehalten.

Der „offene Bereich" dient lediglich der Information und nicht der Sicherheit. Die Karte kann somit auch als „Notizbuch" von außen mit ungeschützten Bemerkungen gefüllt werden.

Durch eine Kombination von individuell änderbarer PIN, offenen und geheimen Schlüsseln, die ebenfalls in dem Kommunikationscomputer gespeichert sind, kann eine Identifikation und Authentifizierung relativ sicher durchgeführt werden. Die Identifikationsnummern sind kryptographisch verschlüsselt. Die Verfahren (z. B. RSA — nach den Entwicklern Rivest, Shamir und Adleman) bieten eine variable Verschlüsselung (abhängig von Datum und Uhrzeit). Der Inhalt wird dadurch für Unbefugte unlesbar. Eine Zerstörung der Karte würde ebenfalls zur Zerstörung der Daten führen.

Die Sicherheit der Arbeitsplatzrechner wird durch die Verwendung einer derartigen Karte sicherlich erhöht, wenngleich auch hierbei nicht ausgeschlossen ist, daß sowohl die PIN ausgespäht wird als auch die Chip-Karte in unrechte Hände geraten kann. Beides zusammen führt zum Öffnen eines Systems, jedes für sich ist jedoch unbrauchbar.

Der Vorteil der nahezu einwandfreien Authentifizierung intensiviert z. B. die bargeldlose „automatische" Zahlung — das „Point-of-sale-System" (POS). POS ermöglicht, die Person zu identifizieren, deren Namen zu speichern und z. B. für die Erstellung von Kundenprofilen und für Werbezwecke zu benutzen. Da die Auswirkungen dieser Datenbeschaffung dem Einzelnen nicht bekannt sein werden, ist diese Datenverwendung aus datenschutzrechtlicher Sicht problematisch.

Diese Entwicklung verweist erneut darauf, daß die Verwirklichung des Datenschutzes unmittelbar mit der technischen und organisatorischen Gestaltung solcher Systeme verbunden ist.

Die Entwicklung der Chip-Karten-Technologie ist noch längst nicht abgeschlossen. Sie kann neue Möglichkeiten der Sicherheit, sie kann aber auch neue Risiken für Datenschutz und Datensicherung schaffen.

Welche Richtung diese Entwicklung und der Einsatz dieser Chip-Karten in der Zukunft nimmt, ist nicht zuletzt auch unter datenschutzrechtlichen Perspektiven zu bewerten.

2.2.3 Überregionale Informationsdatenbanken

Medienkonzerne, Banken, wissenschaftliche Institute usw. bieten Interessierten den Zugriff auf Informationen aus von ihnen zentral gespeicherten Datenbeständen über Unternehmen und Personen an. In diesen Datenbanken werden Informationen in einem noch nie dagewesenen Umfange aus den verschiedensten bis hin zu weltweit vorhandenen Quellen zusammengeführt. Die Entwicklung zu solch immenser Konzentration von auch personenbezogenen Daten steht erst am Anfang. Es muß vermutet werden, daß mit den neueren technischen Möglichkeiten der Verarbeitung von Daten die Fülle der gespeicherten Informationen sowohl hinsichtlich der Zahl der Betroffenen als auch der Zahl der über den einzelnen Betroffenen gespeicherten Daten in allernächster Zeit erheblich zunehmen wird. Aber schon der jetzige Entwicklungsstand stellt den Datenschutz vor neue Aufgaben, die mit den vorhandenen rechtlichen Regelungen kaum noch zu lösen sind.

Es soll versucht werden, diese Entwicklung an dem Beispiel einer Informationsdatenbank eines großen Düsseldorfer Verlagshauses darzustellen.

Unter dem Werbeslogan „Wissen ist Macht" bietet dieses Unternehmen jedem Interessierten zu verhältnismäßig niedrigen Gebühren „geballtes Wissen aus vielen Quellen" an. Nach eigenen Angaben sind in der Datenbank des Unternehmens die Daten aus siebzehn verschiedenen Quellen, wie aus einer großen Wirtschaftsauskunftei, aus Tageszeitungen, Fachzeitungen, Nachschlagewerken, aus anderen in- und ausländischen und internationalen Datenbanken, aus Marketing-Dokumentations- und Informationssystemen und aus wissenschaftlichen Datenbanken, zusammengeführt. In dieser Datenbank sind die Daten aller öffentlichen Register gespeichert.

Der Benutzer kann auf sämtliche Daten sowohl im On-line-Verkehr mittels PC, über Btx oder per Telefon über einen Tonkoppler direkt, als auch über schriftliche Anforderung von Einzel- oder Sammelauskünften zugreifen. Durch die Verknüpfung der Vielzahl der Daten aus den unterschiedlichsten Quellen und den damit einhergehenden Verwertungsmöglichkeiten ergibt sich ein weitgehender Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, der weder gesellschaftspolitisch noch verfassungsrechtlich hingenommen werden kann.

Aus datenschutzrechtlicher Sicht ergeben sich zusätzliche Bedenken durch die Möglichkeiten des Direktabrufes der Daten. Das gilt insbesondere für die aus öffentlichen Registern und aus den Beständen von Auskunfteien gewonnenen Daten, soweit deren Übermittlung schon nach jetziger Rechtslage nur zulässig ist, wenn der Empfänger ein berechtigtes Interesse glaubhaft machen kann und der Übermittlung keine schutzwürdigen Belange des Betroffenen entgegenstehen, weil durch den direkten Zugriff weder das Vorliegen eines berechtigten Interesses noch das Vorhandensein schutzwürdiger Belange des Betroffenen geprüft werden können.

Für den hier dargestellten Fall prüfe ich zur Zeit im Zusammenwirken mit der für die Informationsdatenbank zuständigen Aufsichtsbehörde, wie nach dem jetzt geltenden Recht unerlaubte Datenspeicherungen und -übermittlungen verhindert werden können.

Der Gesetzgeber bleibt jedoch aufgerufen, das Datenschutzrecht so zu gestalten, daß den sich hier ergebenden Gefahren für die Wahrung des informationellen Selbstbestimmungsrechts wirksam begegnet werden kann.

3. Kooperationen

3.1 Kooperation mit dem Datenschutzausschuß der Bremischen Bürgerschaft (Landtag)

An den Sitzungen des Datenschutzausschusses der Bürgerschaft (Landtag) nahm ich beratend teil.

Themen der Sitzungen waren u. a.:

— 7. Jahresbericht des Landesbeauftragten

— 8. Jahresbericht des Landesbeauftragten

  — Stellungnahme des Senats

  — Bericht des Datenschutzaussschusses

— Aktuelle Datenschutzprobleme auf Bundesebene

— Novellierung des Bremischen Datenschutzgesetzes

— Software-Fehler und ihre Erkennung
(Ref. von Prof. Dr. Belli von der Hochschule Bremerhaven)

— Vertretung des Landesbeauftragten

— Schufa-Klausel

— Meldedatenübermittlungsverordnung

Der Datenschutzausschuß der Bremischen Bürgerschaft (Landtag) hat sich im Berichtszeitraum in mehreren Sitzungen sehr ausführlich mit meinem 8. Jahresbericht befaßt und zu den einzelnen Punkten die zuständigen Behördenvertreter hinzugezogen, so daß bereits im Vorfeld verschiedene Datenschutzprobleme gelöst werden konnten.

Folgende datenschutzrechtliche Fragen waren im letzten Jahr Gegenstand von Anfragen und Plenardiskussionen in der Bürgerschaft (Landtag):

Plenarsitzung	Antrag- und Fragesteller, Mitteiler	Fundstelle	Gegenstand
26. 02. 1986	Senat	Drs. 11/559	Gesetz zu dem Staatsvertrag über die Vergabe von Studienplätzen
26. 02. 1986	GRÜNE	PlPr 11/49	Zustimmung des Innensenators für ein einheitliches Polizeigesetz
27. 02. 1986	CDU	Drs. 11/573	Sicherheitsgesetze des Bundes
27. 02. 1986	SPD	Drs. 11/759	Sicherheitsgesetze des Bundes
27. 02. 1986	GRÜNE	Drs. 11/578	Sicherheitsgesetze des Bundes
19. 03. 1986	CDU	Drs. 11/599	Datenverarbeitung in der Justiz
28. 04. 1986	CDU	PlPr 11/53	Ausgleich für die Verlegung des Landesamtes für Datenschutz von Bremerhaven nach Bremen
29. 04. 1986	LfD	Drs. 11/589	8. Jahresbericht des LfD
01. 07. 1986	CDU	PlPr 11/57	Verlegung des Landesamtes für den Datenschutz von Bremerhaven nach Bremen
03. 09. 1986	Senat	Drs. 11/679	Stellungnahme des Senats zum 8. Jahresbericht des LfD
03. 09. 1986	CDU	PlPr 11/59	angebliche Haushaltseinsparungen durch Verlegung des Landesamtes für den Datenschutz
03. 09. 1986	Senat	Drs. 11/682	Gesetz zur Änderung des Bremischen Wassergesetzes
01. 10. 1986	SPD	PlPr 11/61	Datenschutz beim Arbeitsamt Bremen
05. 11. 1986	CDU	Drs. 11/757	Maßnahmen gegen die Ausbreitung von AIDS
06. 11. 1986	Senat	Drs. 11/733	Gesetz über die Ausstellung von Vertretungsbescheinigungen
03. 12. 1986	GRÜNE	Drs. 11/759	Gentechnologie und Fortpflanzungstechniken
28. 01. 1987	DS-Ausschuß	Drs. 11/770	Bericht/Antrag des DS-Ausschusses zum 8. Jahresbericht des LfD

3.2 Mitarbeit im ADV-Ausschuß (AADV) Bremen

Gemäß der ADV-Anweisung vom 21. September 1981 werde ich zu den Sitzungen des ADV-Ausschusses eingeladen. An den Sitzungen nehme ich mit beratender Stimme teil. Im Berichtsjahr wurden u. a. folgende Themen behandelt:

— Einsatz von ADV in den bremischen Häfen — Hauptuntersuchung

— Einsatz von ADV für Wahlen und Volkszählung im Statistischen Landesamt

— Verschiedene Sachstandsberichte zum Projekt „PROSOZ" (Programmierte Sozialhilfe)

— DEMOS-Verfahren (Dezentrales Einwohner-Melde-On-line-System)

— Maschinelle Führung und Pflege der Müllgefäßdatei

— Automatisierte Überwachung und Abrechnung bei der Abwasser-Sammelgrubenentleerung und Fäkalschlammabfuhr aus Kleinkläranlagen

— ISA-Bürokommunikation (ISA-BK) — Hauptuntersuchung —

— Automatisiertes Vollstreckungsregister und Schuldnerverzeichnis (AVUS)

— Einsatz eines PC bei der Marktverwaltung im Stadt- und Polizeiamt

— ADV-Unterstützung für die steuerliche Außenprüfung

— ADV-Geräteausstattung in der zentralen Vollstreckungsstelle des Finanzamtes Bremen-Mitte

— Automationsunterstützung bei Neuorganisation der Finanzämter.

Die in der Übersicht aufgeführten Verfahren enthalten allesamt Beschaffungsanträge von PC's. Diese Beschaffungen werden für isolierte, autonome ADV-Anwendungen und zum Teil in Verbindung mit dem zentralen Rechner des RbV vorgesehen. Bezeichnend war, daß keines der genannten Projekte bei Antragstellung ein Datenschutzkonzept aufwies. Die Anmerkungen „Einsatz von Security-Software", „der Landesbeauftragte wird beteiligt" oder „die Datenschutzbestimmungen werden beachtet" waren die einzigen Hinweise auf die inzwischen hinlänglich bekannte Problematik hinsichtlich des Datenschutzes und der Datensicherheit bei Einsatz von Arbeitsplatzrechnern (PC's). Aus diesen allgemeinen Bemerkungen schließe ich, daß eine datenschutzrechtliche Prüfung der Zulässigkeit der verschiedenen Phasen wie Speicherung, Übermittlung, Zugriff bis zur Antragstellung nicht erfolgt ist. Zwar wurden die Projekte detailliert beschrieben; aus der Beschreibung war auch der Wille zu entnehmen, diese Vorhaben nicht weiter auszuweiten.

Ich muß jedoch feststellen, daß solche Beschreibungen Einzelaussagen bleiben, deren Verbindlichkeit nicht eingelöst werden kann, solange der Senat kein Konzept über Umfang und Wirkung der integrierten Bürokommunikation im Lande Bremen vorgelegt hat.

Erst nach Vorlage eines solchen Konzeptes bin ich in der Lage, das Ausmaß der Datenvernetzung im Lande Bremen zu beurteilen.

Ich möchte in diesem Zusammenhang nochmals darauf hinweisen, daß die Institution des AADV für mich eine wichtige Informationsquelle für geplante ADV-Verfahren darstellt. Häufig erfahre ich hier erstmalig von datenschutzrelevanten Projekten. Ich halte die frühzeitige Beteiligung meiner Behörde aus gestalterischen wie ökonomischen Gründen für unverzichtbar.

Für den Bereich der Stadtgemeinde Bremerhaven und die sonstigen öffentlichen Stellen mit eigenständiger Datenverarbeitung gibt es nur selten Hinweise auf neue ADV-Verfahren oder Bitten um Datenschutzberatung. Ich kann hier meiner gesetzlichen Aufgabe in der Regel nur durch nachträgliche und aufwendige Prüfungen nachkommen.

3.3 Kooperationen mit den Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz

In Sitzungen und Arbeitskreisen der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz wurden u. a. folgende Problemschwerpunkte erörtert:

— Präsentation des Zentralen Verkehrsinformationssystems (ZEVIS) und Besprechung von Datenverarbeitungsproblemen beim Kraftfahrtbundesamt in Flensburg

— Datenschutz- und Sicherheitsgesetze der Bundesregierung

  — Novellierung BDSG und Verwaltungsverfahrensgesetz

  — Bundesverfassungsschutzgesetz

  — MAD-Gesetz

  — Zusammenarbeitsgesetz (ZAG)

  — Änderung des Straßenverkehrsgesetzes (ZEVIS)

  — Paß- und Personalausweisgesetz

  — Änderung des § 163 d StPO

— Telekommunikatitonsordnung

— Datenschutz im Krankenhaus

— Melderechtsfragen, insbesondere Meldedatenübermittlungsverordnung des Bundes

— Justizmitteilungsgesetz

— Archivgesetz

— Personenstandsgesetz

— Überlegungen zur Informationsverarbeitung im Strafverfahren

— Ausländerzentralregister

— Bundesstatistikgesetz

— Volkszählung 1987.

Beschlußfassungen zu den vorgenannten Punkten sind je nach Aktualität als Presseerklärungen zur Veröffentlichung freigegeben worden. Zu Einzelpunkten verweise ich auf Pkt. 5 dieses Berichts und die im Anhang abgedruckten Anlagen.

3.4 Kooperation mit den Obersten Aufsichtsbehörden für den Datenschutz

Wie in den Vorjahren wurde auch im Berichtszeitraum die Zusammenarbeit mit den Obersten Aufsichtsbehörden für den Datenschutz im Rahmen der zweimal jährlich stattfindenden Sitzungen des „Düsseldorfer Kreises" fortgesetzt.

U. a. wurden hierbei folgende Problempunkte erörtert:

— Kreditwirtschaft

  — Schufa-Klausel für Kreditanträge, Konteneröffnungsanträge bzw. Bürgschaftserklärungen

  — Schufa-Merkblatt

  — Schufa-Vertragspartner

  — Schufa-Merkmale

  — Information der Mitarbeiter der Kreditinstitute über das Schufa-Meldeverfahren

  — Schreiben an Altkunden

  — Mögliche Auswirkungen des Verfahrens vor dem Bundeskartellamt

  — Widerspruch gegen die Schufa-Klausel (Merkmal WK) bei Giroverträgen

— Versicherungswirtschaft

  — Schweigepflichtentbindungsklausel

  — Ermächtigungsklausel

  — Verwendung von Match-Codes in der Rechtsschutzversicherung

  — Verwendung von Doppelpostkarten bei Versicherungsanfragen an die Polizei

— Handelsauskunfteien

— Versandhandel

— Adreßverlage und Direktwerbeunternehmen

  — Vermarktung von Adressen von Bewohnern der DDR

— Bildschirmtext

  — Datenschutzrechtliche Probleme (Erfahrungsaustausch)

  — Btx-Staatsvertrag und neue bereichsspezifische Regelungen des Bundes.

Nähere Ausführungen zu einzelnen in der Übersicht aufgeführten Problemkreisen siehe unter Pkt. 6 dieses Berichtes.

3.5 Kooperation mit Kammern, Verbänden, sonstigen Institutionen

Auch in diesem Berichtsjahr habe ich die Kontakte zu bremischen Kammern, Verbänden und sonstigen Institutionen gepflegt. Dies gilt für den Erfa-Kreis Bremen (Erfahrungsaustausch von betrieblichen Datenschutzbeauftragten) ebenso wie für eine Vielzahl von bremischen Kammern, Verbänden, Gewerkschaften, Parteien etc. sowie Schulen, Hochschulen, Volkshochschulen und anderen Weiterbildungseinrichtungen im Lande Bremen. Neben schriftlichen, mündlichen oder telefonischen Stellungnahmen zu datenschutzrechtlichen Fragen ging es dabei häufig auch um den Wunsch, einen Vortrag zu halten oder an einer Podiumsdiskussion teilzunehmen. Ich bin immer bemüht, diesen Anforderungen — so gut es geht — nachzukommen, da ich mir hiervon einen notwendigen Erfahrungsaustausch und die Weitervermittlung des Datenschutzgedankens verspreche.

4. Eingaben und Beschwerden, Registerführung

4.1 Eingaben und Beschwerden

Im Berichtsjahr hatte ich insgesamt 125 **schriftliche** Eingaben und Beschwerden zu bearbeiten. Davon bezogen sich 66 auf öffentliche und 59 auf nicht-öffentliche Stellen. Dabei sind die Fälle, bei denen sich mehrere Petenten bezüglich eines Sachverhaltes beschwert haben, nur einfach gezählt worden. Darunter sind mehrere Beschwerden, die im Einzelfall bis zu 20 Beschwerdeführer hatten.

Daneben erreichten mich im Berichtsjahr eine Vielzahl **mündlicher** oder **telefonischer** Anfragen, Hinweise oder Beratungsersuchen, die zum größten Teil sofort, zum Teil aber auch erst nach weitergehender Sachaufklärung oder örtlicher Prüfung schriftlich erledigt wurden. Die Gesamtzahl dieser Eingaben und Beschwerden ist gegenüber dem Vorjahr leicht gestiegen. Auf genaue Statistik hierüber ist aus arbeitsökonomischen Gründen verzichtet worden.

Der Großteil der Eingaben und Beschwerden aus dem nicht-öffentlichen Bereich betraf Auskunfteien, Adreßhandel, Banken, Versicherungen und Telefondatenerfassung am Arbeitsplatz; einige betrafen auch völlig neuartige Sachverhalte, wie z. B. die Einrichtung eines privaten Mailbox-Systems oder das Angebot von Diensten der Auskunftei über Btx. Auch die bevorstehende Volkszählung führte im Berichtsjahr zu vielen Anfragen und Informationsersuchen.

4.2 Register der meldepflichtigen Stellen

Das Register der meldepflichtigen Stellen gemäß § 39 BDSG umfaßte Ende 1986 insgesamt 109 Eintragungen. Eine Unterteilung nach Art der meldepflichtigen Tätigkeiten sowie der regionalen Ansiedlung im Lande Bremen zeigt folgendes Bild:

Art der Tätigkeit	Insgesamt	Bremen	Bremerhaven
1. Kredit- und Handelsauskunfteien	11	8	3
2. Markt- und Meinungsforschungsinstitute	3	3	—
3. Adreßbuchverlage	3	2	1
4. Datenverarbeitung im Auftrag	92	82	10
davon:			
— Datenerfassungsbetriebe	16	16	—
— Service-Rechenzentren	37	34	3
— DV für verbundene Betriebe	20	17	3
— DV für sonstige Dritte	17	13	4
— Datenlöschung und -vernichtung	2	2	—
Insgesamt	109	95	14

Die Anzahl der meldepflichtigen Stellen hat sich gegenüber dem Vorjahr nicht verändert. Die zunehmende Verbreitung von kleinen und mittleren Datenverarbeitungssystemen im Bereich der privaten Wirtschaft läßt vermuten, daß nicht immer die Meldepflicht gemäß § 39 BDSG beachtet wird.

4.3 Dateienregister

Ende 1986 waren zum Dateienregister des öffentlichen Bereichs insgesamt 1496 (logische) Dateien gemeldet; gegenüber 1985 hat sich damit praktisch keine Veränderung ergeben. Auch die Aufschlüsselung nach manuellen und maschinellen Dateien hat sich nicht wesentlich verändert. Dies ist insofern erstaunlich, als auch im Bereich der öffentlichen Verwaltung im Lande Bremen (Land, Kommunen sowie ihrer Aufsicht unterstehende Körperschaften des öffentlichen Rechts) die automatisierte Datenverarbeitung sich weiter ausbreitet.

Auch hier vermute ich im gewissen Umfang eine Nichtbeachtung der datenschutzrechtlichen Meldepflichten.

5. Öffentlicher Bereich

5.0 Datenschutz beim Einsatz von Arbeitsplatzrechnern

In zunehmendem Maße wird die öffentliche Verwaltung im Lande Bremen mit autonomen Rechnern und Rechnersystemen am Sachbearbeiter-Arbeitsplatz ausgestattet. Angestrebt wird eine integrierte Bürokommunikation, d. h., die Vernetzung der einzelnen Rechner untereinander und der Verbund mit den Rechnern in den zentralen Rechenzentren der Verwaltungen (siehe auch 8. Jahresbericht unter Pkt. 2.2.1.2, S. 19 f.).

Sowohl die Planung als auch der Einsatz werden heute noch im wesentlichen unter rein ökonomischen Gesichtspunkten vorgenommen. Die öffentliche Verwaltung kann zur Lösung ihrer Aufgaben aber nicht nur die Rationalisierung und Kostendeckung sehen, sondern sie trägt auch die Verantwortung gegenüber den besonderen Belangen unserer Bürger, sie trägt auch die Verantwortung für die soziale Beherrschung der Systeme und ist aufgerufen, den Einsatz menschengerecht zu gestalten. Die Wirtschaftlichkeitsbetrachtung des Rechnereinsatzes und die menschengerechte Technikgestaltung schließen sich — gesamtwirtschaftlich betrachtet — nicht aus.

Die Entwicklung der Datenverarbeitung, insbesondere der Informations- und Kommunikationstechniken, wird ebenfalls unter dem Gesichtspunkt des ökonomischen Einsatzes betrieben. Dabei spart man von Hersteller- und Anwenderseite nicht mit Begriffen wie „Humanisierung der Arbeitswelt", „Sicherheit der Daten" oder ähnliches. Schaut man jedoch hinter die Konzepte solcher „sozialen" Verkaufsargumente, so stellt man sehr schnell fest, daß mit Rücksicht auf ein besseres Preis-/Leistungsverhältnis sowohl von seiten der Hardware als auch der Software wenig für den Menschen getan wurde. Das gleiche gilt auch für den Datenschutz, dem nur beiläufige Aufmerksamkeit geschenkt wurde. Die Nennung der Begriffe reicht nicht aus, wenn die Durchführung an der ausschließlich technischen und ökonomischen Grundlage zur Entwicklung von Arbeitsplatzrechnern scheitert.

Ich habe in meinem 8. Jahresbericht in den Vorbemerkungen zu Pkt. 5, S. 28 schon eindringlich auf die Notwendigkeit eines Datenschutzkonzeptes für Arbeitsplatzrechner hingewiesen, stelle jedoch fest, daß ein solches Konzept bisher nicht vorliegt, obwohl sich sowohl Installationen als auch die Benutzung von Arbeitsplatzrechnern rasant ausweiten.

Inzwischen ist zwar zwischen dem Rechenzentrum der bremischen Verwaltung (RbV) und mir eine sogenannte Systemakte diskutiert worden. Ich sehe diese Systemakte als einen ersten Schritt zu einer Einsatzregelung, stelle jedoch fest, daß noch nicht einmal diese technische Begleitakte eingeführt wurde.

Die Stadtgemeinde Bremerhaven hat nach meinen Informationen noch keinerlei Überlegungen dazu angestellt.

Ich halte diesen Zustand für untragbar. Wenn schon die Hersteller den Datenschutz vernachlässigen, so muß aus der Verantwortung der öffentlichen Verwaltung heraus der Schutz und die Sicherheit personenbezogener Daten wenigstens durch umfassende organisatorische Regelungen gewährleistet werden.

5.1 Personalwesen

5.1.1 Schwerpunkte, Handlungsbedarfsfälle

5.1.1.1 PAADIS

Wie in meinem 7. Jahresbericht unter Pkt. 5.1.1.2, S. 18 ff. dargestellt, beabsichtigt die Senatskommission für das Personalwesen (SKP), das Abrechnungsverfahren

für Besoldung, Vergütung, Lohn und Versorgung einer erweiterten Automatisierung zuzuführen. Der Projektname PAADIS ist die Abkürzung für Personaldaten-, Änderungs- und Abrechnungsdialog-Service.

PAADIS ist ein Dialogverfahren, das in seiner ersten Stufe den herkömmlichen Änderungsdienst zu den monatlichen Personalabrechnungen ablösen soll. Es handelt sich um ein datenbankorientiertes Verfahren, das mit dem im Rechenzentrum der bremischen Verwaltung (RbV) installierten Datenbanksystem ADABAS und der Programmiersprache NATURAL entwickelt und auch eingesetzt wird.

Aus den von der SKP zur Verfügung gestellten Unterlagen der Grobdarstellung des Verfahrens ergibt sich, daß PAADIS im wesentlichen folgende Aufgaben erfüllen soll:

— maschinelle Feststellung der zahlungsrelevanten Daten der im öffentlichen Dienst Beschäftigten und der Versorgungsempfänger

— Berechnung der Bruttobezüge und aller damit verbundenen Nebenfunktionen

— Änderungsdienste und Führen der Lohn-, Besoldungs-, Vergütungs- und Versorgungskonten

— Zahlbarmachung der Bezüge/Vorschüsse

— Prüfung der dem Stellenplan entsprechenden Stellenbewirtschaftung bei Einstellung, Umsetzung und Versetzung

— Rechnungslegung zur Ermöglichung der Personalausgabenprüfung, Jahresabschlußarbeiten

— regelmäßige Datenübermittlung nach gesetzlichen Vorschriften, im wesentlichen durch Datenträgeraustausch.

Neben diesen Aufgaben soll PAADIS andere Aufgaben übernehmen, wie sie bisher vom PIS (sog. Personalinformationssystem) zur Bereitstellung von Hilfen für die Personalverwaltung (Personal- und Stellenstruktur) vorgenommen werden, wie auch andere Verfahren mit Daten speisen, wie es etwa für ASteV (Automatisiertes Stellenverzeichnis) vorgesehen ist. Nach Darstellung der SKP stellt PAADIS in seinen Hauptaufgaben keine Änderung oder Erweiterung der bisherigen Aufgabenstellung dar. Jedoch erhält die Lösung der Aufgaben durch die Umstellung auf das Dialogverfahren eine andere Qualität. Hiermit soll eine sachbearbeiterunterstützende und aktuellere Datenerhebung und -pflege für die Personalabrechnung ermöglicht werden.

Beteiligt sollen im wesentlichen die anweisenden Stellen sein, nach Exstallation des Seitenlesers im RbV evtl. auch große Personalstellen. Mit der direkten Einbeziehung der anweisenden Referate in das automatisierte Personalabrechnungsgeschehen können, wie aus den Unterlagen der SKP ersichtlich, einige bisher manuell geführte Karteien und Personalakten aufgelöst werden.

Vorgesehen ist eine zentrale Datenverarbeitung im Datenbankverfahren ADABAS im RbV mit dezentralen Terminals ohne eigene Speicherkapazitäten.

Hinsichtlich der Schnittstellen, On-line-Zugriffe dritter Stellen und der regelmäßigen Datenübermittlungen an Dritte, ist zu sagen, daß durch das Datenbankverfahren eine einfachere Verknüpfung zu anderen direkt zugreifbaren Dateien und Datenbanken gegeben ist. Insbesondere die Schnittstellen mit PIS, ASteV und zur Landeshauptkasse wie auch die Massendatenübermittlungen im Zuge des Meldeverfahrens nach DEVO/DÜVO im Datenträgeraustausch und andere regelmäßige Datenübermittlungen bedürfen meiner besonderen Aufmerksamkeit.

Ich habe dazu eine Stellungnahme abgegeben. Sie enthält im wesentlichen folgende Punkte:

Da das Verfahren PAADIS so angelegt ist, daß Schnittstellen zu anderen EDV-Verfahren angelegt sind, setzt die datenschutzrechtliche Würdigung auch die Einbeziehung der anderen Verfahren voraus.

Unter Zugrundelegung der speziellen rechtlichen Voraussetzungen, die die Aufgabenstellung der SKP tangieren, müssen die Datenschutzüberlegungen zwei Linien folgen. Einmal müssen bei der weiteren Entwicklung von PAADIS die datenschutzrechtlichen Belange der Personengruppen Arbeiter, Angestellte, Beamte und Versorgungsempfänger berücksichtigt werden, soweit deren personen-

bezogene Daten zu den o. g. Zwecken verarbeitet werden sollen. Zum anderen sind die Belange der mit der Verarbeitung dieser Daten beauftragten Beschäftigten bei der SKP und im RbV in diesem Zusammenhang zu berücksichtigen.

Hinsichtlich der Datenschutzanforderungen bezüglich der im öffentlichen Dienst Beschäftigten und Versorgungsempfänger ist hervorzuheben, daß die Verantwortung für das gesamte Verfahren PAADIS auch hinsichtlich der Durchführung beim RbV die SKP trifft. Hier kommt insbesondere den Anforderungen, die das Gesetz an die speichernde Stelle stellt, besondere Bedeutung zu. Weiter wird eine genaue Beschreibung der Organisation und der Zuständigkeiten innerhalb der SKP erforderlich. Eine Funktionstrennung durch Aufbau funktionaler Informationsschranken ist vorzusehen; dabei sind auch Vertretungsregelungen entsprechend der abgeschlossenen Organisationseinheiten, Verantwortlichkeiten und Zugriffsberechtigungen festzulegen. Auch die Möglichkeiten der dienstrechtlichen und technischen Ausgestaltung sind zu berücksichtigen. Inwieweit eine Abgrenzung nach Buchstaben oder betroffenem Personenkreis sinnvoll ist, bedarf noch weiterer Überlegungen. Der Umfang der bei der Verarbeitung verwendeten Daten bleibt einer späteren Untersuchung vorbehalten. Ich setze voraus, daß der bisher gemeldete Katalog von Grunddaten nicht erweitert wird. Welche Daten für den jeweiligen Arbeitsschritt benötigt werden und insbesondere auch die Umsetzung auf Bildschirm-Matrix, bleibt dem Feinkonzept vorbehalten. Da das Speichern und Verändern personenbezogener Daten nur zulässig ist, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist, ist es notwendig, daß jedes personenbezogene Merkmal in PAADIS darauf überprüft wird, ob für die Verarbeitung eine personalrechtliche Vorschrift vorhanden ist und ob die Speicherung dafür auch erforderlich ist. Daher dürfen dem einzelnen Arbeitsbereich nicht mehr Daten, als für die spezielle Sachbearbeitung nötig, zur Verfügung gestellt werden, d. h., Merkmale dürfen nicht generell erhoben und gespeichert werden, wenn sie nur für einen Teil der Beschäftigten erforderlich sind. Auch muß die Frage der Erforderlichkeit für jede einzelne Phase der Datenverarbeitung geprüft werden.

Bei Versetzungen oder Abordnungen muß das Verfahren so ausgestaltet sein, daß keine ungeprüfte Übernahme von Daten aus anderen senatorischen Dienststellen stattfindet.

Hinsichtlich anonymisierter oder kumulativer Auswertungen bedarf es spezieller datenschutzrechtlicher Anforderungen, die noch in Abstimmung mit den Belangen der SKP zu formulieren sind.

Weiter ist ein Verfahren zu entwickeln, das sicherstellt, daß die Rechte der Betroffenen nach den Datenschutzgesetzen, insbesondere Auskunft, Sperrung, Berichtigung und Löschung, sowohl bezüglich der Personalakte als auch bezüglich der Dateien gewährleistet sind.

Hinsichtlich des Datenschutzes der Beschäftigten, die mit PAADIS arbeiten, gilt es, die Zweckbindung der Eingabe- und Prüfprotokolle sicherzustellen. Insbesondere muß gewährleistet sein, daß die durch den On-line-Betrieb anfallenden Protokollierungen nicht zur Erstellung von Leistungsprofilen oder zur Durchführung von Anwesenheits- und Arbeitskontrollen genutzt werden.

Weiterhin ist für das Gesamtverfahren erforderlich, daß die in der Anlage zu § 6 der Datenschutzgesetze formulierten Datensicherungsmaßnahmen beachtet werden und für PAADIS zu einem konkreten Paket von Datensicherungsmaßnahmen in den verschiedenen Phasen der Verarbeitung zusammengefaßt und umgesetzt werden.

Schließlich ergeben sich als Folge des Dialogverfahrens, das gegenüber dem Stapelverfahren ein erhöhtes Datenschutzgefährdungspotential darstellt, spezielle Datenschutzanforderungen. Gleiches gilt für die Anwendung von ADABAS und NATURAL. Da insbesondere unter Berücksichtigung des angewandten Datenbanksystems mit relativ niedrigem Arbeitsaufwand und Kenntnisstand verschiedenste Verknüpfungen, aber auch Selektierungsarbeiten aus dem Datenbestand vorgenommen werden können, eine flexible Anwendung also technisch möglich ist, bedarf es besonderer Sicherheitsvorkehrungen, um solchen Gefahren entgegenzuwirken. Meine Anregungen bezogen sich auf Dateien-, Transaktions-, Bildschirm-, Zugriffs- und Programmschutz.

Wegen der eingangs erwähnten Schnittstellenproblematik und der damit geöffneten vielseitigen Verwendungsmöglichkeit einzelner Daten durch Zweckände-

rung oder -erweiterung bedarf es eines eigenständigen Datenschutzkonzeptes, das noch von der SKP zu erarbeiten ist.

Nicht zuletzt wegen der komplexen Materie eines solchen Verfahrens müssen für die Datenschutzkontrolle von der speichernden Stelle flankierende Maßnahmen ergriffen werden, die mir eine effektive Datenschutzkontrolle ermöglichen.

5.2 Inneres

5.2.1 Innere Sicherheit

5.2.1.1 Schwerpunkte, Handlungsbedarfsfälle

— Anhörung des Innenausschusses zur Änderung des Bundesverfassungsschutzgesetzes und zum Entwurf eines Gesetzes über den Militärischen Abschirmdienst

Am 28. April 1986 fand eine öffentliche Anhörung des Innenausschusses zur Änderung des Bundesverfassungsschutzgesetzes und zum Entwurf eines Gesetzes über den Militärischen Abschirmdienst statt. Die Entwürfe zu den beiden Gesetzen gehörten zu dem sogenannten Sicherheitspaket, das die Bundesregierung in der letzten Legislaturperiode eingebracht hat.

Meine Stellungnahme bezog sich auf folgende Themenbereiche:

— Erforderlichkeit gesetzlicher Informationsverarbeitungsregelungen beim Bundesverfassungsschutz und MAD

— Anforderungen an die wehrhafte Demokratie aus der Entscheidung des Grundgesetzes

— Aufgabenbeschreibung und Befugnisnormen

— Trennungsgebot

— Nachrichtendienstliche Mittel

— Rechtsweggarantie, Klagemöglichkeit und Auskunftsrechte des Bürgers

— Gegenseitige Unterrichtung der Verfassungsschutzämter

— Gemeinsame Datenbestände und Textzusätze

— Wird die föderale Ordnung durch den Entwurf beeinträchtigt?

— Sicherheitsüberprüfungen

— Zweckbindung

— Veröffentlichung von personenbezogenen Daten

— Schaffen Verfahrensvorschriften neue Datenschutzrisiken?

— Anmerkungen zum Entwurf des MAD-Gesetzes und Abgrenzung zum Verfassungsschutz

— Regelungen für die Datenverarbeitung in Akten

— Speicherung von Daten unverdächtiger Bürger.

Den vollständigen Wortlaut meiner Erklärung habe ich als Anlage 3 zu diesem Bericht abgedruckt.

— ISA-BK

Der Senator für Inneres hat beim Projektträger „Humanisierung des Arbeitslebens" einen Antrag gestellt, ihn bei der Einführung der computergestützten Sachbearbeitung im Polizeidienst des Landes Bremen zu unterstützen. Das Projekt soll zunächst als Pilotprojekt in den Kommissariaten 20, 21 und 22 in Bremen-Nord entwickelt werden. Das heutige ISA-System (Informationssystem Anzeigen) ist Ausgangspunkt für das Vorhaben der Entwicklung eines neuen Systems der computergestützten Sachbearbeitung im Polizeidienst. Dabei ist DV-technisch die Integration bzw. der Dialog verschiedener Informationssysteme zwischen dem zentralen Bürokommunikationssystem und den zentral geführten Datenbanken, wie z. B. ISA, INPOL, Fazid, AZR, BZR, DEMOS und ZEVIS vorgesehen. Spezifika des Bremer Modellvorhabens sollen sein zu versuchen, ein flexibles Netz zu entwickeln, das unterschiedliche Mitarbeitergruppen, Aufgabenbereiche, Hierarchie-

ebenen und Standorte einer Behörde verknüpft und über eine einheitliche Schnittstelle den Zugriff des Benutzers auf unterschiedliche Funktionen von Standardsoftware und zugleich auf interne/externe, zentrale/dezentrale, örtliche/überörtliche Datenbanken ermöglicht.

Der Projektansatz macht deutlich, daß eine intensive Datenschutzberatung erforderlich sein wird. Schon jetzt kann absehbar erklärt werden, daß die personelle Situation meiner Dienststelle es nicht erlauben wird, dieses komplexe System unter datenschutzrechtlichen Gesichtspunkten zu begleiten oder gar ein Datenschutzkonzept zu entwickeln. Wenn sich der Innensenator entschließt, ein solch komplexes System als Pilotprojekt nach Bremen zu holen, so muß dafür Sorge getragen werden, daß die zur Begleitung erforderlichen personellen Kapazitäten in meiner Dienststelle geschaffen werden. Eine datenschutztechnische Beratung von anderer Seite kann als ergänzende Maßnahme sicherlich begrüßt werden, beides aber, die datenschutztechnische und datenschutzrechtliche Beratung, sollte insbesondere wegen der Spezifika des Bremischen Polizeigesetzes im Lande Bremen selbst endgültig vorgenommen werden.

Nicht zuletzt dieses Projekt macht deutlich, daß in zunehmendem Maße eine hochgradig sensible Automatisierungsphase in vielen Bereichen der bremischen Verwaltung begonnen hat, ohne daß auch nur ansatzweise diese Entwicklung einhergeht mit einer Aufstockung der Kontroll- und Beratungskapazität in meinem Hause. Die Erfüllung der mir nach dem Bremischen Datenschutzgesetz obliegenden Aufgaben wird mir immer schwerer, ja fast unmöglich gemacht. Diese Entwicklung erfüllt mich mit Sorge.

— **Speicherung eines Merkmals mit dem Hinweis auf AIDS-Ansteckungsgefahr in polizeilichen Auskunftssystemen**

Bereits lange bevor das Thema in der Öffentlichkeit erörtert wurde, hatte ich mich bei dem Senator für Inneres über die im Lande Bremen geübte Praxis unterrichten lassen.

Der Senator für Inneres hat mir erklärt, daß ein Arbeitskreis der Innenministerkonferenz am 5./6. Mai 1986 beschlossen hat, daß bei Personen, die im INPOL-System gespeichert werden und bei denen der Verdacht auf eine AIDS-Erkrankung besteht bzw. bei denen eine solche Erkrankung erwiesen ist, der personenbezogene Hinweis „Ansteckungsgefahr" in der Verbindung mit der freitextlichen Anmerkung „Vorsicht Blutkontakt" aufgenommen werden soll. Die Innenministerkonferenz hat den Arbeitskreis beauftragt, unter Beteiligung der Datenschutzbeauftragten entsprechende Kriterien für eine Speicherung zu erarbeiten.

Bis zum Abschluß dieses Verfahrens werde im Lande Bremen im INPOL-System der personengebundene Hinweis „Ansteckungsgefahr" (ANST) verwandt und im Freitext auf die Gefährdung durch AIDS hingewiesen. Dieser Hinweis im INPOL-System dürfe allerdings nur dann aufgenommen werden, wenn von einem Arzt festgestellt worden ist, daß die betroffene Person AIDS-Überträger ist.

Diese Eingrenzung habe in Bremen dazu geführt, daß im INPOL-System bislang keine Speicherung dieser Art vorgenommen worden sei. Für das Bremer ISA-System gelte, daß bis zum Abschluß des Verfahrens keine Hinweise auf „ANST" bei AIDS-Gefährdung aufgenommen werden.

In den noch stattfindenden Gesprächen zwischen dem Innensenator und mir wird es entscheidend darauf ankommen, die Kriterien für eine Speicherung dieses Merkmals unter engen Voraussetzungen festzulegen. Dabei wird bei Prüfung der Erforderlichkeit und Festlegung des Personenkreises auch das mögliche Risiko für den Polizeibeamten zu berücksichtigen sein.

5.2.1.2 Kurze Darstellung von Problemen und Beschwerden

— Im Rahmen einer Eingabe hatte das Stadt- und Polizeiamt auf meine Anfrage geantwortet. Das Antwortschreiben war mir ohne Umschlag über die **Behördenbotenpost** zugeleitet worden. In diesem Antwortschreiben waren personenbezogene Daten des Betroffenen enthalten. Im Zusammenhang mit dem Betreff war für Unbefugte leicht zu erkennen, wer sich in welcher Angelegenheit bei mir beschwert hat.

Ich habe eine Beanstandung ausgesprochen, weil diese leichtfertige Offenbarung von personenbezogenen Daten einen Verstoß gegen den Verwaltungsgrundsatz der Vertraulichkeit der Bürgereingaben darstellte.

Inzwischen hat der Senator für Inneres das Stadt- und Polizeiamt angewiesen, solche Vorgänge auch dann, wenn sie auf dem behördeninternen Botenwege transportiert werden, in einem verschlossenen Umschlag weiterzuleiten.

— Eine Eingabe richtete sich dagegen, daß dem Betroffenen die Kopie eines Auszuges aus dem von ihm beizubringenden **polizeilichen Führungszeugnis** verwehrt wurde.

Das Stadt- und Polizeiamt hat mir auf Anfrage dargelegt, daß dem Betroffenen gemäß § 30 Abs. 5 Satz 2 Bundeszentralregistergesetz (BZRG) sehr wohl auf Verlangen Einsicht in sein Führungszeugnis gewährt würde. Die Anfertigung einer Fotokopie wäre jedoch nicht verpflichtende Aufgabe der Behörde. Diese Auffasung ist zutreffend.

— Ein Betroffener begehrte **Auskunft** über die bei der **Kriminalpolizei** sowie beim **Verfassungsschutz** in Bremen zu seiner Person gespeicherten Daten. Von seiten der Kriminalpolizei ist ihm mitgeteilt worden, daß Erkenntnisse über Straftaten im Zusammenhang mit politischen Aktionen vorliegen. Daraufhin hat der Betroffene Einsicht in seine Kriminalakte und Löschung aller bei der Kriminalpolizei über ihn gespeicherten Daten beantragt. Eine Einsicht in seine Kriminalakten hat die Kriminalpolizei dem Betroffenen ohne weitere Begründung verweigert, jedoch dargelegt, daß die personenbezogenen Daten rechtmäßig gespeichert seien und nicht gelöscht würden.

Nach § 15 Abs. 2 i. V. m. § 14 Abs. 2 Nr. 1 Bremisches Datenschutzgesetz (BrDSG) kann die Auskunftserteilung unterbleiben für das Landesamt für Verfassungsschutz und die Behörden der Polizei, soweit sie strafverfolgend oder im Rahmen der vorbeugenden Verbrechensbekämpfung tätig werden.

Der Betroffene hat Klage vor dem Verwaltungsgericht Bremen erhoben.

Das Urteil lag bei Redaktionsschluß noch nicht vor.

5.2.2 Meldewesen, Paß- und Ausweiswesen

5.2.2.1 Meldedatenübermittlungsverordnung des Landes

Der Senator für Inneres hat im Berichtsjahr die Arbeiten an der Verordnung zur Durchführung des Meldegesetzes, insbesondere zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden (MeldDUV) wieder aufgenommen und einen neuen Verordnungsentwurf vorgelegt. Ich habe zu diesem Entwurf ausführlich Stellung genommen. Neben einigen grundsätzlichen Ausführungen zu den Voraussetzungen für eine regelmäßige Datenübermittlung und zum Umfang der Verordnungsermächtigung habe ich dabei auch eine Reihe vorgesehener Datenübermittlungen in Frage gestellt.

So habe ich u. a. darauf hingewiesen, daß die regelmäßige Übermittlung von Meldedaten an andere Behörden eine Einschränkung des vom Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 Grundgesetz abgeleiteten Rechts auf informationelle Selbstbestimmung darstellt. Ein solcher Grundrechtseingriff ist nach diesem Urteil nur auf einer verfassungsmäßigen gsetzlichen Grundlage zulässig, aus der sich die Voraussetzungen und der Umfang der Grundrechtsbeschränkung klar und für den Bürger deutlich erkennbar ergeben müssen. Neben diesem Gebot der Normenklarheit hat der Gesetzgeber bei seinen Regelungen auch das Verhältnismäßigkeitsprinzip zu beachten. Zwar braucht er nicht jedes Detail im Gesetz selbst zu regeln, doch muß er alle wesentlichen Voraussetzungen eines solchen Eingriffs hier festlegen. Nur im Rahmen dieser Vorgaben können bei entsprechender Ermächtigung Rechtsverordnungen erlassen werden.

§ 30 Abs. 4 Bremisches Meldegesetz (BremMG) 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 Übermittlung, der Datenempfänger und der zu übermittelnden Daten bestimmt ist. Regelmäßige Datenübermittlungen, die auf einer bereichsspezifischen, den Anforderungen des Bundesverfassungsgerichts entsprechenden Rechtsgrundlage erfolgen, begegnen keinen grundsätzlichen Bedenken. Die zu erlassende Rechtsverordnung kann jedoch nicht fehlende bereichsspezifische Rechtsgrundlagen ersetzen oder schaffen.

Das ergibt sich schon daraus, daß der Verordnungsgeber nach der Vorschrift des § 36 Abs. 2 BremMG nur zum Erlaß von Regelungen zur Durchführung regel-

mäßiger Datenübermittlungen ermächtigt ist, nicht aber zum Erlaß von Vorschriften, die das Recht auf informationelle Selbstbestimmung einschränken. Eine solche Ermächtigung kann auch nicht der Bestimmung des § 36 Abs. 2 Nr. 2 BremMG entnommen werden, wonach u. a. Anlaß und Zweck der regelmäßigen Übermittlungen festzulegen sind. Diese Bestimmung kann nur als Gebot für die Bestimmtheit, in der die Verordnung zu fassen ist, gesehen werden. Da es sich beim Recht auf informationelle Selbstbestimmung um ein Grundrecht handelt, wäre eine weitergehende Ermächtigung auch nicht verfassungskonform.

Nach Art. 67 der Bremischen Landesverfassung steht die gesetzgebende Gewalt ausschließlich dem Volke (Volksentscheid) und der Bürgerschaft zu. Nach Art. 124 der Landesverfassung erläßt der Senat die zur Ausführung eines Gesetzes erforderlichen Rechts- und Verwaltungsverordnungen. Eine Regelungsbefugnis in Richtung einer Einschränkung des informationellen Selbstbestimmungsrechts ist dem Senat entzogen.

In den Fällen, in denen eine gesetzliche Regelung, die die Datenverarbeitung durch den Datenempfänger erlaubt und die den Anforderungen des Bundesverfassungsgerichts entspricht, nicht vorliegt, kann gegebenenfalls der sogenannte Übergangsbonus geltend gemacht werden, da sich das Gesetzeserfordernis erst aufgrund eines gewandelten und spezifizierten Verfassungs- und Grundrechtsverständnisses ergeben hat. Die sich daraus ergebende Zulässigkeit von Eingriffen in das informationelle Selbstbestimmungsrecht ohne ausreichende gesetzliche Ermächtigung für eine Übergangszeit ist jedoch an den von der Rechtsprechung und Lehre herausgearbeiteten Voraussetzungen zu messen. Danach muß die Legitimation von Eingriffen in Grundrechte die Ausnahme bleiben und ist an die Bedingung gebunden, daß die bisherige Praxis nicht ohne gravierende Nachteile für das Gemeinwohl (z. B. Funktionsunfähigkeit staatlicher Einrichtungen) aufgegeben werden kann. Keineswegs darf mit der Figur des Übergangsbonus eine neue, bisher nicht vorhandene regelmäßige Datenübermittlung begründet werden. Zu bemerken bleibt, daß die Übergangszeit dann als abgelaufen angesehen werden muß, wenn der Gesetzgeber das einschlägige Gesetz novelliert und keine ausreichende, den Eingriff erlaubende Vorschrift schafft.

Vor dem Hintergrund dieser Überlegungen habe ich vor allem die regelmäßigen Datenübermittlungen im Wege eines automatisierten Direktabrufs in Frage gestellt. Derartige Datenübermittlungen stellen nach meiner Auffasung einen besonders gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung der meldepflichtigen Einwohner dar, der sich von den übrigen Fällen einer regelmäßigen Datenübermittlung dadurch unterscheidet, daß die Zugriffe bzw. Abrufe ohne Einschaltung der Meldebehörde, sozusagen in „Selbstbedienung" des Datenempfängers, d. h. ohne vorherige Zulässigkeitsprüfung durch die Meldebehörde (wie in § 30 Abs. 1 und 2 BremMG gefordert) erfolgen und außerdem der gesamte Einwohnerdatenbestand, evtl. eingegrenzt auf bestimmte Datenfelder, ständig während der Einschaltzeit des technischen Systems im Zugriff bzw. zum Abruf bereitgehalten wird. Ein so gravierender Eingriff in das Recht auf informationelle Selbstbestimmung bedarf einer besonderen zusätzlichen Rechtfertigung, um ihn gegenüber den anderen Übermittlungsfällen zu begründen. Arbeitserleichterung der betroffenen Behörden oder Fortsetzung einer unter altem Recht entstandenen Praxis allein können solche Eingriffe nicht rechtfertigen. Es müssen zusätzliche, aus dem überwiegenden Allgemeininteresse herleitbare Erfordernisse vorliegen, die vom Gesetzgeber anerkannt wurden.

Bei keiner der im Verordnungsentwurf genannten Behörde habe ich den automatisierten Direktabruf von Meldedaten für zulässig gehalten. Im einzelnen habe ich hierzu ausgeführt:

Die **Finanzämter** haben nach der Abgabenordnung und den spezifischen Steuergesetzen die Aufgabe, Steuern nach Maßgabe der Gesetze gleichmäßig festzusetzen und zu erheben sowie sicherzustellen, daß Steuern nicht verkürzt, zu Unrecht erhoben oder Steuererstattungen oder Steuervergütungen zu Unrecht gewährt oder versagt werden. Eine Befugnis, regelmäßig Personen- und Adreßdaten ohne direkte Beteiligung der Meldebehörde selbständig dort abzurufen, ergibt sich daraus nicht. Es liegt auch keine Verpflichtung der Meldebehörde zur Datenbereithaltung für die Finanzämter vor. Deshalb überzeugen mich die Ausführungen des Senators für Finanzen zur Begründung eines solchen Direktabrufes nicht. Als ein Indiz dafür, daß ein solcher Direktabruf nicht erforderlich ist, kann angesehen werden, daß das Finanzamt Bremerhaven eine solche Überlegung bezüglich

des Bremerhavener Melderegisters nicht angestellt hat. In Flächenländern gibt es eine solche Forderung nicht. Sie wäre auch völlig undenkbar. Die spezielle stadtstaatliche Struktur Bremens kann den Direktabruf jedoch nicht rechtfertigen. Im übrigen ist der Datenkatalog für den angegebenen Zweck, nämlich die Personen- und Adressenfeststellung, viel zu umfangreich und nicht erforderlich. Frühere Namen, Ordens- und Künstlernamen, Tag des Ein- und Auszugs, Standesamt, Sterberegisternummer übersteigen das für diesen Zweck erforderliche Maß bei weitem. Das Ordnungsmerkmal darf nach § 4 Abs. 2 BremMG an die Finanzämter, die Landesbehörden sind, nicht übermittelt werden. Es ist schließlich auch zu fragen, ob die Daten Minderjähriger oder von Personen mit Nebenwohnungen in Bremen übermittelt werden müssen.

Ähnliche Überlegungen gelten für die **Landeshauptkasse.** Weder die Landeshaushaltsordnung noch die Justizbeitreibungsordnung noch eine andere Rechtsvorschrift enthalten einen Hinweis auf die Befugnis der Landeshauptkasse, selbständig aus dem Melderegister Personen- und Adreßdaten abzurufen. Im übrigen ist auch hier festzustellen, daß die Erforderlichkeit in Bremen und Bremerhaven offensichtlich unterschiedlich gesehen wird. Der Datenkatalog ist für den angegebenen Zweck viel zu umfangreich. Frühere Namen, Anschriften (auch die früheren), Tag des Ein- und Auszugs, Standesamt, Sterberegisternummer übersteigen das für diesen Zweck erforderliche Maß. Das Ordnungsmerkmal darf gemäß § 4 Abs. 2 BremMG an die Landeshauptkasse, die eine Landesbehörde ist, nicht übermittelt werden. Schließlich ist auch hier zu fragen, ob die Daten Minderjähriger oder von Personen mit Nebenwohnung in Bremen tatsächlich benötigt werden.

Der automatisierte Direktzugriff des **Senators für Bildung, Wissenschaft und Kunst** auf den Meldedatenbestand Bremens ist für den angegebenen Zweck (Schulpflichtkontrolle) und angesichts der anderen in der Rechtsverordnung vorgesehenen Übermittlungsmöglichkeiten unverhältnismäßig. Der Senator für Bildung, Wissenschaft und Kunst als Datenempfänger ist zu unbestimmt. Die Schulpflichtüberwachung ist nach gegenwärtiger Praxis Aufgabe des kommunalen Schulamtes, nicht der ganzen senatorischen Behörde. Schulpflichtig sind nur bestimmte Einwohner Bremens, nicht alle. Weder das Meldegesetz noch die schulrechtlichen Bestimmungen enthalten gegenwärtig einen Hinweis auf die Befugnis des Senators für Bildung, Wissenschaft und Kunst, selbständig aus dem Melderegister Personen- und Adreßdaten aller in Bremen mit Hauptwohnung oder mit Nebenwohnung gemeldeten Personen abzurufen. Aus den Regelungen im Bremischen Schulgesetz zur Schulpflicht kann man lediglich die Berechtigung herleiten, schulpflichtige Personen und deren Erziehungsberechtigte mitgeteilt zu erhalten. Dies kann in Listenform (wie z. B. in Bremerhaven) oder in Form eines Datenträgeraustausches oder durch Einzelauskunft erfolgen. Ein automatisierter Direktzugriff auf den gesamten bremischen Meldedatenbestand ist dafür nicht erforderlich. Zur Aktualisierung der vom Senator für Bildung, Wissenschaft und Kunst betriebenen zentralen Schülerindividualdatei ist der On-line-Zugriff auf das Melderegister ebenfalls nicht erforderlich. Der Änderungsdienst dieser beim Senator für Bildung, Wissenschaft und Kunst geführten Datei, deren Zulässigkeit ebenfalls in Frage zu stellen ist, kann durch Änderungsmitteilungen der Schulen und des kommunalen Schulamtes erfolgen. Im übrigen ist darauf hinzuweisen, daß das Schulamt Bremerhaven den automatisierten Direktzugriff auf das Bremerhavener Melderegister nicht für erforderlich hält. Auch hier überschreitet der Datenkatalog erheblich das für die Personen- und Adreßfeststellung erforderliche Maß.

Im Fall des **Landeskriminalamtes** gilt ebenfalls, daß die mir ersichtlichen Rechtsgrundlagen den jederzeitigen automatisierten Direktzugriff auf den gesamten Meldedatenbestand Bremens nicht begründen. Die vom Landeskriminalamt genannten Gesetzesbestimmungen (§§ 1, 71 Bremisches Polizeigesetz, §§ 3, 4 BKA-Gesetz, § 16 Bremisches Datenschutzgesetz, § 30 Bremisches Meldegesetz) bieten keine Grundlage. Verwaltungsvorschriften binden zwar die Verwaltung, können aber keine Außenwirkung entfalten; Eingriffe in eine geschützte Grundrechtsposition des Bürgers können sie nicht legitimieren. Es ist zudem zu fragen, aus welchem rechtlichen Grunde der Direktzugriff des Landeskriminalamtes Bremen als zentrale Polizeidienststelle des Landes auf das bremische Melderegister beschränkt ist und wie dieser Zugriff angesichts der vom Senat beschlossenen und inzwischen erfolgten Auflösung des Landeskriminalamtes zu beurteilen ist.

Auch für die Meldedatenzugriffe und -abrufe der **Kfz.-Zulassungsbehörden** (FAZID)- bzw. KOKIS-Zugriffe) gilt, daß weder das Melderecht noch die straßenverkehrsrechtlichen Vorschriften die regelmäßige Übermittlung von Meldedaten durch auto-

5.2.2.2 Paß- und Ausweisgesetz des Bundes, Landespersonalausweisgesetz

Das neue Personalausweisgesetz des Bundes ist am 19. April 1986 verabschiedet worden; es tritt in seinen wesentlichen Bestandteilen am 1. April 1987 in Kraft. Mit diesem Gesetz wird der fälschungssichere und maschinenlesbare Personalausweis in der Bundesrepublik eingeführt. Die Frage, ob dieser Ausweis unbedingt maschinenlesbar sein muß, blieb bis zuletzt umstritten. Im Juli 1986 wurde das Muster des neuen Personalausweises durch Rechtsverordnung des Bundes festgelegt.

Gleichfalls verabschiedet wurde im Berichtsjahr ein neues Paßgesetz mit einer Änderung der Strafprozeßordnung. Das neue Paßgesetz tritt am 1. Januar 1988 in Kraft, die Änderung der Strafprozeßordnung am 1. April 1987. Auch diese Gesetzesänderungen waren bis zuletzt politisch umstritten. Der neue Paß wird ebenfalls maschinenlesbar sein. (Vgl. zu beiden Gesetzgebungsvorhaben auch die Ausführungen in meinem 8. Jahresbericht unter Pkt. 2.1.3.1, S. 14 ff.). Durch die mit dem Paßgesetz verabschiedete Änderung der Strafprozeßordnung wurde die gesetzliche Grundlage für die sogenannte „Schleppnetzfahndung" geschaffen. Zwar hat der Gesetzgeber gegenüber dem ursprünglich vorgelegten Entwurf noch Verbesserungen, d. h. Eingrenzungen vorgenommen, dennoch halte ich es für äußerst problematisch, daß nach der nun verabschiedeten Fassung des § 163 d Strafprozeßordnung (StPO) ein Abgleich von Daten aus der Schleppnetzfahndung mit Daten anderer Dateien vorgenommen werden kann. Ich halte es nach wie vor für richtig, ein Gesamtkonzept bereichsspezifischen Datenschutzes für das Strafverfahren zu schaffen, weil nur so die Zusammenarbeit von Polizei und Staatsanwaltschaft und die erforderliche Konkordanz der Aufgaben und Befugnisse transparent gemacht werden können.

Zur Ausführung des Gesetzes über Personalausweise hat der Senator für Inneres im Berichtsjahr den Entwurf eines Ausführungsgesetzes vorgelegt, das die erforderlichen landesrechtlichen Ergänzungen enthält. Zu diesem Gesetzentwurf habe ich Stellung genommen. Dabei habe ich u. a. angeregt,

— die Behörden, die Daten aus dem Ausweisregister erhalten dürfen, präziser zu bezeichnen,

— eine Regelung dahingehend zu treffen, daß das bei den Personalausweisbehörden zu führende Ausweisregister nicht gemeinsam mit anderen Registern, wie z. B. dem Melderegister, geführt wird,

— den On-line-Zugriff anderer Behörden auf das Personalausweisregister, d. h. die regelmäßige Datenübermittlung im Wege des Direktabrufes, für unzulässig zu erklären,

— wenn regelmäßige Datenübermittlungen z. B. an andere Ausweisbehörden, die Kriminalpolizei etc. für notwendig erachtet werden, dann sollte dies explizit im Ausführungsgesetz des Landes geregelt werden.

Die Innendeputation hat auf Vorschlag des Senators für Inneres meine Anregungen weitgehend übernommen und noch einmal bekräftigt, daß On-line-Zugriffe auf das Personalausweisregister durch andere Behörden weder derzeit bestehen noch künftig beabsichtigt sind.

Regelmäßige Datenübermittlungen an andere als Ausweisbehörden finden nicht statt. Die Personalausweisdaten unterliegen der Zweckbindung.

Zur Ausführung des Paßgesetzes liegt noch kein Gesetzentwurf des Innensenators vor.

5.2.3 Kfz.-Zulassung/Führerschein

5.2.3.1 Führerschein auf Probe

Der „Führerschein auf Probe" ist im vergangenen Jahr durch eine Änderung des Straßenverkehrsgesetzes eingeführt worden. Nach dem Willen des Bundesgesetzgebers wird beim Kraftfahrtbundesamt in Flensburg eine zentrale Datei aller Inhaber einer Fahrerlaubnis auf Probe geschaffen. Neben dem Familiennamen, gegebenenfalls Geburtsnamen, Vornamen, Tag und Ort der Geburt, Geschlecht werden die erteilten Fahrerlaubnisklassen, der Tag des Ablaufs der Probezeit, die erteilende Behörde und die Führerscheinnummer eines jeden Fahranfängers für die Dauer von drei Jahren gespeichert. Die örtlichen Führerscheinstellen sind verpflichtet, dem Kraftfahrtbundesamt diese Daten mitzuteilen. Datenübermittlungen

matisierten Direktabruf rechtfertigen. Aus der Sicht des Datenschutzes sind allein Einzelauskünfte unbedenklich, sofern bei der Zulassungsstelle Zweifel an der Identität oder an der Anschrift des Kfz.-Halters bzw. -Eigentümers vorliegen. Automatisierte Lösungen, wie sie in Bremen bzw. Bremerhaven realisiert sind, stammen aus einer Zeit, als es noch kein Datenschutzrecht und neues Melderecht gab und als Integration und integrierte Datenverarbeitung Ziel aller Datenverarbeitungsentwicklungen war, funktionelle Trennung der Behörden und ihrer Datenverarbeitungsvorgänge sowie Zweckbindung der Daten hingegen noch keine große Rolle spielten. Inzwischen sind aufgrund der Rechtsentwicklung integrierte Systemlösungen ohne weiteres nicht mehr möglich, obwohl die technologische Entwicklung in diese Richtung drängt. Derartige Lösungen werden im übrigen nur in Großstädten oder in kommunalen Gemeinschaftsrechenzentren realisiert, wo die Datenbestände sozusagen unter einem räumlichen und organisatorischen Dach verfügbar sind. Man muß hier auch berücksichtigen, daß die Kfz.-Zulassungsdaten samt Halter- und Eignerdaten nicht nur innerhalb der Verkehrsbehörden ausgetauscht werden, sondern viele andere Stellen, z. B. Finanzbehörden, Kraftfahrtbundesamt Flensburg, Polizei- und Sicherheitsbehörden, Versicherungen, Private ebenfalls Auskünfte erhalten und in Zukunft zum Teil auch einen automatisierten Direktzugriff erhalten werden. Die FAZID- bzw. KOKIS-Zugriffe auf das Melderegister aktualisieren nicht nur die örtlichen Fahrzeugregister in Bremen bzw. Bremerhaven, sondern auch das zentrale Register beim Kraftfahrtbundesamt in Flensburg. Über die dortigen On-line-Anschlüsse können dann weitere Datenbestände aktualisiert werden.

Aus datenschutzrechtlicher Sicht können nur Einzelzugriffe und -abrufe auf das Melderegister im Zusammenhang mit der konkreten Sachbearbeitung hingenommen werden, die auf wenige Merkmale begrenzt sind und wenn sichergestellt ist, daß es sich auch in systemtechnischer Hinsicht um getrennte Datenverarbeitungsverfahren mit eindeutigen Schnittstellen untereinander und klarer Verantwortlichkeit der Behörden handelt. Einen von der konkreten Sachbearbeitung der Zulassungsbehörden abgesetzten, isolierten On-line-Zugriff auf das Melderegister oder eine anlaßbezogene (z. B. Umzug, Tod, Namensänderung) automatisierte Übermittlung von Meldedaten an das FAZID- bzw. KOKIS-Verfahren halte ich unter datenschutzrechtlichem Aspekt nicht für zulässig.

Für die regelmäßige Übermittlung von Daten an die **Schutz- und Kriminalpolizei** im Wege des automatisierten Direktabrufs gilt ebenfalls, daß konkrete bereichsspezifische Regelungen fehlen. Die Schutz- und Kriminalpolizei benötigt die Daten einzelner, ganz bestimmter Personen, nicht jedoch ständig und in Selbstbedienung die Daten aller gemeldeten Einwohner. Die von der Polizei genannten Beispiele zeigen dies deutlich. Den Informationsbedürfnissen der Schutz- und Kriminalpolizei kann m. E. auch durch Einzelfallübermittlungen der Meldebehörden Rechnung getragen werden. Offen blieben dann nur die Fälle, in denen die Schutz- und Kriminalpolizei außerhalb der Dienststunden der Meldebehörde Auskünfte aus dem Melderegister benötigt. Zur Lösung dieser Fälle könnte man daran denken, der Schutz- und Kriminalpolizei Zugang zu einem Auskunftsbildschirm der Meldebehörde zu gewähren, mit dessen Hilfe unter eigener Kennung und eigenem Paßwort der Polizei bestimmte Daten abgefragt werden können (modifizierte Schlüssellösung, ähnlich wie gegenwärtig beim FAZID- und KOKIS-Verfahren). Denkbar wäre auch die Einrichtung von zentralen Auskunftsstellen bei den Meldebehörden, die ständig für Anfragen und Auskünfte zur Verfügung stehen.

Erhebliche Zweifel an der Erforderlichkeit und damit Zulässigkeit einer regelmäßigen Datenübermittlung im Wege des automatisierten Direktabrufes bestehen schließlich im Fall **der Ortspolizeibehörde Bremerhaven, Abteilung für Ordnungswidrigkeiten.** Auch diese Übermittlungsfälle lassen sich durch eine Datenübermittlung im Einzelfall erledigen, ohne daß ein ständiger Zugriff ohne Beteiligung der Meldebehörden auf alle Einwohnerdatensätze — wen auch auf wenige Daten begrenzt — eröffnet wird.

Die Innendeputation hat zur Beratung dieser Materie einen Unterausschuß eingerichtet, der in mehreren Sitzungen den Verordnungsentwurf beraten hat. Neben Vertretern der betroffenen Verwaltungen habe auch ich an diesen Beratungen teilnehmen können. Zum Berichtszeitpunkt waren die Beratungen noch nicht abgeschlossen. Es zeichnet sich aber ab, daß eine Reihe von Übermittlungstatbeständen, wie z. B. der On-line-Zugriff des Senators für Bildung, Wissenschaft und Kunst oder die regelmäßige Übermittlung an das Sozialamt Bremerhaven, aus dem Verordnungsentwurf gestrichen werden. Dies wird dazu führen, daß z. T. langjährige Praktiken der Verwaltung aufgegeben werden müssen. Die Innendeputation wird den Verordnungsentwurf noch im Frühjahr dieses Jahres abschließend behandeln.

aus dieser zentralen Datei sind unter bestimmten Voraussetzungen für wissenschaftliche, statistische und gesetzgeberische Zwecke vom Gesetzgeber zugelassen worden. Die zentrale Datei der Fahranfänger wird Teil des gesamten Informationssystems beim Kraftfahrtbundesamt in Flensburg, das sowohl die Fahranfänger, die Verkehrssünder als auch sämtliche Halter von Fahrzeugen und die Fahrzeugdaten erfaßt.

An der Notwendigkeit einer solchen zentralen Datei der Fahranfänger waren im Gesetzgebungsverfahren von Datenschutzbeauftragten erhebliche Zweifel angemeldet worden. Bereits im 7. und 8. Jahresbericht habe ich auf die datenschutzrechtliche Problematik dieser neuen Regelung hingewiesen. Die Anregungen und Bedenken der Datenschutzbeauftragten sind aber vom Bundesgesetzgeber nicht berücksichtigt worden.

Ich werde den Vollzug der Vorschrift betreffend den „Führerschein auf Probe" aufmerksam verfolgen und durch stichprobenartige Prüfungen feststellen, ob die im Gesetz vorgesehenen technisch-organisatorischen Sicherungsmaßnahmen eingehalten werden und nicht durch zusätzliche Speicherungen personenbezogener Daten, etwa bei den mit der Nachschulung befaßten Stellen, ungerechtfertigte Risiken für die Fahranfänger entstehen.

5.2.3.2 Änderung des Straßenverkehrsgesetzes (Fahrzeugregister-ZEVIS)

Ende 1986 wurde das Straßenverkehrsgesetz nochmals geändert. Mit dieser Änderung des Straßenverkehrsgesetzes wurde die Rechtsgrundlage für die Errichtung und Nutzung des zentralen Verkehrsinformationssystems „ZEVIS" beim Kraftfahrtbundesamt in Flensburg — bestehend aus der zentralen Verkehrssünderdatei und dem zentralen Fahrzeugregister — geschaffen. Gleichfalls wurde mit der Gesetzesänderung die Errichtung und Nutzung der örtlichen Fahrzeugregister bei den Kfz.-Zulassungsstellen neu geregelt. Die Neuregelungen traten Mitte Februar 1987 in Kraft.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in der Vergangenheit mehrfach kritisch mit dieser Gesetzesänderung befaßt. Ich habe im 7. Jahresbericht unter Pkt. 5.2.1.4, S. 30 ff. und im 8. Jahresbericht unter Pkt. 2.1.3.1, S. 13 f. darüber berichtet und auf die datenschutzrechtlichen Probleme aufmerksam gemacht; hinsichtlich der von mir vertretenen Bedenken und Anregungen verweise ich auf diese Ausführungen.

Die jetzt in Kraft getretene Gesetzesfassung zeigt, daß die Kritik der Datenschutzbeauftragten so gut wie nichts bewirkt hat. Die Schaffung einer gesetzlichen Grundlage für die Einrichtung und Nutzung derartiger Register wird zwar grundsätzlich begrüßt. Unter Datenschutzgesichtspunkten muß man diese Gesetzesänderung jedoch als unverhältnismäßigen Eingriff des Staates in das informationelle Selbstbestimmungsrecht des „Verkehrssünders" und des Kfz.-Halters bewerten. Es wird nicht nur eine langjährige Verwaltungspraxis ohne Abstrich rechtlich abgesichert, sondern es werden darüber hinaus völlig neue Datenzugriffe und Datenverarbeitungsvorgänge zugelassen. Daran ändern auch nichts die Beschlußempfehlungen von Bundestag und Bundesrat im Zusammenhang mit dieser Gesetzesänderung, die die Bundesregierung zu einem Erfahrungsbericht nach vier Jahren auffordern.

Zusammengefaßt hier nochmals die nach meiner Auffassung besonders problematischen Punkte:

Zu kritisieren ist zunächst bei dieser Gesetzesänderung, daß eine Phase der verständlichen Bestürzung über terroristische Gewalttaten und Morde genutzt wurde, um bei den Bürgern den Eindruck hervorzurufen, daß der Datenschutz die Ursache für fehlende Fahndungsergebnisse sei. Tatsächlich hat der Datenschutz einer effektiven polizeilichen Datenverarbeitung nie entgegengestanden. Es hat nicht am fehlenden Zugriff auf zentrale Datenbestände gelegen, wenn die Polizei von Terroristen benutzte Fahrzeuge oder deren Fahrer nicht schneller gefunden hat. Die Vorstellung, daß mit einem verstärkten Computer-Einsatz und durch vermehrte Datenflüsse zwischen den Behörden die Terrorismusbekämpfung entscheidende Erfolge erzielen könnte, begegnet erheblicher Skepsis. Die Sicherheitsorgane wissen, daß selbst mit einer Mobilisierung aller verfügbaren Computer dem Terrorismus nicht beizukommen wäre.

In der Gesetzesänderung wurde entgegen der ursprünglichen Entwurfsfassung die engere Zweckbindung der Datennutzung für Nachrichtendienste aufgehoben und

den Nachrichtendiensten damit eine weite Zugriffsmöglichkeit auf das Zentrale Verkehrsinformationssystem (ZEVIS) eröffnet. Dies ist insbesondere deshalb bedenklich, weil die Trennung zwischen gewaltfreien und gewalttätigen Demonstrationen unter dem Gesichtspunkt von Extremismus und Terrorismus nicht mehr vorgenommen wird.

Ganz grundsätzlich muß auch kritisiert werden, daß das Zweckbindungsprinzip stark durchlöchert worden ist. Die Daten aus der Kraftfahrzeugzulassung werden erhoben, um die besondere Verantwortung der Fahrzeughalter praktisch zu verwirklichen. Diese liegt insbesondere in der verkehrs- und zivilrechtlichen Haftung aus der Teilnahme am Straßenverkehr, umfaßt aber keineswegs jede Halterfeststellung zu beliebigen Zwecken anderer Stellen. Jede zweckfremde Verwendung der Daten bedarf einer entsprechenden Rechtfertigung aus überwiegendem Allgemeininteresse und kann nur für genau eingegrenzte Fallgruppen und unter eingeschränkten Bedingungen zugelassen werden. Dies ist in der beschlossenen Gesetzesfassung an mehreren Stellen nicht beachtet worden.

Ein besonderes Risiko liegt auch darin, daß mit dem On-line-Zugriff der Polizei auf die Datenbestände des Kraftfahrtbundesamtes in Form z. B. der sog. Halteranfrage die Kontrolldichte in der Weise erhöht werden kann, daß — wie das in der Praxis vorkommt — die Überprüfung aller abgestellten Kraftfahrzeuge in der Umgebung einer Demonstration bzw. eines Versammlungsortes erfolgen kann. Dabei geht es nicht nur um die Erhöhung der Kontrolldichte, sondern auch um die heimliche Kontrolle des Verkehrsteilnehmers, ohne daß dieser in direktem Kontakt mit der Polizei erkennt, daß seine Daten abgefragt wurden (z. B. Aktion „Gitternetz"). Eine solche Vorgehensweise hat das Bundesverfassungsgericht in seinem Volkszählungsurteil damit kritisiert, daß es darauf hinwies, daß jemand, der unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, versuchen wird, nicht durch solche Verhaltensweisen aufzufallen. Wer also damit rechnet, daß etwa die Teilnahme an einer Versammlung oder an einer Bürgerinitiative behördlich registriert wird, daß ihm dadurch Risiken entstehen können, wird möglicherweise auf die Ausübung seiner diesbezüglichen Grundrechte (Artikel 8, 9 GG) verzichten. Es geht dabei nach Auffassung des Bundesverfassungsgerichts nicht nur um Individualrechte des Bürgers, sondern auch um eine elementare Funktionsbedingung eines freiheitlichen demokratischen Gemeinwesens.

Die in letzter Minute vom Gesetzgeber aufgenommene Übergangsvorschrift in Artikel 2 des Änderungsgesetzes eröffnet auch für den Bundesnachrichtendienst und den Militärischen Abschirmdienst die Nutzung der Fahrzeugregister, ohne daß bereichsspezifische Datenschutzbestimmungen für diese Dienste vorliegen.

Es ist äußerst bedenklich, wenn die für einen bestimmten Zweck erhobenen und gespeicherten Kfz.-Daten dritten Stellen, sei es Polizei, Staatsanwaltschaft oder andere Sicherheitsbehörden, zugänglich gemacht werden, ohne daß die gesetzlichen Voraussetzungen dafür in spezifischen Gesetzen wie die Strafprozeßordnung oder in den Polizeigesetzen des Bundes und der Länder eindeutig und klar festgelegt worden sind.

Der Gesetzgeber hat zur nachträglichen Kontrolle umfangreiche Protokollierungen für die automatisierten Datenabrufe vorgeschrieben. Datenabrufe bremischer oder Bremerhavener Polizeidienststellen beim Kraftfahrtbundesamt sind dort — stichprobenweise — zu protokollieren, Datenabrufe aus den örtlichen Fahrzeugregistern — vollständig — in Bremen bzw. Bremerhaven. Ob hierdurch die Datenabrufe auf das erforderliche und zulässige Maß beschränkt werden können, bleibt abzuwarten.

5.2.3.3 Automatisierung der Kfz.-Zulassung in Bremen und Bremerhaven

Im letzten Jahresbericht hatte ich unter Pkt. 5.2.3.1, S. 34 über die Automatisierung der Kfz.-Zulassung in **Bremen** (sog. FAZID-Verfahren) berichtet. Dieses Verfahren wurde Anfang 1986 im Bereich der Kfz.-Zulassungsstelle Bremen-Stadt eingeführt. Es ist geplant, dieses Verfahren auf die Kfz.-Zulassungsstelle Bremen-Nord und damit dann auf die gesamte Stadt Bremen auszudehnen.

Auch in **Bremerhaven** wurde im Berichtsjahr die Kfz.-Zulassung automatisiert; seit Ende des Jahres läuft hier das sogenannte KOKIS-Verfahren (= Kommunales Kfz.-Informationssystem). Bei beiden Datenverarbeitungs(DV)-Verfahren stellten und stellen sich die gleichen grundsätzlichen Datenschutzprobleme:

Die Verbindung zu anderen kommunalen DV-Verfahren (z. B. Einwohnerwesen) und der Direktzugriff der Polizei auf den gespeicherten Datenbestand. Die regelmäßige Übermittlung von Meldedaten an die Kfz.-Zulassungsstellen als integraler Verfahrensbestandteil dieser neuen DV-Verfahren ist vor Erlaß der Meldedatenübermittlungsverordnung des Landes nicht zulässig; lediglich Einzelauskünfte sind nach dem Bremischen Meldegesetz möglich. Auf diese Problematik hatte ich bereits im letzten Jahresbericht hingewiesen. Vgl. hierzu auch meine Ausführungen zur Meldedatenübermittlungsverordnung unter Pkt. 5.2.2.1 in diesem Bericht.

Hinsichtlich des geplanten On-line-Zugriffs der Polizei auf den FAZID- bzw. KOKIS-Datenbestand habe ich der sogenannten modifizierten Schlüssellösung als Übergangsregelung bis zur Änderung des Straßenverkehrsgesetzes zugestimmt: Während der Geschäftszeit der Kfz.-Zulassungsstellen werden nur Einzelauskünfte an die Polizei per telefonischer oder unmittelbar mündlicher Anfrage erteilt. Außerhalb der allgemeinen Geschäftszeit der Kfz.-Zulassungsstellen erhält ein begrenzter Personenkreis der Polizei Zugang zu einem bestimmten Auskunftsbildschirm der Zulassungsstelle und kann dort unter eigener Kennung (USER-ID) und eigenem Paßwort selbständig spezielle Auskunftsformate aufrufen und abfragen. Diese Datenzugriffe der Polizei werden nach den getroffenen Absprachen sowohl bei der Polizei wie auch systemseitig im Rechenzentrum protokolliert, um die Zulässigkeit dieser Datenzugriffe nachträglich überprüfen zu können.

Mitte Februar 1987 trat die insbesondere von der Polizei und den anderen Sicherheitsbehörden „lang ersehnte" Änderung des Straßenverkehrsgesetzes in Kraft, die einer Vielzahl von Sicherheitsbehörden des Bundes und der Länder den direkten Zugriff auf das örtliche und das überörtliche Fahrzeugregister (ZEVIS) eröffnete. Schon bevor die Gesetzesänderung in Kraft getreten war, wurden sowohl in Bremen als auch in Bremerhaven Vorstellungen der Polizei hinsichtlich ihres direkten Zugriffs auf den FAZID- bzw. KOKIS-Datenbestand entwickelt und z. T. bereits in konkrete ADV-Beschaffungsanträge umgesetzt. Da gegenwärtig die für die Zulassung derartiger On-line-Anschlüsse erforderliche Rechtsverordnung fehlt, müssen die bremischen und Bremerhavener Polizeidienststellen sich noch eine gewisse Zeit mit der Übergangslösung zufrieden geben; auch der ZEVIS-Anschluß muß noch warten. Der Senator für Inneres muß sich überlegen, ob er — ganz oder teilweise — überhaupt von den neu eröffneten Möglichkeiten im Lande Bremen Gebrauch machen will. Es sind grundsätzliche politische und unter Umständen auch rechtliche Gestaltungsentscheidungen für die polizeiliche Informationsverarbeitung und -beschaffung erforderlich, die nur durch eine gesamtheitliche Betrachtungsweise möglich sind. Ein Laufenlassen der Entwicklung ohne solche gestalterischen Eingriffe halte ich auf längere Zeit nicht für verantwortbar.

5.2.4 Amtliche Statistik

5.2.4.1 Volkszählung 1987

— Nachdem im November 1985 das Volkszählungsgesetz 1987 in Kraft getreten ist (vgl. meinen 8. Jahresbericht Pkt. 5.2.4.3, S. 37 f.), haben Länder und Gemeinden im Berichtsjahr damit begonnen, die Durchführung der Volkszählung vorzubereiten. Auch meine Arbeitskraft wurde von dieser Thematik erheblich in Anspruch genommen. Dabei stand die Beratung der mit der Durchführung der Zählung befaßten Stellen im Vordergrund; die eigentliche Prüftätigkeit kann erst in diesem Jahr beginnen.

  Der Senator für Inneres legte im März 1986 den Entwurf einer **Verordnung zur Durchführung des Volkszählungsgesetzes 1987** im Lande Bremen vor, zu dem ich Stellung genommen habe. Mit dieser Rechtsverordnung werden die Erhebungsstellen für die Durchführung der Volkszählung bestimmt, die Aufgaben der Erhebungsstellen festgelegt, Regelungen für die räumliche, organisatorische und personelle Abgrenzung der Erhebungsstellen getroffen und spezielle Vorschriften zur Sicherung der Daten und zum Zählereinsatz erlassen. Die Verordnung trat Anfang Juli 1986 in Kraft.

— Die **Erhebungsstellen in Bremen und Bremerhaven** wurden im Laufe des Jahres 1986 eingerichtet, ihre Leiter und Vertreter bestellt und die ersten Mitarbeiter bereitgestellt. Entsprechend den Anforderungen des Gesetz- und Verordnungsgebers sind die Erhebungsstellen räumlich und organisatorisch von den übrigen Verwaltungsstellen getrennt eingerichtet worden. Die Räumlichkeiten der örtlichen Erhebungsstellen wurden mit einigem Aufwand gegen unbefugten Zutritt und Zugang zum Datenmaterial gesichert, wovon ich mich durch eigene Prüfung

überzeugen konnte. Eine gleiche Sicherung der überörtlichen Erhebungsstelle, d. h. des Statistischen Landesamtes Bremen, konnte bisher noch nicht realisiert werden. Ich habe den Senator für Inneres aufgefordert, noch vor der Haupterhebung im Mai 1987 auch die überörtliche Erhebungsstelle im gleichen Maße gegen unbefugten Zutritt und Zugang zum Datenmaterial zu sichern, wie dies für die örtlichen Erhebungsstellen realisiert wurde.

Die räumliche und organisatorische Trennung der Erhebungsstellen gilt von Beginn der Bearbeitung und Aufbewahrung von Erhebungsvordrucken bis zur Ablieferung dieser Vordrucke an das Statistische Landesamt. Zur Gewährleistung der personellen Abschottung ist durch die Bremische Rechtsverordnung vorgeschrieben, daß die in den Erhebungsstellen tätigen Personen während der Zeit, in der sie Zugang zu Volkszählungsdaten haben, nicht mit Aufgaben des Verwaltungsvollzuges außerhalb der Volkszählung betraut und nicht bei anderen Verwaltungsstellen eingesetzt werden dürfen. Ein Hin- und Herpendeln der Mitarbeiter der Erhebungsstellen zwischen Dienststellen des Verwaltungsvollzuges und Erhebungsstellen ist damit ausgeschlossen. Das Personal der Erhebungsstellen wird zum Teil aus dem vorhandenen Personalkörper der Verwaltung rekrutiert, ist zum Teil auch speziell für diese Aufgabe eingestellt worden. Bei der Gewinnung des Personals für die Erhebungsstellen werden — ohne daß dies ausdrücklich geregelt ist — im Grundsatz die gleichen Unvereinbarkeitskriterien zugrunde gelegt, wie sie im Volkszählungsgesetz 1987 für die Zähler vorgeschrieben sind. Dies wird von mir begrüßt.

— Die Erhebungsstellen und das Statistische Landesamt Bremen haben sich im Berichtsjahr bemüht, die notwendige Anzahl von **Zählern zu gewinnen.** In Bremen werden etwa 4000, in Bremerhaven etwa 1300 Zähler benötigt. Mit Ausfallreserve müssen in Bremen etwa 5000 und in Bremerhaven etwa 1800 Zähler angeworben, geschult, verpflichtet und eingeplant werden. Die Zählergewinnung beruht auf dem Freiwilligkeitsprinzip, d. h. man will von der im Volkszählungsgesetz 1987 gebotenen Möglichkeit zur Zwangsbenennung von Zählern möglichst keinen Gebrauch machen. Die diesbezüglichen Bemühungen der Erhebungsstellen und des Statistischen Landesamtes Bremen scheinen Erfolg gehabt zu haben. Ich habe das Statistische Landesamt aufgefordert, bei der Auswahl der Zähler besonders auf deren Zuverlässigkeit zu achten und sicherzustellen, daß die eingesammelten Erhebungsbögen von den Zählern unverzüglich bei den Erhebungsstellen abzuliefern sind. Wer den Zähler nicht in seine Wohnung lassen möchte, und die ausgefüllten Erhebungsbögen dem Zähler auch nicht aushändigen möchte, ist berechtigt, die Erhebungsvordrucke portofrei innerhalb einer Woche an die Erhebungsstellen zu übersenden oder dort abzugeben. Im Zusammenhang mit der Zählerwerbung erreichten mich verschiedene Anfragen und Beschwerden, in denen u. a. die Verwendung von Name und Dienstanschrift für Werbeschreiben gerügt wurden. Nach Prüfung dieser Vorgänge habe ich jedoch keine Veranlassung zu einer Beanstandung gesehen.

— Neben der Einrichtung der Erhebungsstellen und der Zählergewinnung waren die Erhebungsstellen in Bremen und Bremerhaven im Berichtsjahr damit beschäftigt, die Zählung selbst und vorrangig dabei die **Gebäudevorerhebung** vorzubereiten. Die Gebäudevorerhebung wird postalisch durchgeführt, d. h. ohne den Einsatz von Zählern. Sie begann Ende November und soll Ende März abgeschlossen sein. Erhoben werden von den Eigentümern und Verwaltern der Wohngebäude Angaben zum Gebäude, die dann später von der Erhebungsstelle manuell in die Wohnungsbögen übertragen werden sollen. Zu dieser vorgezogenen Datenerhebung haben mich eine Vielzahl von Bürgeranfragen erreicht, die sich im wesentlichen auf die Zulässigkeit der Datenerhebung, die Auskunftspflicht, die statistische Geheimhaltung, die Verwendung der Daten und Fragebogen sowie die Herkunft der Adreßdaten bezogen. Ich habe mich bemüht, durch Aufklärung und Information die Fragen zu beantworten. Außerdem habe ich zu einzelnen Fragen im Zusammenhang mit der Durchführung der Gebäudevorerhebung Stellung genommen.

— Das Mengengerüst der Zählung und die vom Gesetzgeber an den Zählereinsatz und an die Durchführung der Zählung gestellten Anforderungen, die relativ kurzen Bearbeitungsfristen und die den Auskunftspflichtigen eingeräumten Rückgabemöglichkeiten der Erhebungsbogen machen den **Einsatz von Technik, insbesondere von DV-Technik** bei den bzw. für die Erhebungsstellen naheliegend. Dies um so mehr, als in Bremen wie auch in Bremerhaven große Gemeinschaftsrechenzentren für die Verwaltung existieren und die meisten

Verwaltungsabläufe einschließlich der amtlichen Statistik DV-unterstützt ablaufen. Für die Erhebungsstelle Bremen wurden im Berichtsjahr mehrere Personalcomputer (PC) mit entsprechender Peripherie und Betriebssoftware angeschafft. Auch die Erhebungsstelle Bremerhaven verfügt seit Anfang dieses Jahres über einen Personalcomputer.

Für folgende Aufgaben der Erhebungsstellen wurden bzw. werden DV-Anwendungsprogramme entwickelt:

- Vorbereitung und Durchführung der Gebäudevorerhebung
- Zählerverwaltung und Steuerung des Zählereinsatzes
- Vorbereitung und Organisation der Haupterhebung
- Rücklaufkontrolle der Erhebungsbogen sowie Durchführung etwaiger Erinnerungs-, Mahn-, Verwaltungszwangs- und Bußgeldverfahren.

In **Bremen** sind die Zählerverwaltung und die Steuerung des Zählereinsatzes als autonome PC-Anwendung realisiert; die Gebäudevorerhebung und die Haupterhebung werden durch Batch-Anwendungsprogramme im Rechenzentrum der bremischen Verwaltung unterstützt. Die installierten PC's werden in Anbindung an das Großrechnersystem des Rechenzentrums der bremischen Verwaltung auch zur Dateneingabe bei der Bogenrücklaufkontrolle genutzt. Die Weiterverarbeitung der eingegebenen Daten und das Erinnerungs- und Mahnverfahren sind wiederum als Batch-Anwendung im Rechenzentrum der bremischen Verwaltung geplant. In Bremerhaven werden die Zählerverwaltung und die Steuerung des Zählereinsatzes, die Rücklaufkontrolle und das Erinnerungs- und Mahnverfahren für die Haupterhebung als autonome PC-Anwendung realisiert, während die Vorbereitung und Durchführung der Gebäudevorerhebung und der Haupterhebung sowie das Erinnerungs- und Mahnverfahren bei der Gebäudevorerhebung durch ein Batch-Verfahren auf dem Großrechnersystem unterstützt werden.

— Bei meinen Beratungsgesprächen mit den Erhebungsstellen und den beiden Verwaltungsrechenzentren habe ich die auch vom Senator für Inneres geteilte Auffassung vertreten, daß das **Abschottungsgebot des Volkszählungsgesetzes 1987** und der Bremischen Durchführungsverordnung auch für die von den Erhebungsstellen geplanten bzw. durchgeführten ADV-Verfahren gilt, nicht nur für die Erhebungsstellen als räumliche, personelle und organisatorische Einrichtungen. Die Beauftragung der zentralen Verwaltungsrechenzentren durch die Erhebungsstellen begegnet nach meiner Auffassung keinen grundsätzlichen datenschutzrechtlichen Bedenken, da insoweit Datenverarbeitung im Auftrag erfolgt. Auch der DV-Einsatz für die bzw. bei den Erhebungsstellen ist als solcher datenschutzrechtlich nicht zu beanstanden. Die zentralen Verwaltungsrechenzentren haben jedoch als Auftragnehmer wegen der besonderen Sensibilität und Brisanz der Angelegenheit besonders sorgfältig die Weisungen ihrer Auftraggeber und die bestehenden Sicherungsvorschriften, funktionellen Trennungsgebote und Nutzungsbeschränkungen zu beachten. Die DV-Verfahren und -Arbeiten in den zentralen Verwaltungsrechenzentren für die Erhebungsstellen müssen eindeutig von den übrigen DV-Verfahren der Verwaltung getrennt sein; es müssen eigenständige, völlig abgetrennte DV-Arbeitsgänge unter der ausschließlichen Verantwortung der Erhebungsstellen ablaufen. Technisch denkbare, in andere DV-Verfahren wie z. B. das automatisierte Meldewesen eingebettete DV-Lösungen würden dem Abschottungsgebot widersprechen und wären daher unzulässig. Da es sich hier um ein auch vom Bundesverfassungsgericht für wichtig erachtetes Datenschutzprinzip handelt, werde ich meine Prüftätigkeit deutlich auf diesen Punkt richten.

— Hinsichtlich der **Nutzung der Personalcomputer** in den Erhebungsstellen gilt, daß hierfür ein besonderes Datenschutz- und Datensicherungskonzept zu entwickeln und anzuwenden ist, das sowohl die Bestimmungen des Bremischen Datenschutzgesetzes als auch die besonderen, sich aus dem Volkszählungsgesetz 1987 ergebenden Datensicherungserfordernisse berücksichtigt. So habe ich z. B. angeregt, daß jeder berechtigte PC-Benutzer in der Erhebungsstelle sich durch ein selbst zu verwaltendes Paßwort dem System gegenüber zu erkennen gibt, daß bestimmte Systemprogramme (z. B. Laden von Programmen, Sicherung der Dateien) nur einem kleinen Kreis privilegierter Benutzer zugänglich sein sollen und daß die COPY-Funktion des PC-Betriebssystems so modifiziert wird, daß das Kopieren über das Diskettenlaufwerk unmöglich ist.

— Jegliche **Datenübermittlung an andere Verwaltungsstellen** durch die Erhebungsstellen ist nach der bestehenden Rechtslage unzulässig, ausgenommen sind lediglich Datenübermittlungen im Zusammenhang mit der Durchführung eines eventuellen Verwaltungszwangsverfahrens, Bußgeld- oder Strafverfahrens. Soweit den Erhebungsstellen die Daten des § 11 Volkszählungsgesetz 1987 im Rahmen automatisierter Arbeitsgänge zur Verfügung gestellt werden — wie dies in Bremen und Bremerhaven vorgesehen ist —, ist die Gestaltung der Arbeitsabläufe in den Rechenzentren und bei den Erhebungsstellen so zu strukturieren, daß keinerlei Rückübermittlung an die Datenlieferanten, d. h. an die übermittelnden Behörden erfolgt. Andernfalls werde das strikte Trennungs- und Zweckbindungsgebot des Volkszählungsgesetzes 1987 durchbrochen und die verfassungsgemäße Durchführung der Zählung in Frage gestellt. Von den Erhebungsstellen festgestellte Datenabweichungen sowie Angaben aus den ausgefüllten Erhebungsbogen dürfen in keinem Fall an andere Verwaltungsbehörden wie z. B. das kommunale Steueramt, die Meldebehörde oder die Gewerbemeldestelle übermittelt werden. Dies habe ich bei meinen Beratungsgesprächen mit den Erhebungsstellen und den beiden Rechenzentren immer wieder deutlich gemacht. Der Senator für Inneres, das Statistische Landesamt und ich sind der gemeinsamen Auffassung, daß dieser Punkt strikt einzuhalten ist. Ich werde insbesondere die DV-Arbeitsabläufe in den beiden Verwaltungsrechenzentren nach ihrer programmtechnischen Realisierung unter diesem Gesichtspunkt prüfen. Um eine solche unzulässige Nutzung der Volkszählungsdaten zu verhindern, werde ich anhand der Systemprotokolle dieses in unregelmäßigen Abständen prüfen.

— Da Auskunftspflicht besteht, muß die Erhebungsstelle den Rücklauf der Erhebungsbogen kontrollieren. Da man mit säumigen Auskunftspflichtigen und Verweigerern rechnet, wird ein automatisiertes **Erinnerungs- und Mahnverfahren** entwickelt und eingesetzt. Im Zusammenhang mit diesem Verfahren entsteht zwangsläufig eine Datei der säumigen Auskunftspflichtigen. Diese Datei unterliegt einer strengen Zweckbindung und Nutzungsbeschränkung. Zugang bzw. Zugriff zu den Daten dieser Datei hat ausschließlich die Erhebungsstelle. Dies gilt auch, wenn diese Daten im Rahmen eines Verwaltungszwangsverfahrens oder Bußgeldverfahrens verwendet werden. Den an diesem Verfahren beteiligten anderen Behörden dürfen nur die für ihre Aufgabenerfüllung erforderlichen Daten übermittelt werden. Ein eigener Zugriff dieser Behörden auf diese Datei oder eine separate Verweigererdatei dort ist nicht zulässig.

  Auch die in den Erhebungsstellen angelegten Zählerdateien unterliegen einer strikten Zweckbindung und Nutzungsbeschränkung. Nach Durchführung der Volkszählung, d. h. nach Beendigung der Tätigkeit der Erhebungsstelle, werden diese Dateien nicht mehr benötigt; sie sind dann unverzüglich zu löschen bzw. zu vernichten.

  Hierüber liegt eine Zusage des Senators für Inneres vor.

— Im Zusammenhang mit den eventuell einzuleitenden und durchzuführenden **Bußgeldverfahren** habe ich vorgeschlagen, die Zuständigkeit hierfür durch eine Änderung der entsprechenden Rechtsverordnung auf das Statistische Landesamt zu verlagern. Hierdurch könnte die sonst erforderliche Datenübermittlung an die Bußgeldbehörden, d. h. das Stadt- und Polizeiamt Bremen bzw. die Ortspolizeibehörde Bremerhaven vermieden werden. Bußgeldbescheide, die vom Stadt- und Polizeiamt Bremen bzw. der Ortspolizeibehörde Bremerhaven an säumige bzw. verweigernde Auskunftspflichtige verschickt werden, untergraben nach meiner Auffassung die Glaubwürdigkeit der politischen Erklärungen zur Trennung von Statistik und Verwaltung sowie zur statistischen Geheimhaltung. Ich wiederhole deshalb hier meinen diesbezüglichen Vorschlag.

— Die Erhebungsstellen sind ausschließlich mit der Durchführung der Zählung, d. h. der Datenerhebung betraut. Die **Übernahme und Aufbereitung der erhobenen Daten** ist Aufgabe des Statistischen Landesamtes Bremen. Die **statistische Auswertung und das Erstellen von Statistiktabellen** werden vom Statistischen Landesamt und auf Anforderung vom Statistischen Bundesamt durchgeführt. Die Erhebungsstellen haben nicht die Befugnis, die ausgefüllten Erhebungsbogen auszuwerten. Sie haben die ausgefüllten Erhebungsbogen und alle sonstigen Erhebungsunterlagen und Datenträger vielmehr vollständig, termingerecht und ohne vorherige Auswertung an das Statistische Landesamt zu leiten.

Dies ergibt sich aus der Rechtslage und ist ebenfalls unstrittig.

Zur Ordnungsmäßigkeit der Datenverarbeitung gehört es, daß die im Rahmen der Verbundprogrammierung der statistischen Ämter entwickelten Programme zur Übernahme und Plausibilisierung der erhobenen Daten und zur Erstellung der standardmäßigen statistischen Auswertungen/Tabellierungen vor ihrer Anwendung nicht nur getestet, sondern auch formell freigegeben und dokumentiert werden. Das Statistische Landesamt Bremen und das Rechenzentrum der bremischen Verwaltung sind gefordert, die einschlägigen Bestimmungen des Datenschutzrechts und der ADV-Anweisung genau zu beachten.

— Ende Januar 1987 trat das **neue Bundesstatistikgesetz in Kraft** (vgl. Pkt. 2.1.2.3). Damit hat sich auch der rechtliche Rahmen für die Durchführung der Volkszählung 1987 verändert. In diesem Zusammenhang haben sich einige rechtliche Fragen und Probleme ergeben, die kurzfristig und rechtsverbindlich durch die Innenbehörden des Bundes und der Länder zu klären waren. So beziehen sich z. B. die Fragebogen, Hinweise und Erläuterungen zur Volkszählung 1987 sämtlich auf das inzwischen außer Kraft getretene Bundesstatistikgesetz von 1980. Durch Änderung der Erhebungsbogen bzw. der Erläuterungspapiere ist dies inzwischen ausgeräumt worden. Auch das Verhältnis der Bestimmungen des Volkszählungsgesetzes 1987 und des neuen Bundesstatistikgesetzes zueinander wirft Fragen auf. Die Innenbehörden des Bundes und der Länder haben sich in diesem Zusammenhang auf folgende Rechtsanwendung verständigt:

  — Das Volkszählungsgesetz 1987 ist gegenüber dem Bundesstatistikgesetz lex specialis.

  — Soweit Fragen der Konkurrenz zwischen dem Bundesstatistikgesetz 1980 und dem neuen Bundesstatistikgesetz bestehen, gilt das neue Gesetz.

  — Bundesregierung und Länder sind bereit, auch ohne gesetzliche Verpflichtung akzeptanzfördernde, datenschutzrechtliche oder bürgerfreundliche Regelungen, die das neue Bundesstatistikgesetz enthält, bei der Durchführung der Volkszählung anzuwenden.

  Dies bedeutet z. B., daß die engeren Übermittlungsbestimmungen des Volkszählungsgesetzes 1987 (§ 14) zur Anwendung kommen und nicht die weitergehenden Möglichkeiten des neuen Bundesstatistikgesetzes. Der Senator für Inneres ist aufgefordert, diese einverständliche Absprache der Innenbehörden in konkretes Verwaltungshandeln des Statistischen Landesamtes und des Rechenzentrums der bremischen Verwaltung umzusetzen, z. B. durch besonderen Erlaß.

— Die Durchführung der Volkszählung wird **meine Arbeitskraft** auch im Jahre 1987 erheblich in Anspruch nehmen, wobei dann die Prüftätigkeit im Vordergrund stehen wird. Angesichts der Personalausstattung meiner Dienststelle führt dies zwangsläufig zu einem Kürzertreten in anderen Kontrollbereichen. Der Senat und die Bürgerschaft bleiben auch hier in der Verantwortung des § 27 BrDSG, wonach mir das notwendige Personal zur Verfügung zu stellen **ist.**

  Ich kann glaubhaft für die Öffentlichkeit meine Prüf- und Kontrolltätigkeit nur aufrecht erhalten, wenn mir Senat und Bürgerschaft das dafür notwendige Personal sofort zur Verfügung stellen.

5.2.4.2 Mikrozensus 1986

Das Statistische Landesamt führte auch im Berichtsjahr wieder auf der Grundlage des novellierten und 1985 in Kraft getretenen Mikrozensusgesetzes eine freiwillige Mikrozensus-Testerhebung und eine Mikrozensus-Haupterhebung durch. Mit der freiwilligen Erhebung soll erprobt werden, ob bei künftigen Mikrozensus-Erhebungen ganz oder teilweise auf die Auskunftspflicht verzichtet werden kann. Hierzu werden bis einschließlich 1987 parallel zur jeweiligen Haupterhebung Testerhebungen durchgeführt, bei denen keine Auskunftspflicht besteht.

Bei beiden Erhebungen wird zwischen Erhebungs- und Hilfsmerkmalen unterschieden. Angaben, die als Erhebungsmerkmale erfragt werden, sind für die Statistik bestimmt, während Hilfsmerkmale, nämlich Name und Anschrift der Befragten, nur für die Durchführung der Erhebung bestimmt sind.

Im Lande Bremen betraf die freiwillige Testerhebung rund 800 zu befragende Haushalte; die Rücklaufquote lag hierbei nach Angaben des Statistischen Landesamtes bei ca. 50 Prozent. Die Haupterhebung umfaßt gut 3000 Haushalte. Bei dieser

Erhebung ist wegen der Auskunftspflicht die Rücklaufquote natürlich deutlich höher; Anfang 1987 standen noch die Antworten von rund 80 Haushalten aus.

Im Zusammenhang mit der Durchführung des Mikrozensusgesetzes erhielt ich im Berichtsjahr eine Reihe von Anfragen von Betroffenen. Dabei ging es vor allem um Fragen wie z. B., ob die Befragung datenschutzrechtlich zulässig ist und ob eine Auskunftspflicht besteht. In einer weiteren Eingabe, welche von mehreren Anwohnern einer Straße unterzeichnet wurde, ging es um den Einsatz einer Interviewerin in deren unmittelbarer Nachbarschaft. Die Anwohner führten darüber Beschwerde, daß die Interviewerin nur ca. 10 Min. Wegstrecke von ihnen entfernt wohne und äußerten Besorgnis darüber, daß die durch die Erhebung erlangten Kenntnisse anderweitig verwendet werden könnten. Nach Prüfung des Sachverhaltes habe ich das Statistische Landesamt gebeten, das Erhebungsverfahren hinsichtlich eines „entfernteren" Einsatzes des Interviewers und eines deutlicheren Hinweises auf die Möglichkeit der postalischen Beantwortung der Fragebögen zu ändern.

5.2.5 Ordnungswesen

5.2.5.1 Schwerpunkte, Handlungsbedarfsfälle

— Erlaß eines Gesetzes über die Ausstellung von Vertretungsbescheinigungen

Der Senator für Inneres hat den Entwurf eines Gesetzes über die Ausstellung von Vertretungsbescheinigungen mit der Bitte um datenschutzrechtliche Beurteilung vorgelegt.

Das am 9. Dezember 1986 von der Bremischen Bürgerschaft beschlossene Gesetz regelt die Ausstellung von Bescheinigungen darüber, welche Vertreter von Vereinen, deren Rechtsfähigkeit auf staatlicher Verleihung beruht oder von rechtsfähigen Stiftungen des Bürgerlichen Rechts mit Sitz im Lande Bremen, zu deren Vertretung befugt sind.

Meine Vorschläge, den Zweck der Verwendung der personenbezogenen Daten der Vertretungsberechtigten im Gesetz festzulegen und Art und Umfang der personenbezogenen Daten, die erhoben und mit der Ausstellung von Bescheinigungen an Dritte übermittelt werden, auf das notwendige Maß zu beschränken, sind vom Senator für Inneres durch entsprechende Änderungen des Entwurfes in vollem Umfange berücksichtigt worden. Gleiches gilt für meine Anregung, eine Regelung zu treffen, daß Behörden eine Bescheinigung nur erhalten, wenn dieses für die Durchführung der in ihrer Zuständigkeit liegenden Aufgabe erforderlich ist.

Der Gesetzentwurf sah vor, daß Personen oder Stellen außerhalb des öffentlichen Bereichs dann eine Bescheinigung auszustellen ist, wenn sie ein rechtliches Interesse glaubhaft machen.

Wenn auch nicht verkannt werden soll, daß diese Voraussetzung eine erhebliche Beschränkung der mit der Ausstellung einer Bescheinigung verbundenen Datenübermittlung bedeutet, habe ich dennoch Bedenken, ob bei dieser Regelung im Einzelfall sichergestellt ist, daß das rechtliche Interesse der Bescheinigungsempfänger so qualifiziert ist, daß es in der Lage ist, das schutzwürdige Recht der Betroffenen auf informationelle Selbstbestimmung zurückzudrängen.

Ich habe deshalb angeregt, eine Regelung zu treffen, nach der die für die Ausstellung der Vertretungsbescheinigungen zuständige Stelle in jedem Einzelfall zu einer entsprechenden Prüfung verpflichtet worden wäre.

Diese Anregung hat im Gesetzgebungsverfahren keine Berücksichtigung gefunden. Es bleibt daher zu hoffen, daß die mit der Durchführung des Gesetzes betrauten Stellen die datenschutzrechtlichen Belange der Betroffenen ausreichend wahren.

— Erlaß von Wahlordnungen für die bremischen Deichverbände

Wegen der im Jahre 1986 anstehenden Neuwahlen zu den Vertretungsorganen der bremischen Deichverbände und wegen der erfolgten Satzungsänderungen der Deichverbände hat der Senator für Inneres den Entwurf von Neufassungen von Wahlordnungen für die Deichverbände vorgelegt und um datenschutzrechtliche Beurteilung gebeten.

Die Wahlordnungen sehen vor, daß der Wahlberechtigte oder dessen Stellvertreter auf Verlangen des Wahlvorstandes zur weiteren Prüfung der Wahlberechtigung den Beitragsbescheid des Deichverbandes vorzulegen hat.

Da sich in dem Beitragsbescheid aber auch Angaben über andere mit einem Grundstück in Zusammenhang stehende Abgaben wie Grundsteuern und Müllabfuhrgebühren befinden, sehe ich die Vorlage dieses Bescheides und die damit verbundene Offenbarung personenbezogener Daten als Voraussetzung für die Wahrnehmung eines demokratischen Wahlrechtes als einen zu weitgehenden Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen an.

Leider konnte der Senator für Inneres sich nicht entschließen, meiner Anregung zu folgen, auf die Vorlage des Beitragsbescheides zu verzichten und zum Nachweis der Wahlberechtigung geeignete andere Maßnahmen vorzusehen. Er hat dieses damit begründet, daß nach dem derzeitigen Stand der automatisierten Datenverarbeitung keine Möglichkeit bestünde, die Aufstellung eines Wahlausweises für alle Wahlberechtigten vorzunehmen oder die Briefwahl zu eröffnen. Außerdem sei von der Vorlagepflicht nur ein kleiner Personenkreis betroffen. Den Betroffenen wird allerdings die Möglichkeit eingeräumt, bei der Vorlage des Beitragsbescheides alle die Grundbesitzabgaben betreffenden Beträge unkenntlich zu machen.

Die getroffene Regelung ist datenschutzrechtlich unbefriedigend, weil die wahlberechtigten Grundstückseigentümer in aller Regel ihren Beitragsbescheid für eine Vielzahl anderer Zwecke — z. B. für die Abrechnung mit Mietern — benötigen und deshalb die Angaben nicht unkenntlich machen können.

Die zuständigen Stellen bleiben deshalb aufgerufen, spätestens zur nächsten Wahl eine Regelung zu treffen, die die Vorlage des Beitragsbescheides überflüssig macht. Die ersten Entwürfe der Wahlordnungen enthielten eine Vorschrift, nach der die Mitglieder der Wahlvorstände möglichst in dem Wahlbezirk wohnen sollen, für den der Wahlvorstand gebildet wird. Da bei einer solchen Regelung den Mitgliedern der Wahlvorstände personenbezogene Daten von Wahlberechtigten aus ihrer unmittelbaren Umgebung bekannt werden, habe ich vorgeschlagen, die Vorschrift so zu fassen, daß Wahlvorstandsmitglieder nicht in einem für ihr Wohngebiet zuständigen Wahlvorstand tätig werden sollen.

Die zitierte ursprünglich vorgesehene Vorschrift ist zwar nicht in die Wahlordnungen aufgenommen worden, der Senator für Inneres ist jedoch meiner Anregung, hier eine datenschutzrechtlich positiv wirkende Regelung aufzunehmen, nicht gefolgt.

Mein Vorschlag, die Mitglieder der Wahlorgane bei der Verpflichtung zur Amtsverschwiegenheit besonders auf die Verschwiegenheitspflicht hinsichtlich der ihnen bei der Ausübung ihres Amtes bekannt gewordenen personenbezogenen Daten hinzuweisen, ist bei dem Erlaß der Wahlordnungen nicht berücksichtigt worden.

Ich erwarte, daß die Wahlordnungen rechtzeitig zu den nächsten Wahlen zu den Organen der Deichverbände zugunsten einer datenschutzfreundlicheren Regelung geändert werden.

5.2.6 Ausländerangelegenheiten

5.2.6.1 Schwerpunkte, Handlungsbedarfsfälle

— Datenverarbeitung bei Ausländerbehörden und beim Ausländerzentralregister

Die Durchführung des Ausländergesetzes und einer Reihe weiterer Ausländer betreffende Gesetze ist in der Stadtgemeinde Bremen der beim Stadt- und Polizeiamt und in der Stadtgemeinde Bremerhaven der bei der Verwaltungspolizei eingerichteten Ausländerbehörde übertragen, soweit diese Aufgabe den Ländern obliegt. Diese Behörden sammeln über Ausländer, die sich im Lande Bremen aufhalten, aufgehalten haben oder einen Aufenthalt beabsichtigen, eine Fülle personenbezogener Daten, die teils bei den Betroffenen erhoben werden und teils von einer Vielzahl von Behörden an die Ausländerbehörden übermittelt werden. Auch von Deutschen im Sinne des Art. 116 des Grundgesetzes und von deutschen Staatsangehörigen, die neben der deutschen eine fremde Staatsangehörigkeit haben, werden solche Daten gesammelt.

Bereichsspezifische Rechtsgrundlage für die Erhebung und Verarbeitung dieser Daten sind das Ausländergesetz, die dazu ergangene Rechtsverordnung und einige weitere Ausländer betreffende Gesetze.

Nach meiner Auffassung erfüllen ein großer Teil der datenschutzrechtlich relevanten Vorschriften dieser Rechtsnormen nicht die Anforderungen, die das Bundesverfassungsgericht an Normen gestellt hat, die das Grundrecht auf das informatio-

nelle Selbstbestimmungsrecht einschränken. Das gilt insbesondere für die Forderung nach Normenklarheit. Die Ausländerbehörden sammeln auch wesentlich mehr Daten, als für die ausländerrechtlichen Entscheidungen, die sie nach den genannten Rechtsnormen zu treffen haben, erforderlich sind. Sie haben dieses damit begründet, daß ihnen aus repressiver und präventiver Sicht eine ordnungsbehördliche Aufgabe der Ausländerüberwachung zukomme. Diese Auffassung ist ihnen in früheren Jahren durch Entscheidungen der Verwaltungsgerichtsbarkeit bestätigt worden. Sie kann jedoch nach der dahingehend geänderten Rechtsauffassung, daß es sich bei dem Recht auf informationelle Selbstbestimmung um ein Recht von Verfassungsrang handelt, nicht mehr aufrecht erhalten werden. Das Recht auf informationelle Selbstbestimmung steht jedermann, also auch allen in der Bundesrepublik Deutschland lebenden Ausländern zu.

Der Umfang der praktizierten Datenverarbeitung ergibt sich im wesentlichen aus der Allgemeinen Verwaltungsvorschrift zur Ausführung des Ausländergesetzes. Diese kann jedoch deren Zulässigkeit nicht begründen. Das Bundesverfassungsgericht hat in seinem Urteil zum Volkszählungsgesetz 1983 ausdrücklich erwähnt, daß Verwaltungsvorschriften nicht in der Lage sind, das Recht auf informationelle Selbstbestimmung einzuschränken.

Ein großer Teil der von den Ausländerbehörden gesammelten Daten wird an ein beim Bundesverwaltungsamt geführtes Ausländerzentralregister übermittelt. Einer Vielzahl von Behörden, aber auch nicht-öffentlichen Stellen werden Auskünfte aus diesem Register erteilt. Der Umfang der hier stattfindenden Verarbeitung personenbezogener Daten mag der Tatsache entnommen werden, daß von etwa 10 Millionen Personen weit über 100 Millionen Daten gespeichert sind. Eine ausreichende Rechtsgrundlage für die Führung dieses Registers und der damit verbundenen Datenverarbeitung ist nicht vorhanden. Das Gesetz über die Errichtung eines Bundesverwaltungsamtes weist diesem lediglich die Aufgabe der Registerführung zu. Diese Rechtsgrundlage reicht nicht aus und ist von mir kritisiert worden.

Unter Federführung des Bundesministers des Innern wird zur Zeit das bestehende Ausländerzentralregister überarbeitet. Erste Entwürfe der Neukonzeption sind den Datenschutzbeauftragten inzwischen vorgelegt worden. Die Landesbeauftragten für den Datenschutz sind bei der Erarbeitung der Konzeption leider nicht beteiligt worden. Sie haben gemeinsam mit dem Bundesbeauftragten für den Datenschutz einen Arbeitskreis gebildet, der sich mit der vorgelegten Neukonzeption des Ausländerzentralregisters befaßt hat. Ich habe mich an diesem Arbeitskreis beteiligt. Er hat einen Entwurf einer ersten Stellungnahme der Konferenz der Datenschutzbeauftragten zur Beratung und Beschlußfassung vorgelegt.

Ich begrüße grundsätzlich die Schaffung einer verfassungsrechtlich notwendigen Regelung sowohl für die Datenverarbeitung beim Bundesverwaltungsamt als auch für die Kommunikation der Teilnehmer mit dem Ausländerzentralregister. Im Verlauf der weiteren Beratungen gilt es zu vermeiden, daß es übermäßig in das „System zum Schutze der inneren Sicherheit" eingebunden wird. Es muß vermieden werden, daß die für Ausländer konzipierte Sondervorschrift zu einer allgemeinen Diskriminierung der Betroffenen als potentielle Rechtsbrecher führt.

Ich erwarte, daß durch die im Zusammenhang mit der Neukonzeption des Ausländerzentralregisters notwendig werdenden Änderungen der ausländerrechtlichen Regelungen auch eine ausreichende Rechtsgrundlage für die vorher erwähnte Datenverarbeitung bei den Ausländerbehörden geschaffen wird, da die dort geübte Praxis ohne Rechtsgrundlage höchstens noch für eine Übergangszeit hingenommen werden kann.

5.3 Rechtspflege und Strafvollzug

5.3.1 Schwerpunkte, Handlungsbedarfsfälle

5.3.1.1 Fassung der Vordrucke für Zeugenladungen in Strafsachen

Ein Datenschutzbeauftragter eines anderen Bundeslandes wies darauf hin, daß die vom Arbeitgeber auszufüllende Bescheinigung über den Verdienstausfall auf der Rückseite des Vordrucks für die Ladung von Zeugen in Strafsachen enthalten ist. Auf diese Weise könne der Arbeitgeber die auf der Vorderseite des Vordrucks angeführten Namen der Angeklagten erfahren. Deshalb wurde vorgeschlagen, einen neuen Vordruck einzuführen, der im Durchschreibewege ausgefüllt werden könnte und bei dem in der Durchschrift die Felder mit dem Namen des Angeklag-

ten geschwärzt wären; auf der Rückseite dieser Durchschrift könnte dann die Bescheinigung über den Verdienstausfall vorgesehen werden.

Ich habe dem Senator für Rechtspflege und Strafvollzug gegenüber diesen Vorschlag unterstützt und gebeten, ihn zu übernehmen.

Der Senator für Rechtspflege und Strafvollzug hat die Auffassung vertreten, daß die Bedenken gegen die bisherige Praxis nicht von außerordentlicher Bedeutung seien, und er habe erhebliche Zweifel daran, ob mit der vorgeschlagenen Änderung der gewünschte Zweck erzielt werden könnte. Darüber hinaus hat er aus seiner Sicht unverhältnismäßig hohe Mehrkosten angeführt, so daß er an der bisherigen Praxis festhalten wolle. Ich habe den Senator für Rechtspflege und Strafvollzug gebeten, noch einmal zu prüfen, ob nicht nach Verbrauch der Formulare ein den Datenschutzanforderungen entsprechendes Verfahren entwickelt werden kann.

In der Neuauflage von Vordrucken kann ich keine unverhältnismäßig hohen Mehrkosten erkennen.
Ein nur angenommener geringer Verwaltungsaufwand rechtfertigt nicht, von einer Änderung der Vordrucke abzusehen. Die Weitergabe personenbezogener Daten an Dritte — in diesem Falle an den Arbeitgeber — darf nur im überwiegenden Allgemeininteresse und aufgrund einer klaren Rechtsgrundlage geschehen. Der Staat hat bei seinem Verwaltungshandeln daher das informationelle Selbstbestimmungsrecht zu respektieren und das Verfahren so zu gestalten, daß unnötige Beeinträchtigungen ausbleiben.

Der Senator für Rechtspflege und Strafvollzug hat mitgeteilt, daß er die Gerichte nochmals um Prüfung meiner Vorschläge gebeten hat.

5.3.1.2 Einführung der elektronischen Datenverarbeitung in der Bremer Justiz

Im Rahmen einer kleinen Anfrage einer Bürgerschaftsfraktion wurde der Senat um Auskunft gebeten, welches Konzept zur Einführung der elektronischen Datenverarbeitung in der Bremer Justiz verfolgt wird.

In seiner Antwort hat der Senat dargelegt, daß die Effektivität des gerichtlichen Rechtsschutzes nach rechtsstaatlichen Grundsätzen entscheidend daran gemessen werden muß, innerhalb welchen Zeitraumes ein rechtsuchender Bürger mit einer richterlichen Entscheidung rechnen kann. Die angespannte Haushaltslage sowie die seit Jahren zunehmende Geschäftsbelastung der Gerichte und Staatsanwaltschaften mache es aus der Sicht des Senats erforderlich, die Verfahrensabläufe mit möglichst weitgehend technischen Hilfsmitteln zu vereinfachen. Die Justizministerkonferenz habe der Gesellschaft für Mathematik und Datenverarbeitung in Bonn einen Untersuchungsauftrag für die Rationalisierungsmöglichkeiten — insbesondere im Geschäftsstellenbereich der Gerichte — erteilt. Der Abschlußbericht komme zu dem Ergebnis, daß die herkömmlichen Rationalisierungsmöglichkeiten in diesem Bereich weitgehend erschöpft seien. Nennenswerte weitere Rationalisierungsmöglichkeiten beständen nur noch durch die Einführung der elektronischen Datenverarbeitung.

Zu diesem Zweck hat die Justizministerkonferenz schon im Jahre 1969 eine Bund-Länder-Kommission für Datenverarbeitung in der Justiz eingesetzt. Sie hat die Aufgabe, die Arbeitsgebiete der Justizverwaltung auf die Automationseignung und -würdigkeit zu untersuchen. Schwerpunktmäßig hat sich die Kommission mit der Entwicklung folgender Projekte befaßt:

— EDV-Grundbuch

— Automatisierung des Mahnverfahrens

— Automatisierung der Geldstrafen, Vollstreckung und Gerichtskosteneinziehung.

Nachdem eine Projektgruppe in Bayern im Auftrag der Bund-Länder-Kommission für Datenverarbeitung in der Justiz das EDV-Verfahren **„Automatisierung des Grundbuchs** unter Berücksichtigung der **Integration mit dem Liegenschaftskataster"** entwickelt hat, hat der Ausschuß für ADV 1982 die Einsetzung einer Arbeitsgruppe „EDV-Grundbuch/Liegenschaftskataster" eingesetzt, die die Übernahme des EDV-Verfahrens vorbereiten sollte. Als festsstand, daß Bremen nicht in der Lage ist, ein EDV-Verfahren dieser Größenordnung allein einzuführen, wurde das entwickelte automatisierte Grundbuchverfahren nicht weiter verfolgt. Für Eigentümerverzeichnis und Liegenschaftskataster soll eine gemeinsame EDV-Lösung erarbeitet werden.

Auch das EDV-Verfahren **„Gerichtskosten und Geldstrafenvollstreckung"** soll aus wirtschaftlichen Gründen nicht isoliert eingeführt, sondern mit anderen Automatisierungsverfahren integriert werden. Hierbei wird an das bei der Staatsanwaltschaft Bremen bereits eingeführte EDV-Verfahren CANASTA und die aktuellen EDV-Planungen der Arbeitsgruppe „Haushalts-, Kassen- und Rechnungswesen" gedacht.

Als weiteres EDV-Projekt mißt der Senat dem **EDV-Mahnverfahren** größere Bedeutung bei. Die Landesjustizverwaltung Baden-Württemberg hat im Auftrag der Bund-Länder-Kommission für Datenverarbeitung in der Justiz eine Automationslösung zur Bearbeitung gerichtlicher Mahnverfahren entwickelt. Da eine Einführung dieses EDV-Projektes für Bremen allein unwirtschaftlich erscheint, wird in der Senatsverwaltung gegenwärtig geprüft, ob eine gemeinsame Lösung mit Hamburg möglich ist.

Darüber hinaus nennt der Senat als einen weiteren Schwerpunkt der zukünftigen EDV-Entwicklungen das justizspezifische **Bürokommunikationssystem SOJUS** (Software-System zur Unterstützung operativer Hilfsaufgaben in der Justiz). SOJUS ist ein justizspezifisches Bürosystem zur Unterstützung der Geschäftsstellen- und Kanzleitätigkeiten bei den Gerichten und Staatsanwaltschaften. Es ersetzt als Eintragungs- und Auskunftssystem die bisher notwendige manuelle Register- und Kalenderführung in den Gerichten und Staatsanwaltschaften und ermöglicht die Erstellung einer Vielzahl von Auswertungen und Übersichten auf der Basis der abgespeicherten Verfahrensdaten usw.. Dieses System setzt auf der Ebene der Sachbearbeitung (Eingangsstelle/Geschäftsstelle) an und berührt als Auswirkung besonders den Schreibbereich.
Ich werde die Entwicklung auf diesem Gebiet besonders beachten und erwarte eine frühzeitige Beteiligung.

Beim Amtsgericht Bremen soll das Schuldnerverzeichnis (Karteikarten) und das Vollstreckungsregister (Buch) durch das **ADV-Verfahren AVUS** (Automatisiertes Vollstreckungs- und Schuldnerverzeichnis) ersetzt werden, mit dem auch Textverarbeitung durchgeführt werden kann.

Auf dem System sollen nur das Vollstreckungsregister und das Schuldnerverzeichnis geführt werden. Eine darüber hinausgehende Nutzung als Textverarbeitungssystem sowie die Übernahme weiterer Funktionen mit Ausnahme einer eventuellen Automatisierung des Handelsregisters ist nicht vorgesehen. Bei dem Einsatz der mittleren Datentechnikanlage handelt es sich um eine separate Lösung, eine Verknüpfung mit anderen Systemen ist nicht vorgesehen. Ein Anschluß der Amtsgerichte Blumenthal und Bremerhaven und die Führung einer Datei dieser Gerichte wird nicht angestrebt.

Auf Grundlage dieser mir vom Senator für Rechtspflege und Strafvollzug mitgeteilten Voraussetzungen habe ich eine Stellungnahme darüber abgegeben, was an datenschutzrechtlichen Vorkehrungen bei der Einführung von AVUS zu treffen ist. Meine Ausführungen bezogen sich dabei sowohl auf das Schuldnerverzeichnis als auch auf das Vollstreckungsregister. Ich habe Regelungen zum Arbeitnehmerdatenschutz und zur Entwicklung eines Datensicherheitskonzeptes gefordert. Schließlich habe ich in meiner Stellungnahme darauf hingewiesen, daß die Vorschrift des § 915 Zivilprozeßordnung (ZPO) demnächst datenschutzgerechter gestaltet werden sollte (vgl. auch meine Ausführungen unter Pkt. 5.3.1.5). So ist bekannt, daß den Vollstreckungsgerichten vielfach die zur einwandfreien Identifizierung eines Schuldners notwendigen Daten nicht bekannt sind und deshalb auch nicht in das Schuldnerverzeichnis eingetragen werden können. Damit ist aber das Risiko von Verwechslungen und damit die Beeinträchtigung schutzwürdiger Belange Dritter verbunden. Richtig ist, daß diese Probleme nicht durch die Automatisierung hervorgerufen werden, die leichtere, gegebenenfalls häufigere Nutzung des Schuldnerverzeichnisses könnte aber zu einer Häufung der Probleme führen. Ich erwarte daher, daß das ADV-Verfahren bei einer Novellierung umgehend den neuen Bedingungen angepaßt werden wird.

Da sich meine Stellungnahme lediglich auf die Beschaffungsmaßnahme bezog, gehe ich davon aus, daß bei der Installation der Anlage weitere datenschutzrechtliche Beratung erforderlich sein wird.

Die in diesem Beitrag dargestellte zunehmende Automatisierung auch im Bereich der Justizverwaltung in Bremen erfordert umfassende Datenschutzkonzepte. Ich gehe davon aus, daß ich vor Einführung der genannten und weiterer geplanter Automatisierungsverfahren in die Planungen einbezogen werde.

5.3.1.3 Akteneinsicht in Gerichtsakten zu Forschungszwecken

In verschiedenen Fällen hatte ich zu prüfen, ob zu Forschungszwecken Dritten Einsicht in Gerichtsakten zu gewähren sei. Grundsätzlich ist darauf hinzuweisen, daß die Verarbeitung personenbezogener Daten zu Forschungszwecken einer ausreichenden normenklaren bereichsspezifischen Rechtsgrundlage bedarf. Urteile können Dritten daher zur Zeit nur in der Form zur Verfügung gestellt werden, daß sie keinen Personenbezug mehr erkennen lassen. Ist die Weitergabe von Urteilen in nicht-anonymisierter Form beabsichtigt, ist die Übermittlung des vollständigen Inhalts des Urteils nur mit vorheriger Einwilligung des Betroffenen möglich. An einem solchen Ergebnis kann auch eine sogenannte datenschutzrechtliche Erklärung des Forschers, er werde das Datengeheimnis beachten und er unterwerfe sich meiner Kontrolle, nichts ändern. Die Verletzung des Persönlichkeitsrechts geschieht bereits in der Offenbarung des gesamten Urteilsinhalts, nicht erst durch Veröffentlichung der wissenschaftlichen Ergebnisse. Diese Auffassung wird u. a. auch durch das Urteil des Bundesverfassungsgerichts (NJW 86, 1243) bestätigt, das erklärt hat, daß aus Artikel 5 Abs. 3 Grundgesetz (GG) kein verfassungsunmittelbarer Anspruch auf Akteneinsicht zu Forschungszwecken herzuleiten ist.

Im vorliegenden Fall war aufgrund einer Eingabe datenschutzrechtlich zu prüfen, ob eine Akteneinsicht in Gerichtsakten der Familiengerichte zu Forschungszwecken datenschutzrechtlich zulässig war. Neben der oben skizzierten Rechtslage waren § 34 Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit (FGG), § 621 a Abs. 1 Zivilprozeßordnung (ZPO) bei dem Verfahren nach dem Gesetz über die Angelegenheit der freiwilligen Gerichtsbarkeit im übrigen und auch bei Verbundsachen (§ 623 ZPO) gemäß § 299 Abs. 2 ZPO bei der Entscheidung über das Recht auf Einsicht in Gerichtsakten durch Dritte zu berücksichtigen.

Nach § 299 Abs. 2 ZPO wird die Einsicht ohne Einwilligung der Parteien gewährt, wenn der Antragsteller ein rechtliches Interesse glaubhaft macht, gemäß § 34 FGG ist ein berechtigtes Interesse glaubhaft zu machen.
Der Begriff des rechtlichen Interesses ist enger als derjenige des berechtigten Interesses. Jeder, dessen Rechtskreis durch den Akteninhalt berührt wird, besitzt ein rechtliches Interesse. Zu entscheiden war daher, ob dies auf jemanden, der die Akten lediglich zu wissenschaftlichen Zwecken einsehen will, zutrifft. Die persönlichen Rechte des Forschers werden durch den Akteninhalt nicht berührt, trotzdem wird das rechtliche Interesse in diesem Fall vielfach damit begründet, daß das Forschungsinteresse ein öffentlich-rechtliches Interesse sei, was ausreichen müsse.

Eine solche weite Auslegung des § 299 Abs. 2 ZPO halte ich für nicht vertretbar. Ehescheidungsakten betreffen unter Berücksichtigung des Bundesverfassungsgerichts (BVerfGE 34, 209) den privaten Lebensbereich der Ehepartner, der unter dem Schutz auf freie Entfaltung der Persönlichkeit im Zusammenhang mit Verpflichtung aller staatlichen Gewalt zur Achtung der Menschenwürde steht. Die Intimsphäre ist auch von den Gerichten zu wahren. Nur im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgebotes dürfen Vorgänge offenbart werden. Dabei sind alle wesentlichen persönlichen und tatsächlichen Umstände des Einzelfalls zu würdigen.

Regelmäßig dürfte daher dem Schutz der Persönlichkeit der Betroffenen ein sehr viel stärkeres Gewicht zuzubilligen sein als dem reinen wissenschaftlichen Interesse an der Verwertung der Akten. Auch wenn solche Rechtstatsachenforschungen der Fortentwicklung des geltenden Rechts dienen, ist nicht ersichtlich, warum dies nicht mit Hilfe z. B. anonymisierter Abschriften der Akten möglich sein sollte.

§ 299 Abs. 2 ZPO sollte daher normenklarer gefaßt werden.

Aber auch einer Akteneinsicht nach § 34 FGG konnte ich nicht zustimmen. Ein berechtigtes Interesse als Voraussetzung für die Akteneinsicht ist jedes vollständige, durch die Sachlage gerechtfertigtes Interesse, auch ein wirtschaftliches Interesse. Da dieses Interesse sehr viel umfassender ist, könnte man die Einsicht zu Forschungszwecken hier für zulässig halten. Aber auch bei § 34 FGG ist im Rahmen der Ermessensentscheidung der starke Eingriff in die Intimsphäre bei der Einsicht in die hier in Frage stehenden Akten gegen das Forschungsinteresse abzuwägen. Die personenbezogene Auswertung der Akten ist in der Regel unverhältnismäßig, da anonymisierte Abschriften denselben Zweck erfüllen würden.

Ich halte daher weiterhin eine Akteneinsicht in Scheidungsakten der Familiengerichte für datenschutzrechtlich nicht zulässig und begrüße, daß der Senator für Rechtspflege und Strafvollzug meine datenschutzrechtlichen Bedenken im wesentlichen teilt.

In einem anderen Fall war im Rahmen eines **Forschungsprojektes** „Sachverständigen-Gutachten zur Schuldunfähigkeitsbeurteilung" der Senator für Rechtspflege und Strafvollzug gebeten worden, die Einsicht in Schwurgerichtsakten des Landgerichts Bremen zu ermöglichen.

Der Senator für Rechtspflege und Strafvollzug teilt die Auffassung, wonach die Akteneinsicht in Strafakten durch Dritte nur zulässig ist, wenn die Zustimmung der Betroffenen vorliegt oder die Akten anonymisiert sind. Der Bitte des Forschungsinstituts konnte daher nicht entsprochen werden.

Diese Beispiele zeigen, daß eine Forschungsklausel bei der Novelle des Bremischen Datenschutzgesetzes dringend geboten ist.

5.3.1.4 Justizmitteilungsgesetz (MiZi, MiStra)

Der Senator für Rechtspflege und Strafvollzug hat mir den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz) des Bundesministers der Justiz mit Stand vom 8. September 1986 zur Stellungnahme zugeleitet. Durch dieses Gesetz sollen offensichtlich die jetzt geltenden Verwaltungsvorschriften der Mitteilungen in Zivilsachen (MiZi) und der Mitteilungen in Strafsachen (MiStra) abgelöst werden.

Eine von den Datenschutzbeauftragten des Bundes und der Länder eingesetzte Arbeitsgruppe hat zu den einzelnen gesetzlichen Vorschriften eine in koordinierter Abstimmung erarbeitete Stellungnahme zu den einzelnen Rechtsvorschriften erarbeitet, auf deren Darstellung im einzelnen hier verzichtet werden soll.

Grundsätzlich ist zu bemerken, daß die von mir erhobenen Forderungen und dargestellten Prinzipien, die ich zu den Anordnungen über MiStra und MiZi erhoben habe (vgl. zuletzt 8. Jahresbericht Pkt. 5.3.1 und 5.3.2, S. 39 mit Anlage), nicht an Bedeutung verloren haben, da der Entwurf des Bundesministers der Justiz sie leider nicht in ausreichendem Maße berücksichtigt. Der Entwurf ist aber ein erster konkreter Schritt auf dem Weg zu einer nach dem Volkszählungsurteil des Bundesverfassungsgerichts unumgänglich gewordenen gesetzlichen Verankerung des Mitteilungswesens im Justizbereich.

Da der Entwurf sich bewußt auf Mitteilungen von Amts wegen an öffentliche Stellen beschränkt, die Aufgaben außerhalb des zugrundeliegenden Strafverfahrens wahrzunehmen haben, und für Mitteilungen an Verfahrensbeteiligte sowie für Mitteilungen auf Ersuchen wegen des Sachzusammenhanges mit dem Akteneinsichtsrecht auf die einzelnen Prozeßordnungen verweist, müssen dann hier ebenfalls noch die entsprechenden gesetzlichen Grundlagen geschaffen werden.

Die geringe Regelungsdichte, die den Entwurf durchweg kennzeichnet, ist enttäuschend. Der vom Bundesverfassungsgericht mehrfach postulierte Grundsatz der Normenklarheit bedeutet auch, daß Beschränkungen des Grundrechts auf informationelle Selbstbestimmung nicht lediglich durch Regelungen mit generalklauselartiger Weite erfolgen dürfen. Die im Entwurf enthaltenen generalklauselartigen Bestimmungen lassen Anlaß und Umfang der vorgesehenen Datenverarbeitung nicht hinreichend deutlich erkennen und bergen zudem die Gefahr in sich, daß etwaige ergänzende, auf besondere Fallgruppen bezogene Regelungen mit ihren den verfassungsrechtlichen Vorgaben angepaßten Beschränkungen schlicht umgangen werden. Der Gesetzgeber sollte seine Kompetenz hier im Interesse einer möglichst bundeseinheitlichen Verfahrensweise voll ausschöpfen. Der jetzt vorgelegte Entwurf macht jedenfalls in weitem Maße landesrechtliche Regelungen erforderlich. Leider macht der Entwurf nicht hinreichend deutlich, in welchem Umfange er bewußt auf eine Regelung zugunsten landesgesetzlicher Ausfüllung verzichtet hat.

Insgesamt ist zu sagen, daß je präziser und abschließender die Mitteilungspflichten auf bundes- oder landesrechtlicher Ebene gesetzlich geregelt worden sind, desto eher werden diese Regelungen es ermöglichen, die Durchführungskompetenz den Geschäftsstellen zu übertragen.

Sollte es gleichwohl bei der vorgesehenen geringen Regelungsdichte des Entwurfs bleiben, so dürfte eine Ausfüllung des vorgegebenen Rahmens keinesfalls durch bloße Verwaltungsvorschriften erfolgen; vielmehr müßten weitere Rechtsnormen (Gesetz, Rechtsverordnung) erlassen werden. Dies ergibt sich nicht zuletzt aus dem Grundsatz des Gesetzesvorbehalts, den das Bundesverfassungsgericht im Volkszählungsurteil für das Grundrecht auf informationelle Selbstbestimmung eindeutig bestätigt hat. Der möglichen Intention, das neue Justizmitteilungsgesetz in der Fassung des Entwurfs durch die gegebenenfalls noch in einzelnen Punkten refor-

miert geltende MiStra und MiZi zu konkretisieren, muß bereits heute mit Nachdruck entgegengetreten werden.

Ich gehe davon aus, daß die Arbeiten am Justizmitteilungsgesetz in der neuen Legislaturperiode zügig fortgesetzt werden und werde den Senator für Rechtspflege und Strafvollzug auch bei den weiteren Schritten datenschutzrechtlich beraten.

5.3.1.5 Schuldnerverzeichnis nach § 915 ZPO

Nach § 915 Abs. 4 Zivilprozeßordnung (ZPO) hat das Vollstreckungsgericht ein Verzeichnis der Personen zu führen, die vor ihm eine eidesstattliche Versicherung abgegeben haben oder gegen die wegen einer verweigerten eidesstattlichen Versicherung die Haft angeordnet ist (Schuldnerverzeichnis). Eine allgemeine Vorschrift des Bundesministers der Justiz vom 1. August 1955 regelt die Erteilung und die Entnahme von Abschriften oder Auszügen aus dem Schuldnerverzeichnis.

In meinem 8. Jahresbericht (vgl. unter Pkt. 5.3.1.6, S. 41 ff.) habe ich auf die dringende Notwendigkeit einer Novellierung dieser Vorschriften hingewiesen und einige dabei zu berücksichtigende Datenschutzanforderungen dargestellt.

Ging ich damals noch davon aus, daß es zu einer baldigen Novellierung kommen würde, so muß ich jetzt leider mitteilen, daß der Bundesjustizminister sich im Laufe des Jahres 1986 entschlossen hat, in der abgelaufenen Legislaturperiode keine Gesetzesnovelle mehr in den Bundestag einzubringen. Entscheidend ist dabei offensichtlich gewesen, daß das Bundesjustizministerium von den Wirtschaftsverbänden zu einer weiteren Öffnung des Schuldnerverzeichnisses gedrängt wird, während die Datenschutzbehörden die Erteilung einer Auskunft aus dem Schuldnerverzeichnis durch das Amtsgericht jeweils von dem Nachweis eines berechtigten Interesses abhängig machen, und daß die zum Bezug berechtigten Körperschaften des öffentlichen Rechts ihren Mitgliedern keine aus Abdrucken aus dem Schuldnerverzeichnis hergestellte Listen zur Verfügung stellen sollen, sondern nur Einzelauskünfte erteilen sollen.

Ich bedaure, daß das Bundesjustizministerium die überfällige Novellierung des § 915 ZPO in der letzten Legislaturperiode nicht vorangebracht hat und hoffe, daß die längst fällige datenschutzgemäße Überarbeitung des § 915 ZPO in dieser Legislaturperiode zügig erledigt wird.

5.3.1.6 Informationsverarbeitungsregelungen im Strafverfahren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz haben auf ihrer Sitzung am 24./25. November 1986 Überlegungen zur Informationsverarbeitung im Strafverfahren verabschiedet, die bei der Novellierung der einschlägigen Gesetze aus datenschutzrechtlicher Sicht Berücksichtigung finden sollen. Die Vorlage für die Konferenz war in einer Arbeitsgruppe unter meiner Federführung erstellt worden.

Dabei sind folgende Themenschwerpunkte berücksichtigt worden:

- Befugnisnormen für die Informationserhebung und gesetzliche Regelungen der Fahndungsmaßnahmen im Strafverfahren
  - Ausschreibung des Beschuldigten zur Festnahme
  - Ausschreibung des Beschuldigten zur Aufenthaltsermittlung
  - Ausschreibung von Zeugen zur Aufenthaltsermittlung
  - Öffentlichkeitsfahndung
  - Befugnisnormen für besondere Fahndungsmethoden und den Einsatz technischer Mittel
    - Raster-Fahndung
    - SPUDOK und entsprechende automatisierte Sammlungen und Suchsysteme
    - polizeiliche Beobachtung
    - erkennungsdienstliche Behandlung
    - Informationserhebung in Versammlungen zu Zwecken der Strafverfolgung

- — Einsatz lesender oder mithörender technischer Geräte und Bildaufzeichnungen/Video
- — Informationserhebung durch Inanspruchnahme von Informanten oder durch den Einsatz von V-Personen und verdeckten Ermittlern

— Allgemeine Befugnisnormen für die Speicherung und sonstige Verwendung von Daten

— Gesetzliche Regelung für die Nutzung und die Weitergabe von Daten

- — Allgemeine Regelungen für die Datenweitergabe im Verhältnis Staatsanwaltschaft/Polizei
- — Weitergabe von Daten zwischen Staatsanwaltschaften
- — Informationssysteme zur Strafverfolgung, zentrale Namensdateien und Aktennachweissysteme
- — Berichtspflichten in Strafsachen (BeStra)

— Wahrnehmung der Rechte des Beschuldigten, andere am Verfahren Beteiligter, Dritter und der Öffentlichkeit

- — Akteneinsichtsrechte
  - — Akteneinsicht für öffentliche Stellen
  - — Akteneinsicht durch die Verteidigung
  - — Akteneinsicht durch den verteidigerlosen Beschuldigten
  - — Akteneinsicht durch Privat- und Nebenkläger oder durch Rechtsanwälte zur Geltendmachung von Ansprüchen Dritter
  - — Akteneinsicht für wissenschaftliche Zwecke
- — Wahrung der Rechte des vom Strafverfahren Betroffenen und am Strafverfahren Beteiligter bei Mitteilungen personenbezogener Angaben durch die Staatsanwaltschaft und Gerichte
- — Öffentlichkeit und Schutz der Persönlichkeit (§§ 169 ff. GVG); Nennnung des Angeklagten durch Aushang im Gericht; Verzicht auf das Verlesen von Papieren in geeigneten Fällen (§ 249 StPO)
- — Auskünfte an die Medien
- — Kontrolle von Gerichtsbesuchern und Speicherung der Daten durch andere Behörden

— Aufbewahrungs- und Löschungsbestimmungen

— Aussage- und Zeugnisverweigerungsrechte

— Organisatorische Maßnahmen

Den vollständigen Wortlaut des Konferenzbeschlusses habe ich in Anlage 4 zu diesem Bericht abgedruckt.

5.3.1.7 Staatsanwaltschaftliches Informationssystem (SISY)

Aufgrund eines Beschlusses der Generalstaatsanwälte und des Generalbundesanwaltes aus dem Jahre 1984 hat die Konferenz der Justizminister und Senatoren beschlossen zu prüfen, ob der Aufbau eines eigenständigen länderübergreifenden staatsanwaltschaftlichen Informationssystems (SISY) betrieben werden sollte. Ging man zunächst davon aus, daß lediglich ein Bedürfnis für einen länderübergreifenden Austausch zur Bekämpfung der Schwerkriminalität und bei besonderen Formen der Kriminalität besteht, so hat eine auf Bundesebene eingesetzte Arbeitsgruppe die Erfassung sämtlicher staatsanwaltschaftlicher Verfahren in ein bundesweites Verbundsystem vorgeschlagen. Ein solches System würde den direkten Zugriff aller Benutzer, d. h. aller Staatsanwaltschaften, auf die gespeicherten Daten ermöglichen.

Der Senator für Rechtspflege und Strafvollzug hat mich gebeten, aus datenschutzrechtlicher Sicht hierzu Stellung zu nehmen.

Die technisch-organisatorische Ausgestaltung dieses Systems ist noch nicht abschließend erkennbar. Es besteht jedoch die Tendenz, neben teilweise schon vor-

handenen regionalen Systemen (in Bremen z. B. CANASTA) ein Bundeszentralsystem einzurichten und organisatorisch dem Bundeszentralregister (BZR) zuzuordnen. In das System sollen Justizdaten von sämtlichen Verfahren, die bei den einzelnen Staatsanwaltschaften anhängig werden, eingegeben werden. Neben den Daten zur Person des jeweiligen Beschuldigten sollen Daten über Tatvorwurf, Tatzeit, Verfahrensstand, Fahndungsmaßnahmen, Haftsachen über laufende Vollstreckungsmaßnahmen und das jeweilige Aktenzeichen in die Datenbank aufgenommen werden. Dabei soll insbesondere hinsichtlich des Tatvorwurfs, des Verfahrensstandes bzw. -ausganges und der laufenden Vollstreckung eine weitgehende Detaillierung der Daten erfolgen.

Bei Realisierung des derzeit vorgesehenen Konzeptes zu SISY würde sich folgendes ergeben:

Nach Einführung von SISY stehen jeder Staatsanwaltschaft in der Bundesrepublik die Daten sämtlicher, auch geringfügiger Vergehen über einen längeren Zeitraum personenbezogen abrufbereit zur Verfügung. Neben den laufenden Verfahren stehen auch die Daten aller eingestellten Verfahren bzw. Verfahren, in denen Freisprüche erfolgten, langfristig zur Verfügung.

In einer vorläufigen Stellungnahme habe ich gegen das geplante Vorhaben aus den Gesichtspunkten der Erforderlichkeit und Verhältnismäßigkeit erhebliche datenschutzrechtliche Bedenken geäußert.

Dazu habe ich das geplante Verfahren SISY auf die beabsichtigten Zielsetzungen hin untersucht, nämlich Sicherung der Strafverfolgung, Zusammenfassung von Verfahren und Überprüfung von Einstellungsmöglichkeiten, Indizwirkung anderer Verfahren für laufende Ermittlungsverfahren, für Einstellungen gemäß §§ 153, 153 a Strafprozeßordnung (StPO), für U-Haft-Entscheidungen und für Bewährungsentscheidungen, Gesamtstrafenbildung und Sicherung von Vollstreckungsmaßnahmen sowie Effektivierung der Strafverfolgung.

In meiner Stellungnahme habe ich auf die derzeit fehlenden notwendigen gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren (vgl. Pkt. 5.3.1.6 dieses Berichts) hingewiesen. Schließlich habe ich empfohlen zu prüfen, inwieweit die konsequente Ausnutzung der bestehenden Informationswege, insbesondere unter Berücksichtigung der Strafverfolgung und der vorbeugenden Verbrechensbekämpfung dienenden polizeilichen Informationssysteme nicht auf viele Teile der geplanten Datenverarbeitung verzichtet werden kann. Darüber hinaus vermag ich nicht zu erkennen, warum auf die etwa im polizeilichen Bereich gewonnene Regionalstruktur bei einem staatsanwaltschaftlichen Informationssystem verzichtet werden sollte. Insbesondere wenn es sich um leichte bis mittlere Kriminalität handelt, die erfahrungsgemäß auch keinen überregionalen Bezug hat.

Gerade die dauernde Kontrollmöglichkeit sämtlicher Personen, die einen geringfügigen Rechtsverstoß begangen haben oder denen sogar ein solcher Rechtsverstoß nicht nachgewiesen werden konnte (Einstellung nach § 170 StPO), stellt einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Das Rehabilitierungsinteresse gerade derjenigen, die nur einen geringen Verstoß begangen haben, würde durch das angestrebte Informationssystem SISY ganz wesentlich beeinträchtigt. Unter diesem Gesichtspunkt würden diese Personen sogar schlechter stehen als derzeit Straftäter, die verurteilt wurden, da z. B. das Bundeszentralregister zum Teil kürzere Tilgungsfristen vorsieht als z. B. das bremische System CANASTA.

Auch den Regelungen der Strafprozeßordnung ist zu entnehmen, daß das Allgemeininteresse an einer effektiven Strafverfolgung nicht zu einer unverhältnismäßigen Einschränkung von Grundrechten führen darf. Ganz generell müssen daher vor der Entscheidung über die Einführung eines derart weitreichenden Systems grundsätzlich die Formen der Datenverarbeitung im Zuge der Strafverfolgung und die damit verbundenen Aufgabenwahrnehmungen durch die Polizei und Staatsanwaltschaft diskutiert und geregelt werden. Es gilt dabei, einen Zustand zu vermeiden, parallele unterschiedlich aktuelle Datenbestände bei Polizei und Staatsanwaltschaft vorzufinden.

Ich gehe davon aus, daß der Senator für Rechtspflege und Strafvollzug mich über die Entwicklung des Verfahrens ebenso wie die Generalstaatsanwaltschaft auf dem laufenden hält, damit ich die Entwicklung auf diesem Gebiet datenschutzrechtlich begleiten kann.

5.3.1.8 Öffentliche Bekanntmachung der Entmündigung gem. § 687 ZPO

Das Bundesverfassungsgericht befaßt sich aufgrund eines Vorlagebeschlusses mit der Frage, ob die durch § 687 Zivilprozeßordnung (ZPO) zwingend vorgeschriebene öffentliche Bekanntmachung der Entmündigung wegen Trunksucht nicht gegen Grundrechte verstößt. Das Bundesverfassungsgericht hat mich um Stellungnahme gebeten.

Die öffentliche Verbreitung personenbezogener Informationen stellt insbesondere dann einen schweren Eingriff in das allgemeine Persönlichkeitsrecht dar, wenn die verbreitete Nachricht geeignet ist, den Ruf des Betroffenen und deren Angehörigen zu schädigen und ihr Ehrgefühl zu verletzen. Aus dem Gesichtspunkt des durch Artikel 2 Grundgesetz (GG) in Verbindung mit Artikel 1 Abs. 3 GG auch der rechtsprechenden Gewalt aufgegebenen Pflicht zur Wahrung allgemeiner Persönlichkeitsrechte ist darum die öffentliche Bekanntgabe solcher personenbezogener Daten nur gerechtfertigt, wenn sie durch gewichtigere Interessen gefordert ist.

Ich hatte mich mit dieser Frage bereits im 8. Jahresbericht (vgl. dort unter Pkt. 5.3.2, dritter Spiegelstrich) befaßt und habe gegenüber dem Bundesverfassungsgericht darauf hingewiesen, daß nicht nur im Falle der öffentlichen Bekanntmachung der Entmündigung ein Eingriff in Persönlichkeitsrechte der Betroffenen vorliegt, sondern daß ich in der Bekanntgabe der Rücknahme einer solchen Entscheidung (Bemündigung) einen ebenso gravierenden Eingriff sehe. Darüber hinaus ist zu bedenken, daß die Bekanntgabe einer solchen Entscheidung geeignet ist, das Ansehen der Betroffenen herabzusetzen. Dies gilt insbesondere bei dem Verfahren nach § 687 ZPO hinsichtlich der Trunksucht, weil der Alkoholismus in weiten Bevölkerungskreisen ausschließlich als Folge von Haltlosigkeit und Willensschwäche und nicht so sehr als eine Krankheit verstanden wird. Meiner gegenüber dem Senator für Rechtspflege und Strafvollzug damals ausgesprochenen Bitte zu prüfen, ob dem Erfordernis der öffentlichen Bekanntgabe nach § 687 ZPO unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nicht dadurch entsprochen werden könne, daß im Gerichtsgebäude ein Aushang angebracht würde und meine Bitte zu prüfen, ob nicht insbesondere bei Bemündigungen auf eine Bekanntgabe in den Medien verzichtet werden könne, wurde mit Hinweis auf die Verordnung über die Veröffentlichung amtlicher Bekanntmachungen vom 12. November 1985 im Lande Bremen nicht entsprochen.

Unter Berücksichtigung dieser Praxis habe ich gegenüber dem Bundesverfassungsgericht erklärt, daß ich dazu neige, das Interesse des Betroffenen und seiner Angehörigen an der Geheimhaltung höher zu bewerten als das Allgemeininteresse an einer solchen Bekanntmachung, auch weil ich Zweifel an dem Bedarf der Wirtschaft an solchen Bekanntmachungen und an der Effektivität dieses Verfahrens habe.

Ich habe daher erklärt, daß ich die Vorschrift des § 687 ZPO in Verbindung mit der Veröffentlichungsverordnung grundsätzlich für verfassungsrechtlich bedenklich und für verzichtbar halte.

Über die Entscheidung des Bundesverfassungsgerichts werde ich zu gegebener Zeit berichten.

5.3.2 Kurze Darstellung von Problemen und Beschwerden

— Aufgrund einer Anfrage war zu prüfen, ob der vom Vormundschaftsgericht vorgelegte **Fragebogen zur Überprüfung der Tätigkeit der Vormünder** durch das Gesetz gedeckt sei und ob der Vormund verpflichtet ist, den Fragebogen vollständig auszufüllen.

  Nach § 1839 Bürgerliches Gesetzbuch (BGB) hat der Vormund dem Vormundschaftsgericht auf Verlangen jederzeit über die Führung der Vormundschaft und über die persönlichen Verhältnisse des Mündels Auskunft zu erteilen. Diese Vorschrift soll dem Vormundschaftsgericht die Aufsichtsführung erleichtern. Die Auskunftspflicht erstreckt sich auf die gesamte Führung der Vormundschaft, also auch auf die vermögensrechtliche Verwaltung. Insoweit ist der vom Vormundschaftsgericht vorgelegte Fragebogen durch das Gesetz gedeckt. Das Gesetz stellt in entscheidendem Maße auf den Schutz des Mündels ab, so daß auch in Bezug auf gesetzliche Vorschriften kein Grund zur Beanstandung gegeben ist.

  Fraglich ist aber in jedem Einzelfall, ob alle im Fragebogen abverlangten Daten für das bestimmte Verhältnis bedeutsam und erforderlich sind. Es besteht daher durchaus eine Prüfungsmöglichkeit des Vormundes, Fragen, die er in

dem Verfahren für nicht bedeutsam hält, zunächst offen zu lassen. Dem Vormundschaftsgericht steht dann zu, im Wege des Fragerechts und der Aufsichtsführung die für das konkrete Mündelverhältnis erforderlichen Angaben vom Vormund zu verlangen.

— Durch einen Hinweis bin ich darauf aufmerksam gemacht worden, daß **Anfragen der Familiengerichte** wegen Antwartschaften auf Leistungen der betrieblichen Leistungsversorgung zur Durchführung des Versorgungsausgleichs durchweg in ungekennzeichneten normalen Briefumschlägen versandt werden. Das führt dazu, daß als „vertraulich" bezeichnete Anfrageformulare bei den angeschriebenen Firmen wie normale Geschäftspost geöffnet werden und der sensible Inhalt einer Vielzahl von Mitarbeitern bekannt wird.

  Ich habe daher dem Senator für Rechtspflege und Strafvollzug vorgeschlagen, bei Anfragen in Familienrechtssachen von Gerichten an Privatfirmen den Briefumschlag mit dem Zusatz „Personalabteilung — streng vertraulich" zu kennzeichnen. Nach Mitteilung des Senators für Rechtspflege und Strafvollzug hat der Präsident des Hanseatischen Oberlandesgerichts in Bremen inzwischen veranlaßt, daß künftig ein entsprechender Hinweis in das Anschriftenfeld aufgenommen wird.

5.4 Bildung, Wissenschaft und Kunst

5.4.1 Änderung des Bremischen Schulverwaltungsgesetzes

Die vom Senator für Bildung, Wissenschaft und Kunst eingesetzte Arbeitsgruppe, an der ich mich beteiligt habe, hat im Berichtsjahr ihre Arbeit mit der Vorlage eines Gesetz- und Verordnungsentwurfs nebst Begründung abgeschlossen. Der Senator für Bildung, Wissenschaft und Kunst hat im Herbst des letzten Jahres die verwaltungsinterne Abstimmung durchgeführt und in einem ersten Durchgang den Senat mit diesem Gesetzgebungsvorhaben befaßt. Der Senat hat beschlossen, Stellungnahmen von den zuständigen Verbänden und den anderen betroffenen Institutionen einzuholen. Es ist geplant, im März dieses Jahres dem Senat die überarbeitete Fassung des Gesetzentwurfs zur abschließenden Beratung zuzuleiten und danach die Bremische Bürgerschaft damit zu befassen. Es kann damit gerechnet werden, daß noch in dieser Legislaturperiode der Bremischen Bürgerschaft, d. h. im laufenden Jahr neue Datenschutzbestimmungen für den Schulbereich beschlossen werden.

Nach der umfangreichen Vorberatung dieses Gesetzgebungsvorhabens sind noch folgende Punkte als besonders erörterungsbedürftig verblieben:

— Die gesamte Datenverarbeitung der Schulen und Schulbehörden einschließlich derjenigen des Schulärztlichen Dienstes soll ohne Rücksicht auf die Art der Verarbeitung einbezogen werden. Deshalb kommt den begrifflichen Festlegungen des Gesetzes, d. h. der Ein- und Ausgrenzung von Tatbeständen große Bedeutung zu (z. B. Klassenbuch, Lehrerkalender, Leistungskontrollen).

— Die Erforderlichkeit und Bestimmtheit einzelner Schülerdaten, die von den Schulen erhoben, gespeichert, verwendet und übermittelt werden dürfen, z. B. das Merkmal „Aufenthaltsrecht bei Ausländern", „Gesundheitliche Auffälligkeiten und Behinderungen". In diesem Zusammenhang wird die stärkere Berücksichtigung der Elterneinwilligung bei der Speicherung sensibler Daten und bei der Übermittlung von Daten gefordert.

— Das Verbot einer automatisierten Speicherung von Verhaltensdaten, Daten über besondere pädagogische, soziale und therapeutische Maßnahmen, über gesundheitliche Auffälligkeiten, über Behinderungen und über die Ergebnisse der schulärztlichen Untersuchungen. Derartige schülerbezogene Daten dürfen nur durch die Schule in der sogenannten Schullaufbahnakte und nicht in einer automatisierten Datei des Senators für Bildung, Wissenschaft und Kunst bzw. des Magistrats Bremerhaven gespeichert werden. Dies gilt auch für Sonderschüler.

— Die schülerbezogene Datenverarbeitung bei den Schulbehörden. Vor allem die Einrichtung und der Betrieb von automatisierten zentralen Schülerdateien bei den Schulbehörden werden hinsichtlich ihrer Erforderlichkeit und Zweckbestimmung, dem Datenkatalog, eventuellen Datenübermittlungen und Datenabgleichen (z. B. mit dem Melderegister) in Frage gestellt.

— Weitergehende Regelungen für die Nutzung der schüler- und elternbezogenen

Daten für eigene Untersuchungen der Schulbehörden und für wissenschaftliche Forschungsvorhaben, für schulplanerische und schulstatistische Auswertungen sind erforderlich.

— Gesetzliche Festlegung von Aufbewahrungs- und Löschungsfristen für die gespeicherten Daten und die vorhandenen Unterlagen.

5.4.2 Bremisches Weiterbildungsgesetz — Datenschutzbestimmungen

Aufgrund verschiedener Eingaben hatte ich mich in der Vergangenheit mehrfach mit den von den Trägern der Weiterbildung verwendeten Teilnehmerlisten und Teilnehmerfragebogen zu befassen. Vgl. hierzu auch meinen 7. Jahresbericht unter Punkt 5.4.2, S. 48.

Den im Lande Bremen anerkannten Trägern der Weiterbildungseinrichtungen werden nach dem Bremischen Weiterbildungsgesetz Zuschüsse zu den Kosten der Weiterbildungsmaßnahmen gewährt. Als Beleg zum Verwendungsnachweis wird die Teilnehmerliste in Kopie oder im Original an das Landesamt für Weiterbildung gegeben und auch dort aufbewahrt.

Die Teilnehmerlisten enthalten personenbezogene Angaben der Teilnehmer wie z. B. Name, Alter, Anschrift und Beruf.

Das Landesamt für Weiterbildung stützt die Erhebung der Teilnehmerdaten auf die Vorschriften über die Zuschußgewährung nach § 7 Abs. 3 des Bremischen Weiterbildungsgesetzes und auf die zu diesem Gesetz erlassenen Richtlinien.

Diese Rechtsgrundlagen können die Datenerhebung bei den Teilnehmern jedoch nicht rechtfertigen. Die Erhebung der Teilnehmerdaten ist nach meiner Anregung nur auf freiwilliger Grundlage, d. h. mit Einwilligung der Betroffenen, zulässig (§ 3 BrDSG).

Mit Vertretern des Rechnungshofes und des Landesamtes für Weiterbildung wurde deshalb versucht eine Lösung zu finden, die sowohl datenschutzrechtlichen als auch haushaltsrechtlichen Anforderungen Rechnung trägt. Ein zunächst gefundener Kompromiß scheiterte aber an der Zustimmung des Landesbeirates für Weiterbildung.

Nach meiner Auffassung bleiben nunmehr zur Lösung des Problems nur zwei Wege:

— Das differenzierte Zuschußsystem wird aufgegeben zugunsten eines pauschalen Zuschußsystems, weil dann auch die differenzierte Datenerhebung bei den Teilnehmern und die teilnehmerbezogene Abrechnung der Zuschüsse aufgegeben werden können.

— Im Bremischen Weiterbildungsgesetz werden bereichsspezifische Datenschutzregelungen für die Erhebung, Speicherung und Verwendung von Teilnehmerdaten geschaffen.

Der Senator für Bildung, Wissenschaft und Kunst ist aufgefordert, hierzu eine grundsätzliche Entscheidung zu treffen.

Von den Teilnehmern der Weiterbildungsveranstaltungen werden außerdem mittels eines sog. Teilnehmerfragebogens ohne Namensangabe Daten wie Geschlecht, Alter, Beruf, Bildungsabschluß etc. erhoben. Diese Daten werden für die Weiterbildungsstatistik benötigt. Eine Rechtsgrundlage, die zur Angabe der Daten verpflichtet, ist ebenfalls nicht vorhanden. Auf meine Anregung hin wurden diese Fragebögen mit dem Hinweis versehen, daß die Angaben zu statistischen Zwecken erbeten werden und daß die Beantwortung freiwillig sei.

5.5 Jugend und Soziales

5.5.1 Schwerpunkte, Handlungsbedarfsfälle

5.5.1.1 Fragebogen für Pflegekindbewerber

Wenn Pflegekindbewerber ein Kind aufnehmen wollen, müssen sie einen entsprechenden Antrag beim Jugendamt stellen und dazu einen Fragebogen ausfüllen.

Ich habe die bei den Jugendämtern Bremen und Bremerhaven verwendeten Formulare überprüft und bin zu dem Ergebnis gekommen, daß eine Vielzahl dort abgefragter Angaben für die Entscheidung der Jugendämter nicht erforderlich ist. So wurden u. a. Angaben hinsichtlich der Wohnverhältnisse und des Arbeitgebers

abgefragt. Außerdem enthielt der Fragebogen eine generelle Einwilligungserklärung, wonach Auskünfte von den behandelnden Ärzten und dem Amtsarzt eingeholt werden. Des weiteren werden Anfragen an das Bundeszentralregister gerichtet. Hierzu war im Fragebogen des Jugendamtes Bremen ein allgemeiner Hinweis enthalten, während der Fragebogen des Jugendamtes Bremerhaven noch nicht einmal einen solchen Hinweis enthielt.

Inzwischen haben beide Jugendämter meiner Anregung entsprechend die Formulare datenschutzgerechter gestaltet, so daß nur noch die für die Prüfung der Voraussetzungen nach § 29 Jugendwohlfahrtsgesetz (JWG) erforderlichen Angaben abgefragt werden. Danach darf die Erlaubnis nur erteilt werden, wenn das leibliche, geistige und seelische Wohl des Pflegekindes gewährleistet ist.

Das amtsärztliche Gesundheitszeugnis enthält nur noch für das Jugendamt die Mitteilung, ob gesundheitliche Bedenken bestehen bzw. nicht bestehen. Die Einwilligungserklärung ist nunmehr dahingehend formuliert worden, daß der Antragsteller in die Weitergabe ausschließlich seiner Anschrift an das Gesundheitsamt zum Zwecke der Einladung zur Untersuchung einwilligt.

Wegen der Erteilung eines Führungszeugnisses haben beide Ämter meinen Vorschlag übernommen, daß die Antragsteller in die Datenübermittlung zwischen dem Bundeszentralregister und dem Jugendamt nach § 31 Bundeszentralregistergesetz (BZRG) in Verbindung mit § 29 JWG einwilligen. Des weiteren werden die Betroffenen nunmehr darauf hingewiesen, daß sie in analoger Anwendung des § 30 Abs. 5 Satz 3 BZRG Einsicht in das Führungszeugnis verlangen und nach Satz 4 dieser Vorschrift verlangen können, daß das Führungszeugnis — soweit es Eintragungen enthält — zunächst an ein von den Betroffenen benanntes Amtsgericht zur Einsichtnahme durch sie übersandt wird.

5.5.1.2 Programmierte Sozialhilfe (PROSOZ)

Der Modellversuch mit dem Dialogsystem PROSOZ ist 1986 fortgeführt und wird sich bis ins Jahr 1987 hineinziehen. Die Projektleitung PROSOZ hat zwei private Unternehmen beauftragt, zwei Teilkonzepte zu erarbeiten, nämlich das Datenschutzkonzept mit den rechtlichen Abwägungen und das Datensicherungskonzept. Beide Auftragnehmer wurden verpflichtet, die Entwicklung dieser Konzepte in enger Abstimmung mit mir gemeinsam bis Oktober 1986 zu erarbeiten. Es reicht nicht aus, daß von einem Auftragnehmer erstmalig nach Ablauf dieser Frist mit mir Kontakt aufgenommen worden ist.

Diese Vorgehensweise, die keine inhaltliche Abstimmung mit mir ermöglicht hat, genügt nicht den Anforderungen der datenschutzrechtlichen Überprüfbarkeit von Datenschutz- und Datensicherungskonzepten.

Ich halte diese Art meiner Beteiligung und die Trennung von Datenschutz und Datensicherung für unzweckmäßig. Die wenigen Diskussionen mit den Auftragnehmern haben mir gezeigt, daß die Auftragnehmer durch die Projektleitung PROSOZ von dem generellen Fortgang des Projektes nicht unterrichtet worden sind, um dies bei der Konzepterarbeitung berücksichtigen zu können.

Die Datenschutzkonzepte sind mir bisher nicht zur Verfügung gestellt worden.

Die mit diesem Projekt gemachten Erfahrungen zeigen, daß die Entwicklung eines Datenschutzkonzeptes, von meiner Beratung losgelöst, zu einer Situation führen kann, in der ich mich veranlaßt sehe, bei der Einführung dieses Projektes trotzdem umfangreiche Beratungen vornehmen zu müssen. Damit tritt bei mir die ursprünglich vorgesehene Entlastung in meiner Dienststelle trotzdem nicht ein, und die Mittel für die Erstellung eines Datenschutzkonzeptes sind für Fremdaufträge verbraucht worden. Hinzu kommt, wenn ich aufgrund meiner Kontrolle feststelle, daß weitere Datenschutzmaßnahmen erforderlich sind, zusätzliche Kosten entstehen.

Hieraus kann ich nur die Empfehlung ableiten, die erforderlichen Beratungskapazitäten in meiner Dienststelle vorzusehen, um so die für das Land notwendige Beratung zu gewährleisten.

5.5.2 Kurze Darstellung von Problemen und Beschwerden

— Das Sozialamt Bremerhaven führt bei Schriftverkehr mit Antragstellern über dem Anschriftenfeld des Empfängers als Absender die Bezeichnung „Sozialamt" und versendet die Schriftstücke in einem Fensterumschlag.

Die Behörde hat entsprechend meiner Empfehlung angeordnet, daß in der **Absenderangabe nur noch die Organisiationsbezeichnung** (z. B. 50/...) verwendet werden darf.

— Ein Betroffener wandte sich dagegen, daß beim Sozialamt Bremerhaven in Widerspruchsangelegenheiten eine Kopie der kompletten **Niederschrift über die Sitzung des Widerspruchsausschusses in den jeweiligen Sozialhilfeakten** enthalten sei. Die Niederschrift beinhalte die Entscheidungen über mehrere Widersprüche verschiedener Betroffener. Soweit ein Betroffener von seinem Akteneinsichtsrecht Gebrauch mache und die Niederschrift einsehe, erfahre er auch, welche Empfehlungen der Ausschuß in anderen Widerspruchsangelegenheiten ausgesprochen hat.

Ich habe die Behörde darauf hingewiesen, daß im Rahmen des Akteneinsichtsrechts somit hinsichtlich der anderen Fälle gegenüber dem einsichtnehmenden Betroffenen das Sozialgeheimnis unbefugt offenbart wird und angeregt, nur die entsprechenden Protokollauszüge den jeweils dafür bestimmten Sozialhilfeachten zuzuordnen.

Das Sozialamt Bremerhaven verfährt nunmehr so.

5.6 Gesundheitswesen

5.6.1 Schwerpunkte, Handlungsbedarfsfälle

5.6.1.1 Datenschutz in den Krankenanstalten

Seit Jahren bemängele ich und weise darauf hin, daß es an der Zeit ist, krankenhausspezifische Datenschutzregelungen zu schaffen und damit auf eine rechtliche Grundlage zu stellen. Bis heute liegt ein Entwurf nicht vor.

In meinen Uberprüfungen des Zentralkrankenhauses Reinkenheide in Bremerhaven und der bremischen Krankenanstalten (letztere Prüfung ist noch nicht abgeschlossen) hat sich der Regelungsbedarf bestätigt. Darüber hinaus gab es aber auch Fälle, bei denen geltendes Recht nicht konsequent beachtet wurde.

Dieses möchte ich an einigen Beispielen verdeutlichen:

— die ungeschützte Patientenaufnahme in Reinkenheide (siehe dazu Pkt. 5.6.1.3),

— der ungenügende Zugriffsschutz bei dem Patientenabrechnungsverfahren in den bremischen Krankenanstalten, Stationäres Abrechnungsverfahren (StAB). Hier mußte ich feststellen, daß der organisierte Paßwort- und Programmschutz in der Regel wissentlich umgangen wird. Zwar wird eine Zugriffssoftware zur Verfügung gestellt, doch wird sie in der Praxis umgangen. Dieses Softwarepaket sieht die datenschutzrechtlich gebotene Zugriffsdifferenzierung für verschiedene Sachbearbeiter und Führungskräfte vor.

In der Praxis ist in vielen Krankenhausbereichen dieser Systemschutz dadurch gröblich verletzt worden, daß der höchste Zugriffsberechtigte für sich das System eröffnet und sich nach Beendigung seiner Tätigkeit nicht wieder abmeldet. Dadurch wird den nachfolgenden minderberechtigten Nutzern der umfangreiche und uneingeschränkte Zugriff auf die Patientendaten eröffnet. Die für die Zugriffsberechtigung verwendeten Paßwörter der Bediensteten in Krankenhäusern werden ihres Schutzzweckes restlos beraubt, wenn, wie dies offensichtlich allgemeine Praxis zu sein scheint, die Paßwörter offen an den Bildschirmen hinterlegt werden.

Neben den Problemen der medizinischen Dokumentation (vgl. auch Pkt. 5.6.1.2) muß festgestellt werden, daß zusätzliche medizinische Daten (z. B. Nebendiagnosen) der Verwaltung zur Verfügung gestellt werden, ohne daß dafür eine Rechtsgrundlage erkennbar ist.

5.6.1.2 Medizinische Dokumentation und statistische Auswertung (MEDUSA-K)

Das ADV-Verfahren MEDUSA-K (Medizinische Dokumentation und statistische Auswertung — Kurzform), über das ich bereits im letzten Jahresbericht (vgl. Pkt. 5.8.1.7, S. 54) berichtet hatte, ist mir zur datenschutzrechtlichen Beurteilung vorgelegt worden.

Bei MEDUSA-K handelt es sich um ein komplexes Diagnose-, Therapie- und Dokumentationsverfahren, das verschiedenen Zwecken dienen soll:

— Bei Verhandlungen mit den Krankenkassen über die Vereinbarung von Pflege-

sätzen als Argumentationshilfe zur Darstellung der Leistungsgerechtigkeit und Leistungsfähigkeit der Krankenhäuser

— Darstellung des überregionalen Versorgungsauftrages der Kliniken

— Führen einer Diagnosestatistik, wie es die Wirtschaftsprüfung der kommunalen Krankenhäuser Bremens gefordert hat

— Diagnosefindung und Anwendung von Therapieformen zur Unterstützung des medizinisch-ärztlichen Personals der Krankenhäuser

— Diagnose- und Dokumentationsverfahren zur Darstellung und Überschaubarmachung des Klinikgeschehens

— Verbesserung des krankenhausinternen Betriebsablaufes und dessen Organisation

— Führung eines Kosten- und Leistungsnachweises entsprechend dem § 16 Abs. 4 Nr. 1 Bundespflegesatzverordnung (BPflV) zur Regelung der Pflegesatzvereinbarungen

— Führung einer Diagnosestatistik mit Operationen und der Verweildauer der Patienten gemäß § 24 Abs. 2 BPflV.

Die Aufzählung macht deutlich, daß die in MEDUSA-K vorgehaltenen Daten nicht nur entsprechend den Anforderungen der einzelnen Krankenhäuser, sondern insgesamt flexibel zu den verschiedenen Zwecken verarbeitet werden sollen. Auch die Verfahrensbeschreibung nennt als eine Anforderung an das Verfahren MEDUSA-K die Anpassung an sich ändernde Informationsbedürfnisse wegen der Vielgestaltigkeit der Krankenhausaufgaben und den Wechsel der Aufgabenstellungen und der nur bedingt vorhersehbaren weiteren Anforderungen. Um diesem Ziel zu genügen, sollen variable Felder im Datensatz vorgesehen werden.

Aus datenschutzrechtlicher Sicht muß das Verfahren MEDUSA-K den Anforderungen des Bremischen Datenschutzgesetzes (BrDSG) genügen und darf nicht gegen die ärztliche Schweigepflicht gemäß § 203 Strafgesetzbuch (StGB) verstoßen.

Eine gesetzliche Regelung, die eine Befugnis zur Durchbrechung der ärztlichen Schweigepflicht zum Zwecke der Erstellung verschiedener Statistiken enthält, liegt nicht vor. Die §§ 16 Abs. 4 und 24 Abs. 2 BPflV verpflichten die Krankenhäuser, nur eine Diagnosestatistik sowie die Anzahl der durchgeführten Operationen, ab 1. Januar 1988 auch die Verweildauer im Krankenhaus und das Alter der Patienten in anonymisierter Form zu erfassen.

MEDUSA-K aber sieht zunächst eine personenbezogene Erfassung der Daten, verbunden mit einem Abgleich und der Übermittlung weiterer Daten aus dem Stationären-Abrechnungs-Verfahren (StAB-Verfahren) vor. Erst danach ist eine Teilanonymisierung der Daten durch Verwendung einer „Anonymisierungsnummer" anstelle der Aufnahmenummer vorgesehen. Ein Weglassen des Namens und der Aufnahmenummer allein reicht jedenfalls bei dem vorgesehenen dezidierten Datensatz bei MEDUSA-K nicht aus, um in allen Fällen eine Deanonymisierung auszuschließen. Auch soll die Erfassung der nur für MEDUSA-K vorgesehenen Daten teilweise nicht durch medizinisches, sondern durch Verwaltungspersonal durchgeführt werden.

Das vorgestellte Verfahren kann aus meiner Sicht auch nicht durch eine Einwilligungserklärung seitens des Patienten legalisiert werden.

Eine Einwilligung seitens des Patienten setzt voraus, daß der Betroffene die Tragweite seiner Entscheidung im wesentlichen zu überblicken vermag. Dazu bedürfte es der umfassenden Aufklärung, u. a. über die Zwecke des MEDUSA-K-Verfahrens. Diese sind aber, wie oben dargestellt, variabel. Hinzu tritt, daß die Vorschriften der BPflV von einer vollständigen Dokumentation aller Fälle ausgehen. Dies kann bei der Freiwilligkeit zur Teilnahme an MEDUSA-K nicht gewährleistet werden.

Ich setze mich daher gegenüber dem Senator für Gesundheit und Sport dafür ein, daß das Verfahren MEDUSA-K gesetzlich geregelt wird und die Regelungen den Anforderungen aus dem Volkszählungsurteil entsprechen. Hierauf kann nur dann verzichtet werden, wenn die Erfassung der Daten durch den Arzt oder seine berufstätigen Gehilfen vorgenommen wird und sichergestellt ist, daß die Daten tatsächlich anonymisiert sind.

5.6.1.3 Teilprüfung des Zentralkrankenhauses Reinkenheide — ZKHR —

Aufgrund einer Eingabe habe ich die Patientenaufnahme im Großraumbüro, die Telefondatenerfassung und den Einsatz „unkontrollierter" Personal-Computer überprüft.

Die Überprüfung umfaßte im wesentlichen die technischen und organisatorischen Datensicherungsmaßnahmen gemäß § 6 Bremisches Datenschutzgesetz (BrDSG). Die Rechtsgrundlagen zur Datenspeicherung waren nicht Gegenstand der Prüfung.

— Patientenaufnahme

Im ZKH Reinkenheide wird die Datenaufnahme für neu aufzunehmende Patienten in einem offenen Büro durchgeführt, in dem zwei Bildschirmarbeitsplätze und ein Etikettendrucker untergebracht sind. Die Terminals sind mit dem Zentralrechner im Rechenzentrum des Magistrats verbunden. Die Bildschirmgeräte (Aufnahmeplätze) sind provisorisch voneinander getrennt und erlauben die gleichzeitige Datenaufnahme zweier Patienten.

Die wartenden Patienten sitzen im selben Raum und können die Aufnahmegespräche genauestens verfolgen. Neben den generellen Aufnahmedaten werden teilweise Anamnesedaten erhoben. Diese Daten unterliegen sowohl der ärztlichen Schweigepflicht als auch dem Datenschutzrecht.

Die vorgefundene Arbeitsorganisation konnte die Einhaltung der ärztlichen Schweigepflicht und des Datenschutzrechtes nicht gewährleisten.

Ich habe deshalb gemäß § 22 BrDSG gegenüber dem Magistrat der Stadt Bremerhaven eine Beanstandung ausgesprochen.

— Telefondatenerfassung

Zur Telefondatenerfassung wird im ZKH Reinkenheide ein programmierbares Gebührenaufzeichnungsgerät verwendet. Dieses Gerät ist mit einem Festspeicher und einem Drucker für die Ausgabe der Rechnungen ausgestattet. Die Rechnung selbst wird mit der vierstelligen Nebenstellennummer versehen, ohne daß der Name aufgedruckt wird. Datenschutzrechtlich bedenklich ist, daß zusätzlich die **vollständigen Zielnummern** des Angerufenen gespeichert und ausgedruckt werden.

Ich habe vorgeschlagen, durch Software-Änderungen die Telefonnummer nur als Fragment aufzunehmen (Vorwahlnummer und Telefonnummer ohne die letzten beiden Stellen).

Nach dem Ausdruck der Rechnungen sollen die Daten gelöscht werden. Aus technischen Gründen (z. B. Wiederholung bei Papierbruch) erfolgt die **Löschung** nicht automatisch. Sie wird über Tastatureingabe gestartet. Eine fehlerhafte Eingabe kann bewirken, daß der Löschvorgang nicht erfolgreich war, die Daten also erhalten bleiben. Da das Ergebnis dem Sachbearbeiter auf dem Protokoll nicht angezeigt wird, erfährt er von der nicht vollzogenen Löschung nichts und wird deshalb auch eine Korrektur nicht vornehmen. Die Daten bleiben somit für unbestimmte Zeit ungerechtfertigt erhalten.

Ich habe gefordert, die Software so ändern zu lassen, daß der Löschvorgang vollständig protokolliert und das Ergebnis z. B. als Kontostand-Anzeige angezeigt wird, damit eine Sichtkontrolle ermöglicht wird.

Die **Rechnungen** werden entweder über die Stationen offen verteilt (bei längerem Aufenthalt) oder bei Entlassung dem Patienten oder Angehörigen zur Bezahlung übergeben.

Ich habe veranlaßt, daß die Verteilung auf den Stationen in verschlossenen Fensterbriefumschlägen vorgenommen wird. So wird inzwischen verfahren.

— Einsatz „unkontrollierter" Personal-Computer (PC)

In einigen Bereichen des ZKH Reinkenheide sind PC eingesetzt, ohne daß dies der Verwaltung in allen Fällen bekannt ist. Einige dieser PC's wurden ausschließlich für die medizinische Datenverarbeitung verwendet. Die Problematik der mangelnden Kontrollierbarkeit von eingesetzten autonomen Arbeitsplatzrechnern ist hier ebenso wie in der gesamten Verwaltung gegeben. Es gibt kein Datenschutzkonzept. Die Sicherheit der auf den Disketten gespeicherten Daten ist weder technisch noch organisatorisch gewährleistet. Die Kontrolle, wie die auf den Disketten gespeicherten Daten verwendet oder vor unbefugter Einsichtnahme geschützt werden, ist bei diesem unkontrollierten und wild wuchernden PC-Einsatz unmöglich.

Bei meiner Prüfung habe ich darüber hinaus feststellen müssen, daß selbst die hochsensible Blutspenderdatei in einem solchen ungesicherten PC-Verfahren geführt wurde.

Ich habe das an Ort und Stelle bemängelt. Inzwischen ist mir mitgeteilt worden, daß die Blutspenderdatei mit einem Paßwortschutz versehen worden ist. Diese Maßnahme reicht für sich allein jedoch nicht aus. Ich habe die Krankenhausleitung aufgefordert, unverzüglich für ihren Bereich ein Datenschutz-Konzept für den PC-Einsatz vorzulegen.

5.6.1.4 Befunddokumentation und Arztbriefschreibung im Krankenhaus (BAIK)

Probeweise wird seit 1985 in der Chirurgie II im Zentralkrankenhaus (ZKH) Reinkenheide das Verfahren BAIK benutzt. Es handelt sich um ein Verfahren, das in der Universität Frankfurt entwickelt wurde und zwischenzeitlich in der Bundesrepublik in kommunalen Krankenhäusern im Einsatz ist. Zu der Software

— Textsystem (DOC) und

— Textretrieval-System (IATROS)

ist ein Rechner installiert, der gleichzeitig auch Datenerfassungs- und Prüffunktionen erlaubt. Es handelt sich dabei um ein Rechner-System mit Festplatte und angeschlossenem Diskettenlaufwerk sowie einem Matrixdrucker. Außerdem ist ein Akustikkoppler angeschlossen, der erlaubt, daß Programmodifikationen bzw. Korrekturen und Fehlerursache (Software-Wartung) von der Universität Frankfurt im Fernwartsystem durchgeführt werden. Die Telefonverbindung kann ausschließlich vom ZKH eröffnet werden. Die Datenübertragung erfolgt über das vorhandene Telefonnetz mittels des Akustikkopplers; der Anstoß zur Datenübermittlung erfolgt ausschließlich durch das ZKH. Diese Datenfernübertragung war zum Zeitpunkt der Uberprüfung fehlerhaft, weil die Daten unvollständig übertragen wurden.

Dieses Verfahren wird bisher nur in der Chirurgie II erprobt. Das System ist jedoch so ausgelegt, daß es auch Bestandteil eines Bürokommuniktionsnetzes innerhalb eines Krankenhauses oder in Verbindung mit dem Zentralrechner des Magistrats arbeiten kann. Diese Ausweitung des Systems ist geplant. Neben Textbausteinen sind auf dem System Daten über Patienten, Ärzte und Hausärzte in Dateien gespeichert. Die Dateien waren unvollständig zum Dateienregister gemeldet. Eine Beschreibung liegt ebenfalls nicht vor. Der Rechner wird derzeit nur von zwei Personen bedient, die eine Berechtigung dem Rechner gegenüber nachweisen müssen. Das System ist allerdings insoweit offen, als in dem Raum, in dem das Gerät untergebracht ist, verschiedene Schreibkräfte arbeiten und somit Einblick in die Arbeit mit dem BAIK-System haben können. Zwar ist das Paßwortsystem in mehreren Stufen angelegt, läßt sich jedoch leicht ausspähen, da das benutzerabhängige Paßwort über lange Zeit nicht geändert wurde.

Die Klinikleitung war der Ansicht, daß die Dateien deshalb nicht gemeldet werden müssen, da sich das System noch in der Erprobungsphase befinde. Es stellte sich jedoch heraus, daß in dieser Phase bereits mit echten personenbezogenen Daten gearbeitet wurde.

Eine solche Datenverarbeitung ist rechtswidrig, und sie eröffnet für den Bürger unkalkulierbare Risiken. Die Verwendung von Originaldaten in der Testphase verletzt die Grundsätze der ordnungsgemäßen Datenverarbeitung.

Es fehlten die notwendigen Voraussetzungen für die Datensicherung.

So steht der Rechner offen in einem Raum, in dem auch andere Arbeiten verrichtet werden. Die Zugangskontrolle ist damit nicht gewährleistet. Außerdem wird nicht kontrolliert, ob Datenträger befugt entfernt werden. Inwieweit Datenübermittlungen durch das Fernwartsystem durchgeführt werden, konnte nicht festgestellt werden. Eine Kontrolle ist nicht vorhanden. Ebenso ist nicht gewährleistet, daß die Benutzung durch Unbefugte nicht vorgenommen wird. Die Zugriffsberechtigung wird insoweit nicht hinreichend genug geprüft.

Wir haben den Magistrat unmißverständlich aufgefordert, diese Mißstände unverzüglich zu beseitigen.

5.6.1.5 Übermittlung von Dialyse-Patientendaten

In meinem 8. Jahresbericht habe ich unter Pkt. 5.8.1.4, S. 53 berichtet, daß auch in Bremen nicht anonymisierte Krankheitsdaten von Dialyse-Patienten ohne deren Einwilligung an die European Dialysis and Transplant Association (E.D.T.A.) mit

Sitz in London übermittelt werden. Ich habe dieses beanstandet und den Senator für Gesundheit und Sport gleichzeitig aufgefordert zu überprüfen, inwieweit in Bremen ähnliche Übermittlungen von Patientendaten erfolgen und mir das Ergebnis mitzuteilen.

Eine entsprechende Mitteilung liegt mir bisher nicht vor.

Das Problem der Übermittlung von Daten der Dialyse-Patienten wurde inzwischen von den Datenschutzaufsichtsbehörden unter Beteiligung der Frankfurter Universität diskutiert. Es wurde Einigung dahingehend erreicht, daß die Datenübermittlung nur mit Einwilligung der Betroffenen zulässig ist. Über den Inhalt einer entsprechenden Einwilligungserklärung wurde ebenso Einigung erzielt.

Mit einer Unterlassung der Löschung der ohne Einwilligung der Betroffenen an die E.D.T.A. übermittelten und dort gespeicherten Daten kann ich mich höchstens bis zu einer Vereinbarung über eine bundeseinheitliche Vorgehensweise einverstanden erklären.

5.6.1.6 Fernsehgeräte-Verleih in den Krankenanstalten

Im Zentralkrankenhaus „Links der Weser" wurde die Fernsehgeräte-Nutzung von Patienten direkt von privaten Verleihern angeboten. Dazu kam regelmäßig ein privater Verleiher auf die Stationen und erfragte die neu eingelieferten Patientennamen, die er auch erhielt. Anschließend suchte er diese Patienten auf, um mit ihnen einen Verleihvertrag abzuschließen. Diese Vorgehensweise war sowohl aus datenschutzrechtlicher Sicht als auch aus der Sicht der ärztlichen Schweigepflicht unzulässig. Eine rechtliche Grundlage für die Bekanntgabe personenbezogener Daten außerhalb des Behandlungsvertrages ist nicht erkennbar. Da bereits der bloße Besuch eines Arztes oder der Aufenthalt im Krankenhaus der ärztlichen Schweigepflicht unterliegt, die auch die berufstätigen Gehilfen zu wahren haben, lag hier in der Offenbarung gegenüber dem Verleiher ein Verstoß gegen § 203 Strafgesetzbuch (StGB) vor. Nur auf ausdrücklichen Wunsch des Patienten nach einem Fernsehgerät kann daher der Kontakt mit dem Verleiher vom Pflegepersonal hergestellt werden. Der Wunsch muß ausschließlich vom Patienten ausgehen.

Inwieweit ähnliches auch in anderen Krankenanstalten geschieht, war nicht erkennbar. Ich habe deshalb den Senator für Gesundheit und Sport gebeten, zu diesem konkreten Vorfall im besonderen und der Situation in anderen Krankenhäusern im allgemeinen Stellung zu nehmen und gleichzeitig die Situation in anderen öffentlichen Krankenhäusern zu überprüfen.

5.6.2 Kurze Darstellung von Problemen und Beschwerden

— Ein **kommunales Krankenhaus** in Bremen (ZKH St.-Jürgen-Straße) war von einer Inkassogesellschaft aufgefordert worden, das **Entlassungsdatum eines Patienten** zu **übermitteln.** Als Begründung für diese Art der Übermittlung waren sowohl eine Vollmacht einer Teilzahlungsbank als auch der Vollstreckungstitel eines Amtsgerichtes beigefügt. Der entsprechende Arzt des ZKH bezweifelte die Rechtmäßigkeit dieser Übermittlung.

  Es war zu prüfen, ob berechtigtes Interesse des Empfängers und gleichzeitige Einhaltung der schutzwürdigen Belange des Betroffenen nach § 13 Bremisches Datenschutzgesetz (BrDSG) vorlagen. Da hier das Interesse an der Übermittlung nicht aus dem Vollzug des Behandlungsvertrages, den der Patient mit dem Krankenhaus abgeschlossen hatte, herzuleiten war, konnte von einem berechtigten Interesse nicht gesprochen werden. Außerdem handelte es sich hier um besonders sensible Daten, die dem Arztgeheimnis unterliegen und somit für Gläubigerinteressen nicht genutzt werden dürfen.

  Die Auskunftsverweigerung war zu Recht erfolgt.

5.7 Bauwesen

5.7.1 Schwerpunkte, Handlungsbedarfsfälle

5.7.1.1 Erlaß eines Entwässerungsortsgesetzes

Der Senator für das Bauwesen hat mir den Entwurf einer Neufassung des Entwässerungsortsgesetzes mit der Bitte um datenschutzrechtliche Beurteilung vorgelegt.

Mit dem am 16. September 1986 verkündeten Entwässerungsortsgesetz wird insbesondere auch das Ziel verfolgt, die Wahrnehmung der Abwasserbeseitigungs-

pflicht der Stadtgemeinde Bremen in den nicht kanalisierten Stadtrandgebieten zu verbessern.

Die Abwasserbeseitigungspflicht war nach der bis dahin geltenden Regelung in diesen Fällen weitgehend den Grundstückseigentümern übertragen. Sie wird nunmehr von den für die Abwasserbeseitigung zuständigen Behörden wahrgenommen. Diesen Behörden sind gleichzeitig umfangreiche Kontrollbefugnisse hinsichtlich der Einleitung von Schmutzwasser in die Kanalisation, den Betrieb, die Unterhaltung und die Entleerung von Schmutzwassersammelgruben, Kleinkläranlagen usw. eingeräumt worden.

Der Senator für das Bauwesen teilte in dem Zusammenhang auf Anfrage mit, daß die Wahrnehmung dieser Kontrollbefugnisse die Führung eines Registers über alle natürlichen und juristischen Personen erforderlich mache, die unter im Entwässerungsortsgesetz festgelegten besonderen Bedingungen Schmutzwasser in die Kanalisation einleiten oder Schmutzwassersammelgruben, Kleinkläranlagen oder Leichtflüssigkeitsabscheider betreiben. In diesem Register sei eine Vielzahl personenbezogener Daten für eine wirksame Überwachung der Abwasserbeseitigung zu speichern. Dazu gehöre auch die dem jeweiligen Grundstück aus der öffentlichen Wasserversorgung zugeführte Frischwassermenge. Die Registerführung solle mittels ADV erfolgen. Im Rahmen der Überwachung seien Übermittlungen personenbezogener Daten an andere Behörden, z. B. an das Bauordnungsamt, erforderlich.

Da die Stadtgemeinde Bremen sich bei der Entleerung von Sammelgruben, Kleinkläranlagen und Leichtflüssigkeitsabscheidern privater Unternehmen zu bedienen gedenke, sei eine regelmäßige Übermittlung personenbezogener Daten aus dem Register an diese erforderlich.

Meine Prüfung hat ergeben, daß die beabsichtigte Erhebung und Verarbeitung personenbezogener Daten unzulässig sein würde, da die einschlägigen Gesetze, nämlich das Wasserhaushaltsgesetz und das Bremische Wassergesetz, keine den Anforderungen des Bundesverfassungsgerichtsurteils zum Volkszählungsgesetz 1983 genügende Erlaubnisvorschrift für den damit verbundenen erheblichen Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung enthalten.

Bei dieser Gelegenheit habe ich festgestellt, daß die bisherige Praxis, nach der die Stadtwerke Bremen für die Berechnung der Kanalbenutzungsgebühr die einem Grundstück zugeführte Frischwassermenge regelmäßig an die für die Gebührenberechnung zuständige Stelle übermittelt, datenschutzrechtlich unzulässig war, da auch hierfür eine Erlaubnisvorschrift in den genannten einschlägigen Gesetzen nicht vorhanden war. Da das Bremische Wassergesetz am 29. März 1984, also nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983, geändert worden ist, konnte hierfür wohl auch nicht mehr der sogenannte Übergangsbonus in Anspruch genommen werden. An dieser Beurteilung ändert auch der Tatbestand nichts, daß die Stadtwerke Bremen mit der Berechnung und Einziehung der Kanalbenutzungsgebühr betraut sind. Eine Übermittlung der von den Stadtwerken im Rahmen eines Vertragsverhältnisses erhobenen Daten an die für die Gebührenberechnung zuständige, von der Stadtgemeinde Bremen beliehene Stelle der Stadtwerke ohne Erlaubnisvorschrift ist unzulässig.

In Gesprächen mit dem Senator für das Bauwesen, dessen datenschutzfreundliche Kooperationsbereitschaft in dieser Angelegenheit nicht unerwähnt bleiben sollte, konnte erreicht werden, daß den an der Gesetzgebung beteiligten Stellen Gesetzentwürfe vorgelegt worden sind, welche die sich aus der Aufgabe der Abwasserbeseitigungspflicht ergebende notwendige Verarbeitung personenbezogener Daten auf eine Rechtsgrundlage stellt, wie sie vom Bundesverfassungsgericht gefordert worden ist. In das Bremische Wassergesetz wurde eine Vorschrift aufgenommen, nach der die Erhebung, Verarbeitung und Übermittlung solcher Daten erlaubt wird. Die Gemeinden werden ermächtigt, genauere Regelungen darüber zu treffen. In das Entwässerungsortsgesetz wurde eine Vorschrift aufgenommen, die den Tatbestand der Führung des erwähnten Registers und die Zweckbestimmung dieses Registers regelt. Die Vorschrift regelt abschließend Art und Umfang der Daten, die erhoben und verarbeitet werden dürfen. Sie enthält abschließende Übermittlungsregelungen und Löschungsvorschriften.

In das Ortsgesetz über die Erhebung einer Kanalbenutzungsgebühr wurde wegen der dargestellten Problematik der Datenübermittlung von den Stadtwerken zu den für die Festsetzung und Einziehung der Kanalbenutzungsgebühren zuständi-

gen Stellen über die einem Grundstück zugeführte Frischwassermenge eine Vorschrift aufgenommen, die als ausreichende gesetzliche Grundlage für diese Datenübermittlung angesehen werden kann. Die Ermächtigung für diese Regelung ist durch die bereits erwähnte Änderung des Wassergesetzes geschaffen worden.

Zur Zeit prüfe ich, inwieweit der Stadtgemeinde Bremen deswegen die Verpflichtung obliegt, die Betroffenen hinsichtlich dieser Datenübermittlung zu informieren und aufzuklären.

5.7.1.2 Akteneinsicht durch die Kriminalpolizei beim Bauordnungsamt

Im Berichtsjahr hat mich der Senator für das Bauwesen gebeten, zu der Frage der Einsichtnahme der Kriminalpolizei in Akten des Bauordnungsamtes Stellung zu nehmen.

Die Kriminalpolizei möchte für Ermittlungsvorgänge, insbesondere bei Kapitalverbrechen, auf Unterlagen des Bauordnungsamtes zurückgreifen.

Begründend dafür führt das Stadt- und Polizeiamt aus, daß diese Vorgehensweise die Arbeit wesentlich erleichtern, beschleunigen und präzisieren könne, da das Vermessen von Gebäuden, Teilen davon und deren Lage zueinander künftig entfallen könne.

Ich habe gegen die Einsichtnahme in Akten des Bauordnungsamtes erhebliche Bedenken und diese dem Senator für das Bauwesen mitgeteilt.

Ich halte die damit verbundene Übermittlung von personenbezogenen Daten Betroffener wegen der Zweckentfremdung der Daten auch für datenschutzrechtlich nicht zulässig. Das gilt um so mehr, als die Kriminalpolizei in solchen Fällen meistens nicht in Sachen der Betroffenen ermittelt. Bei dem vorgeschlagenen Verfahren würde meines Erachtens auch der bei einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu beachtende Grundsatz der Verhältnismäßigkeit verletzt, da das Verfahren vornehmlich der Arbeitserleichterung der Kriminalpolizei dienen soll und das angestrebte Ziel auch ohne einen solchen Eingriff erreicht werden kann.

Ich habe als Lösungsmöglichkeit vorgeschlagen, daß der Kriminalpolizei bei Ermittlungen in bestimmten Strafverfahren Ablichtungen aus den Akten des Bauordnungsamtes zur Verfügung gestellt werden können. Beim Ablichten wären dann personenbezogene Daten, wie z. B. Angaben zum Bauherrn, Planfertiger, prüfenden Beamten und zu Nachbarn abzudecken. Aber auch bei einem solchen Verfahren wären die so erteilten Auskünfte auf ein Minimum zu beschränken, da sich für die Kriminalpolizei die übermittelten Daten ohne Schwierigkeiten Personen zuordnen lassen.

Sollte es zwischen dem Senator für das Bauwesen und der Kriminalpolizei zu einer Einigung über das von mir vorgeschlagene oder ein ähnliches Verfahren kommen, könnte ich meine datenschutzrechtlichen Bedenken unter der Voraussetzung zurückstellen, daß festgelegt wird, in welchen Strafverfahren bei Ermittlungen eine entsprechende Datenübermittlung erfolgen soll.

5.7.2 Kurze Darstellung von Problemen und Beschwerden

— Ein Bürger beschwerte sich darüber, daß dem **Bauordnungsamt und dem Liegenschaftsamt** aus Anlaß einer **Anmeldung für eine Wohnung** in einem „Kaisenbewohnerhaus" unzulässigerweise personenbezogene Daten **vom Einwohnermeldeamt übermittelt** worden seien oder daß diese Daten vom Bauordnungsamt oder dem Liegenschaftsamt ohne Rechtsgrundlage erhoben worden sein sollen.

Bei der Behandlung dieser Beschwerde habe ich folgende Feststellungen machen können:

Das Einwohnermeldeamt übermittelt dem Bauordnungsamt in bestimmten Abständen eine Liste, in der Vorname, Familienname und Anschrift solcher Personen verzeichnet sind, die sich in Dauerkleingartengebieten angemeldet haben. Eine Ablichtung dieser Liste wird wiederum durch das Bauordnungsamt an das Liegenschaftsamt gesandt, damit dieses feststellen kann, ob Zuzüge für solche Kleingärten zu verzeichnen sind, bei denen die Stadtgemeinde Bremen Grundstückseigentümer ist und die Grundstücke vom Liegenschaftsamt verwaltet werden.

Vermutet das Liegenschaftsamt als Verpächter aufgrund so bekannt gewordener Daten, daß eine vertragswidrige Nutzung (für Wohnzwecke) des Dauerkleingartens vorliegt, gibt es diese Daten über den Landesverband der Klein-

gärtner Bremen e.V. als Generalpächter an den jeweiligen Kleingartenverein als Zwischenpächter weiter mit der Aufforderung festzustellen, ob eine vertragswidrige Nutzung vorliegt.

Bei der Übermittlung der Daten vom Einwohnermeldeamt an das Bauordnungsamt handelt es sich um eine regelmäßige Datenübermittlung im Sinne des § 30 Abs. 4 des Bremischen Meldegesetzes (BremMG) in der Fassung vom 20. Januar 1986 (Brem.GBl. Nr. 1 S. 1).

Nach dieser Vorschrift ist die regelmäßige Datenübermittlung durch die Meldebehörde an andere Behörden oder öffentliche Stellen nur zulässig, soweit dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zweckes der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist.

Nach § 36 Abs. 2 Nr. 2 BremMG ist der Senator für Inneres ermächtigt, durch Rechtsverordnung für die Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden Anlaß und Zweck der Übermittlungen, die Datenempfänger, die zu übermittelnden Daten sowie ihre Form festzulegen.

Eine solche Rechtsverordnung liegt bisher nicht vor. Der Entwurf der Meldedatenübermittlungsverordnung befindet sich zur Beratung in der Innendeputation. Es gibt auch keine andere bundes- oder landesrechtliche gesetzliche Vorschrift, welche die Voraussetzungen des § 30 Abs. 4 BremMG erfüllt und eine solche regelmäßige Datenübermittlung erlaubt.

Nach § 38 Abs. 2 und 4 BremMG dürfen jedoch regelmäßige Datenübermittlungen, die am Tage des Inkrafttretens des BremMG in der zitierten Fassung zugelassen waren, bis zum Erlaß der Rechtsverordnung, längstens jedoch bis zum 31. Dezember 1987, weiterhin vorgenommen werden.

Das bedeutet für den vorliegenden Fall, daß die regelmäßige Übermittlung dann zulässig wäre, wenn diese zur rechtmäßigen Erfüllung der in der Zuständigkeit des Bauordnungsamtes liegenden Aufgabe erforderlich wäre, d. h., wenn diese die ihm übertragene Aufgabe ohne Kenntnis der Daten nicht erfüllen könnte und die Daten beim Betroffenen nur mit unverhältnismäßig hohem Aufwand erheben könnte oder von einer Datenerhebung nach der Art der Aufgabe abgesehen werden müßte.

Nach meinen bisherigen Feststellungen vermag ich die Erforderlichkeit im vorher beschriebenen Sinne nicht zu erkennen. Meines Erachtens könnte die dem Bauordnungsamt übertragene Aufgabe von diesem durch andere geeignete Maßnahmen erfüllt werden.

Soweit das Bauordnungsamt die ihm übermittelten Daten bisher mittels abgelichteter Liste an das Liegenschaftsamt weitergegeben hat, stellt dieses einen Verstoß gegen das geltende Datenschutzrecht dar.

Das ergibt sich schon aus § 30 Abs. 5 BremMG, wonach der Datenempfänger die ihm übermittelten Daten nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm übermittelt wurden. Nach den Angaben des Bauordnungsamtes bzw. denen der Meldebehörden sind dem Bauordnungsamt die Daten für die Kontrolle der Einhaltung der baurechtlich zulässigen Nutzung baulicher Anlagen in Dauerkleingartengebieten übermittelt worden. Zu erwähnen bleibt, daß das Liegenschaftsamt durch diese unzulässige Übermittlung auch in den Besitz personenbezogener Daten solcher Personen gekommen ist, bei deren Kleingarten die Stadtgemeinde Bremen nicht Eigentümer ist.

Ich habe dem Bauordnungsamt meine Rechtsauffassung mitgeteilt und dieses um Stellungnahme gebeten.

Das Bauordnungsamt hat mir daraufhin mitgeteilt, es werde die von der Meldebehörde übermittelten personenbezogenen Daten nicht mehr an das Liegenschaftsamt weitergeben. Im übrigen könne es jedoch meiner Auffassung der Unzulässigkeit der Datenübermittlung nicht folgen und weise diese auf das Entschiedenste zurück.

Ich sehe eine grundsätzliche Klärung dieser Problematik als dringend geboten an, da es an einer ausreichenden gesetzlichen Grundlage für eine derartige Datenübermittlung mangelt.

Eine Beibehaltung der bisherigen Praxis kann aus datenschutzrechtlicher Sicht nicht hingenommen werden.

5.8 Wirtschaft und Außenhandel

5.8.1 Schwerpunkte, Handlungsbedarfsfälle

5.8.1.1 Neufassung der Wahlordnung für die Wahlen zu den Arbeitnehmerkammern

Der Senator für Wirtschaft hat mir den Entwurf einer Neufassung der Wahlordnung für die Wahlen zu den Arbeitnehmerkammern mit der Bitte um datenschutzrechtliche Beurteilung vorgelegt.

In vorbildlichem Zusammenwirken mit dem Senator für Wirtschaft und Außenhandel und den Arbeitnehmerkammern sind in dem Verordnungsentwurf sowohl die datenschutzrechtlich notwendigen als auch wünschenswerten Regelungen aufgenommen oder die Vorschriften entsprechend geändert worden. Der Umfang der personenbezogenen Daten, die in das Wählerverzeichnis aufgenommen werden, ist auf das notwendige Maß beschränkt worden. Alle Mitglieder der Wahlorgane werden auf die Wahrung des Datengeheimnisses besonders verpflichtet.

Problematisch geblieben sind die Vorschriften, die regeln, daß die Wählerverzeichnisse nach der Durchführung der Wahl bei den Arbeitnehmerkammern als Mitgliederverzeichnisse verbleiben sollen.

Da die personenbezogenen Daten der Wahlberechtigten den Arbeitnehmerkammern von den Arbeitgebern für den Zweck Durchführung der Wahlen übermittelt werden, wird mit diesen Bestimmungen eine zweckentfremdete Verwendung der Daten normiert.

Dieses stellt einen neuen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar und bedarf daher einer verfassungsgemäßen gesetzlichen Regelung. Ob der Verordnungsgeber einen solchen Eingriff regeln kann, ist davon abhängig, ob das Gesetz über die Arbeitnehmerkammern eine entsprechende Ermächtigung enthält. Eine solche Ermächtigung ist dem Arbeitnehmerkammerngesetz nicht zu entnehmen.

Die vorgenommene Regelung kann im Hinblick auf die den Arbeitnehmerkammern übertragenen Aufgaben und auf den Tatbestand, daß die Arbeitnehmerkammern sonst über keine Mitgliederverzeichnisse verfügen und auf anderem Wege wohl auch nicht erhalten können, für eine Übergangsfrist als zulässig angesehen werden. Nach der Rechtsprechung des Bundesverfassungsgerichts kann eine solche Frist in Ausnahmefällen, in denen sich die Notwendigkeit einer gesetzlichen Regelung durch geänderte Verfassungsinterpretationen ergeben hat, dann angewendet werden, wenn gravierende Nachteile für das Gemeinwohl zu erwarten sind, falls die bisherige Praxis aufgegeben wird.

Der Gesetzgeber bleibt aufgerufen, das Problem alsbald zu regeln.

Es konnte erreicht werden, daß die Arbeitnehmerkammern die Betroffenen über die Verwendung der Wählerverzeichnisse als Mitgliederlisten durch öffentliche Bekanntmachung zu unterrichten haben.

5.8.1.2 Datenübermittlung durch Gewerbebehörden an Dritte

In meinem letzten Jahresbericht habe ich unter Pkt. 5.10.1.2, S. 61 berichtet, daß mit dem Senator für Wirtschaft und Außenhandel eine Übergangslösung hinsichtlich der Erteilung von Auskünften aus dem Gewerbemelderegister an Stellen außerhalb des öffentlichen Bereichs vereinbart worden ist. Danach übermitteln die Gewerbebehörden Daten ohne Zustimmung der Betroffenen nur noch in solchen Fällen, in denen der Auskunftssuchende glaubhaft machen kann, daß die Auskunft zur Durchsetzung zivilrechtlicher Ansprüche dient und er sich die Angaben nicht auf andere Weise beschaffen kann. Das in meinem Bericht erwähnte Verwaltungsverfahren, das eine Handelsauskunftei gegen diese Auskunftspraxis anhängig gemacht hatte, ist mittlerweile rechtsbeständig im Sinne der Rechtmäßigkeit der Auskunftspraxis der Gewerbebehörden abgeschlossen.

Inzwischen hat sich die Handelskammer an den Herrn Senator für Wirtschaft und Außenhandel gewandt mit der Bitte, Bremen möge sich wirtschaftsfreundlich präsentieren und bis zu einer zu erwartenden bundesgesetzlichen Regelung, die vermutlich eine Weitergabe von Daten aus Verwaltungsbeständen zulassen werde, die früher geübte Auskunftserteilung im Interesse der bremischen Wirtschaft ermöglichen, zumal in sämtlichen anderen Bundesländern die Erteilung von Auskünften aus den Gewerbeanzeigen unangefochtene Praxis sei. Bremen möge der

zu erwartenden gesetzlichen Regelung nicht durch restriktive Verwaltungsanordnungen vorgreifen. Rechtlich sei eine einengende Auskunftspraxis auch nicht geboten, da schützenswerte Belange der in den Gewerbeanzeigen erfaßten Betriebe nicht ersichtlich seien. Es handele sich um rein betriebsbezogene Daten, die nicht datenschutzrechtlichen Beschränkungen unterlägen. Die Angaben zum Betriebsinhaber seien nicht derart tief in der Privatsphäre angesiedelt, daß eine Weitergabe nicht gerechtfertigt wäre, wenn ein berechtigtes geschäftliches Interesse an den Gesamtdaten des Unternehmens dargelegt werde.

Das zu Grundrechtsrang erhobene Recht auf informationelle Selbstbestimmung finde dort seine Grenze, wo ihm gesetzlich garantierte Rechte anderer entgegenstünden.

Der Senator für Wirtschaft und Außenhandel hat mich um Stellungnahme gebeten.

Der Auffassung der Handelskammer, daß eine restriktive Auskunftspraxis nicht geboten ist, vermag ich nicht zu folgen.

Die dahingehende rechtliche Beurteilung der Handelskammer, daß es sich bei den Angaben in den Gewerbeanzeigen um betriebsbezogene Daten handelt und diese deshalb nicht den datenschutzrechtlichen Beschränkungen unterliegen, wird von mir nicht geteilt.

Die Wirtschaftsverbände haben bei der Beratung des Bundesdatenschutzgesetzes (BDSG) zwar gewünscht, daß Angaben über die Teilnahme einer Person am Wirtschaftsleben generell aus dem Datenschutz ausgenommen werden sollten; der Gesetzgeber ist diesen Wünschen aber nicht gefolgt. In der Begründung des Regierungsentwurfs zum BDSG heißt es dazu: „Es konnte jedoch nicht soweit gegangen werden, wie vorgeschlagen wurde, auch natürliche Personen vom Schutze des Gesetzes auszunehmen, soweit sie wettbewerblich am Wirtschaftsleben teilnehmen, schon deshalb nicht, weil eine Abgrenzung zwischen personenbezogenen Daten über ein und dieselbe Person kaum möglich ist und eine solche Regelung deshalb zu Rechtsunsicherheiten führen würde."

Auch der Innenausschuß des Deutschen Bundestages ist diesen Vorschlägen nicht gefolgt. In seinem Bericht zum Entwurf des BDSG führte er folgendes aus: „Abgelehnt hat der Ausschuß nach sorgfältiger Erörterung den aus Kreisen der Wirtschaft unterbreiteten Vorschlag, alle seine geschäfts- oder gewerbliche Tätigkeit einer einzelnen Person betreffenden Daten aus dem Schutzbereich des Gesetzes auszunehmen. Eine solche Ausnahme scheitert nach Ansicht des Ausschusses am Fehlen eindeutiger Abgrenzungskriterien für rein private und geschäftliche Daten".

So sind z. B. auch die Angaben über die finanzielle Situation einer GmbH, die als Teil der Angaben über die Person des alleinigen Gesellschafters und Geschäftsführers der GmbH für Kreditauskünfte gespeichert sind, nach einem Urteil des Bundesgerichtshofes personenbezogene Daten des Gesellschafters/Geschäftsführers.

Soweit die Handelskammer geltend macht, daß es sich in diesem Fall um Daten handele, die weniger tief in der Privatsphäre der Betroffenen angesiedelt seien, ist darauf zu verweisen, daß alle Informationen, die über die Bezugsperson etwas aussagen, in den Anwendungsbereich des Datenschutzrechts einbezogen sind. Eine Beschränkung auf personenbezogene Informationen, die der Intim- und Privatsphäre zuzurechnen sind, oder eine Ausklammerung sogenannter weniger sensitiver Daten kennt das Datenschutzrecht nicht. Das Bundesverfassungsgericht hat in seinem Urteil zum Volkszählungsgesetz 1983 dazu ausgeführt, daß Datenschutz unabhängig davon besteht, welche personenbezogenen Daten berührt sind.

Wenn die Handelskammer darauf verweist, daß das Grundrecht auf informationelle Selbstbestimmung Einschränkungen unterworfen werden kann, so ist diesem zuzustimmen. Auch das Bundesverfassungsgericht hat in seinem Urteil zum Volkszählungsgesetz ausgeführt, daß dem Einzelnen dieses Recht nicht schrankenlos im Sinne einer absoluten, uneingeschränkten Herrschaft über „seine" Daten zustünde. Allerdings hat das Bundesverfassungsgericht klar festgestellt, daß eine Einschränkung dieses Rechts allein aufgrund einer verfassungsgemäßen gesetzlichen Grundlage möglich ist. Nach den Ausführungen des Bundesverfassungsgerichts bedarf es dazu grundsätzlich einer bereichsspezifischen Norm. Nur ausnahmsweise reichen Generalklauseln in den Datenschutzgesetzen als Auffangnormen aus. Das gilt insbesondere für Fälle, bei denen, wie im vorliegenden Falle, ein gesetzlicher Auskunftszwang gegeben ist.

Eine solche bereichsspezifische Norm ist für den vorliegenden Fall die Gewerbeordnung. § 14 der Gewerbeordnung normiert die Anzeigepflicht für das stehende Gewerbe und schränkt damit das Recht auf informationelle Selbstbestimmung des betroffenen Gewerbetreibenden ein und erlaubt der zuständigen Behörde, personenbezogene Daten der Betroffenen zu erheben, zu speichern und für Zwecke der Durchführung der Gewerbeordnung zu verarbeiten. Die Vorschrift enthält aber keine Erlaubnis für die Übermittlung dieser Daten an Dritte außerhalb des öffentlichen Bereichs. Eine solche Weitergabe würde eine Verwendung für einen anderen Zweck als dem der Eingriffsermächtigung zugrunde liegenden bedeuten. Nach herrschender Rechtsmeinung und Rechtsprechung bedarf es dafür einer ausdrücklichen gesetzlichen Regelung.

Aus diesem Grunde hat die Bundesregierung vorgeschlagen, mit dem Entwurf eines Gesetzes zur Änderung des Titels III der Gewerbeordnung und anderer gewerblicher Vorschriften dem § 14 der Gewerbeordnung einen neuen Absatz anzufügen, der die Übermittlung personenbezogener Daten aus den Gewerbeanzeigen an Personen und Stellen außerhalb des öffentlichen Bereichs im bestimmten Umfange unter bestimmten Voraussetzungen zulassen sollte. Der Gesetzgeber hat diese Ergänzung im Laufe der Beratung des Gesetzentwurfs fallengelassen, da die Regelung der Übermittlung von Daten durch Behörden erst nach Auswertung der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 erfolgen soll.

Die von der Handelskammer gewünschte Weitergabe der Daten aus den Gewerbeanzeigen läßt sich auch nicht mit dem sogenannten „Übergangsbonus" begründen. Das Bundesverfassungsgericht hat in Fällen, in denen sich für ein Verwaltungshandeln ein Gesetzeserfordernis erst aufgrund eines gewandelten und spezifizierten Verfassungs- und Grundrechtsverständnisses ergeben hat, die Zulässigkeit von Eingriffen in Grundrechte für eine Übergangsfrist als Ausnahme anerkannt, um eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen zu vermeiden, die der verfassungsmäßigen Ordnung noch ferner stände als der bisherige Zustand. Das Bundesverfassungsgericht hat zur Anwendung bisheriger Regelungen während einer Übergangsfrist ausgeführt, daß bis zur Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber sich die Befugnisse der Behörden auf das zu reduzieren haben, was im konkreten Fall für die Abwehr gravierender Nachteile für das Gemeinwohl unerläßlich ist. Im vorliegenden Falle sind solche gravierenden Nachteile für das Gemeinwohl nicht zu erkennen. Außerdem sind solche Fristen zu begrenzen. Die Frist endet spätestens mit dem Zeitpunkt, in dem der Gesetzgeber das einschlägige Gesetz novelliert und keine ausreichende, den Eingriff in das Grundrecht erlaubende Vorschrift schafft. Dadurch, daß der Deutsche Bundestag die Gewerbeordnung novelliert hat und die beabsichtigte Einfügung einer die gewünschte Datenweitergabe erlaubenden Vorschrift fallengelassen hat, kann eine solche Übergangsfrist nicht mehr in Anspruch genommen werden.

Aus Vorstehendem ergibt sich, daß die von den zuständigen Behörden geübte restriktive Auskunftspraxis nicht, wie von der Handelskammer vermutet, auf einer „restriktiven Verwaltungsordnung" beruht, sondern aufgrund der Rechtslage rechtmäßiges Handeln der Verwaltung beinhaltet, zu dem sie auch verpflichtet ist.

Die von der Handelskammer gewünschte Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs ist somit datenschutzrechtlich unzulässig.

Da die Handelskammer mitgeteilt hat, daß die Erteilung solcher Auskünfte in allen anderen Bundesländern unangefochtene Praxis ist, habe ich die Landesbeauftragten für den Datenschutz der übrigen Bundesländer auf dieses Problem aufmerksam gemacht und gebeten, mir die Praxis ihres Bundeslandes mitzuteilen.

Zur Zeit liegen mir noch nicht aus allen Bundesländern Rückäußerungen vor. Die bisher vorliegenden Antworten lassen aber erkennen, daß in der Mehrheit der Bundesländer eine ähnliche Praxis geübt wird wie in Bremen. So hat mir z. B. der Bayerische Landesbeauftragte für den Datenschutz mitgeteilt, daß er meine Rechtsauffassung teilt und aus diesem Grunde jede Datenübermittlung an Dritte, besonders auch im Hinblick auf die neuere Rechtsprechung des Bayerischen Verfassungsgerichtshofes, für problematisch hält. Er hat deshalb ebenso wie ich den Bayerischen Staatsminister für Wirtschaft und Verkehr dringend an die Notwendigkeit des Erlasses präziser bereichsspezifischer Normen für die Erhebung, Verarbeitung und Nutzung von Daten über Gewerbetreibende erinnert.

5.9 Finanzwesen

5.9.1 Steuern

5.9.1.1 Schwerpunkte, Handlungsbedarfsfälle

— Entwurf einer Kontrollmitteilungsverordnung nach § 93a der Abgabenordnung

In meinem letzten Jahresbericht habe ich unter Pkt. 2.1.3.4, S. 18 f. berichtet, daß mit dem am 19. Dezember 1985 vom Bundestag beschlossenen Steuerrechtsbereinigungsgesetz ein neuer § 93a in die Abgabenordnung (AO) aufgenommen worden ist, der die Bundesregierung ermächtigt, durch Rechtsverordnung zu bestimmen, daß Behörden in bestimmten Fällen den Finanzbehörden über erlassene Verwaltungsakte oder bei Zahlungen an Dritte Mitteilungen zu machen haben (Kontrollmitteilungen).

Eine Unterkommission der Finanzbehörden des Bundes und der Länder hat einen Entwurf einer Kontrollmitteilungsverordnung vorgelegt. Dieser Entwurf normiert auch Mitteilungspflichten von Sozialleistungsträgern an die Finanzbehörden.

Ich halte eine solche Mitteilungsverpflichtung für unzulässig. Nach § 71 des Sozialgesetzbuches X (SGB X) ist die Offenbarung von Sozialdaten für die Sicherstellung der Besteuerung auf Einzelauskünfte unter Wahrung des Subsidiaritätsprinzips auf Fälle der Amtshilfepflicht und auf Fälle des Verdachts auf Steuerstraftaten beschränkt.

Die Zulässigkeit kann auch nicht damit begründet werden, daß der § 93a AO eine Ergänzung des die Auskunftspflicht Beteiligter und anderer Personen regelnden § 93 AO darstellt und daß dieser in § 71 des Sozialgesetzbuches aufgeführt ist und somit die Offenbarung von Sozialdaten im Sinne regelmäßiger Mitteilungen erlaubt.

Beide Vorschriften regeln unterschiedliche Verfahren. § 93 AO sieht vor, daß für die Besteuerung zunächst der Betroffene zur Auskunft verpflichtet ist. Erst wenn dieser seiner Auskunftspflicht nicht nachkommt, können Dritte befragt werden. § 93a AO sieht dagegen vor, daß unabhängig von der Mitwirkungsbereitschaft des Betroffenen regelmäßig Mitteilungen gemacht werden. Der sich aus dem Verordnungsentwurf ergebenden weiteren Einschränkung des Sozialgeheimnisses vermag ich nicht zuzustimmen.

Der Verordnungsentwurf sieht vor, daß Behörden den Finanzbehörden den Erlaß solcher Verwaltungsakte mitzuteilen haben, welche die Versagung oder Einschränkung einer steuerlichen Vergünstigung zur Folge haben können.

Ich habe erhebliche Zweifel, ob diese Vorschrift mit der Ermächtigung des Verordnungsgebers in § 93a AO vereinbar ist. Die Ermächtigung beschränkt sich auf solche Fälle, bei denen der Verwaltungsakt eine Versagung oder Einschränkung einer steuerlichen Vergünstigung zur Folge hat.

Die vorgesehene Ausweitung dahingehend, daß schon die Möglichkeit des Eintritts der genannten Folgen eines Verwaltungsaktes eine Mitteilungspflicht begründen soll, kann im Verwaltungsvollzug zu einer vom Gesetzgeber nicht gewollten und datenschutzrechtlich nicht zu vertretenden Ausweitung der Kontrollmitteilungen führen.

Der Verordnungsentwurf nimmt öffentlich-rechtlich organisierte Kreditinstitute von der Mitteilungspflicht aus. Diese Ausnahme ist bereits vom Gesetzgeber im § 93a AO geregelt. Er sieht eine Mitteilungspflicht allerdings in den Fällen vor, in denen die Kreditinstitute über die Vergabe von Mitteln aus öffentlichen Haushalten entscheiden oder dabei beteiligt sind. Da § 93a AO eine solche Einschränkug der Ausnahme von der Mitteilungspflicht nicht vorsieht und eine abschließende Regelung darstellt, ist eine Ermächtigung für eine solche Vorschrift nicht gegeben. Nach dem Verordnungsentwurf sind die Betroffenen in bestimmten Fällen darüber zu unterrichten, daß Mitteilungen an die Finanzbehörden erfolgen.

Meines Erachtens sollte eine grundsätzliche Unterrichtungspflicht normiert und die Unterlassung nur auf das notwendige Maß beschränkt werden. Zum informationellen Selbstbestimmungsrecht gehört auch, daß der Bürger erfährt, welche perzonenbezogenen Daten zu welchem Zweck und mit welchen Rechtsfolgen für ihn übermittelt werden.

— **Erlaß einer Steuer-Daten-Abrufverordnung nach § 30 Abs. 6 Satz 2 der Abgabenordnung**

Wie ich in meinem letzten Jahresbericht unter Pkt. 2.1.3.4, S. 18 bereits berichtet habe, ist der § 30 der Abgabenordnung (AO) durch das am 19. Dezember 1985 vom Bundestag beschlossene Steuerrechtsbereinigungsgesetz 1986 zur Sicherung des Steuergeheimnisses geändert worden.

Den besonderen Bedingungen der automatisierten Datenverarbeitung ist dadurch Rechnung getragen worden, daß schon der unbefugte Abruf von im automatisierten Verfahren gespeicherten Daten eine Verletzung des Steuergeheimnisses bedeutet. Der Bundesminister der Finanzen ist ermächtigt worden, durch Rechtsverordnung zu bestimmen, welche technischen und organisatorischen Maßnahmen gegen den unbefugten Abruf von Daten zu treffen sind und näher zu regeln, bei welchen Datenarten der Abruf zulässig ist und wer zum Abruf berechtigt ist.

Der Entwurf einer entsprechenden Verordnung ist nunmehr vom Bundesminister für Finanzen vorgelegt worden.

Danach darf ein Datenabrufverfahren nur eingerichtet werden, wenn die bereitgehaltenen Daten dazu bestimmt und ihrer Art nach geeignet sind, der Durchführung von bestimmten Verfahren in Steuersachen zu dienen.

Es fehlt eine dahingehende Einschränkung, daß die Daten für die genannten Verfahren auch erforderlich sein müssen. Die entsprechenden Vorschriften des Verordnungsentwurfes enthalten keine nähere Bestimmung der Arten der Daten, die geeignet und erforderlich sind für die Durchführung der genannten Verfahren. Dieses ist den obersten Finanzbehörden und den Leitern der Gemeindeverwaltungen überlassen. Ich bezweifle, ob diese unbestimmten Regelungen dem Grundsatz der Normenklarheit gerecht werden.

Weiter sieht der Entwurf vor, daß die obersten Finanzbehörden und die Leiter der Gemeindeverwaltungen technische und organisatorische Maßnahmen zu treffen haben, die geeignet sind, den Datenabruf durch nicht zugriffsberechtigte Personen auszuschließen, eine Überschreitung der Zugriffsberechtigung zu verhindern und die nachträgliche Feststellung zu ermöglichen, aufgrund welcher Zugriffsberechtigungen Daten abgerufen werden können. Die genannten Maßnahmen sollen jedoch dann unterbleiben können, wenn sie nicht in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

Auf keinen Fall kann die Bestimmung hingenommen werden, nach der technische und organisatorische Maßnahmen völlig unterbleiben können. Solche Schutzmaßnahmen sind schon verfassungsrechtlich geboten. Es kann auch nicht ausgeschlossen werden, daß eine solche Regelung in Anbetracht der den öffentlichen Stellen zur Verfügung stehenden knappen Ressourcen im Vollzug dazu führt, daß Schutzmaßnahmen weitgehend mit der Begründung ihrer Unangemessenheit unterbleiben. Auch sollte die Festlegung der Gruppen der Zugriffsberechtigten und der Zugriffsberechtigungen durch den Verordnungsgeber erfolgen und nicht den obersten Finanzbehörden und den Leitern der Gemeindeverwaltungen übertragen werden.

Bei dem Abruf personenbezogener Daten durch Abrufende anderer Behörden als der speichernden Stelle sieht der Verordnungsentwurf eine Überprüfung der Abrufe durch eine stichprobenweise maschinelle Aufzeichnung vor. Dieses Prüfungsverfahren sollte in erforderlichen Fällen auch für Abrufe aus den speichernden Stellen vorgesehen werden.

Ich werde im Zusammenwirken mit den übrigen Datenschutzbeauftragten um eine entsprechende datenschutzrechtliche Verbesserung der Steuerdatenabrufverordnung bemüht bleiben.

— **Übermittlung von Besteuerungsgrundlagen durch die Finanzämter an die Stadtgemeinden**

Nach § 31 der Abgabenordnung (AO) sind die Finanzbehörden u. a. berechtigt, Besteuerungsgrundlagen an Gemeinden einschließlich der Körperschaften des öffentlichen Rechts zur Festsetzung von solchen Abgaben weiterzugeben, die an die Besteuerungsgrundlagen, Steuermeßbeträge und Steuerbeträge anknüpfen. Zu den Besteuerungsgrundlagen gehören nach einhelliger Rechtsauffassung nicht die Personalien der Steuerpflichtigen und die Objekte der Besteuerung (z. B. Bezeichnung eines Grundstücks).

Tatsächlich aber werden im Lande Bremen wie auch in einigen anderen Bundesländern für die Festsetzung kommunaler Abgaben und Gebühren solche Daten an die Gemeinden oder Körperschaften des öffentlichen Rechts übermittelt. Beispielhaft können hier die Festsetzungen der Müllabfuhrgebühren und der Deichbeiträge genannt werden.

Da die Abgabenordnung durch das Steuerrechtsbereinigungsgesetz 1986 geändert worden ist, kann für die Übermittlungspraxis auch nicht mehr der sogenannte Übergangsbonus in Anspruch genommen werden. Soweit in der Stadtgemeinde Bremen die Festsetzung und Einziehung kommunaler Abgaben durch das Gesetz zur Übertragung der Aufgaben des Steueramts der Freien Hansestadt Bremen auf die Finanzämter bei Finanzämtern liegt, ändert das nichts daran, daß die Verwendung der Daten für die Festsetzung kommunaler Abgaben unzulässig ist. Das Bayerische Staatsministerium des Innern hat zur Lösung des Problems angeregt, den § 31 AO dahingehend zu ändern, daß die jetzt geübte Übermittlungspraxis rechtlich abgedeckt ist. Ich habe gegen ein solches Vorhaben keine datenschutzrechtlichen Bedenken. Die jetzige unzulässige Übermittlungspraxis kann jedoch nicht mehr für einen längeren Zeitraum hingenommen werden.

— Kontrollmitteilungen bei der Besteuerung von Hunden

Ein Bürger hat mir mitgeteilt, daß er von Bremerhaven in das niedersächsische Umland verzogen und bei dieser Gelegenheit seiner Verpflichtung nach dem Ortsgesetz betreffend die Hundesteuer nachgekommen sei, indem er der Stadt Bremerhaven die Beendigung seiner Hundesteuerpflicht gemeldet habe.

Die Stadtverwaltung der Stadt Bremerhaven habe die auf diese Weise von ihm erhobenen personenbezogenen Daten an seine neue Wohnsitzgemeinde in Niedersachsen in Form einer Kontrollmitteilung übermittelt, obwohl er dort wegen Abgabe seines Hundes nicht mehr hundesteuerpflichtig geworden sei. Er hat mich gebeten zu prüfen, ob diese Datenübermittlung datenschutzrechtlich zulässig sei.

Eine Rückfrage beim Steueramt Bremerhaven hat ergeben, daß die Gemeinden fast aller Bundesländer bei der Durchführung der jeweiligen Ortsgesetze/Satzungen über die Hundesteuer Kontrollmitteilungen austauschen, wenn ein Hundesteuerpflichtiger seinen Wegzug aus der Gemeinde meldet oder den Verkauf eines Hundes anzeigt.

Das Finanzamt Bremen-Mitte als für die Durchführung des Hundesteuergesetzes der Stadtgemeinde Bremen zuständige Behörde hat bestätigt, daß es sich an dem Austausch solcher Kontrollmitteilungen beteilige.

Das Steueramt Bremerhaven und das Finanzamt Bremen-Mitte haben erklärt, daß eine dringende Notwendigkeit bestehe, den Austausch solcher Kontrollmitteilungen beizubehalten. Sie seien bei der Besteuerung von Hunden auf die Angaben Dritter über besteuerungserhebliche Tatsachen angewiesen. Wollten sie alle Angaben, die sie jetzt durch Kontrollmitteilungen erhalten, selbst erheben, würde sich für sie ein erheblicher finanzieller Aufwand ergeben.

Der Austausch solcher Kontrollmitteilungen stellt einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar, der nach der Rechtsprechung des Bundesverfassungsgerichts einer bereichsspezifischen gesetzlichen Grundlage bedarf, die den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit genügen muß. Als solche gesetzliche Grundlage ist für den vorliegenden Fall das Bremische Abgabengesetz anzusehen. Dieses enthält jedoch keine Vorschrift, die den Austausch solcher Kontrollmitteilungen erlaubt.

Das Steueramt Bremerhaven hat geltend gemacht, daß die Datenübermittlung bis zu einer gesetzlichen Regelung durch die Inanspruchnahme des sogenannten Übergangsbonus erlaubt sei, da die Hundesteuer das wichtige ordnungspolitische Ziel verfolge, die Hundehaltung einzudämmen und den mit ihr verbundenen Belästigungen und Gefahren für die Allgemeinheit entgegenzuwirken.

Dem vermag ich nicht zu folgen. Das Bundesverfassungsgericht hat in ständiger Rechtsprechung die Zulässigkeit von Eingriffen in das informationelle Selbstbestimmungsrecht ohne ausreichende gesetzliche Ermächtigung für eine Übergangszeit nur ausnahmsweise in solchen Fällen für zulässig erklärt, in denen die bisherige Praxis nicht ohne gravierende Nachteile für das Gemeinwohl aufgegeben werden kann. Einen solchen gravierenden Nachteil für das Gemeinwohl vermag ich im vorliegenden Fall nicht zu erkennen, zumal die Hundesteuergesetze der Stadtgemeinden Bremen und Bremerhaven mit dort festgelegten Meldepflichten

und Sicherungs- und Überwachungsvorschriften wirkungsvolle Mittel für die Sicherung der Hundesteuer vorsehen. Die vorgetragenen finanziellen Erwägungen können eine Inanspruchnahme des Übergangsbonus nicht rechtfertigen.

Das Finanzamt Bremen-Mitte hält den Austausch von Kontrollmitteilungen auch deshalb für zulässig, weil nach dem Bremischen Abgabengesetz für alle Steuern, die von den Landesfinanzbehörden oder von der Stadtgemeinde Bremerhaven verwaltet werden, die Abgabenordnung als Verfahrensvorschrift anzuwenden ist. Die Abgabenordnung regelt im § 93a abschließend, in welchen Fällen Kontrollmitteilungen durch eine Verordnung vorgesehen werden können. Die hier in Rede stehenden Kontrollmitteilungen gehören nicht dazu. Die im Entwurf vorliegende Verordnung nach § 93a der Abgabenordnung sieht solche Kontrollmitteilungen ebenfalls nicht vor (vgl. Pkt. 5.9.1.1), so daß auch damit die Zulässigkeit nicht begründet werden kann.

5.10 Sonstige öffentliche Stellen, Körperschaften, Kammern u. a.

5.10.1 Datenerhebung durch die Steuerberaterkammer bei der Zulassung zur Abschlußprüfung nach dem Berufsbildungsgesetz

Mehrere Betroffene haben mich gebeten zu prüfen, ob die von der Steuerberaterkammer mit dem Antrag auf Zulassung zur Abschlußprüfung für den Beruf des Steuerberatungsgehilfen durchgeführte Datenerhebung in vollem Umfange datenschutzrechtlich zulässig ist. Die von den Betroffenen dazu geäußerten Zweifel bezogen sich insbesondere auf die Forderung auf Vorlage eines Lebenslaufes, in dem u. a. Angaben über den Beruf der Eltern des Antragstellers und vom Antragsteller durchgemachte Krankheiten enthalten sein sollten.

Die Steuerberaterkammer hat die Vorlage eines Lebenslaufes aufgrund einer entsprechenden Bestimmung der Prüfungsordnung für den Ausbildungsberuf „Fachgehilfe in steuer- und wirtschaftsberatenden Berufen" verlangt, die von ihr nach § 41 des Berufsbildungsgesetzes (BerufsBildG) erlassen worden ist. Bei dieser Prüfungsordnung handelt es sich um Satzungsrecht. Eine Einschränkung des Rechtes auf informationelle Selbstbestimmung bedarf jedoch einer gesetzlichen Grundlage. In den hier einschlägigen Rechtsvorschriften, nämlich dem Berufsbildungsgesetz und der Verordnung über die Berufsausbildung zum Fachgehilfen in steuer- und wirtschaftsberatenden Berufen sind keine Bestimmungen enthalten, welche die Forderung nach Einreichung eines Lebenslaufes und die damit verbundene Erhebung personenbezogener Daten in dem sich daraus ergebenden Umfange zulassen.

Die mit der Vorlage eines Lebenslaufes in üblicher Form verbundene Erhebung der personenbezogenen Daten des Antragstellers ist im übrigen weder für das Zulassungsverfahren zur Abschlußprüfung noch für die Durchführung der Abschlußprüfung erforderlich. Für das Zulassungsverfahren sind die Daten deshalb nicht erforderlich, weil nach dem Berufsbildungsgesetz zur Abschlußprüfung zuzulassen ist, wer die Ausbildungszeit zurückgelegt hat, an den vorgesehenen Zwischenprüfungen teilgenommen hat, die vorgeschriebenen Berichtshefte geführt hat und dessen Berufsausbildungsverhältnis in ein dafür vorgesehenes Verzeichnis eingetragen ist. Auch bei der Zulassung in besonderen Fällen müssen ähnliche sachliche Voraussetzungen erfüllt werden. Wegen der hier vorliegenden Besonderheiten genügt in diesen Fällen eine zusätzliche Darstellung des beruflichen Werdeganges.

Für die Durchführung der Abschlußprüfung sind die genannten Daten nicht erforderlich, da der Prüfungsausschuß nach dem Berufsbildungsgesetz mit der Abschlußprüfung nur festzustellen hat, ob der Ausgebildete die erforderlichen Fertigkeiten beherrscht, die notwendigen praktischen und theoretischen Kenntnisse besitzt und mit dem ihm im Berufsschulunterricht vermittelten, für die Berufsausübung wesentlichen Lehrstoff vertraut ist.

Das Beschwerdeverfahren konnte dadurch erledigt werden, daß die Steuerberaterkammer sich in bemerkenswert datenschutzfreundlicher Kooperationsbereitschaft entschließen konnte, ab sofort auf die Vorlage eines Lebenslaufes zu verzichten und bereits eingereichte zurückzugeben. Sie strebt eine entsprechende Änderung der von ihr erlassenen Prüfungsordnung an.

Bei der Prüfung dieser Angelegenheit konnte ich feststellen, daß alle mir zur Verfügung stehenden Prüfungsordnungen, die im Lande Bremen nach dem Berufsbildungsgesetz erlassen worden sind, die Vorlage eines Lebenslaufes als Voraussetzung zur Zulassung zur Abschlußprüfung fordern. Das ist offensichtlich darauf zurückzuführen, daß eine vom Berufsbildungsausschuß herausgegebene Musterprüfungsordnung eine entsprechende bundesweite Empfehlung enthält.

Die zuständigen Stellen haben mir auf Anfrage mitgeteilt, daß sie ab sofort bis zur endgültigen Klärung der Angelegenheit auf die Vorlage eines Lebenslaufes verzichten wollen.

Im Interesse einer bundeseinheitlichen rechtmäßigen Handhabung habe ich meine datenschutzrechtliche Beurteilung an die mit der Durchführung des Berufsbildungsgesetzes befaßten Stellen und an die übrigen Datenschutzbeauftragten herangetragen.

Überwiegend haben diese Stellen mir mitgeteilt, daß sie die von mir vertretene Auffassung teilen.

Der Bundesminister des Innern hält allerdings eine Beibehaltung der genannten Datenerhebung, abgesehen von der Angabe des Berufes der Eltern, für erforderlich. Er begründet dieses insbesondere damit, daß diese Daten geeignet seien, „in einem gewissen Umfange schon bei der Meldung zu einer berufsbegründenden Prüfung evtl. Hindernisse in der Person des Antragstellers ausfindig zu machen, die einer späteren Ausübung des Berufs (trotz bestandener Prüfung) entgegenstehen können. Unter diesem Aspekt könne es bei einzelnen Berufen — beispielsweise bei solchen, die im Bereich der Gesundheitsversorgung/Heilbehandlung angesiedelt seien — durchaus von Belang sein, Daten über durchgemachte Krankheiten von Prüfungsbewerbern abzufragen, insbesondere dann, wenn es sich um ansteckende Krankheiten handele, die für den inzwischen genesenen Prüfungsbewerber selbst nicht mehr gefährlich seien, gleichwohl aber eine Gefährdung anderer darstellen könnten (z. B. AIDS). Gleiches werde — je nach Art der Erkrankung — für Geistes- oder Erbkrankheiten gelten."

Dieser Auffassung vermag ich nicht zu folgen. Wie bereits dargelegt, hat der Gesetzgeber die Aufgabenstellung der zuständigen Stellen und der Prüfungsausschüsse bei den Abschlußprüfungen abschließend geregelt. Die vom Bundesminister des Innern genannten Aufgaben gehören nicht dazu. Die Beurteilung der gesundheitsbezogenen Eignung von Auszubildenden für den Ausbildungsberuf obliegt den niedergelassenen Ärzten nach den Bestimmungen des Jugendarbeitsschutzgesetzes. Darüber hinaus bestehen für bestimmte Gewerbebereiche oder Berufe Verpflichtungen, Gesundheitszeugnisse vorzulegen. Beispielhaft kann hier das Bundesseuchengesetz erwähnt werden.

Die vom Bundesminister des Innern vorgetragenen Gründe verdeutlichen die Gefahr, daß eine nicht auf das notwendige Maß beschränkte Datenerhebung bei Prüfungsausschüssen dazu führen kann, daß bei ihren Entscheidungen, bei denen ihnen ein erheblicher Beurteilungsspielraum eingeräumt ist, sachfremde Erwägungen einfließen.

Bei der Behandlung dieser Angelegenheit hat sich außerdem gezeigt, daß die datenschutzrelevanten Vorschriften des Berufsbildungsgesetzes einer Änderung bedürfen, um den Anforderungen des Bundesverfassungsgerichts an bereichsspezifischen Datennormen gerecht zu werden.

5.10.2 Apothekerkammer

Aufgrund einer Eingabe habe ich die Datenverarbeitung in der Apothekerkammer Bremen überprüft. Nach der Kammersatzung, die von der Kammerversammlung der Apothekerkammer verabschiedet ist, müssen u. a. die Beiträge für die angeschlossenen Apotheken ermittelt und die Rechnungen und der Jahresabschluß erstellt werden.

Die Buchführung wird auf einem programmierbaren Buchungssystem durchgeführt. Die Programme befinden sich auf einer Datenkassette und werden von einer Software-Firma erstellt und gepflegt. Die Kammerbediensteten können Änderungen offensichtlich nicht durchführen, da das System keine Schreibfunktion, sondern nur eine Lesefunktion für Kassetten aufwies. Andere allgemeine Daten waren offensichtlich auf der Kassette nicht gespeichert. Die personenbezogenen Daten wurden auf Magnetkonten geführt, die mittels Lese- und Schreibstation bearbeitet werden konnten. Die Magnetkontenkarten enthielten Umsätze und Beiträge der einzelnen Apotheken und wurden offen aufbewahrt. Ebenso lagen die Auswertungen für jeden offen lesbar aus, bevor sie abgeheftet oder versandt wurden. Ich habe die Kammerbediensteten auf § 6 Bremisches Datenschutzgesetz (BrDSG) (Anlage) hingewiesen und sie aufgefordert, sowohl den Raum als auch die Karteikästen zu verschließen.

Die Bediensteten der Kammer waren nicht auf das Datengeheimnis gemäß § 5 Abs. 2 BrDSG verpflichtet. Begründet wurde das damit, daß der Inhalt des Datenschutzgesetzes in der Kammer nicht bekannt sei. Außerdem waren die vorhandenen Dateien nach § 21 BrDSG i. V. m. der Datenregisterverordnung nicht gemeldet. Beides führte zu einer förmlichen Beanstandung nach § 22 Abs. 1 BrDSG. Die Kammer hat bisher lediglich zur Frage der Verpflichtung auf das Datengeheimnis Stellung genommen und inzwischen die Bediensteten verpflichtet.

Die Meldung zum Dateienregister steht noch aus.

6. Nicht-öffentlicher Bereich

6.1 Vorbemerkungen

Wie in jedem Jahr wird in diesem Kapitel die Tätigkeit des Landesbeauftragten als Aufsichtsbehörde nach dem 3. und 4. Abschnitt des Bundesdatenschutzgesetzes dargestellt.

Die Schwerpunkte in diesem Abschnitt bilden einerseits die Stellungnahmen zu Verfassungsbeschwerden, die beim Bundesverfassungsgericht vorliegen, nämlich zur Datenverarbeitung der Schufa und zur Telefondatenerfassung und andererseits die Prüfung einer bundesweit tätigen Handelsauskunftei mit selbständiger Geschäftsstelle in Bremen.

Ohne Aussagen aus den früheren Jahresberichten hier zu wiederholen, sei aber darauf hingewiesen, daß die Novelle zum Bundesdatenschutzgesetz auch für die Datenverarbeitung nicht-öffentlicher Stellen dringend beraten und verabschiedet werden muß. Herausragende Themen müssen auch hier die Diskussion des Arbeitnehmerdatenschutzes, bereichsspezifische Regelungen für Kreditinformationssysteme und die Erweiterung der Rechte der Aufsichtsbehörden sein.

6.2 Kreditinformationssystem der Schufa

6.2.1 Verfahren vor dem Bundeskartellamt

In meinem letzten Jahresbericht hatte ich die mit den Banken getroffenen Vereinbarungen bezüglich der Neuordnung des Schufa-Verfahrens dargestellt. Diese sollten in Ausführung zu der Entscheidung des Bundesgerichtshofes (BGH) vom 19. September 1985, durch die die von den Banken bis dahin verwendete Schufa-Klausel für nichtig erklärt wurde, die Datenschutzanforderungen sicherstellen.

Ein Schwerpunkt der damals geführten Verhandlungen betraf den Kreis der Anschlußkunden an das Schufa-System; dieser sollte auf das datenschutzrechtlich erforderliche Maß eingeschränkt werden. Anschlußkunden sind nicht-öffentliche Stellen, die Auskünfte aus dem Schufa-System erhalten und auch Daten für das Auskunftssystem melden.

Auf Anregung der Obersten Aufsichtsbehörden für den Datenschutz wurde daher einigen Anschlußkunden, die kein eigenes kreditorisches Risiko eingingen, von der Schufa der Anschlußvertrag gekündigt.

Dies hat in einigen Fällen zu kartellrechtlichen Verfahren geführt. Dabei handelt es sich u. a. um Auto-, Geräte- und Wohnungsvermieter, um Wohnungsbaufinanzierer (Bausparkassen und Versicherungen) und um Inkassobüros. Die Problematik wurde vor dem Bundeskartellamt mit Vertretern der Kreditwirtschaft, den Datenschutzaufsichtsbehörden und der gekündigten Wirtschaftszweige erörtert. Es galt, eine Lösung zu finden, die sowohl den Anforderungen des Datenschutzes als auch des Kartellrechts genügt. Unter den Datenschutzaufsichtsbehörden besteht Einigkeit darüber, daß der Kreis der Schufa-Anschlußpartner so klein wie möglich zu halten und auf Kredit gewährende Unternehmen zu beschränken ist.

Nach Mitteilung des Bundeskartellamtes sind die gegen die Schufa wegen „Diskrimierung" anhängig gemachten Verfahren bis auf den Bereich der Automobilvermieter abgeschlossen worden. Das Bundeskartellamt hat in den nachfolgend aufgezählten Fällen bestätigt, daß eine Kündigung nicht gegen kartellrechtliche Bestimmungen verstößt und daher die Schufa auch in Zukunft berechtigt ist, die Aufnahme eines solchen Vertragspartners abzulehnen. Die Kündigung war daher gegenüber Unternehmen zulässig,

— die kein typisches Geldkredit- oder Warenkreditrisiko tragen

— die nur gewerblichen Kunden Kredit einräumen

— die die gewerbliche Wohnungsvermietung und die kurzzeitige Mobiliarvermietung betreiben

— die Personalanfragen und -abfragen vor Einleitung gerichtlicher Maßnahmen vornehmen sowie bestimmte Versicherungsgeschäfte, aufgekaufte Fremdforderungen und sogenannte Policendarlehen absichern wollen.

Dem gegenüber hat das Bundeskartellamt festgestellt, daß für folgende Unternehmen weiterhin die Möglichkeit eines Schufa-Anschlusses bestehen muß, die

— Langzeitvermietung von Mobilien betreiben, die bei wirtschaftlicher Betrachtung dem sogenannten Leasing nahekommen,

— Grundpfandrechtlich gesicherte Kredite gewähren und zwar unabhängig davon, ob es sich um Kreditinstitute oder andere kreditgewährende Unternehmen handelt.

Nach meinen Informationen werden die Schufa-Gesellschaften in den nächsten Tagen denjenigen bisherigen Anschlußkunden, denen die Anschlußverträge zum 30. Juni 1986 gekündigt und deren Kündigungen bis zum Abschluß des beim Kartellamt anhängigen kartellrechtlichen Verfahrens ausgesetzt worden sind, mitteilen, daß die Kündigungsaussetzung zum 31. März 1987 entfällt und damit die Kündigungen wirksam werden. Soweit ein Anschluß gekündigter Unternehmen an die Schufa zukünftig weiter kartellrechtlich möglich sein muß, wird diesen Unternehmen ein neuer Vertrag angeboten werden.

Weil einigen Unternehmen von der Schufa gekündigt wurde, gehen diese nunmehr dazu über, den Bürger aufzufordern, eine Selbstauskunft vor dem Geschäftsabschluß beizubringen.

Gegen diese Praxis bestehen ebenfalls datenschutzrechtliche Bedenken. Zum einen enthält die Selbstauskunft erheblich mehr Daten als etwa einem B-Anschlußkunden der Schufa (erhält nur sog. Negativdaten) zur Verfügung stehen, zum anderen würde auf diese Art und Weise die Kündigung umgangen; eine solche Forderung könnte daher sittenwidrig sein.

Im Zusammenhang mit dem Anschluß der Inkasso-Büros wurde die Frage erörtert, in welchen Fällen der Schufa Suchaufträge erteilt werden können; die Datenschutzaufsichtsbehörden sind der Auffassung, daß das System nicht generell für Suchaufträge geöffnet werden sollte. Suchaufträge werden erteilt, wenn ein Schuldner mit unbekannter Adresse verzogen und nicht auffindbar ist. Bei Suchaufträgen wird das Merkmal „SU" bei der Schufa gespeichert. Tritt der Schuldner bei einem Schufaanschlußkunden in Erscheinung, ergeht automatisch eine Meldung an die Stelle, die den Suchauftrag erteilt hat. Suchaufträge sollten nur zur Durchsetzung eigener Forderungen, nicht jedoch bei Verkauf der Forderungen, möglich sein. Suchaufträge können daher nur in Zusammenhang mit Kreditvergaben von Schufa-Vertragspartnern erteilt werden. Die Möglichkeit, Suchaufträge zu erteilen, ist infolgedessen auf Vertragspartner der Schufa für eigene Forderungen zu beschränken. Inkassobüros können somit nicht selbständige Vertragspartner der Schufa sein. Wird ein Inkassobüro mit dem Einzug von Forderungen eines Schufa-Anschlußpartners beauftragt, obliegt es dem Anschlußpartner, den Suchauftrag zu erteilen.

6.2.2 Widerspruch gegen die Schufa-Klausel

Die Vereinbarungen zwischen dem zentralen Kreditausschuß und den Datenschutzaufsichtsbehörden sahen vor, daß alle Kreditinstitute ihre Kunden, mit denen sie schon eine Geschäftsbeziehung unterhielten, über die neue Schufa-Klausel (vgl. Anlage 5) und das neue Auskunftsverfahren benachrichtigen. In diesem Schreiben an die sogenannten Altkunden, das ebenfalls mit den Datenschutzaufsichtsbehörden abgestimmt war, wurden die Kunden auf die Möglichkeit hingewiesen, Widerspruch gegen zukünftige Datenübermittlungen an die Schufa einzulegen, sowie Widerspruch gegen die bisherige Speicherung ihrer Daten bei der Schufa einzulegen. Soweit die Kunden von diesem Widerspruch keinen Gebrauch machten, gingen die Kreditinstitute von dem Einverständnis des Kunden mit dem neuen Schufa-Melde- und Auskunftsverfahren aus. Die Widerspruchslösung wurde gewählt, weil es von der Kreditwirtschaft für zu aufwendig gehalten wurde, jedem einzelnen Kunden die neue Schufa-Klausel zur Unterschrift vorzulegen.

Entgegen der Hoffnung der Kreditwirtschaft, nur in ganz wenigen Fällen werde die Widerspruchslösung in Anspruch genommen, zeigten die Eingaben und meine Gespräche mit Kreditinstituten im Lande Bremen, daß die Kunden in einem nicht erwartet hohen Maße ihr Widerspruchsrecht nutzten.

Die praktische Handhabung des Widerspruchsrechts durch die Kreditinstitute führte erneut zu Beschwerden aus der Bevölkerung. Diese Beschwerden aus der Bevölkerung richteten sich zum einen dagegen, daß nach Einlegung eines Widerspruchs seitens der Kreditinstitute erklärt wurde, die Kontoführung könne nicht weiter aufrecht erhalten werden, zum anderen dagegen, daß die Sachbearbeiter einzelner Kreditinstitute den Kunden vor Einlegung des Widerspruchs mit der Begründung warnten, danach werde er (der Kunde) dastehen wie der schlimmste Schuldner, ihm würde von keiner Seite mehr ein Kredit eingeräumt werden. Mit diesen und anderen Einschüchterungsversuchen sollten die Kunden von der Wahrnehmung ihrer Rechte abgehalten werden. Aufgrund meiner Erfahrungen habe ich den Eindruck gewonnen, daß das Widerspruchsverfahren bei den Kreditinstituten unterschiedlich kundenfreundlich gehandhabt wird.

Aufgrund der eingehenden Beschwerden und Veröffentlichungen in Zeitungen haben die Datenschutzaufsichtsbehörden sehr eingehend die verschiedenen Fallgestaltungen erörtert, die sich beim Widerspruch des Kunden gegen die Schufa-Klausel bei Altverträgen oder nach Abschluß eines Vertrages auf der Grundlage der neuen Schufa-Klausel hinsichtlich der Datenübermittlung an die Schufa und der dortigen Speicherung zu Auskunftszwecken ergeben können.

Bei diesen Überlegungen war zu berücksichtigen, daß die Funktionsfähigkeit des Kreditinformationssystems der Schufa auch in Fällen des „Widerspruchs gegen die Schufa-Klausel" erhalten bleiben muß, da die Schufa entsprechend den Ausführungen des BGH im Schufa-Urteil vom 19. September 1985 in der Lage sein muß, möglichst vollständig und aktuell über kreditrelevante Daten zu informieren.

Zu klären war daher, in welchen Fällen der Widerspruch eines Kunden im Informationssystem der Schufa (mit einem sogenannten „WK-Merkmal") gekenzeichnet werden müsse.

Die Aufsichtsbehörden gingen davon aus, daß das WK-Merkmal weder als ein im herkömmlichen Sinne „positives" noch als ein „negatives" Merkmal zu bewerten ist. Die Zulässigkeit der Übermittlung dieses Merkmals muß daher in Abwägung nach § 24 BDSG im Einzelfall getroffen werden. Ergibt die Abwägung, daß die Beauskunftung dieses Merkmals im Interesse der Aussagefähigkeit des Schufa-Kreditinformationssystems unverzichtbar ist, so ist auch die Übermittlung dieses Merkmals an die Schufa zulässig.

In Fällen des Widerspruchs von Altkunden nach bereits erfolgter Übermittlung und Speicherung sogenannter „Negativdaten" sind diese Übermittlungen anhand der mit der Kreditwirtschaft auf der Grundlage des Schufa-Urteils vom 19. September 1985 festgelegten Kriterien zu prüfen. Aufgrund des Ergebnisses dieser Überprüfung ist im Einzelfall eine Löschung zu veranlassen. Bei ausschließlich positiven Daten, z. B. erledigter Kredit, kommt nur eine Löschung in Betracht, sofern der Kunde nicht nach entsprechender Aufklärung an der weiteren Speicherung interessiert ist. Eine Übermittlung des Merkmals „WK" kommt in solchen Fällen nicht in Betracht. Gleiches gilt für die Fälle, in denen lediglich die Eröffnung eines Girokontos bei der Schufa gespeichert ist.

Zusammenfassend gilt daher für Altkunden: Legt ein Kunde, über den nur Positivmerkmale gespeichert sind, Widerspruch ein, so sind alle Daten bei der Schufa zu löschen. Dies gilt für Girokonten, Bürgschaften und Kredite — erledigte und laufende — gleichermaßen. Sind auch Negativmerkmale über den Kunden gespeichert, so wird „WK" gespeichert. Außer WK können bei einem Widerspruch keine neuen Daten aus der Geschäftsverbindung der Schufa übermittelt werden.

Ein anderes Problem stellt sich bei sog. Neukunden. Dies sind Kunden, die z. B. ein Girokonto bei einem Kreditinstitut neu eröffnen wollen. Aus der Praxis der Aufsichtsbehörden läßt sich berichten, daß Kreditinstitute dann eine Kontoeröffnung ablehnen, wenn der Kunde von seinem Widerspruchsrecht gegen die Datenübermittlung an die Schufa Gebrauch machen will, selbst dann, wenn von vornherein klar ist, daß das Konto nur auf Guthabenbasis geführt werden soll und nur geführt werden kann.

Zwar sind Kreditinstitute nicht verpflichtet, ein Konto einzurichten, zumal es immer noch die Möglichkeit des Kunden gibt, bei der Post ein Girokonto zu eröffnen, die nicht am Schufa-System teilnimmt. Dies würde aber faktisch zu einer Rechtsverkürzung des informationellen Selbstbestimmungsrechts des Kunden führen. Nach meiner Erkenntnis wird diese strenge Linie aber nicht von allen Kreditinstituten gleichermaßen gehandhabt. Daß nicht alle Kreditinstitute bereit sind, Konten ohne

kreditorisches Risiko einzurichten, um dem Bürger zu ermöglichen, sein Recht auf informationelle Selbstbestimmung wahrnehmen zu können, ist bedauerlich.

6.2.3 Verfahren vor dem Bundesverfassungsgericht

— Dem Bundesverfassungsgericht liegt eine **Verfassungsbeschwerde zur Datenverarbeitung bei Banken und Kreditauskunfteien** vor, zu der ich um Äußerung gebeten worden bin. Folgender datenschutzrelevanter Tatbestand ist zu beurteilen:

Der Kläger eröffnete am 4. September 1979 bei der beklagten Bank ein Kontokorrentkonto. Das von der Beklagten verwendete und vom Kläger unterzeichnete Antragsformular (Kontoeröffnungsantrag) enthält u. a. folgende Klausel: „Über diese Kontoverbindung werden der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) Daten zur Speicherung im Rahmen ihrer Tätigkeit übermittelt . . ."

Am 6. April 1982 bestätigte die Beklagte dem Kläger unter Bezugnahme auf ihre allgemeinen Geschäftsbedingungen die Einräumung eines Kredits in Höhe von DM 30 000,— mit einer Laufzeit bis 30. April 1983. Eine Übermittlung dieser besonderen Kreditgewährung an die zuständige bayerische Schufa GmbH in München seitens der Beklagten erfolgte zu diesem Zeitpunkt und offensichtlich auch später nicht.

Am 4. August 1982 wurde das Kontokorrentkonto von der Beklagten gekündigt. Da der Kläger bis zu einem gesetzten Termin (18. August 1982) keine Zahlungen leistete, wurden die Kreditbürgen in Anspruch genommen, die Forderung der Beklagten also ausgeglichen.

Im November 1982 richtete die Beklagte an die bayerische Schufa GmbH in München folgende Meldung: „Kreditkündigung DM 27 632,— vom 4. August 1982". Diese Meldung wurde bei der Schufa zur Person des Klägers gespeichert. Nach Speicherung der Daten standen diese und die bereits vorhandenen Daten für Auskünfte an die Anschlußkunden der Schufa zur Verfügung.

Der Kläger bestreitet die Zulässigkeit der Datenübermittlung durch die Beklagte an die Schufa und damit die Zulässigkeit der weiteren Datenverarbeitung, insbesondere der Datenspeicherung und der Datenübermittlung an Dritte durch die bayerische Schufa GmbH in München. Er fühlt sich durch die Datenübermittlung an die Schufa und die Datenverarbeitung bei der Schufa in seinem Grundrecht auf informationelle Selbstbestimmung verletzt.

— Um den Sachverhalt richtig würdigen zu können, ist es notwendig, zunächst einige Ausführungen zum **Schufa-Kredit-Informationssystem** zu machen:

Die Schufa arbeitet inzwischen weitgehend mit Verfahren der automatisierten Datenverarbeitung. So betreiben z. B. die vier norddeutschen Schufa-Gesellschaften Berlin, Bremen, Hamburg und Hannover im Kundenrechenzentrum eines großen Datenverarbeitungsherstellers (Siemens) in Hamburg ein gemeinsames, zentral und einheitlich auch für andere Schufa-Gesellschaften (Düsseldorf, Mannheim, München) entwickeltes automatisiertes Datenverarbeitungsverfahren. Die beteiligten norddeutschen Schufa-Gesellschaften sind über Datenfernübertragungseinrichtungen an das Rechenzentrum in Hamburg angeschlossen, d. h. sie können dort unmittelbar über Leitung auf die in einer Datenbank gespeicherten Daten entsprechend ihrer Zugriffsbefugnis zugreifen, einzelne Daten abfragen, ändern oder löschen. Der Rechner in Hamburg ist mit einem entsprechenden Rechnersystem in Düsseldorf (das die Schufa-Gesellschaften Düsseldorf, Mannheim, München betreiben) gekoppelt, womit ein unmittelbarer Datenaustausch zwischen diesen Rechnern und damit auch zwischen den beteiligten Schufa-Gesellschaften und Schufa-Geschäftsstellen möglich ist.

Für bestimmte große Anschlußkunden der Schufa, z. B. Versandhandelshäuser, wurde die Möglichkeit des sogenannten DATA-Verfahrens für Sammelanfragen entwickelt. Hierbei werden die Anfragen des Schufa-Anschlußkunden per Standleitung oder auf Magnetband dem Rechenzentrum zugeleitet und dort in einem alle Stunden ablaufenden Verarbeitungslauf (nicht im Dialog) weiterverarbeitet. Wenn eine Übereinstimmung zwischen den Identitätsangaben des Schufa-Kunden und denjenigen des Schufa-Datenbestandes besteht, wird die Anfrage des Kunden beantwortet, d. h. er erhält automatisiert ohne weitere Beteiligung der zuständigen Schufa-Gesellschaft bzw. -Geschäftsstelle die ge-

wünschte Auskunft, entweder wieder über Standleitung oder per Magnetband. Wird keine vollständige Personenidentität festgestellt, geht der Fall zur manuellen Weiterverarbeitung an die zuständige Schufa-Gesellschaft bzw. -Geschäftsstelle.

Auch die übrigen Schufa-Gesellschaften und Schufa-Geschäftsstellen setzen ein einheitliches automatisiertes Datenverarbeitungsverfahren ein, jedoch auf Rechnern eines anderen großen Datenverarbeitungsherstellers (IBM). Eine unmittelbare Kopplung der (IBM-)Rechner mit den (Siemens-)Rechnern besteht zur Zeit nach meinen Informationen nicht; technisch wäre sie jedoch ohne weiteres möglich. Allerdings findet zwischen beiden Anwendergruppen ein Datenträgeraustausch (Magnetband) statt, so daß das Schufa-System insgesamt als bundesweites Verbundsystem bezeichnet werden kann.

— Die **Schufa ist eine Gemeinschaftseinrichtung der kreditgebenden Wirtschaft.** Sie verfügt in der Bundesrepublik über insgesamt 13 regionale, rechtlich und wirtschaftlich selbständige Gesellschaften in der Rechtsform der GmbH, die der Bundes-Schufa — Vereinigung der deutschen Schutzgemeinschaften für allgemeine Kreditsicherung e.V. in 6200 Wiesbaden, Kronprinzenstr. 28 — als Koordinierungsgremium angehören. Gesellschafter der regionalen Schufa-Gesellschaften sind Sparkassen, Banken, Volksbanken und Raiffeisenbanken, Teilzahlungsbanken sowie Einzel- und Versandhandelsunternehmen. Die 13 regionalen Schufa-Gesellschaften haben insgesamt 32 Geschäftsstellen im Bundesgebiet eingerichtet. Die Schufa arbeitet mit ähnlichen Organisationen in Österreich und den Niederlanden zusammen; es bestehen Verträge zwischen der Bundsschufa e.V. und den jeweiligen ausländischen Organisationen.

In den Dateien der Schufa-Gesellschaften waren Ende 1985 nach eigenen Angaben die Daten von insgesamt etwa 22 Millionen Personen gespeichert. Die Daten erhält die Schufa zum größten Teil von ihren Vertragspartnern bzw. Anschlußkunden, zu einem Teil aber auch aus öffentlichen Registern, Verzeichnissen (z. B. Schuldnerverzeichnis gem. § 915 ZPO) etc. sowie aus sonstigen Informationsquellen wie z. B. amtlichen Bekanntmachungen in Tageszeitungen bzw. im Bundesanzeiger und von den Betroffenen selbst. Es gab Ende 1985 nach Angaben der Schufa über 30 000 Vertragspartner, d. h. Anschlußkunden der Schufa-Gesellschaften. Neben den Kreditinstituten sind dies vor allem Bausparkassen, Hypothekenbanken, Kreditkartengesellschaften, Leasinggesellschaften, Kaufhäuser- und Ladenketten, Direktvertriebsfirmen, Versandhäuser, Kfz.-Handelsunternehmen, Heimwerkermärkte, Brennstoffhandel, Elektrohandel, Möbelhandel, Textil- und Teppichhandel, Getränkehandel, Versorgungsunternehmen, Handwerksbetriebe. Die Anzahl der Anschlußkunden ist im Berichtsjahr aufgrund der Vereinbarungen mit den Datenschutzaufsichtsbehörden allerdings reduziert worden.

Den Anschlußkunden der Schufa-Gesellschaften werden nach eigenen Angaben der Schufa pro Jahr über 25 Millionen Auskünfte erteilt, von denen ca. 80 Prozent auf die Kreditinstitute entfallen. Die meisten Anfragen gehen telefonisch ein und werden auch so beantwortet. Daneben gibt es schriftliche oder fernschriftliche (Telex, Teletex) Anfragen sowie Anfragen im Rahmen des sogenannten DATA-Verfahrens.

Die Schufa-Gesellschaften speichern Kreditdaten nur bis zur Höhe von DM 50 000,— netto, Daten aus der Führung von Girokonten und Negativdaten ohne Begrenzung nach Betrag und Ursprung, wobei Bagatellbeträge von weniger als DM 100,— nicht gespeichert werden. Kreditdaten über DM 50 000,— werden von der KSV (= Kreditschutzvereinigung GmbH, vgl. Anschrift der Bundes-Schufa) gespeichert und für Auskünfte an ihre Kunden bereitgehalten. Gesellschafter der KSV sind Teilzahlungsbanken. Ihre Arbeitsweise entspricht im wesentlichen derjenigen der Schufa-Gesellschaften. Die KSV hat auch Zugang zu den Dateien der Schufa-Gesellschaften.

— Bei der **datenschutzrechtlichen Würdigung** des vorgetragenen Sachverhalts sind folgende Überlegungen von Bedeutung:

— Das Recht auf informationelle Selbstbestimmung gilt auch im privaten Bereich.

Das Bundesverfassungsgericht hat es für wesentlich angesehen, daß jemand, der nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen der sozialen Umwelt be-

kannt sind und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, in seiner Freiheit wesentlich gehemmt werden kann, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem so verstandenen Recht auf informationelle Selbstbestimmung wäre daher eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der die Bürger nicht mehr wüßten, wer was wann und bei welcher Gelegenheit über sie wisse. Auch der private Bereich gehört zur „sozialen Umwelt" des einzelnen, in der ohne seine Kenntnis Wissen über ihn angesammelt und gegen ihn verwendet werden kann. Als objektive Wertentscheidung der Verfassung ist das Recht auf informationelle Selbstbestimmung daher auch für die Gestaltung und Auslegung der Rechtsbeziehungen zwischen Privaten von erheblicher Bedeutung; es ist nicht nur als Abwehrrecht mit unmittelbarer Wirkung im Verhältnis Bürger—Staat verstehbar.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 27./28. März 1984 zu den Auswirkungen des sogenannten Volkszählungsurteils ebenfalls die Wirksamkeit des Rechts auf informationelle Selbstbestimmung für den nicht-öffentlichen Bereich festgestellt. Das Recht auf informationelle Selbstbestimmung knüpfe an Art. 2 Abs. 1 und Art. 1 Abs. 1 Grundgesetz (GG) an und gelte nicht nur für die Datenverarbeitung der öffentlichen Verwaltung, sondern auch für die Datenverarbeitung nicht-öffentlicher Stellen. Der Gesetzgeber sei aufgerufen, für die Datenverarbeitung privater Stellen ebenfalls die notwendigen Folgerungen aus dem Urteil zu ziehen.

Die Auffassung, daß das informationelle Selbstbestimmungsrecht auch im privaten Bereich gilt, wird jedoch bestritten; das informationelle Selbstbestimmungsrecht gelte nur im Verhältnis Bürger—Staat, nicht jedoch im Verhältnis Bürger—Bürger. Hierbei wird meines Erachtens allerdings verkannt, daß Grundrechte entweder im Wege der Drittwirkung oder bei Schadensersatzansprüchen über sonstige Rechte im Sinne des § 823 II Bürgerliches Gesetzbuch (BGB) Einfluß auf private Verhältnisse nehmen.

Für die Geltung des informationellen Selbstbestimmungsrechts im Verhältnis Kunde—Kreditinstitut spricht die Tatsache, daß es sich bei der Schufa-Klausel nicht um einen zwischen den Beteiligten frei ausgehandelten Vertragsteil handelt, sondern um Konditionen, die bei nahezu allen Kreditinstituten gleich sind. Der Kunde hat gegenüber der Bank faktisch keinen Verhandlungsspielraum. Ähnlich wie im Arbeitsrecht, wo die Lehre von der Drittwirkung der Grundrechte mitentwickelt wurde, ist auch im Verhältnis Kreditinstitut—Kunde von einem besonderen Schutzbedürfnis des Kreditnehmers gegenüber dem wirtschaftlich stärkeren Kreditgeber auszugehen.

— Zur Zulässigkeit der Datenübermittlung an die bayerische Schufa GmbH in München.

Eine wirksame Einwilligung des Betroffenen/Klägers in die Datenübermittlung an die bayerische Schufa GmbH in München und die dortige Weiterverarbeitung der Daten, d. h. ihre Speicherung, Veränderung und Löschung, liegt nicht vor. Zwar hat der Kläger im Kontoeröffnungsantrag 1979 die sogenannte Schufa-Klausel unterschrieben, wegen ihrer unklaren, unbestimmten und einseitig benachteiligenden Ausgestaltung ist sie jedoch unwirksam. Der Bundesgerichtshof hat in seinem Urteil vom 19. September 1985 (III ZR 213/83) eine ähnliche Schufa-Klausel wegen Verstoßes gegen § 9 des Gesetzes zur Regelung des Rechts der allgemeinen Geschäftsbedingungen (AGB-Gesetz) für unwirksam erklärt und dem Kläger/Betroffenen einen Unterlassungsanspruch nach § 13 AGB-Gesetz eingeräumt.

Da eine wirksame Einwilligung des Betroffenen/Klägers zur Übermittlung seiner Daten an die bayerische Schufa GmbH in München nicht vorliegt, muß die erfolgte Datenübermittlung vor dem Hintergrund der einzig erkennbaren gesetzlichen Erlaubnisnorm, nämlich dem § 24 BDSG beurteilt werden. Nicht eingehen will ich auf das Verhältnis des vertraglich eingeräumten Bankgeheimnisses auf der einen Seite und die gesetzlichen Offenbarungsbefugnisse nach § 24 BDSG auf der anderen Seite. Bei meinen Ausführungen gehe ich von der herrschenden Meinung aus, daß die drei in § 24 BDSG genannten Alternativen gleichberechtigt nebeneinander stehen, obwohl ich der Auffassung bin, daß für die Anwendung der dritten Alternative „berechtigte Interessen und schutzwürdige Belange" kein Raum ist, soweit

vertragliche Vereinbarungen vorliegen oder die Parteien ersichtlich vertragliche Vereinbarungen für die Datenverarbeitung beabsichtigt hatten, diese aber aufgrund rechtlicher Beurteilung wirksam nicht zustande gekommen sind.

Geht man mit der herrschenden Meinung davon aus, daß die dritte Alternative des § 24 Abs. 1 BDSG als Auffangtatbestand gilt, stellt sich grundsätzlich die Frage, ob diese allgemeine Regelung noch verfassungskonform für die hier interessierenden Verhältnisse ausgelegt werden kann. Offensichtlich ist die übermittelnde Stelle nicht in der Lage, die schutzwürdigen Belange des Betroffenen ausreichend zu berücksichtigen; darüber hinaus habe ich aus der Praxis die Erfahrung, daß eine Einzelfallabwägung tatsächlich nur in den seltensten Fällen vorgenommen wird.
Bei der Auslegung der schutzwürdigen Belange des Betroffenen/Klägers im Sinn von § 24 BDSG sind auch seine Grundrechte und damit sein Recht auf informationelle Selbstbestimmung zu berücksichtigen. Danach bestehen Zweifel, ob die im November 1982 erfolgte Meldung der Kreditkündigung an die bayerische Schufa GmbH mit § 24 BDSG begründet werden kann. Die Meldung der Kreditkündigung erfolgte, ohne daß die Einräumung des Kredites im April 1982 gemeldet worden war. Außerdem erfolgte sie zu einem Zeitpunkt, als die Forderung der Beklagten bereits ausgeglichen war (ca. 3 Monate später).
Eine unverzügliche Meldung, zu der die Beklagte nach ihrem Anschlußvertrag mit der bayerischen Schufa GmbH verpflichtet gewesen wäre, liegt offensichtlich nicht vor. Daneben könnte ein Verstoß der Beklagten gegen ihren Anschlußvertrag mit der Schufa gegeben sein und daher die erst im November 1982 erfolgte Meldung der Kreditkündigung — da verspätet und ohne Hinweis auf die Erledigung des Kredites — unzulässig sein. Der Anschlußvertrag mit den Regelungen über die Behandlung personenbezogener Kundendaten hat meines Erachtens nicht nur Wirkungen zwischen den Vertragsparteien, sondern entfaltet auch Schutzwirkungen zugunsten der Bankkunden, so daß der Kläger durch das vertragswidrige Verhalten der Bank auch in eigenen Rechten verletzt ist.

— Zur Zulässigkeit der Datenspeicherung, Datenveränderung und Datenübermittlung durch die bayerische Schufa GmbH.

Die Datenspeicherung bei der bayerischen Schufa GmbH ist ohne wirksame Einwilligung des Betroffenen/Klägers nach § 32 Abs. 1 BDSG nur zulässig, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Es ist also nach dieser Gesetzbestimmung erforderlich, daß die bayerische Schufa GmbH prüft, ob schutzwürdige Belange des Betroffenen beeinträchtigt werden. Ob in diesem Fall eine derartige Prüfung bei der bayerischen Schufa GmbH erfolgt ist, läßt sich aus den Sachverhaltsunterlagen nicht entnehmen. Aus meiner Prüfungserfahrung, die durch ähnliche Erfahrungen anderer Datenschutzaufsichtsbehörden bestätigt wird, kann ich sagen, daß auch bei den Schufa-Gesellschaften und -Geschäftsstellen wegen der Massenhaftigkeit der Meldungen schutzwürdige Belange der Betroffenen nicht im einzelnen geprüft werden. Die übermittelten Daten werden in aller Regel ohne derartige Prüfungen in den Datenbestand eingegeben und dabei lediglich auf formale und logische Richtigkeit geprüft. Diese Plausibilitätsprüfung ist aber nicht mit der Prüfung der schutzwürdigen Belange des Betroffenen gleichzusetzen.

Die Meldung der Kreditkündigung ohne eine vorangegangene Meldung der Kreditgewährung dürfte mit großer Wahrscheinlichkeit eine Nachfrage der bayerischen Schufa GmbH bei der Beklagten ausgelöst haben. Hierbei hätten der Schufa die zeitlichen Diskrepanzen und der tatsächliche Ablauf des Geschehens und damit auch der Verstoß gegen den bestehenden Anschlußvertrag auffallen müssen. Aus der Tatsache, daß die Kreditkündigung in den Schufa-Datenbestand eingegeben wurde, läßt sich entnehmen, daß die schutzwürdigen Belange des Betroffenen nur eine untergeordnete, wenn überhaupt eine Rolle gespielt haben. Ohne die vom BDSG geforderte Prüfung der schutzwürdigen Belange ist die Datenspeicherung jedoch nicht zulässig, zumal es sich bei der Meldung „Kreditkündigung" um ein sogenanntes Negativmerkmal handelt und sich für den Betroffenen aus der Weitergabe dieser möglicherweise verkürzten und damit fehlerhaften Information erhebliche Beeinträchtigungen seiner schutzwürdigen Belange ergeben.

Soltle die bayerische Schufa GmbH die gemeldete Kreditkündigung ohne Nachfrage bei der beklagten Bank und damit ohne die vorausgegangene Kreditgewährung und inzwischen erfolgte Tilgung des Kredites gespeichert haben, wären auch in diesem Fall die schutzwürdigen Belange des Betroffenen beeinträchtigt. Die vom BDSG verlangte Prüfung der schutzwürdigen Belange wäre entweder nicht erfolgt oder einseitig zu Lasten des Betroffenen vorgenommen worden. Die Zulässigkeit der Datenspeicherung wäre auch in diesem Fall zu bezweifeln.

Im Ergebnis läßt sich also festhalten, daß erhebliche Zweifel an der Zulässigkeit der Speicherung des Merkmals „Kreditkündigung" bei der bayerischen Schufa GmbH bestehen.

Das Hinzufügen neuer Daten und Informationen zu vorhandenen Daten erfüllt den datenschutzrechtlichen Tatbestand der Datenveränderung. Das Verändern personenbezogener Daten ist nach § 33 BDSG ohne wirksame Einwilligung des Betroffenen nur zulässig, soweit schutzwürdige Belange dadurch nicht beeinträchtigt werden. Auch hier ist also vom Gesetz eine Prüfung der schutzwürdigen Belange des Betroffenen gefordert. Da eine solche Prüfung — wie dargelegt — offenkundig nicht vorgenommen wurde oder nur einseitig zu Lasten des Betroffenen/Klägers, ist auch die Zulässigkeit der erfolgten Datenveränderung zu bezweifeln.

— Zum Widerrufs-, Berichtigungs- und Löschungsverlangen des Betroffenen/Klägers.

Im Datenschutzrecht gibt es kein Widerrufsrecht. Nach § 4 BDSG i. V. m. §§ 26 und 27 bzw. 34 und 35 BDSG stehen dem Betroffenen Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsansprüche gegenüber der beklagten Bank bzw. der bayerischen Schufa GmbH zu. Vor allem die Berichtigungs- und Löschungsansprüche des Betroffenen sind hier von Interesse.

Nach § 27 Abs. 1 bzw. § 35 Abs. 1 BDSG sind personenbezogene Daten von der Beklagten bzw. der bayerischen Schufa GmbH zu berichtigen, wenn sie unrichtig sind. Die Unrichtigkeit muß feststehen; eines Verlangens des Betroffenen bedarf es dann nicht mehr. Die speichernde Stelle muß unverzüglich von sich aus tätig werden. Da die beklagte Bank mit erheblicher Zeitverzögerung eine offenkundig unvollständige und damit auch unrichtige Meldung an die bayerische Schufa GmbH getätigt hat, ist der Berichtigungsanspruch des Betroffenen/Klägers gegeben. Der Betroffene hat in jedem Fall Anspruch auf eine korrekte und vollständige Datenspeicherung — sofern eine solche überhaupt zulässig ist. Die Pflicht zur Datenberichtigung trifft sowohl die beklagte Bank als auch die bayerische Schufa GmbH.
Das Löschungsverlangen des Betroffenen/Klägers richtet sich primär gegen die bayerische Schufa GmbH. Maßgebend hierfür ist § 35 Abs. 3 BDSG. Danach können — zulässig gespeicherte — personenbezogene Daten gelöscht werden, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Derartige Belange sind hier nicht erkennbar. Im Gegenteil: Es ist der erklärte Wille des Klägers, daß das für ihn ungünstige Merkmal „Kreditkündigung" gelöscht wird. Die bayerische Schufa GmbH könnte also die monierten Daten des Betroffenen löschen. Im Hinblick auf die Unvollständigkeit der Schufa-Meldung und die vertragswidrige Verzögerung dieser Meldung sowie die Erledigung des Darlehens ist der Löschungsanspruch des Betroffenen gerechtfertigt. Unzulässig gespeicherte Daten sind gemäß § 35 Abs. 3 Satz 2 BDSG zu löschen. Sollte die Speicherung des Merkmals „Kreditkündigung" auch nach Meinung des Gerichts unzulässig sein, dann wäre dieses Merkmal unverzüglich im Schufa-Datenbestand zu löschen. Das Merkmal ist auf jeden Fall fünf Jahre nach der Einspeicherung zu löschen, wenn der Betroffene es verlangt. Ein solches Verlangen liegt hier vor, die Schufa hat in ihrem Vertragswerk eine dreijährige (statt fünfjährige) Löschungsfrist; sie löscht erledigte Daten drei Jahre nach Eingabe des Erledigungsvermerks. Diese Dreijahresfrist war 1986 erfüllt. Das Merkmal „Kreditkündigung" und alle damit zusammenhängenden Daten waren, soweit keine weiteren Datenspeicherungen zur Person nach diesem Vorgang erfolgt sind, spätestens Anfang 1986 zu löschen.

— Zur Sicherung des Rechts auf informationelle Selbstbestimmung bei Auskunftssystemen der Kreditwirtschaft reichen die Vorschriften des Bundesdatenschutz-

gesetzes nicht aus. Notwendig sind vielmehr **bereichsspezifische Regelungen,** die den technischen Ausbaustand und die Entwicklungsmöglichkeiten der bestehenden Systeme berücksichtigen. Im Bereich der Kreditvergabe werden — wie übrigens auch in vielen anderen gesellschaftlichen Bereichen — Entscheidungen in zunehmendem Maße mit Hilfe computergestützter Informationssysteme gefällt. Diese Systeme werden von den Benutzern häufig als einzige „Quelle der Wahrheit" angesehen, auch wenn sie nur unvollständige Angaben enthalten, die möglicherweise zu falschen Schlüssen führen. Die Konsequenzen können für den Betroffenen existenzbedrohend werden. Unbestritten kommt Informationssystemen, wie dem der Schufa, überragende Bedeutung für einen ordnungsgemäßen Wirtschaftsablauf zu. Bereichsspezifische gesetzliche Regelungen müssen zwischen den Informationsbedürfnissen der Kreditgeber und dem informationellen Selbstbestimmungsrecht der Kreditnehmer einen gerechten Ausgleich schaffen.

Ich vertrete die Meinung, daß ein lückenloser Datenschutz hergestellt werden muß, der die Datenverarbeitungsvorgänge für den Bürger verständlich und transparent macht. Dies ist die Voraussetzung dafür, daß der Bürger die ihm in der Privatautonomie zustehenden Entscheidungen über Form und Umfang der Verarbeitung seiner Daten auch tatsächlich vornimmt. Hierzu zählt nicht nur, die Informationsbeziehungen zu beschränken, transparent zu machen und dem Bürger umfangreiche Auskunftsrechte zu gewähren, sondern auch, die Möglichkeiten der Aufsichtsbehörde zu erweitern und nicht — wie das Bundesdatenschutzgesetz (BDSG) derzeit in einem Anwendungsbereich regelt — daran zu binden, daß ein betroffener Bürger begründet darlegen muß, daß er bei der Verarbeitung seiner Daten in seinen Rechten verletzt worden ist. Gerade dieser Nachweis ist von den Betroffenen angesichts des vielschichtigen Beziehungsgeflechts verschiedener Informationssysteme und den mannigfaltigen Auswertungsmöglichkeiten der gespeicherten Daten selten möglich.

Um den Ansprüchen gerechter zu werden, ist es seitens des Gesetzgebers erforderlich, nicht nur die Regelungen im 3. und 4. Abschnitt des BDSG um einige allgemeine Komponenten zu ergänzen und zu erweitern, sondern es bedarf daneben spezifischer Regelungen, die die Rechte und Pflichten auch der Kredit- und Wirtschaftsauskunfteien näher beschreiben. Aus der Praxis ist jedenfalls eine immer größer werdende Verflechtung der verschiedenen Auskunftsbeziehungen sowie ein Zusammenwachsen des Adreßhandels, der Kredit- und Wirtschaftsauskunfteien und des Inkassowesens festzustellen, was zu einer immer tieferen Abbildung der Betroffenen führt. Die geltenden Datenschutzbestimmungen für diesen Bereich sind nicht ausreichend, um solchen Tendenzen wirkungsvoll zu begegnen.

6.3 Datenschutz im Versand- und Einzelhandel

6.3.1 Kein Datenschutzgespräch mit dem Versandhandel

Die grundsätzlichen datenschutzrechtlichen Fragestellungen konnten wiederum nicht mit den zuständigen Stellen des Versandhandels erörtert werden. Die seit mehreren Jahren von den Obersten Aufsichtsbehörden getragene gemeinsame Initiative, mit dem Bundesverband des Deutschen Versandhandels ins Gespräch zu kommen, ist von dieser Seite weiter auf Ablehnung gestoßen.

Zu erörtern wären etwa Fragen der Datenverarbeitung beim Versandhandel im Zusammenhang mit Schufa-Anfragen (z. B. Schufa-Anfragen über Mitbesteller oder über Ehegatten bei Erstbestellern und Sammelbestellern), Fragen, wie dem Bürger die Informationsbeziehungen und Informationsflüsse beim Versandhandelsunternehmen transparenter gemacht werden können, wie auch Fragen der Direktwerbung durch den Versandhandel.

Das Gespräch über mehr Transparenz bei der Datenverarbeitung des Versandhandels wurde vom Bundesverband des Deutschen Versandhandels mit folgenden Begründungen abgelehnt:

— Von Transparenz stehe nichts im Bundesdatenschutzgesetz.

— Das Volkszählungsurteil des Bundesverfassungsgerichts handele davon ebensowenig und schon gar nicht mit Bezug auf den privaten Bereich.

— Von dem BGH-Urteil zur Schufa-Klausel der Banken schließlich sei der Versandhandel schon von vornherein nicht betroffen.

Die sich nunmehr über Jahre hinziehende Gesprächsunwilligkeit des Versandhandels macht einmal mehr deutlich, daß der Bundesgesetzgeber dringend die Stellung der Aufsichtsbehörden verbessern muß, wenn überhaupt erreicht werden soll, daß in diesem Bereich Datenschutzregelungen Eingang finden sollen.

Solange aber von der Anlaßaufsicht nicht abgerückt wird und den Aufsichtsbehörden in krassen Fällen keine Anordnungs- und Untersagungsbefugnisse eingeräumt werden, bleibt es dabei, daß die Aufsichtsbehörden jeweils nur im begründeten Einzelfall kontrollieren können und der Gesetzgeber es schließlich dem einzelnen Bürger überläßt, im Klageweg seine Rechte geltend zu machen.

Solange daher von den Aufsichtsbehörden nicht eine allgemeine Anpassung der Datenverarbeitung an die gesetzlichen Regelungen gefordert werden kann, verbleibt es bei der verwaltungsaufwendigen Einzelfallprüfung, vielleicht noch verbunden mit einer Vielzahl von nachfolgenden gerichtlichen Auseinandersetzungen seitens der Betroffenen, da die Aufsichtsbehörden gegenüber datenverarbeitenden Firmen ja keine Durchsetzungsbefugnis haben.

6.3.2 Anzeige der Bankleitzahl und Kontonummer an der Kasse bei Zahlung mit Scheck

Einige größere Kaufhäuser in Bremen verwenden Kassen, bei denen der Kunde lediglich einen unterschriebenen Blankoscheck dem/derKassierer/in überreichen muß. Die noch fehlenden Angaben werden von der Kasse auf den Scheck gedruckt. Mehrere Kunden solcher Kaufhäuser haben sich an mich gewandt und um datenschutzrechtliche Prüfung gebeten, weil sie verunsichert waren, als an der Kasse die Bankleitzahl und die Kontonummer im Display erschienen.

Ich hatte daher die Unternehmen um datenschutzrechtliche Stellungnahme gebeten, die folgendes Bild ergeben hat:

Sofern ein Kunde mit Scheck zahlen möchte, erfaßt der/die Kassierer/in die Kontonummer und Bankleitzahl des Kunden. Die Angaben werden auf dem Protokolldrucker in der Kasse angedruckt und an der Kundenanzeige optisch dargestellt.

Das Andrucken auf dem Protokolldrucker diene dazu, bei Verlust, z. B. Raub von Schecks, gegenüber den Versicherungen einen Nachweis über die entstandene Schadenshöhe zu führen.

Die Kundenanzeige sei dafür vorgesehen, daß der Kunde verfolgen könne, was der/die Kassierer/in gerade mache. Im Bildschirm werde auch der Kaufbetrag und das Rückgeld für den Kunden sichtbar gemacht. Die Kontonummer und die Bankleitzahl werde angezeigt, damit der Kunde die eingegebenen Angaben visuell überprüfen könne.

Da ich nicht ausschließen kann, daß der Kunde erheblich verunsichert würde, wenn bei der Abrechnung unkontrollierbare Informationen eingegeben würden, habe ich eine Unterdrückung der Anzeige nicht gefordert. Das Sichtbarmachen von Kontonummer und Bankleitzahl bei mit Scheck bezahlenden Kaufhauskunden an den Registrierkassen habe ich daher als Problem der Datensicherheit gem. § 6 Bundesdatenschutzgesetz (BDSG) angesehen und den betroffenen Firmen empfohlen, die Kassen bzw. den Bildschirm nach Möglichkeit so anzuordnen, daß Dritte von diesen Daten keine Kenntnis erlangen können.

6.4 Prüfung einer großen Handelsauskunftei

Auch in diesem Berichtsjahr erhielt ich wieder eine Vielzahl von Anfragen und Eingaben zur Datenerhebung und Datenverarbeitung der Auskunfteien. Die Fragen und Probleme sind fast immer die gleichen — seit Jahren schon. In meinem letzten Jahresbericht habe ich unter Pkt. 6.4, S. 70 ff., ausführlich über einige dieser Fragen und Probleme berichtet.

Im Berichtsjahr habe ich bei einer großen Wirtschaftsauskunftei eine Datenschutzprüfung gemäß § 40 Bundesdatenschutzgesetz (BDSG) durchgeführt. Hierbei standen nicht einzelne Bürgereingaben und Beschwerden im Vordergrund, sondern grundsätzliche Datenschutzfragen. Die Auskunftei ist als eingetragener Verein mit einer Kommanditgesellschaft als Betriebsgesellschaft organisiert; sie gehört mit 108 anderen, ähnlich organisierten Vereinen einem Verband an, der ebenfalls als eingetragener Verein organisiert ist. Nach außen treten die Vereine und der Verband unter einer einheitlichen Bezeichnung auf, so daß der Eindruck einer bundesweit einheitlichen Organisation entsteht.

Die Auskunftei hat ihre Tätigkeit, insbesondere ihre Auskunftstätigkeit und die von ihr ebenfalls betriebene Inkassotätigkeit automatisiert, d. h. sie verfügt über eine DV-Anlage mit entsprechender bundeseinheitlicher Software, mit deren Hilfe der Auskunftsdatenbestand und der Inkassobestand verarbeitet werden. Die Prüfung dieses DV-Verfahrens warf einige grundsätzliche Datenschutzfragen auf.

— Monatliche Übersendung von Sicherungskopien an das zentrale Verbandsrechenzentrum

Einmal pro Monat wird von der örtlichen Auskunftei eine sogenannte Sicherungskopie des gesamten Datenbestandes, d. h. der Auskunftsdaten und der Inkassodaten auf Magnetband abgezogen und dieses Band dem zentralen Verbandsrechenzentrum zur weiteren Verarbeitung übersandt. Im Verbandsrechenzentrum wird diese „Sicherungskopie" zur Aktualisierung der hier vorhandenen Datenbank verwendet. Da alle Verbandsmitglieder monatlich eine derartige „Sicherungskopie" übersenden, verfügt der Verband in seiner Datenbank über ein vollständiges und relativ aktuelles Duplikat der örtlichen Datenbestände aller Verbandsmitglieder. Die Übersendung der monatlichen „Sicherungskopien" an das Verbandsrechenzentrum hat nach meiner Auffassung entgegen der Auffassung der Beteiligten weniger etwas mit Datensicherung als vielmehr mit der Aktualisierung der Datenbank beim Verband zu tun. Die Einlassungen der Auskunftei und des Verbandes an dieser Stelle halte ich vor dem Hintergrund der praktizierten Datenbankanwendung im Verbandsrechenzentrum nicht für überzeugend. Auch die Darlegung, daß es sich bei der Datenverarbeitung des Verbandes um Auftragsdatenverarbeitung gemäß § 37 BDSG handelt, der Verband also nur entsprechend den Weisungen der Auskunfteien handelt, konnte bei der Prüfung nicht nachvollzogen werden. Konkrete schriftliche oder mündliche Weisungen für die einzelnen Datenverarbeitungs-Arbeitsgänge im Verbandsrechenzentrum werden von den örtlichen Auskunfteien nicht erteilt. Es liegt ein allgemeiner Beschluß der Verbandsmitglieder vor, der

— die Übermittlung einer monatlichen Sicherungsgeneration der Auskunftsdaten und

— die Nutzung bzw. Verwendung der übermittelten Daten durch den Verband

betrifft. Dieser Beschluß ist jedoch so allgemein und offen, daß von einer weisungsgebundenen Auftragsdatenverarbeitung des Verbandes unter voller Verantwortung der auftraggebenden einzelnen Auskunftei nicht gesprochen werden kann. Der Beschluß der Verbandsmitglieder formuliert denn auch:

„Wegen der Vielzahl der technischen Möglichkeiten, die die EDV bei der Auswertung der Archive ... bietet, ist eine abschließende Aufzählung aller denkbaren Verfahren unmöglich."

Es bleibt also festzuhalten, daß der Verband ohne konkrete schriftliche oder mündliche Weisungen im Rahmen eines allgemeinen und sehr weitgehenden Verbandstagsbeschlusses seine Datenverarbeitung betreibt. Nicht die einzelne auftraggebende Auskunftei steuert die Datenverarbeitung beim Verband, sondern es drängt sich der Eindruck auf, daß der Verband selbst die neuen Nutzungs- und Verwendungsmöglichkeiten des gespeicherten Datenmaterials findet. Die für die Zulässigkeit der Datenverarbeitung verantwortliche einzelne Auskunftei kann ihre datenschutzrechtlichen Pflichten — wenn überhaupt — nur unzulänglich erfüllen.

— On-line-Abfragesystem

Die geprüfte Auskunftei stellt ihre Daten Dritten selbst nicht im Rahmen eines solchen Abfragesystems zur Verfügung. On-line-Zugriffsprozeduren hat jedoch das Verbandsrechenzentrum entwickelt. Nach Angaben des Verbandes sind derzeit etwa 40 Mitglieder der örtlich als Vereine organisierten Auskunfteien an das On-line-Abfragesystem des Verbandsrechenzentrums angeschlossen. Sie können also selbst im Wege der Selbstbedienung Daten abrufen. Auch diese Anwendung erfolgt auf der Basis eines allgemeinen Beschlusses der Verbandsmitglieder, der sich allerdings mehr mit der Verrechnung der anfallenden Erlöse als mit der Regelung systemtechnischer Details und der konkreten Beauftragung durch die Verbandsmitglieder beschäftigt. Im Rahmen dieses On-line-Abfragesystems werden die in der Datenbank des Verbandsrechenzentrums vorhandenen Daten den an das System angeschlossenen Teilnehmern zur selbständigen Abfrage und Nutzung zur Verfügung gestellt. Die vom Bundesdatenschutzgesetz in § 32 Abs. 2 verlangte vorherige Darlegung

und Prüfung des berechtigten Interesses an einer Datenübermittlung erfolgt nicht. Die örtliche Auskunftei, in deren Auftrag und nach deren Weisung diese regelmäßige Datenübermittlung angeblich erfolgt, erfährt erst im nachhinein von Zugriffen auf ihre Daten. Über Telex wird ihr nämlich ein bis zwei Tage später mitgeteilt, wer wann auf welchen Datensatz mit welchem Grund zugegriffen hat.

Die bisher vorgetragene Argumentation reicht nicht aus, um die Vereinbarkeit mit dem geltenden Datenschutzrecht festzustellen.

In diesem Zusammenhang ist noch auf ein weiteres Problem hinzuweisen. Nach dem geltenden Datenschutzrecht (§ 34 Abs. 2 BDSG) hat ein Betroffener einen Auskunftsanspruch über die zu seiner Person gespeicherten Daten. „Werden Daten automatisch verarbeitet, kann der Betroffene Auskunft auch über die Personen und Stellen verlangen, an die seine Daten regelmäßig übermittelt werden." Die Auskunftserteilung an die Betroffenen müßte als nach dieser Gesetzesbestimmung auch die Teilnehmer am On-line-Abfragesystem umfassen, da dieses Abfragesystem den Tatbestand der regelmäßigen Datenübermittlung erfüllt. Die tatsächlich erteilten Auskünfte an die Betroffenen enthalten diese Angaben jedoch nicht. Begründet wird dieses damit, daß die Regelmäßigkeit der Datenübermittlung sich auf den Betroffenen beziehen muß und das Bereithalten zum Abruf allein nicht zur Begründung des erweiterten Auskunftsanspruchs ausreicht. Ich teile diese Rechtsauffassung nicht.

— GENIOS-Wirtschaftsdatenbank

Nach einem Beschluß der Mitglieder des Verbandes, d. h. der Auskunfteien, wurde der Verband beauftragt, Verhandlungen mit Anbietern bzw. Betreibern von Wirtschaftsdatenbanken zu führen mit dem Ziel, die in der Datenbank des Verbandszentrums gespeicherten Daten anderen Wirtschaftsdatenbanken zur Nutzung anzubieten. In Verfolgung dieses Beschlusses hat der Verband im Jahre 1985 einen Vertrag mit dem Düsseldorfer Verlagshaus abgeschlossen, wonach er seine Datenbank in den Datenpool der GENIOS-Wirtschaftsdatenbank einbringt und damit Dritten zur Nutzung überläßt. Die Wirtschaftsdatenbank GENIOS wird von einem großen Verlagshaus in Düsseldorf betrieben. Sie bietet ihren Nutzern einen direkten Zugriff auf verschiedene in einem Datenpool der Wirtschaftsdatenbank gespeicherte Datenbestände. Alle zwei Monate übermittelt der Verband seither der GENIOS-Wirtschaftsdatenbank ein neues Datenband.

Auch diese Datenverwendung wird seitens der Auskunftei bzw. seitens ihres Verbandes mit dem datenschutzrechtlichen Institut der Auftragsdatenverarbeitung begründet, bei dem die einzelne Auskunftei angeblich Herr der Daten bleibt und jeder Verarbeitungsschritt nach ihren Weisungen und unter ihrer vollen Verantwortung abläuft. Dies ist nach meinen bisherigen Feststellungen jedoch eine reine Fiktion, denn weder das Verlagshaus noch die GENIOS-Wirtschaftsdatenbank haben sich bisher bei der zuständigen Datenschutzaufsichtsbehörde zum Register nach § 39 BDSG angemeldet. Uber die Zugriffe auf die in der GENIOS-Wirtschaftsdatenbank gespeicherten Daten erhält die einzelne Auskunftei, die doch Herr der Daten sein soll, noch nicht einmal nachträglich irgendeine Information. Das spricht dafür, daß hier der Tatbestand einer unzulässigen Datenübermittlung vorliegt.

— Bonitätsgeprüfte Adressen

Die Auskunftei bietet ihren Mitgliedern und Kunden auch die Selektion von bonitätsgeprüften Marketing-Adressen und von Negativ-Merkmalen an. Nach bestimmten, vom Kunden vorgegebenen Kriterien wie z. B. Branche, Rechtsform, Postleitzahlbereich, Umsatzgröße, Zahlungsverhalten, Bonitätsklasse etc. können aus dem zentralen Datenbestand im Verbandsrechenzentrum Adressen selektiert und über Drucker (Liste, Adreßaufkleber) oder auf Magnetband bzw. Diskette ausgegeben werden. Im Rahmen dieses Verfahrens ist es auch möglich, die eigenen Kundendaten oder einen angemieteten Adreßdatenbestand am Datenbestand der Auskunfteien vorbeizuführen und nach speziellen Kriterien wie z. B. Bonität, Zahlungsverhalten zu selektieren (sogenannter Waschabgleich). Auch diese Verarbeitungspraxis wird seitens der Auskunfteien und seitens des Verbandes mit einem Verbandstagsbeschluß und mit dem datenschutzrechtlichen Institut Auftragsdatenverarbeitung begründet. Diese Begründung halte ich ebenfalls nicht für haltbar. Die jeweils beteiligten Auskunfteien erfahren auch hierbei erst im Nachhinein von der erfolgten Datenübermittlung.

Eine vorherige Prüfung des berechtigten Interesses der Kunden an den einzelnen Daten durch die örtliche Auskunftei ist weder vorgesehen noch möglich. Nach Auffassung aller Datenschutzaufsichtsbehörden ist die Nutzung der für Auskunfteizwecke gespeicherten Daten für beliebige andere Zwecke und ohne vorherige Prüfung des berechtigten Interesses an der Übermittlung der einzelnen Daten höchst problematisch.

Die noch nicht abgeschlossene juristische Bewertung der festgestellten Sachverhalte wird noch vorgenommen und mit der geprüften Auskunftei abschließend erörtert.

6.5 Versicherungswirtschaft

6.5.1 Schweigepflichtentbindungsklausel

Im letzten Jahresbericht habe ich unter Pkt. 6.5.2, S. 73 dargestellt, daß die Vertreter der Aufsichtsbehörden für den Datenschutz in den Ländern in Gesprächen mit der Versicherungswirtschaft erreichen wollen, daß die Schweigepflichtentbindungsklausel auf ein erforderliches Maß eingeschränkt wird. Die bisherige Klausel ermächtigt insbesondere Ärzte und Behörden zu einer für den Betroffenen unüberschaubaren Menge von Auskünften gegenüber den Versicherungsunternehmen. Im Berichtszeitraum haben sich die Vertreter der Datenschutzaufsichtsbehörden darauf verständigt, daß die von ihnen eingerichtete Arbeitsgruppe „Versicherungswirtschaft" mit Vertretern der Versicherungswirtschaft ein weiteres Gespräch unter Beteiligung des Bundesaufsichtsamtes für das Versicherungswesen führen soll.

In den Gesprächen haben die Vertreter der Versicherungswirtschaft erneut die Notwendigkeit der Schweigepflichtentbindungsklausel herausgestellt. Insbesondere bei einer Lebensversicherung sei zu berücksichtigen, daß im Todesfalle eine Einwilligung des Betroffenen nicht mehr möglich sei. Ohne eine umfassende Schweigepflichtentbindungsklausel könnten die Lebensversicherungen nicht mehr die erforderlichen Auskünfte von den Behörden hinsichtlich der Todesursache erhalten. Im übrigen hätten sich die Anfragen gegenüber den Sozialversicherungsträgern erheblich verringert, so daß ein akuter Regelungsbedarf zum gegenwärtigen Zeitpunkt nicht bestünde. Hinsichtlich der von den Datenschutzaufsichtsbehörden ausgesprochenen Empfehlung, die Schweigepflichtentbindung erst im Schadensfalle und die Zukunftswirkung auf Unfälle mit Todesfolge zu beschränken, haben die Vertreter der Versicherungswirtschaft nicht aufgreifen wollen.

Die Gespräche mit den Vertretern der Versicherungswirtschaft und dem Bundesaufsichtsamt für das Versicherungswesen werden fortgesetzt.

6.5.2 Datenverarbeitungs-Ermächtigungsklausel

Im Rahmen der Gespräche zwischen den Datenschutzaufsichtsbehörden, der Versicherungswirtschaft und dem Bundesaufsichtsamt für das Versicherungswesen sind auch Umfang und Formulierung der Ermächtigungsklausel zur Datenübermittlung an zentrale Dateien der Versicherungswirtschaft erörtert worden, denn die bereits acht Jahre alte Klausel muß entsprechend den Anforderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts sowie dem Urteil des Bundesgerichtshofes zur Gültigkeit von Einwilligungserklärungen (Schufa-Entscheidung) neu formuliert werden.
Die Unterzeichnung der Klausel wird den Versicherungsnehmern abverlangt, damit die Versicherungsunternehmen etwaige Sonderwagnisse (Lebensversicherer) oder Vertragskündigungen (Rechtsschutzversicherer) prüfen können. Die Klausel ermächtigt zur Datenübermittlung und damit Prüfung im Rahmen eines beantragten Versicherungsvertrages. Eine darüber hinausgehende Datenübermittlung an zentrale Dateien im Falle des Nichtzustandekommens eines Versicherungsvertrages sowie Übermittlungen bei später beantragten Versicherungsverträgen wird von dieser Ermächtigungsklausel nicht abgedeckt. Soweit an einer Datenübermittlung bei Nichtabschluß eines Vertrages festgehalten werden soll, bedarf es einer entsprechenden Neuformulierung der Ermächtigungsklausel. Im Falle später beantragter Versicherungsverträge halten es die Datenschutzaufsichtsbehörden für erforderlich, für jeden Fall der Anbahnung eines Versicherungsvertrages eine Ermächtigungsklausel unterzeichnen zu lassen.

Die Vertreter der Versicherungswirtschaft haben sich bereit erklärt, eine transparente Ermächtigungsklausel zu formulieren, die auch eine Regelung über den Umgang mit Daten für den Fall des Nichtzustandekommens eines Vertragsabschlusses enthalten soll.

Die Angelegenheit bedarf einer weiteren Erörterung.

6.5.3 Verwendung von Match-Codes in der Rechtsschutzversicherung

Der Verband der Haftpflichtversicherer, Unfallversicherer, Autoversicherer und Rechtsschutzversicherer e.V. (HUK-Verband) beabsichtigt, in der zentralen Registrierstelle Rechtsschutz aus den ihm gemeldeten Daten sogenannte Match-Codes zu erstellen. Der Match-Code wird wie folgt gebildet:

— die ersten fünf Buchstaben des Nachnamens

— die ersten drei Buchstaben des Ortsnamens

— die ersten zwei Buchstaben der Straße

— Angaben zum meldenden Unternehmen (VU-Nummer und Versicherungsschein bzw. Schadennummer)

Die zu diesem Zweck an den HUK-Verband übermittelten Datensätze sollen 4 Wochen nach Erstellung dieser Match-Codes vernichtet werden. Der HUK-Verband führt dann nur noch Match-Code-Dateien. Im Rahmen der Bearbeitung eines Versicherungsantrages wird aus den personenbezogenen Daten des angehenden Versicherungsnehmers der Match-Code erstellt und bei der zentralen Registrierstelle Rechtsschutz abgeglichen, um eventuelle Risiken und Wagnisse festzustellen.

Sinn und Zweck des Aufbaus dieser Match-Code-Dateien ergeben sich aus § 19 Abs. 2 der Allgemeinen Bedingungen über die Rechtsschutzversicherungen (ARB). Danach ist die Rechtsschutzversicherung berechtigt, einen Versicherungsvertrag bei zweimaliger Inanspruchnahme innerhalb eines Jahres zu kündigen. Die Meldung erfolgt nach Kündigung, in der Regel wegen „übergebührmäßiger Inanspruchnahme der Versicherung durch den Versicherungsnehmer, unabhängig von einer Prüfung der Gründe der Inanspruchnahme" (vgl. 6. Jahresbericht unter Pkt. 6.1.2, S. 59 unten ff.).

Die Versicherungswirtschaft vertrat zunächst die Auffassung, eine Match-Code-Datei stelle eine anonymisierte Datensammlung dar, die nicht den Bestimmungen des Bundesdatenschutzgesetzes unterliegt. Die Datenschutzaufsichtsbehörden haben aber klargestellt, daß bei diesem Verfahren tatsächlich keine Anonymisierung im Sinne des Bundesdatenschutzgesetzes stattfindet. Bei dem Antrag eines Betroffenen auf Abschluß eines Versicherungsvertrages wird aus seinen personenbezogenen Daten ein Match-Code erstellt und mit der bestehenden Match-Code-Datei abgeglichen. In einem solchen Falle besteht die Möglichkeit, einen bereits vorhandenen Match-Code zu deanonymisieren. Aufgabe ist es ja gerade, bei einem Neuantrag möglicherweise von anderen Unternehmen abgelehnte oder gekündigte Kunden zu reidentifizieren, auch wenn die Zusammensetzung des Match-Codes nicht immer ausreicht, um im Falle eines Auskunftsersuchens Dritter die notwendige eindeutige Zuordnung zu ermöglichen. Allein schon aus diesem Grunde unterliegt eine solche Match-Code-Datei sehr wohl den Datenschutzbestimmungen.

Ein Problem des von dem HUK-Verband gewählten Match-Codes liegt darin, daß in vielen Fällen bereits mit dem normalen Telefon- oder Adreßbuch eine Deanonymisierung möglich ist. Die Datenschutzaufsichtsbehörden werden daher nach Ablauf einer Probephase mit dem HUK-Verband in Verbindung treten und erörtern, ob der Match-Code verbessert werden muß, um sicherzustellen, daß einerseits die übermittelten Daten tatsächlich weitestgehend anonymisiert werden und andererseits gesicherte Auskünfte erteilt werden können und deutlich machen, daß bei Auskunftsersuchen Betroffener Auskunftspflicht besteht, wenn aufgrund der von diesem mitgeteilten Angaben eine Deanonymisierung möglich ist und folglich eine Zuordnung der gespeicherten Daten zur Person des Betroffenen erfolgen kann.

Die Übermittlung von Daten an die zentrale Registrierstelle Rechtsschutz bleibt aus datenschutzrechtlicher Sicht nach wie vor bedenklich, da entsprechend den vom Bundesgerichtshof zur Wirksamkeit der Schufa-Klausel aufgestellten Grundsätzen die bisher verwendete Ermächtigungsklausel unwirksam sein dürfte. Es bedarf daher einer neuen Klausel, die dem Kunden die erforderliche Transparenz in das von den Versicherungen praktizierte Verfahren bietet. Dazu gehört auch die ausdrückliche Einwilligung des Kunden, daß die Versicherung auch bei Ablehnung eines Versicherungsvertrages seine personenbezogenen Daten an die zentrale Registrierstelle meldet und daraus den Match-Code erstellt (vgl. meine vorstehenden Ausführungen zur DV-Ermächtigungsklausel).

Da davon auszugehen ist, daß andere Versicherungssparten entsprechende Verfahren entwickeln werden, erhält diese Problematik eine zunehmende Bedeutung.

Ich werde über die weiteren Beratungen berichten.

6.6 Mieterdatenschutz

6.6.1 Datenübermittlung durch Wohnungsvermittler

Ein Betroffener wandte sich dagegen, daß ein Wohnungsvermittler die zum Zwecke der Wohnungsvermittlung angegebenen Daten an seinen ehemaligen Vermieter übermittelt habe.

Eine Prüfung in den Geschäftsräumen und eine Befragung des Wohnungsvermittlers haben keinen nachweisbaren Anhaltspunkt ergeben, daß hier eine Datenübermittlung an Dritte vorgenommen worden ist.

Des weiteren habe ich festgestellt, daß die dort beschäftigten Personen — soweit sie mit der Datenverarbeitung betraut sind — nicht auf das Datengeheimnis verpflichtet waren. Ich habe daher den Wohnungsvermittler gebeten, eine von mir vorformulierte Verpflichtungserklärung seinen Beschäftigten zur Unterschrift vorzulegen.

Im übrigen lagen keine Erklärungen vor, daß die Kunden in die Übermittlung ihrer personenbezogenen Daten eingewilligt haben. Nach § 3 Satz 2 Bundesdatenschutzgesetz (BDSG) bedarf die Einwilligung grundsätzlich der Schriftform. Ich habe daher dem Wohnungsvermittler empfohlen, seine Kunden auf diese Möglichkeit hinzuweisen und eine entsprechende schriftliche Einwilligung einzuholen. Dafür genügt ein zusätzlicher Vermerk auf der Rückseite der vom Wohnungsvermittler benutzten Karteikarten, den der Kunde dann unterschreibt.

Außerdem habe ich angeregt, zur Vermeidung eventueller Pannen die nicht mehr erforderlichen Karteikarten nicht in den Mülleimer zu werfen, sondern sie direkt bei der Müllverbrennungsanlage zur Vernichtung abzuliefern. Die Vernichtung der Karteikarten sollte in einem angemessenen Zeitraum nach vollständiger Zahlung der Maklercourtage, im übrigen nach Ablauf der jeweils nach dem Bürgerlichen Gesetzbuch (BGB) geltenden Verjährungsfristen erfolgen.

6.6.2 Bekanntgabe von Wasserverbrauchsdaten bei Wohnungseigentum

Nach wie vor erreichen mich Anfragen, die die Bekanntgabe von Abrechnungsdaten gegenüber den anderen Miteigentümern behandeln. In einem Fall beklagte sich ein Betroffener darüber, daß die Hausverwaltung ihm gegenüber die Bekanntgabe von Wasserverbrauchsdaten der anderen Miteigentümer unter Bezug auf den Datenschutz verwehrt habe.

Wie in meinem 8. Jahresbericht unter Pkt. 6.10.6, S. 79 f. dargelegt, ist die Übermittlung solcher Daten nach § 24 Abs. 1 Bundesdatenschutzgesetz (BDSG) nur insoweit zulässig, als es zur Wahrung der Interessen der Miteigentümer erforderlich ist und dabei schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden. Demnach ist zu prüfen, inwieweit die Interessen der Miteigentümer, die Ordnungsmäßigkeit der Verwaltung prüfen zu können und sich vor wirtschaftlichem Schaden zu schützen, den schutzwürdigen Belangen des Betroffenen, seine personenbezogenen Daten nicht den Miteigentümern zugänglich zu machen, vorgehen.

Ich gehe davon aus, daß Hausverwaltungen bei der Vorlage der Verbrauchsabrechnungen die schutzwürdigen Belange der anderen Miteigentümer berücksichtigen.

6.6.3 Datenübermittlung an Kleingärtnervereine

In einer Eingabe wurde moniert, daß der Landesverband der Gartenfreunde Bremen e.V. bei der Neuanlage von Kleingärten sogenannte Pachtvorverträge mit Kleingarteninteressenten abschließt und deren Anschriften an bereits bestehende Kleingartenvereine weiterleitet. Soweit ein Kleingärtnerverein noch zu gründen ist, wurden die Daten dieser Interessenten an Kleingärtner weitergeleitet, die an einer Vereinsgründung interessiert sind.

Obwohl der Landesverband die betreffenden Personen vor dem Abschluß der Vorverträge über diese Verfahrensweise informiert, habe ich den Verband gebeten, eine Beschreibung der Datenübermittlung zwischen dem Landesverband und den Kleingärtnervereinen in den Pachtvertrag bzw. -vorvertrag aufzunehmen und insoweit eine Einwilligung des Betroffenen zu erhalten.

6.7 Arbeitnehmerdatenschutz

6.7.1 Bekanntgabe von Abmahnungen einzelner Arbeitnehmer durch den Arbeitgeber gegenüber dem Betriebsrat

In einer Anfrage ging es darum, ob der Arbeitgeber verpflichtet ist, Abmahnungen gegenüber einzelnen Arbeitnehmern ohne deren Zustimmung dem Betriebsrat zur Kenntnis zu geben.

Die Bekanntgabe von Abmahnungen gegenüber dem Betriebsrat richtet sich nach § 83 Abs. 1 Betriebsverfassungsgesetz (BetrVG). Nach dem materiellen Personalaktenbegriff sind Abmahnungen Teile der Personalakte. Nach herrschender Rechtsprechung wird dem Betriebsrat aus Gründen des Persönlichkeitsschutzes kein eigenständiger und jederzeitiger Anspruch auf Einsicht in die Personalakte gewährt und deshalb auch die generelle Vorlage von Abmahnungsschreiben nicht zugestanden. Etwas anderes könnte im Einzelfall nur gelten, wenn Informationen aus der Personalakte zur Erfüllung der Betriebsratsarbeit unumgänglich notwendig wären oder durch die Vorgänge Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 1 BetrVG berührt würden.

6.7.2 Datenübermittlung zwischen zwei Arbeitgebern

Ein Arbeitgeber hat personenbezogene Daten (Urlaubsdaten) eines Mitarbeiters an einen anderen Arbeitgeber weitergeleitet, nachdem der Beschäftigte dorthin überwechselte.

Das Vertragsverhältnis zwischen dem bisherigen Arbeitgeber und dem Arbeitnehmer ist beendet. Nach herrschender Rechtsmeinung bestehen zwischen dem Arbeitnehmer und seinem früheren Arbeitgeber vertragsähnliche Beziehungen; das beendete Vertragsverhältnis wirkt nach und bestimmt insofern die Voraussetzungen, unter denen die Informationen zu erteilen sind. Der Arbeitgeber ist deshalb — wie auch beim Zeugnis — gehalten, sich am Arbeitsverhältnis zu orientieren und seine Auskunft auf richtige Angaben und zutreffende Beurteilungen zu beschränken. Die Auskunft des ehemaligen Arbeitgebers an den neuen Arbeitgeber war — soweit sie inhaltlich richtig war — zulässig.

Datenschutzgerechter wäre es, wenn der neue Arbeitgeber seinen Arbeitnehmer auffordern würde, vom bisherigen Arbeitgeber eine Urlaubsbescheinigung vorzulegen.

6.7.3 Datensammlung durch Betriebsräte

Anläßlich einer Beschwerde hatte ich mich mit der Frage zu beschäftigen, ob und inwieweit ein Betriebsrat Unterlagen über die Mitarbeiter sammeln darf.

Nach § 99 Abs. 1 Betriebsverfassungsgesetz (BetrVG) hat der Arbeitgeber dem Betriebsrat vor jeder Einstellung die erforderlichen Bewerbungsunterlagen vorzulegen. Nach herrschender Rechtsmeinung bedeutet dies, daß der Betriebsrat Einsicht in diese Unterlagen nehmen kann; jedoch hat er keinen Anspruch darauf, daß ihm diese Unterlagen zur Verfügung gestellt werden. Er kann sich schriftliche Aufzeichnungen aus den Unterlagen machen. Zweifelhaft ist, ob er sich auch Kopien der Unterlagen anfertigen darf. Da nach § 99 Abs. 1 BetrVG die erforderlichen Unterlagen jedoch nur „vorzulegen" sind, spricht manches dafür, daß der Betriebsrat hier nicht berechtigt ist, sich Kopien der Unterlagen zu fertigen. Dies liefe praktisch auf ein „zur Verfügung stellen" der Unterlagen hinaus, was der Gesetzgeber dem Betriebsrat in § 99 BetrVG aber gerade nicht zugestehen wollte.

Erst recht läßt sich aus den angeführten Normen des Betriebsverfassungsgesetzes nicht herleiten, daß der Betriebsrat Unterlagen, die ihm über die Verpflichtung des § 99 Abs. 1 BetrVG hinaus zur Verfügung gestellt worden sind, bei sich aufbewahren darf.

Da Bewerbungsunterlagen als Bestandteile von Personalakten anzusehen sind, werden durch die Anfertigung und Sammlung von Kopien Personalnebenakten angefertigt, so daß hier gegen das Prinzip der „Einheitlichkeit der Personalakte" verstoßen wird.

Die Vorschrift des § 83 Abs. 1 BetrVG räumt lediglich dem betroffenen Arbeitnehmer ein Einsichtsrecht in seine Personalakte ein. Aus der Möglichkeit, ein Mitglied des Betriebsrates hinzuzuziehen, kann ein Einsichtsrecht des Betriebsrates nicht hergeleitet werden. Die Einsicht des Betriebsrates in die Personalakte oder Bestandteile der Personalakte ist daher nur mit Zustimmung des betroffenen

Arbeitnehmers zulässig, so daß nach allem eine Datensammlung durch den Betriebsrat grundsätzlich nicht zulässig ist.

6.7.4 Tonbandaufzeichnungen von Telefondaten

Ich habe zuletzt im 7. Jahresbericht unter Pkt. 6.1.3, S. 67 ff. zur Erfassung und Verarbeitung von Telefondaten umfassend Stellung genommen. Nun hat sich das Bundesarbeitsgericht in seiner Entscheidung vom 27. Mai 1986 (Az.: 1 ABR 48/84) mit der Problematik der Telefondatenerfassung im Arbeitsverhältnis auseinandergesetzt. Gegenstand der Entscheidung ist ein Spruch der Einigungsstelle, der zu einer bereits geschlossenen Betriebsvereinbarung erging. Wie die Betriebsvereinbarung differenziert auch der Spruch der Einigungsstelle zwischen extern ausgehenden Privatgesprächen und dienstlich externen ausgehenden Gesprächen. Danach sollen bei extern ausgehenden Privatgesprächen für die Ortsgespräche die Gebühreneinheiten und Kosten je Monat, für Ferngespräche das Datum, die Uhrzeit, die Gebühreneinheit und Kosten je Monat, für beide die Nebenstellennummer erfaßt werden. Bei dienstlichen externen ausgehenden Gesprächen sollen für Ortsgespräche die Gebühreneinheiten und Kosten je Monat, für Ferngespräche je Gespräch das angewählte Land außerhalb der Bundesrepublik, der angewählte Ort im Bundesgebiet und West-Berlin, die Kosten und Gesprächseinheiten, Datum, Uhrzeit, die angewählte Teilnehmernummer, die Summe der Kosten je Monat und Nebenstelle und für beide die Nebenstellennummer erfaßt werden.

Nach der Betriebsvereinbarung werden unter dienstlichen Telefongesprächen sowohl die Dienstgespräche als auch Gespräche aus dienstlichem Anlaß verstanden. Letztere sind nach der getroffenen Vereinbarung Privatgespräche, die der Mitarbeiter aus dienstlichem Anlaß führen muß sowie notwendige Anrufe bei Ärzten, Krankenhäusern oder Krankenkassen.
Ansonsten entspricht der dem Beschluß zugrunde liegende Sachverhalt dem im 7. Jahresbericht beschriebenen Verfahren der Telefondatenerfassung.

Die wichtigsten Aussagen der Entscheidung lassen sich wie folgt zusammenfassen:

Die Einführung und Anwendung eines Telefondatenerfassungssystems, das die Nebenstelle, den Tag, die Uhrzeit, die Zielnummer und die Dauer eines von dem Betrieb aus geführten externen Telefongesprächs ausdruckt, ist gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) mitbestimmungspflichtig.

Durch Art. 10 Grundgesetz (GG) werden Privatpersonen nicht unmittelbar dazu verpflichtet, das Fernmeldegeheimnis zu wahren. Da mit diesem Grundrecht aber auch eine Wertentscheidung getroffen wurde, muß auf diese auch im Rahmen von Privatrechtsbeziehungen Rücksicht genommen werden. Insofern ist die Betriebsvereinbarung und der Spruch der Einigungsstelle an dieser Wertentscheidung zu messen.

Es liegt aber auch kein Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG und in den des § 10 Fernmeldegesetz (FernmG) vor, wenn der Betreiber einer Fernmeldeanlage selbst von der Benutzung der Fernmeldeanlage und den näheren Umständen Kenntnis erhält und diese aufzeichnet.

Ein Telefondatenerfassungssystem im oben beschriebenen Sinne speichert personenbezogene Daten des anrufenden Arbeitnehmers und möglicherweise des Angerufenen im Sinne des Bundesdatenschutzgesetzes. Wenn die Einführung und Anwendung eines solchen Systems durch Betriebsvereinbarung oder den Spruch einer Einigungsstelle geregelt ist, so ist dieses Telefondatenerfassungssystem „erlaubt" im Sinne des § 3 Bundesdatenschutzgesetz (BDSG), ohne daß es darauf ankommt, ob die Voraussetzungen des § 23 BDSG erfüllt sind, weil die normativen Bestimmungen bei der Betriebsvereinbarung andere Rechtsvorschriften im Sinne von § 3 Satz 1 Nr. 1 BDSG sind. Konsequenterweise hält das Gericht es demnach auch für möglich, daß der Datenschutz der Arbeitnehmer durch Betriebsvereinbarungen verschlechtert werden kann*, da der Arbeitnehmerdatenschutz nicht unabdingbarer Mindeststandard sei. Dieser Erlaubnistatbestand bezieht sich allerdings nur auf die Zulässigkeit der Verarbeitung von Arbeitnehmerdaten, kann jedoch nicht auch die Zulässigkeit der Datenverarbeitung von Daten der Angerufenen regeln, weil insoweit dem Betriebsrat und dem Arbeitgeber die Regelungszuständigkeit fehlt. Danach ist es allein Sache des Arbeitgebers, für die daten-

* Mit dieser Argumentation stellt sich das Bundesarbeitsgericht, wie es selbst zitiert, sowohl gegen eine verbreitete Auffassung in der Literatur als auch gegen die herrschende Datenschutzrechtsauffassung. Diese Argumentation zeigt, daß es dringend geboten ist, den Arbeitnehmer-Datenschutz gesetzlich zu regeln.

schutzrechtliche Zulässigkeit der Telefondatenerfassung gegenüber den angerufenen Dritten Sorge zu tragen. Durch den Spruch der Einigungsstelle werden Rechte auf Datenschutz gegenüber Dritten nicht verletzt, da die zu deren Gunsten bestehenden Vorschriften des Datenschutzgesetzes es nicht verbieten, die Voraussetzungen dafür zu schaffen, daß die Telefondatenerfassung gegenüber den Arbeitnehmern datenschutzrechtlich zulässig ist.

Im übrigen stellt das Gericht fest, daß die oben beschriebene Regelung sich im Rahmen der Regelungsautonomie der Betriebspartner hält und die Grundsätze für den Persönlichkeitsschutz des Arbeitnehmers sowie die grundgesetzliche Wertentscheidung für einen freien und ungehinderten Fernsprechverkehr berücksichtigt werden. Auch führt der Spruch der Einigungsstelle schließlich nicht zu einer unzulässigen Überwachung und Behinderung der Betriebsratstätigkeit insofern, als in der Betriebsvereinbarung vorgesehen ist, für Betriebsratsgespräche vom Betriebsratstelefon — soweit es sich um Ferngespräche handelt — auch Zeitpunkt und Dauer des einzelnen Gesprächs, für vom Nebenstellenapparat des Betriebsratsvorsitzenden oder seines Stellvertreters geführte Ferngespräche darüber hinaus auch die Zielnummer zu erfassen. Letztendlich hält sich auch der Spruch der Einigungsstelle im Rahmen des Ermessens im Sinne von § 76 Abs. 5 Satz 4 BetrVG.

Das von der Einigungsstelle ausgeübte Ermessen ist im Rahmen der richterlichen Billigkeitskontrolle auch dann nicht zu beanstanden, wenn der Spruch der Einigungsstelle im wesentlichen den Interessen des Arbeitgebers Rechnung trägt. Das sei aber nur dann der Fall, wenn Folgeregelungen getroffen wurden, die den sich aus der technischen Überwachung der Arbeitnehmer ergebenden Überwachungsdruck abbauen. Diese Folgeregelungen müssen dem Arbeitnehmer die Sicherheit geben, daß aus seinem Verhalten keine unzutreffenden Schlüsse gezogen und keine nicht berechtigten und nicht einsichtigen Reaktionen hergeleitet werden. Insofern werden diese Folgeregelungen als ein geeignetes Mittel angesehen, die bei einer technischen Überwachung sich ergebenden widerstreitenden Interessen der Arbeitnehmer und des Arbeitgebers auszugleichen. Da solche Folgeregelungen in der der Entscheidung zugrundeliegenden Betriebsvereinbarung vorgesehen sind, stellte das Gericht auch insoweit keinen Ermessensmißbrauch im konkreten Fall fest.

Ein Ermessensmißbrauch liegt nach Ansicht des Gerichts auch nicht deswegen vor, weil bei Dienstgesprächen und Privatgesprächen aus dienstlichem Anlaß die Erfassung der vollen Zielnummer des Angerufenen gestattet wird. Zur Begründung wird angeführt, daß bei Dienstgesprächen der Arbeitgeber ohnehin vom Arbeitnehmer Auskunft darüber verlangen könne, mit wem er Dienstgespräche geführt habe, da es sich insoweit um die Erbringung der vertraglich geschuldeten Arbeitsleistung handele. Bezüglich der Privatgespräche aus dienstlichem Anlaß könne die bezweckte Kontrolle nur dann durchgeführt werden, wenn der Gesprächsteilnehmer bekannt sei. Hier sei es sinnvoll und angemessen, gleich die volle Zielnummer dieser Gespräche zu erfassen, da damit die Kontrolle für beide Seiten erleichtert würde. Eine nur teilweise erfaßte Zielnummer würde die Möglichkeit beinhalten, daß der Arbeitnehmer einen Gesprächspartner nenne, mit dem ein Privatgespräch aus dienstlichem Anlaß geführt worden sein solle, obwohl tatsächlich ein Privatgespräch mit einem Teilnehmer geführt worden sei, dessen Anschlußnummer ebenfalls die erfaßten Ziffern der Zielnummer aufwiesen. Ob letzteres eine realistische Annahme ist, soll hier dahingestellt bleiben.

In einer neueren Entscheidung hat das Bundesarbeitsgericht (Az.: 1 AZR 267/85) die Entscheidung vom Mai 1986 insoweit korrigiert, als der Arbeitgeber nicht alle Dienstgespräche registrieren darf. Nach dieser Entscheidung ist der Arbeitgeber nicht berechtigt, bei dienstlichen Telefonaten die vollständige Rufnummer des Gesprächspartners zu erfassen, soweit der Arbeitnehmer in seiner Eigenschaft als Berufspsychologe die Klienten anruft. In diesem Fall spielt das Berufsgeheimnis des Psychologen nach § 203 Strafgesetzbuch (StGB) eine besondere Rolle, das ein vertrauliches Beratungsgespräch zwischen Klienten und Psychologen ermöglichen soll. Insoweit hat dieses Urteil auch für die anderen in § 203 Abs. 1 StGB aufgeführten Personengruppen Bedeutung.

6.7.5 Weitergabe von Privatanschriften der Beschäftigten an einen Verlag

Aufgrund einer Beschwerde von Beschäftigten eines metallverarbeitenden Betriebes hatte ich zu prüfen, ob es zulässig ist, daß der Arbeitgeber Adreßlisten mit der Privatanschrift der Betriebsangehörigen an einen Verlag in Köln weitergibt. Dieser Verlag veröffentlicht und verschickt kostenlos an alle ihm bekanntgege-

benen Arbeitnehmer eine von den Arbeitgeberverbänden finanzierte Zeitschrift, die allgemeinwirtschaftliche, sozial- und gesellschaftspolitische Themen aus Sicht der Arbeitgeber behandelt.

Da keinerlei Auftrags- oder Abrechnungsverhältnis zwischen dem geprüften Betrieb und dem Verlag bestand, schied schon aus diesem Grunde eine Anwendung der § 31 Abs. 1 Nr. 3 und § 37 Bundesdatenschutzgesetz (BDSG) aus. Gegen eine Datenverarbeitung im Auftrag spricht auch, daß der Verlag wenigstens in einem Falle ohne eine Weisung vom Arbeitgeber von sich aus die Daten eines Arbeitnehmers auf dessen Eingabe hin gelöscht hat.

Die Weitergabe der Arbeitnehmeradreßdaten beurteilt sich somit nach § 24 BDSG.

Die Übermittlung der Daten des Petenten war sowohl nach § 24 Abs. 1 als auch nach § 24 Abs. 2 BDSG unzulässig, da sie

— nicht im Rahmen der Zweckbestimmung des Arbeitsverhältnisses erfolgte und

— schutzwürdige Belange der betroffenen Arbeitnehmer beeinträchtigt werden.

Zwar ist dem Arbeitgeber zuzugestehen, daß auf seiner Seite ein berechtigtes Interesse vorhanden ist, den Arbeitnehmern die Zeitschrift zukommen zu lassen.

Auf der anderen Seite war aber zu berücksichtigen, daß der einzelne Arbeitnehmer dem Betrieb seine Daten nur zur Erfüllung des Arbeitsverhältnisses und der sich daraus ergebenden Rechte und Pflichten zur Verfügung gestellt hat. Durch eine Weitergabe zu anderen Zwecken wird sein verfassungsrechtlich garantiertes Recht verletzt, selbst darüber zu befinden, an wen und zu welchen Zwecken seine Daten weitergeleitet werden.

Hinzu kommt, daß durch die Zusendung der Zeitschrift an seine Privatadresse die Privatsphäre der Betroffenen berührt wird.

Ich habe daher der Betriebsleitung nahegelegt, in Zukunft wie folgt zu verfahren:

— Die Geschäftsleitung wirkt darauf hin, daß Daten der Arbeitnehmer, die der Zusendung der Zeitschrift widersprechen oder widersprochen haben, beim Verlag gelöscht werden.

— Bei künftig geplanten Datenübermittlungen neu eingestellter Beschäftigter für den genannten Zweck hat die Geschäftsleitung vor der Übermittlung den Arbeitnehmer über den Zweck der Übermittlung aufzuklären und seine schriftliche Einwilligung gemäß § 3 BDSG einzuholen.

Durch eine solche Regelung wird das Interesse des Arbeitgebers an einer umfassenden Informationstätigkeit nicht unzulässig begrenzt. Er hat jederzeit die Möglichkeit, die Zeitschrift im Betrieb auszulegen und den gleichen Personenkreis zu erreichen oder von den einzelnen Arbeitnehmern die Zustimmung zur Zusendung und der damit verbundenen Datenweitergabe einzuholen.

Die Umsetzung der von mir vorgeschlagenen Regelung steht nach meinen Erkenntnissen bei dem Betrieb noch aus.

6.8 Gesundheitsbereich

6.8.1 Diavortrag über extrakorporale Befruchtung

Während eines Diavortrages wurden den Angaben eines Teilnehmers zufolge personenbezogene Daten von Patientinnen eingeblendet. Meine Prüfung ergab, daß tatsächlich in gefilmten Therapiebogen Name, Anschrift, Telefonnummer, Datum der letzten Regel und andere Menstruationsdaten aufgeführt waren. Der Referent, ein Arzt, war zunächst der Meinung, daß die Angaben aus der Ferne des Zuschauerraumes nicht lesbar seien und deshalb auch kein Bruch der ärztlichen Schweigepflicht oder eine Verletzung des Datenschutzgesetzes gegeben sei.

Ich habe den Arzt darauf hingewiesen, daß hier eine Verletzung der ärztlichen Schweigepflicht vorlag, da Daten aus der Krankenakte bekanntgegeben wurden. Auch die angeblich schlechte Lesbarkeit ist kein Rechtfertigungsgrund, da je nach Entfernung die Daten lesbar waren.

Darüber hinaus habe ich den Arzt auf § 3 Nr. 2 und § 24 Abs. 1 Bundesdatenschutzgesetz (BDSG) hingewiesen. Da hier eine Einwilligung nicht vorlag, wurde zusätzlich gegen Datenschutzbestimmungen verstoßen.

Der Arzt wurde aufgefordert, die personenbezogenen Daten aus dem Vortrag zu löschen bzw. unkenntlich zu machen und künftig für solche oder ähnliche Fälle eine Einverständniserklärung der/des Betroffenen einzuholen.

6.8.2 Langzeitstudie eines Arzneimittelherstellers

In einer Eingabe wurde kritisiert, daß in der Praxis einer Frauenärztin personenbezogene Daten erhoben werden, die mit der Behandlung nichts zu tun haben, und zwar ohne Einverständnis der Patientinnen. Es handelt sich dabei um eine Vorstudie zur Patientenselektion für eine epidemiologische Langzeitstudie eines Arzneimittelherstellers zur Erprobung eines Präparates zur hormonalen Empfängnisverhütung. Diese Studie läuft über 6 Monate. Die vom Hersteller herausgegebenen Fragebogen werden patientenbezogen bei der Ärztin geführt. Danach werden die Fragebogen unter Angabe einer Identifikationsnummer ohne Angabe des Patientennamens an den Hersteller übermittelt.

Der Hersteller beruft sich bei der Studie auf § 40 Arzneimittelgesetz, der sowohl eine schriftliche Einwilligungserklärung der Patienten als auch deren vorherige Aufklärung als Voraussetzung einer Arzneimittelerprobung vorschreibt. Die Datenübermittlung wie auch der zu erhebende Umfang der Daten sind im Arzneimittelgesetz nicht geregelt.

Neben den Verlaufsdaten wurden im Fragebogen auch Angaben zur Anamnese erhoben, die eine Reidentifizierung ermöglichen.

Es wurden folgende personenbezogene Anamnesedaten aufgenommen:

Geburtsjahr; Größe; Rasse; Kardiovasculäre Erkrankungen der Eltern (Herzinfarkt, Hirnschlag, Krampfadern); Diabetes der Eltern (juvenil, Altersdiabetes, Tablettenbehandlung, Insulintherapie); Zyklus (regelmäßig, unregelmäßig); Zwischenblutungen; mittlere Blutungsdauer in Tagen; Datum der letzten Periode; Raucherin; Anzahl Zigaretten/Tag; Alkoholkonsum; Anzahl Geburten/Aborte; Datum der letzten Fehlgeburt; bisherige Kontrazeption; gynäkologische Erkrankungen mit dem Hinweis „Patientin nicht in Studie aufnehmen" mit Mammae, Vuloa, Vagina, Portis, Uterus, Ovarion; Erkrankungen folgender Systeme: Blut, Endokrinologie (Schilddrüse, Nebenniere, Diabetes); Magen-Darm; Leber-Galle; Herz; Hypertonie; Nieren-Harnwege; Atmungsorgane; Knochen, Gelenke; ZNS; Krebs an Brust, Unterleib etc.; Dauermedikation (Art).

Obwohl bei einigen Positionen die Nichtaufnahme in die Studie vorgesehen war, wurde der Fragebogen trotzdem mit den entsprechenden Merkmalen (s. oben) weitergegeben.

Bei der Kontrolle stellte sich heraus, daß außer der fehlenden Zustimmung nach § 40 Arzneimittelgesetz auch keine Einwilligungserklärung nach § 3 des Bundesdatenschutzgesetzes vorlag. Da die Vorstudie auch nicht Bestandteil des Behandlungsvertrages ist, ist die Speicherung der genannten Daten und deren Übermittlung an den Arzneimittelhersteller unzulässig. Die Ärztin wurde aufgefordert, die Daten sofort zu löschen und jede weitere Datenübermittlung an den Arzneimittelhersteller zu unterlassen.

Ich habe den Senator für Gesundheit und Sport über den Vorgang informiert. Da der Arzneimittelhersteller seinen Sitz nicht in Bremen hat, habe ich die Aufsichtsbehörden gebeten, in ihrem Zuständigkeitsbereich die Vorkommnisse zu überprüfen und mich über die Ergebnisse ihrer Prüfungen zu unterrichten.

Der Vorgang zeigt einmal mehr, daß bereichsspezifische Datenschutzregelungen nicht nur für die Bereiche der Gesundheitsverwaltung und der Krankenhäuser erforderlich sind, sondern ebenso dringlich auch für den privaten Bereich der Gesundheitsversorgung (z. B. für Arzneimittelhersteller).

6.8.3 Geltung der ärztlichen Schweigepflicht bei privatärztlichen Verrechnungsstellen sowie freien Rechenzentren

Auf Bundesebene war die Frage zu entscheiden, ob und gegebenenfalls inwieweit die Weitergabe von Patientendaten an privatärztliche Verrechnungsstellen und an andere Servicerechenzentren aus datenschutzrechtlicher Sicht und unter Beachtung des § 203 Strafgesetzbuch (StGB) zulässig ist.

Hierzu hat der Senator für Rechtspflege und Strafvollzug nach Abstimmung mit der Generalstaatsanwaltschaft die Auffassung vertreten, daß die Mitteilung von Patientendaten ohne deren ausdrückliche Einwilligung an freie Rechenzentren

unter § 203 Abs. 1 Nr. 1 StGB fällt, weil die Bediensteten freier Rechenzentren nicht der strafrechtlichen Schweigepflicht nach § 203 Abs. 1 Nr. 6 StGB unterliegen. Ich teile diese Auffassung.
Der Senator für Gesundheit und Sport hat inzwischen auf meine Bitte die Ärztekammer Bremen auf diese Problematik hingewiesen.

Die Ärzte- und Zahnärztekammer hat in ihrem Mitteilungsblatt die Mitglieder auf diese Rechtslage hingewiesen.

6.9 Bildschirmtext

Nach dem Bremischen Gesetz zum Staatsvertrag über Bildschirmtext vom 17. Juli 1984 bin ich auch zuständig für den Vollzug des Artikels 9 des Btx-Staatsvertrages im öffentlichen Bereich und zugleich zuständige Verwaltungsbehörde im nicht-öffentlichen Bereich. Artikel 9 des Btx-Staatsvertrages enthält die spezifischen Datenschutzregelungen für Bildschirmtext.

Ende 1986 gab es nach Angaben der Deutschen Bundespost insgesamt 58 365 Btx-Anschlüsse (= Zahl der gültigen Anschlußkennungen aller Anbieter und Teilnehmer), darunter 3528 Anbieter und 218 angeschlossene externe Rechner. In meinem Zuständigkeitsbereich gab es Ende 1986 etwa 430 Btx-Anschlüsse, darunter ca. 30 Btx-Anbieter. Insgesamt waren Ende 1986 im Btx-System 589 330 Seiten gespeichert. Gegenüber dem Jahr vorher ist die Zahl der Anschlüsse, d. h. der Teilnehmer zwar gestiegen, die Zahl der Btx-Anbieter, der Leitseiten und der insgesamt gespeicherten Seiten jedoch gesunken.

Ich habe im Berichtsjahr erste Prüfungen in dem für mich neuen Aufgabenfeld vorgenommen. Die Leitseiten und einige Informationsseiten der rund 30 Btx-Anbieter meines Zuständigkeitsbereichs wurden auf Einhaltung der Bestimmungen des Btx-Staatsvertrages zum Datenschutz überprüft. Dabei habe ich festgestellt, daß einige Btx-Anbieter ihre Kennzeichnungspflicht, die sie nach dem Btx-Staatsvertrag (Artikel 5) haben, nicht korrekt handhaben. Diese Vorgänge habe ich an den Senator für Inneres abgegeben, der hierfür zuständige Aufsichtsbehörde ist.

In diesem Zusammenhang ergab sich das Problem, daß die Deutsche Bundespost sich unter Hinweis auf das Bremische Ausführungsgesetz zum Btx-Staatsvertrag weigerte, mir die Anschrift eines Btx-Anbieters zu nennen, der keine ausreichende Anbieterkennzeichnung in seinen Angebotsseiten hatte. Ohne Kenntnis des genauen Namens und der Anschrift eines Anbieters ist es mir nicht möglich, meinen gesetzlichen Aufgaben nachzukommen. Die Weigerung der Deutschen Bundespost ist auch deshalb unverständlich, weil der Bundesminister für das Post- und Fernmeldewesen seine Oberpostdirektionen angewiesen hat, den Informationswünschen der Datenschutzbeauftragten „im Wege der Amtshilfe" zu entsprechen.

Aufgrund einer Eingabe und durch eigene Prüfungen habe ich außerdem festgestellt, daß eine bundesweit agierende Auskunftei mit Sitz in Köln ihre Auskünfte und sonstigen Dienste einem geschlossenen Benutzerkreis über Bildschirmtext anbietet. Neben der Erteilung von Auskünften bietet diese Auskunftei auch bonitätsgeprüfte Adressen und Negativ-Daten sowie Inkassodienste an. Da ich nicht zuständig war, habe ich den Vorgang zur weiteren Prüfung an die zuständige Aufsichtsbehörde in Nordrhein-Westfalen abgegeben.

6.10 Sonstige Fälle aus dem nicht-öffentlichen Bereich

6.10.1 Austausch von personenbezogenen Daten unter weiterbildenden Instituten

Eine Sozialpädagogin hatte sich um Teilnahme an einer Weiterbildungsveranstaltung für Psychotherapie in Bremen beworben und eine Absage erhalten. Nach einer weiteren Bewerbung in einem anderen Institut, nach der sie ebenfalls eine Absage erhielt, erkundigte sie sich nach dem Grund. Diese Rücksprache ergab, daß ihr von Mitarbeitern dieses letzteren Institutes gesagt wurde, sie habe sich ja schon bei einem anderen Institut beworben und dort eine Absage erhalten und man richte sich bei Bewerbungen nach dieser Absage. Die Befürchtung, daß ein regelmäßiger Datenaustausch stattfindet, führte die Sozialpädagogin zu der Beschwerde.

Die Überprüfung ergab, daß ein derartiger Austausch nicht nachgewiesen, aber auch nicht ausgeschlossen werden konnte, daß es aufgrund persönlicher Kontakte zwischen beiden Instituten zu einem Informationsaustausch kam.

Ich habe die Institute darauf hingewiesen, daß der Austausch personenbezogener Daten für Bewerber und Teilnehmer von Weiterbildungsveranstaltungen gegen den Grundsatz der Vertraulichkeit aufgrund vorvertraglicher Pflichten verstößt.

Die geprüften Institute sagten zu, daß sie unseren Rechtsstandpunkt beachten werden.

6.10.2 Tonbandaufzeichnungen von Telefondaten

Aufgrund einer Beschwerde wurde das Problem aufgeworfen, ob es zulässig ist, daß ein Busunternehmen Telefongespräche, z. B. Bestellungen ohne Kenntnis des Anrufers auf Tonband aufzeichnet. Ich habe die Firma darauf hingewiesen, daß nach § 201 Abs. 1 Strafgesetzbuch (StGB) mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft wird, wer unbefugt

— das nicht öffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder

— eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

Neben den geschäftlichen Belangen des Unternehmens habe ich weiter darauf hingewiesen, daß einer solchen Tonbandaufzeichnung auch keinerlei rechtliche Beweiskraft anhaftet, da eine solche rechtswidrige Aufzeichnung dem Beweisverwertungsverbot unterliegt.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 31. Januar 1973 (2BvR454/71) festgestellt, daß das Grundrecht aus Art. 2 Abs. 1 Grundgesetz (GG) auch Rechtspositionen schützt, die für die Entfaltung der Persönlichkeit notwendig sind. Dazu gehört in bestimmten Grenzen ebenso wie das Recht am eigenen Bild, das Recht am gesprochenen Wort. Grundsätzlich darf jeder selbst und allein bestimmen, wer sein Wort aufnehmen soll, sowie ob und vor wem seine auf einem Tonträger aufgenommene Stimme wieder abgespielt werden darf.

Tonbandaufzeichnungen dürfen daher nur dann vorgenommen werden, wenn vorher sowohl der Anrufer als auch der Angerufene einwilligt, daß das Telefongespräch aufgenommen werden soll.

6.10.3 Video-Aufzeichnungen im Sex-Shop

In einer Eingabe hatte sich der Betroffene beschwert, beim Betreten eines Sex-Shops von einer Videokamera gefilmt worden zu sein. Er bat mich um Prüfung, inwieweit die heimliche Filmaufnahme mit dem Datenschutzrecht konform geht.

Das Problem des Einsatzes von Videokameras ist von mir bereits im 7. Jahresbericht für den öffentlichen Bereich und im 8. Jahresbericht für den privaten Bereich aufgegriffen worden.

Nach bestehender Rechtslage ist das Bundesdatenschutzgesetz (BDSG) — ebenso wie die landesrechtlichen Datenschutzgesetze — auf Videoaufnahmen nicht anwendbar. Die Abbildung einer Person, unabhängig davon, ob sie in digitalisierter oder analoger Form vorliegt, ist ein personenbezogenes Datum i. S. von § 2 Abs. 1 BDSG.

Heimlich aufgenommene Videoaufnahmen berühren das Persönlichkeitsrecht des Betroffenen. Das Bundesverfassungsgericht (BVerfG) hat in seinem „Lebach-Urteil" festgestellt, daß das Recht auf freie Entfaltung der Persönlichkeit und die Menschenwürde jedem einzelnen einen autonomen Bereich privater Lebensgestaltung sichert, in dem er seine Individualität entwickeln und wahren kann. Das Recht, „für sich zu sein" und „sich selber zu gehören" umfaßt nach Auffassung des Gerichts auch das Recht am eigenen Bild.

Das „Recht am eigenen Bild" ist eine Rechtsfigur, die aus dem Kunst-Urheber-Recht stammt. Im Zusammenhang mit dem Kunstschutz regelt das Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) von 1907 auch das Recht am Bildnis, d. h. an der „äußeren Erscheinungsweise einer Person". Nachdem durch § 141 Ziffer 5 des Urheberrechtsgesetzes (UrhG) vom 1. Januar 1966 der Schutz von Bildnissen nach dem im übrigen aufgehobenen KunstUrhG von 1907 ausdrücklich aufrechterhalten worden ist, sind die §§ 22 bis 24 KunstUrhG weiter geltendes Recht. Danach dürfen Bildnisse grundsätzlich nur mit Einwilligung des Abgebildeten veröffentlicht oder verbreitet werden. Diese Regelung ist ihrem Sinn und Zweck nach auch auf Filmwerke auszudehnen.

Die Regelungen des KunstUrhG beziehen sich jedoch nur auf die Veröffentlichung von Bildnissen, während die Anfertigung bzw. Herstellung im KunstUrhG nicht

geregelt ist. Der Bundesgerichtshof (BGH) sieht daher ungenehmigte Filmaufnahmen grundsätzlich als eine Verletzung des allgemeinen Persönlichkeitsrechts an. Nur in Ausnahmefällen könne die Erschleichung einer Bildherstellung aus überwiegendem Interesse der Allgemeinheit oder eines einzelnen gestattet sein. In seiner aus dem Jahre 1966 stammenden Entscheidung führt das Gericht weiter aus, daß die Fortschritte der Technik leichter ermöglichen, heimliche Bildaufnahmen herzustellen, sie zu vervielfältigen und einer breiten Öffentlichkeit vorzuführen. Das erfordere besonderen Anlaß, auf eine Wahrung der vom Recht gesetzten Schranken zu achten und einem Mißbrauch des leichter verletzbar gewordenen Persönlichkeitsrechts vorzubeugen.

Dieser Gedanke des BGH kommt auch im Urteil des BVerfG zum Volkszählungsgesetz zum Ausdruck:

„Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient — neben speziellen Freiheitsverbürgungen — das in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann."

Bei dem Problem heimlich hergestellter Videoaufnahmen ist zu berücksichtigen, daß nach heutigem Stand der Technik miniaturisierte Videokameras problemlos installiert werden können, so daß die Betroffenen die Überwachung nicht merken. Die Geräte verfügen inzwischen über derart lichtstarke Objektive, so daß auch Aufnahmen in wenig ausgeleuchteten Räumen ermöglicht werden. Sie sind inzwischen für jedermann erschwinglich und haben daher eine große Verbreitung. Die Technikentwicklung gerade auf dem Gebiet der Musterkennung ermöglicht, daß mit Hilfe von Computern Videobänder durch Rastervergleiche automatisch personenbezogen ausgewertet werden können. In Japan werden bereits Videoüberwachungssysteme eingesetzt, die im laufenden Verkehr Autokennzeichen erfassen und computerisiert auswerten. Hier ist der Schritt zum Einsatz automatisierter Personenerkennungssysteme nicht weit.

Angesichts der Gefahren für das Persönlichkeitsrecht erscheint es notwendig, eindeutige rechtliche Regelungen für die Herstellung von Bildnissen aufzustellen. Nach geltendem Recht bleibt dem Betroffenen nur der Weg einer Klage nach § 823 Bürgerliches Gesetzbuch (unerlaubte Handlung). Mit Blick auf die dargestellte Technikentwicklung wäre durchaus daran zu denken, den Datenschutzaufsichtsbehörden bzw. Datenschutzbeauftragten besondere Kontroll- und Sanktionsbefugnisse bei unerlaubten Bildaufnahmen zu geben.

Für den konkreten Fall wurde festgestellt, daß mir nach gegenwärtiger Rechtslage keine Möglichkeit gegeben ist, gegen heimlich angefertigte Bildaufnahmen einzuschreiten. Der Betroffene wurde auf den Zivilrechtsweg verwiesen.

6.10.4 Datenübermittlung eines Auktionshauses

Ein Auktionshaus in Bremen war aufgefordert worden, an die Kunstverwertungsgesellschaft Auskunft darüber zu erteilen, welche Originale von Werken der von dieser Gesellschaft vertretenen Künstler unter Beteiligung des Auktionshauses veräußert werden, und zwar mit der Angabe des Namens und der Anschrift der jeweiligen Veräußerer sowie der Höhe des Veräußerungserlöses.

Zu prüfen war die Berechtigung zur Datenübermittlung. Nach § 26 Abs. 3 Urheberrechtsgesetz (UrhG) kann der Kunsthändler oder Versteigerer nur Auskunft darüber verlangen, welche Originale von Werken des Urhebers innerhalb des letzten, vor dem Auskunftsersuchen abgelaufenen Kalenderjahres veräußert wurden. Eine Übermittlung an Dritte, d. h. die Kunstverwertungsgesellschaft, ist nicht gerechtfertigt. Auch nach § 26 Abs. 4 UrhG, der die Übermittlung von Name und Anschrift des Veräußerers sowie die Höhe des Veräußerungserlöses erlaubt, ermöglicht nicht die Übermittlung an die Kunstverwertungsgesellschaft, wenn dem Urheber der Anteil bezahlt worden ist.

Im übrigen handelt es sich bei dem § 26 UrhG um eine Rechtsvorschrift, die Einzelauskünfte, keineswegs listenmäßige oder pauschalierte Auskünfte zuläßt.

Das Ansinnen der Verwertungsgesellschaft mußte deshalb mangels vorhandener Rechtsvorschrift aus datenschutzrechtlicher Sicht abgelehnt werden.

6.11 Ordnungswidrigkeiten

— Im letzten Jahresbericht habe ich unter Pkt. 6.11, S. 81 berichtet, daß noch ein Ordnungswidrigkeitenverfahren aus dem Jahre 1984 beim Amtsgericht Bremerhaven anhängig ist, weil der Prozeßvertreter die Verhandlung der Sache immer wieder hinauszögern konnte. Inzwischen ist dieses Verfahren mit einem Urteil des Amtsgerichts Bremerhaven beendet worden. Dem Geschäftsführer einer Auskunftei wurde eine Geldbuße in Höhe von DM 500,— auferlegt, wegen eines Verstoßes gegen § 32 Abs. 2 Bundesdatenschutzgesetz (BDSG).

Dem lag folgender Sachverhalt zugrunde: Die Auskunftei erhält von ihren Mitgliedern Meldungen über ihre Kunden und erfaßt diese auf strukturierten Karteikarten. Die anderen Mitglieder werden unverzüglich schriftlich über neue Negativeintragungen unterrichtet; Gründe für das Vorliegen eines berechtigten Interesses dieser Mitglieder an der Übermittlung und die Mittel für ihre glaubhafte Darlegung wurden nicht aufgezeichnet, so daß ein Verstoß gegen § 32 Abs. 2 BDSG festgestellt wurde. Des weiteren wurde festgestellt, daß die Kunden, deren personenbezogene Daten an die Mitglieder des betroffenen Unternehmens übermittelt wurden, über die Speicherung und Übermittlung ihrer Daten entgegen der Vorschrift des § 34 Abs. 1 BDSG nicht unterrichtet worden waren.

Der Ansicht der Auskunftei, daß das Auskunftsverfahren insbesondere im Hinblick auf die besondere Geschäftsbeziehung zu den Mitgliedern den Bestimmungen des Datenschutzgesetzes genüge, ist das Gericht nicht gefolgt. Nach dem Urteil reicht die einfache Mitgliedschaft nicht aus, um in jedem Fall ein berechtigtes Interesse anzunehmen und auf eine Aufzeichnung der Mittel für eine glaubhafte Darlegung dieses Interesses zu verzichten. Der Sinn und Zweck der Bestimmung besteht darin festzustellen, daß jede einzelne Übermittlung auf ihre Zulässigkeit überprüft wird. Die Aufsichtsbehörde soll anhand der Aufzeichnungen in die Lage versetzt werden festzustellen, ob die jeweilige Übermittlung zulässig war. Hinsichtlich der Benachrichtigungspflicht hat das Urteil bestätigt, daß es eben nicht ausreicht, in Verbandsmitteilungen allgemein auf die Tatsache der Speicherung hinzuweisen. Es ist vielmehr erforderlich, daß die einzelnen Kunden tatsächlich darüber Kenntnis erlangen, daß über sie personenbezogene Daten gespeichert sind. Nur so kann der Kunde sein gesetzliches Recht auf Auskunft wahrnehmen. Das Gericht hat mit dem ergangenen Urteil meine Rechtsauffassung in vollem Umfange bestätigt.

— In einem anderen Fall mußte ich dem Geschäftsführer einer Firma, die neben einem Reiseunternehmen auch einen Adreßhandel betrieb, ein Bußgeld in Höhe von 5000,— DM auferlegen. Die Firma hatte mehreren gemeinnützigen Organisationen mehrere Tausend Anschriften aus dem Kundenkreis des Reiseunternehmens verkauft und ca. 200 000 Anschriften gegen Entgelt angeboten. Die Firma ist ihrer Verpflichtung aus § 39 BDSG zur Meldung dieser Tätigkeit innerhalb eines Monats trotz entsprechender Belehrung durch Mitarbeiter meiner Behörde nicht nachgekommen. Außerdem hatte der Geschäftsführer meinen mit der Überprüfung beauftragten Mitarbeitern unvollständige Auskünfte über den Adreßhandel und die Herkunft und Lagerung der angebotenen Adressen gegeben und ihnen den Zutritt zu den Geschäftsräumen unter Androhung von Gewalt verwehrt. Damit hat er gegen § 30 Abs. 2 und 3 BDSG verstoßen, wonach er der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen und das Betreten der Geschäftsräume zu dulden hat.

Gemäß § 42 Abs. 1, 3 und 4 BDSG stellt dieses Verhalten eine Ordnungswidrigkeit dar.

Gegen meinen Bußgeldbescheid hat der Geschäftsführer Einspruch eingelegt. Ich habe das Verfahren an die Staatsanwaltschaft abgegeben.

— Mehrere Ordnungswidrigkeitenverfahren habe ich nach der Anhörung wegen Geringfügigkeit eingestellt.

7. Verwaltungsautomation ist Gestaltungsaufgabe

Die Erörterung der vielfältigen Einsatzmöglichkeiten neuer Informations- und Kommunikationstechniken auf kommunaler und Landesebene zeigt, daß die Verwaltung vor einer grundsätzlichen Neustrukturierung steht. Es stellen sich Fragen über die Gestaltungsprinzipien, wie verändern Computer, elektronische Textver-

arbeitung, die modernen Formen der Nachrichtenübertragung etc. die Arbeitsweise innerhalb der Verwaltung und den Verkehr der Verwaltungsbehörden untereinander und mit Dritten. Wie kann künftig der Bürger als Benutzer an öffentlichen Informationssystemen teilhaben, welche Konzepte lassen sich denken und welche sind datenschutzverträglich. Wer entscheidet verantwortlich, wie die Strukturen einzelner Behörden, ja des gesamten öffentlichen Verwaltungsnetzes aussehen und wie damit die öffentlichen Aufgaben erfüllt werden können. Inwieweit entwickelt man eigene Konzepte, eigene Programme etc., inwieweit wird auf Fremdentwicklungen zurückgegriffen. Wie wird bei dem Einkauf von Fremdentwicklungen sichergestellt, daß bremisches Landesrecht ungeschmälert berücksichtigt bleibt. Die Autonomie eines Landes wird auch auf dieser Ebene in Frage gestellt, wenn Fremdprogramme, die auf eine Rechtssituation eines dritten Landes zugeschnitten sind, im Lande Bremen eingesetzt werden, ohne daß im Detail Änderungsmöglichkeiten eröffnet sind. Der Gesetzgeber ist auch hier aufgerufen sicherzustellen, daß seine in Form von Gesetzen getroffenen autonomen Entscheidungen vollständig umgesetzt werden. Kriterien der Gestaltung der „Verwaltung der Zukunft" sind sicherlich neben wirtschaftlichen Überlegungen, gesetzliche Aufgabenoptimierung, Versorgung der Bürgerbedürfnisse, Einbettung in organisatorische Vorgaben etc. auch und nicht zuletzt die glaubwürdige Gewährleistung des Datenschutzes für Bürger und Beschäftigte.

In der Schlußbetrachtung möchte ich deshalb perspektivisch die Frage nach der Verantwortung des Gesetzgebers für derartig grundsätzliche Verankerungen aufgreifen. In einigen Bundesländern hat der Gesetzgeber die Gestaltung durch den Erlaß von ADV-Organisationsgesetzen übernommen. Der Senat löst die Aufgabe bisher durch eine ADV-Anweisung. An dieser Stelle und mit der Absicht, einen Denkprozeß in Gang zu setzen, möchte ich auch für das Land Bremen darauf aufmerksam machen, daß bei der umfangreichen Veränderung, die für die gesamte öffentliche Verwaltung bevorsteht, die Frage der parlamentarischen Verantwortung und die parlamentarische Entscheidung gefordert sein könnte. Die Diskussion um die Gestaltung von Informations- und Kommunikationstechnik hat auch die Frage aufgeworfen, inwieweit Verantwortung durch Verfahrensnormen gesichert werden kann, wobei materielle Kriterien vorzugeben wären. Wenn wesentliche Entscheidungen dem Parlament vorzubehalten sind, dann ist die Neustrukturierung der gesamten öffentlichen Verwaltung sicherlich eine solche.

Bremerhaven, den 27. März 1987

Dr. Alfred Büllesbach,

Landesbeauftragter für den Datenschutz

Anlage 1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986

zum Datenschutz im Krankenhaus

Die Datenschutzbeauftragten haben in ihrer Entschließung vom 27./28. März 1984 über die Auswirkungen des Volkszählungsurteils auf die Notwendigkeit hingewiesen, auch im Bereich des Gesundheitswesens bereichsspezifische gesetzliche Regelungen zu erlassen. Die ärztliche Schweigepflicht und die allgemeinen Datenschutzgesetze reichen nicht aus, alle Fälle, in denen im Bereich des Krankenhauses das Persönlichkeitsrecht des Patienten berührt wird, angemessen zu lösen. Konkrete Regelungen für diesen Bereich sind insbesondere deshalb notwendig, weil automatisierte Datenverarbeitung in immer stärkerem Maße im Krankenhausbereich auch für die Verarbeitung medizinischer Daten eingesetzt wird. Die zunehmende Komplexität der Verarbeitung und Nutzung von Patientendaten führt dazu, daß für den einzelnen Patienten der Umfang und die Zwecke der Verwendung seiner Daten undurchschaubar werden. Der Bürger muß aber auch künftig die Gewähr haben, daß das Vertrauensverhältnis zwischen Arzt und Patient (Arzt-/Patientengeheimnis) und sein Persönlichkeitsrecht gewahrt bleiben.

Bisher wird die Datenverarbeitung in Krankenhäusern vielfach aufgrund sehr weit gefaßter formularmäßiger Einwilligungen gerechtfertigt. Die Einwilligung kann jedoch in vielen Fällen keine ausreichende Grundlage für die Verarbeitung von Patientendaten sein, da für den Patienten die Informationsmöglichkeit und die Entscheidungsfreiheit häufig eingeschränkt sind.

Maßstab für den Umfang der Erhebung, Verarbeitung und Nutzung von Patientendaten muß stets die Behandlung des Patienten sein. Eine zusätzliche vom Behandlugszweck nicht gedeckte Datenerhebung, -verarbeitung und -nutzung bedarf einer besonderen Legitimation.

Auch die für die Behandlung verwendeten Vordrucke und Aufnahmeverträge müssen diesen Grundsätzen angepaßt werden. Die zuständigen Stellen werden aufgefordert, ihre Vordrucke und Aufnahmeverträge entsprechend zu überarbeiten.

Zur Wahrung des Patientengeheimnisses ist es geboten, im Krankenhaus den ärztlichen Bereich von der Verwaltung informationell abzuschotten. Daraus folgt, daß z. B. die Akten der Krankenhausverwaltung getrennt von denjenigen des ärztlichen Bereichs zu führen sind. Daraus folgt weiter, daß auch im ärztlichen Bereich nur vom jeweils behandelnden Arzt auf die Daten zugegriffen werden kann.

Läßt das Krankenhaus Patientendaten bei anderen Stellen im Auftrag verarbeiten, wird das Arztgeheimnis durchbrochen. Auch besteht die Gefahr einer Grundrechtsbeeinträchtigung durch Verknüpfung von medizinischen Daten und solchen aus anderen Bereichen und durch überregionale Konzentration medizinischer Daten. Die Verarbeitung medizinischer Daten außerhalb des eigenen Krankenhauses sollte daher — in eingeschränktem Umfang — allenfalls bei einem anderen Krankenhaus zugelassen werden.

Das Krankenhaus steht im Zentrum vielfältiger Informationsanforderungen, nicht zuletzt von Sozialleistungsträgern und anderen öffentlichen Stellen. Diese Informationsanforderungen sind häufig nicht normenklar festgelegt. Ihre Notwendigkeit muß überprüft, die gesetzlichen Grundlagen müssen präzisiert werden. Dies gilt insbesondere dann, wenn die Übermittlung zu belastenden Konsequenzen für den Patienten im Verwaltungsvollzug (z. B. Führerscheinentzug) führen kann.

Der Patient darf ohne sein Wissen und sein Einverständnis grundsätzlich nicht zum Objekt der Forschung mit Daten gemacht werden, die zu seiner Behandlung erhoben werden. Die Verarbeitung von Daten zu Forschungszwecken ohne Beteiligung des Patienten sollte nur zugelassen werden, wenn dies im Interesse der wissenschaftlichen Forschung unabdingbar ist und die Rahmenbedingungen der Verarbeitung durch den Gesetzgeber näher festgelegt sind. Dies gilt auch für gemeinsame Dokumentationssysteme mehrerer behandelnder Einrichtungen.

Das informationelle Selbstbestimmungsrecht umfaßt auch das Recht des Patienten, Einsicht in Patientenakten und ärztliche Unterlagen zu nehmen und Auskunft zu erhalten, sofern nicht überwiegende Geheimhaltungsinteressen anderer entgegenstehen.

Eine undifferenzierte, zeitlich unbefristete Aufbewahrung von Patientenunterlagen darf es auch im Krankenhaus nicht geben. Deshalb müssen die Krankenhäuser prüfen, wann welche Patientenunterlagen ohne Beeinträchtigung schutzwürdiger Belange der Patienten vernichtet werden können.

Anlage 2

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986

zum Entwurf einer Telekommunikationsordnung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht des Bundesministers für das Post- und Fernmeldewesen, die Bedingungen für die Benutzung der Einrichtungen für das Fernmeldewesen in einer einheitlichen Telekommunikationsordnung (TKO) neu zu regeln und an einer Stelle zusammenzufassen. Damit soll auch der technischen Entwicklung Rechnung getragen werden: Die Digitalisierung der Telekommunikation führt zu einer bisher nicht gekannten Speicherung von Verbindungs-, Abrechnungs- und Benutzungsdaten. Auch der Inhalt der Kommunikation wird zunehmend elektronisch gespeichert.

Das Bundesverfassungsgericht hat gerade vor dem Hintergrund der zunehmenden elektronischen Datenverarbeitung in seinem Urteil zum Volkszählungsgesetz 1983 die Bedeutung des Rechts auf informationelle Selbstbestimmung unterstrichen und daraus Grundsätze abgeleitet. Diese sind auch für die TKO von Bedeutung, da die Bürger auf die Inanspruchnahme der einzelnen Dienste in zunehmendem Maße angewiesen sind. Der Entwurf trägt diesen Anforderungen nicht hinreichend Rechnung:

1. Jeder der Telekommunikationsdienste birgt technisch bedingte Risiken in sich, die vom Teilnehmer nicht ohne weiteres erkennbar sind, bei der Nutzung aber berücksichtigt werden müssen. Deshalb sollte in die TKO eine Vorschrift aufgenommen werden, die die Deutsche Bundespost verpflichtet, die Teilnehmer des jeweiligen Dienstes über dessen wesentliche technische Bedingungen und Risiken bei der Benutzung des Telekommunikationsnetzes zu informieren und sie auf sicherheitsförderndes bzw. sicherheitsgefährdendes Nutzungsverhalten hinzuweisen.

2. Die in § 4 TKO genannten öffentlichen Telekommunikationsdienste werden nicht hinreichend präzise umschrieben. Diese Dienste dürfen nur zugelassen werden, soweit sich aus den ihren Einsatz regelnden gesetzlichen Bestimmungen die Voraussetzungen und der Umfang der Einschränkung des Rechts auf informationelle Selbstbestimmung klar und für den Bürger erkennbar ergeben.

3. Durch Veränderung der technischen und betrieblichen Funktionsbedingungen ist eine inhaltliche Umgestaltung einzelner Dienste ohne Änderung der entsprechenden Bestimmungen in der TKO möglich (§ 5 TKO). Eine derartige Ermächtigung der Deutschen Bundespost ist mit den Forderungen des Bundesverfassungsgerichts nach Transparenz der Datenverarbeitung und nach Schaffung einer normenklaren gesetzlichen Grundlage für eine Einschränkung des Rechts auf informationelle Selbstbestimmung nicht vereinbar. Gleiches gilt für die Regelung des § 3 Abs. 1 Satz 3 TKO, nach der das öffentliche Telekommunikationsnetz für sonstige, in der TKO nicht geregelte Telekommunikationszwecke freigegeben werden kann.

4. Die im Zusammenhang mit den öffentlichen Telekommunikationsdiensten maßgeblichen datenschutzrelevanten Begriffe wie „Teilnehmer", „Anbieter", „Abrechnungsdaten", „Verbindungsdaten", „Benutzungsdaten" etc. sollten bei den nach § 2 TKO in einem Anhang zu dieser Verordnung festgelegten Begriffsbestimmung aufgeführt werden. In einem Anhang sollten ferner die bei der Nutzung der einzelnen Dienste anfallenden personenbezogenen Daten erläutert werden. Nur so kann der Bürger als Nutzer der öffentlichen Kommunikationsdienste entsprechend einer Forderung des Bundesverfassungsgerichts wissen, welche personenbezogenen Daten die Deutsche Bundespost wann und bei welcher Gelegenheit über ihn verarbeitet.

5. Wiederholt wird die Zulässigkeit der Verarbeitung personenbezogener Daten damit begründet, daß sie aus „betriebsbedingten Gründen" erforderlich sei. Dieser Rechtsbegriff bedarf einer Definition in der TKO, aus der hervorgeht, welcher Art diese Gründe sein können, wobei die Eigenart der verschiedenen Dienste zu brücksichtigen ist.

6. Die Allgemeinen Vorschriften zum Datenschutz in Teil VII Abschnitt 2 TKO bedürfen der Ergänzung und Präzisierung:

   — Wann Bestandsdaten, Verbindungsdaten und Gebührendaten zu löschen sind, ist teils überhaupt nicht, teils nur unbestimmt geregelt. So dürfen Verbindungsdaten aus „betriebsbedingten Gründen" auf unbestimmte Zeit gespeichert werden. Gleiches gilt, wenn der Teilnehmer „eine andere Art der Verarbeitung" beantragt hat; die Voraussetzungen hierfür werden nämlich nicht festgelegt.

   — Auch die Bestimmungen über die Verarbeitung der Gebührendaten müssen so formuliert werden, daß keine unzulässigen Schlüsse auf ein Teilnehmerverhalten gezogen werden können.

   — Die Regelungen umfassen nicht alle bei der Post anfallenden Daten. Beispielsweise fehlen Regelungen zu den Inhalten der Informationen und den beim Betrieb der Dienste anfallenden Daten.

   — Die Vorschriften erlauben der Post, alle Daten zu beliebigen „Telekommunikationszwecken" zu verwenden. Unerläßlich ist eine Nutzungsbeschränkung auf die Zwecke der jeweils in Anspruch genommenen Dienste.

   — Die Regelung der Befugnis, Daten weiterzugeben, ist zu umfassend und unklar. Insbesondere sollten Verbindungsdaten von jeder Übermittlung ausgeschlossen bleiben.

   — Trotz der Fülle der besonderen Sensitivität der bei der Post vorhandenen personenbezogenen Daten fehlen spezielle Vorschriften über die Datensicherung.

Insgesamt dürfen die allgemeinen Datenschutzregelungen nicht hinter dem Standard der neuen Mediengesetzgebung zurückbleiben.

7. Auch die Regelungen zu den einzelnen Diensten berücksichtigen die Interessen der Bürger nur unzureichend:

   — Beim Telefondienst ist der „Zwangseintrag" der Teilnehmer im Telefonbuch vorgesehen. Insbesondere nach dem Volkszählungsurteil bestehen Zweifel, ob dies mit dem informationellen Selbstbestimmungsrecht noch vereinbar ist.

   — Unter welchen Voraussetzungen die Post Daten über einzelne Telefonverbindungen, insbesondere die gewählte Rufnummer, registriert und an wen sie Auskunft darüber gibt, ist nicht geregelt. Das gleiche gilt für die sog. Fangschaltung. Beim Funktelefon speichert die Post ohne Rechtsgrundlage detaillierte Verbindungsdaten.

   — Trotz seiner Annäherung an die Struktur der Datenschutzbestimmungen des Bildschirmtext-Staatsvertrages (Btx-StV) bleibt der Regelungsgehalt des § 387 TKO hinter Art. 9 Btx-StV zurück. Dies betrifft insbesondere die Regelung zu den Verbindungsdaten sowie Definition und Umfang der Vergütungsdaten. Ein klares Verbot der Übermittlung von Vergütungsdaten an Dritte fehlt. Ferner fehlt ein Verbot der Übermittlung von Daten, die im Zusammenhang mit der Übermittlung von Mitteilungs- und Antwortseiten anfallen. Unzureichend ist auch der Umfang der technischen und organisatorischen Maßnahmen zur Datensicherung geregelt.

8. Abgesehen von Kritik an Einzelbestimmungen des Entwurfs der TKO bleiben wesentliche Fragen offen:

   — Eine auf den Netzbereich beschränkte Regelung, für die allein der Bund zuständig ist, muß wesentliche Aspekte der Medienordnung ungeregelt lassen. Auch die in die Länderkompetenz fallenden Nutzungs- und Anwendungsbereiche werfen Datenschutzprobleme auf, die von der jeweiligen Netzstruktur abhängig sind, und die bereits bei der Konzeption der Dienste berücksichtigt werden müssen.

   — Auch bei der in Aussicht genommenen Regelung weiterer Dienste (z. B. Breitbandkommunikationsdienste, Fernwirkdienste) sind entsprechende spezielle Datenschutzregelungen in die TKO aufzunehmen.

   — Zur Fortentwicklung der datenschutzrechtlichen Möglichkeiten der TKO wird die Post aufgefordert, bei der Neu- und Umgestaltung einzelner Telekommunikationsdienste datenschutzfreundliche Lösungen zu realisieren. So sollten Überlegungen angestellt werden, ob nicht z. B. ein Dienst zur Verschlüsselung der Nachrichten sowie Verfahren der Gebührenzählung bzw. -abrechnung beim Teilnehmer eingeführt werden können.

   — In Anbetracht der Bedeutung einer künftigen Telekommunikationsstruktur und im Hinblick auf künftige Diensteinführungsentscheidungen sind nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder verfassungsrechtliche Zweifel angebracht, ob die Verordnungsermächtigung aus § 14 PostVwG für die Regelung solcher wesentliche Bereiche des öffentlichen Lebens bestimmender Sachverhalte noch als ausreichend anzusehen ist oder ob nicht vielmehr der Gesetzgeber die wesentlichen Entscheidungen treffen muß.

Anlage 3

Dr. jur., Dipl. sc. pol. Alfred Büllesbach
Landesbeauftragter für den Datenschutz

Stellungnahme zum Entwurf Bundesverfassungsschutzgesetz und zum Entwurf MAD-Gesetz entsprechend des Fragen- und Sachverständigenkataloges für die öffentliche Anhörung am 28. April 1986 im Innenausschuß des Deutschen Bundestages

Einleitung

Die Diskussion über die Notwendigkeit legislatorischer Schritte für die Verfassungsschutzbehörde in Bund und Ländern ist bereits seit einigen Jahren in Gange. Erste Ergebnisse dieser öffentlichen Diskussion haben im Lande Bremen bereits 1981 dazu geführt, das Gesetz zur Änderung des Gesetzes über den Verfassungs-

schutz im Lande Bremen und zur Ausführung des Gesetzes der Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 23. März 1981 zu beschließen. Im Land Nordrhein-Westfalen wurde erstmalig am 15. Juli 1981 ein Verfassungsschutzgesetz erlassen. Diese frühzeitige Novellierungsdiskussion wurde durch das Volkszählungsurteil vom 15. Dezember 1983 auf den Bund und die übrigen Länder ausgedehnt. Es ist inzwischen anerkannt, daß bereichsspezifische Regelungen für die Informationsverarbeitung der Verfassungsschutzbehörden in präziser und normenklarer Form notwendig sind.

Die Diskussion um die Schaffung bereichsspezifischer Rechtsregelungen im Verfassungsschutzbereich steht notgedrungen vor dem Spannungsverhältnis der Gewährleistung individueller Persönlichkeitsrechte und der staatlichen Sicherheit. Bereichsspezifische Regelungen müssen daher anerkannte Verfassungsrechtsprinzipien verwirklichen und für die Tätigkeit der Verfassungsschutzbehörden einwandfreie Rechtsgrundlagen schaffen. Diese Forderung ergibt sich nicht nur aus den Datenschutzgedanken heraus, sondern prinzipiell aus dem Verfassungsrechtsprinzip der Gewährleistung der Persönlichkeitsrechte und der Rechtsstaatlichkeit. Eine bereichsspezifische Datenschutzregelung wird deshalb immer auch mit materieller Rechtsveränderung einhergehen. Eine mögliche Verbindung solcher Rechtsveränderungen zeigten die Zielsetzung und die Schwerpunkte des Änderungsgesetzes im Lande Bremen, das drei Ziele verfolgte, nämlich die Verwirklichung eines den gegenwärtigen Rechtsvorstellungen entsprechenden bereichsspezifischen Datenschutzes, die Verbesserung der parlamentarischen Kontrolle der Exekutive auf dem Gebiet des Verfassungsschutzes und schließlich die Straffung der Verfassungsschutztätigkeit.

Als anerkannte Rechtsvorstellung ist in einem Verfassungsschutzgesetz auch hinsichtlich der Informationsverarbeitung der Grundsatz der Trennung von Aufgaben- und Befugnisnormen zu verwirklichen. Hierbei ist die besondere Gefährdungslage zu beachten, die sich bei der Sammlung von Informationen über Bürger durch Verfassungsschutzbehörden ergibt. Durch diese Trennung lassen sich auch für die verschiedenen Stufen der Datenverarbeitung, die grundrechtsrelevante Handlungen darstellen, unterschiedliche Regelungen schaffen. Besonderer rechtlicher Würdigung bedarf die Informationsübermittlung. Hierzu ist zu differenzieren hinsichtlich der Informationsübermittlung von Verfassungsschutzbehörden an andere Sicherheitsbehörden (Polizei, Staatsanwaltschaft), wie die Übermittlung an andere öffentliche Stellen und schließlich das Verhältnis der Verfassungsschutzbehörden zu privaten Dritten. Bei diesen Überlegungen ist grundsätzlich die Frage des Grundrechtsschutzes und der Amtshilfe, sowie die Gewährleistung der informationellen Gewaltenteilung sowohl zwischen den verschiedenen Sicherheitsbehörden als auch zwischen der allgemeinen und besonderen öffentlichen Verwaltung aufzugreifen.

Ein Vergleich der vorhandenen Verfassungsschutzgesetze in Bund und Ländern zeigt, daß folgende Prinzipien überwiegend in den bisherigen Gesetzen bereits geregelt waren:

— Verbot der Angliederung an polizeiliche Dienststellen

— keine polizeilichen Befugnisse für den Verfassungsschutz

— Amtshilfe und Auskunftserteilungsregelung

— Mitteilungspflichten von Behörden an den Verfassungsschutz

— Weitergabe von Erkenntnissen durch den Verfassungsschutz

— Parlamentarische Kontrolle des Verfassungsschutzes.

Neben diesem Regelungsraster sind durch den Datenschutz neue Rechtsprobleme hinzugetreten:

— Die Anwendung nachrichtendienstlicher Mittel bei Vorliegen tatsächlicher Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten im Sinne des § 3 Abs. 1 Bundesverfassungsschutzgesetz

— Die Beachtung des Verhältnismäßigkeitsgesichtspunktes bei der Erforschung des Sachverhaltes

— Die Gewährleistung des Rechtsweges, ähnlich wie bereits bisher nach dem G10-Gesetz bei Eingriffen im Kernbereich der Privatsphäre

— Verhinderung der Umgehung der Trennung von Verfassungsschutz- und Polizeibehörden durch rechtswidrige Amtshilfepraktiken

— Rechtliche Zulässigkeitsregelungen für die Speicherung personenbezogener Informationen

— Löschungsregelungen für personenbezogene Informationen beim Verfassungsschutz

— Minderjährigenschutz in besonderer Weise

— Differenzierende Übermittlungsregelungen hinsichtlich der Übermittlung personenbezogener Informationen durch den Verfassungsschutz an Strafverfolgungsbehörden, an Stellen, die einen Antrag auf Mitwirkung nach § 3 Abs. 2 gestellt haben, an übrige staatliche Stellen und an andere als staatliche Stellen.

Die generelle Problematik der Eröffnung des Rechtsweges stellt sich auch im Zusammenhang mit der Gewährleistung eines Auskunftsrechtes (vgl. hierzu Alfred Büllesbach, Informationstechnologie und Datenschutz, München 1985, Seite 167 bis 172).

1. **Zur Erforderlichkeit gesetzlicher Regelungen**

Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 sind Einschränkungen des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse zulässig. Diese Einschränkungen bedürfen einer gesetzlichen Grundlage, die den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit genügen muß. Die Voraussetzungen und der Umfang der Beschränkungen müssen für den Bürger erkennbar geregelt sein. Aufklärungs- und Auskunftspflichten müssen ergänzend für eine ausreichende Transparenz sorgen. Die Daten, deren Erhebung und Verwendung geregelt wird, müssen für den festgelegten Verwendungszweck geeignet und erforderlich sein. Das Recht auf informationelle Selbstbestimmung darf grundsätzlich nur aufgrund bereichsspezifischer Regelungen eingeschränkt werden. Generalklauseln, wie sie in den allgemeinen Datenschutzgesetzen als Auffangnormen vorgesehen sind, reichen nicht aus. Insbesondere für die Informationsverarbeitung der Verfassungsschutzbehörden ergibt sich deshalb aus dem Volkszählungsurteil, daß präzise gesetzliche Grundlagen erforderlich sind, da die Tätigkeit der Verfassungsschutzbehörden in besonderem Maße in das informationelle Selbstbestimmungsrecht eingreift und für die Öffentlichkeit fast vollständig im geheimen und ohne Kontrolle durch den Betroffenen stattfindet. Für einen effektiven Grundrechtsschutz ist in bereichsspezifischen Regelungen deshalb auch die vollständige Kontrolle durch unabhängige Datenschutzbeauftragte zu ermöglichen.

Die Gesetzgebungskompetenz zur ausschließlichen Gesetzgebung hat der Bund nach Artikel 73 Nr. 10 b GG zum Schutze der freiheitlich-demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (Verfassungsschutz). Artikel 73 Nr. 10 GG differenziert in den Buchstaben a, b und c verschiedene Bereiche, in denen der Bund die Zusammenarbeit des Bundes und der Länder regelt. Ob die Zuordnung der Tätigkeit, die sich aus Artikel 73 Nr. 10 c GG, nämlich zum Schutze gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden in den Kompetenzbereich des Verfassungsschutzes zählen, kann im Hinblick auf die Differenzierungen nach a, b, c und der damit verbundenen differenzierten Behörden- und Gesetzesstruktur bezweifelt werden. § 3 Abs. 1 Nr. 3 sowohl der bisherigen als auch der Regelung im Entwurf des Bundesverfassungsschutzgesetzes überträgt diese Aufgabe dem Verfassungsschutz. Die Differenzierung in Artikel 73 Nr. 10 nach a, b und c legt die Überlegung nahe, daß der Verfassungsgeber für die unterschiedlichen Aufgaben verschiedene Organisationen und Einrichtungen sich vorgestellt haben mag. Da es sich hier um eine sehr grundsätzliche Fragestellung handelt, würde es den Rahmen dieser Abhandlung sprengen, hier vertiefte verfassungsrechtliche Aussagen zu treffen. Bei Gelegenheit einer Anhörung zu diesem Gesamtkomplex soll aber wenigstens darauf hingewiesen werden, daß es hier durchaus unterschiedliche verfassungsrechtliche und organisatorische Überlegungen geben kann. Aus der Sicht eines Sachverständigen ergibt sich daraus die umgekehrte Fragestellung, welche Überlegungen hat der Bundesgesetzgeber im Vorfeld einer Neufassung des Bundesverfassungsschutzgesetzes zu diesem Komplex angestellt. Für die Differenzierungsüberlegung spricht meines Erachtens auch Artikel 87 Abs. 1 Satz 2, der aufzählt, daß durch Bundesgesetz für unterschiedliche Aufgaben verschiedene Stellen eingerichtet werden können.

2. **Anforderungen an die wehrhafte Demokratie aus der Entscheidung des Grundgesetzes**

Ohne auf die umfangreiche Diskussion zur wehrhaften Demokratie innerhalb der Politikwissenschaft einzugehen, verweise ich aus datenschutzrechtlicher Sicht darauf, daß es auch zur wehrhaften Demokratie gehört, dem Bürger sein Recht auf informationelle Selbstbestimmung zu erhalten, das ihm individuelle Selbstbestimmung ermöglicht und das ihm insbesondere die Entscheidungsfreiheit beläßt, selbst zu entscheiden über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit, sich entsprechend dieser Entscheidung auch tatsächlich verhalten zu können. Denn wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimung zu planen oder zu entscheiden. Das Bundesverfassungsgericht fährt fort, daß mit dem Recht auf informationelle Selbstbestimmung eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar wären, in der die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Hieraus folgt für das Bundesverfassungsgericht, daß es sich nicht nur um Beeinträchtigung der individuellen Entfaltungschancen des einzelnen handelt, sondern daß es insbesondere auch um das Gemeinwohl dabei geht (auch das ist Teil der wehrhaften Demokratie), weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich-demokratischen Gemeinwesens ist.

3. **Aufgabenbeschreibung und Befugnisnormen**

Die präzise Aufgabenbeschreibung ist dringend geboten, da sich aus ihr auch der zulässige Umfang der Informationsverarbeitung ergibt. Die in § 3 Abs. 1 verwendeten Begriffe wie etwa „Strebungen gegen die freiheitlich-demokratische Grundordnung" oder „Gefährdung auswärtiger Belange" sind unpräzise. Unklar bleibt insbesondere, unter welchen Voraussetzungen Einzelpersonen beobachtet werden dürfen, wie weit die Beobachtung auf beeinflußte Organisationen ausgedehnt werden darf und wo die Schwelle von der Ausübung der Grundrechte hin zur verfassungsfeindlichen Bestrebung überschritten wird. Deshalb ist es umso erforderlicher, die Voraussetzungen der Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten im Rahmen der Erfüllung der Aufgaben des Verfassungsschutzes präziser und für den Bürger transparenter zu regeln.

Hinsichtlich der Befugnisse zur Mitwirkung bei Sicherheitsüberprüfungen vgl. meine Ausführungen unter Punkt 11 meiner Stellungnahme.

Die Trennung von Aufgaben- und Befugnisnormen, wie sie im Entwurf angelegt ist, ist grundsätzlich zu begrüßen. Die Regelung der Informationsverarbeitung durch den Verfassungsschutz hat den Anforderungen der Normenklarheit zu entsprechen. Der Bürger muß den gesetzlichen Bestimmungen entnehmen können, aus welchem Anlaß, in welcher Form und zu welchem Zweck der Verfassungsschutz personenbezogene Daten verarbeiten darf. Deshalb ist es grundsätzlich richtig, die Verarbeitung personenbezogener Daten durch den Verfassungsschutz von der Erhebung, über die Speicherung und die Übermittlung einschließlich der Berichtigung, Sperrung und Löschung zu regeln. Notwendig ist es aber auch, jegliche andere Art der Verarbeitung und Verwendung, ganz gleich ob sie in Akten oder in Dateien erfolgt, einzubeziehen. Hier weist der Entwurf gravierende Mängel auf.

§ 6 läßt die Erhebung personenbezogener Informationen zu, soweit dies zur Erfüllung der Aufgaben der Verfassungsschutzbehörden erforderlich ist. Eine derart uferlose Sammlungsbefugnis kann schon deshalb nicht hingenommen werden, weil die verfassungsrechtlich gebotene Güterabwägung im Einzelfall ergeben kann, daß vorrangige Individualrechte einer personenbezogenen Erfassung entgegenstehen, obwohl dies zur Aufgabenerfüllung erforderlich wäre. Dies gilt vor allem in den vom Brockdorf-Beschluß des Bundesverfassungsgerichts abgesteckten Bereichen der Ausübung des Demonstrationsrechtes, aber gleichermaßen hinsichtlich solcher Personen, die selbst keinerlei verfassungswidriger Bestrebungen verdächtigt sind. Im Bereich der Beobachtung verfassungswidriger Bestrebungen ohne Gewaltbezug sollte die personenbezogene Speicherungsbefugnis überhaupt davon abhängig gemacht werden, daß der Extremismusbezug in der Person des zu Speichernden vorliegt.

Die in § 7 getroffene Regelung über die Speicherung, Veränderung und sonstige Nutzung personenbezogener Daten darf nicht — wie jetzt vorgesehen — auf Dateien beschränkt bleiben, zumal es heute bereits möglich ist, auf komplexe Aktensammlung gezielt und mit Hilfe automatisierter Verfahren zu schließen. Überdies muß die Vorschrift um die Festlegung fester Überprüfungs- und Löschungsfristen, differenziert nach den einzelnen Aufgabenbereichen, erweitert werden.

Entsprechend der Forderung der Datenschutzbeauftragten beschränkt der Entwurf die Pflichten anderer Behörden, den Verfassungsschutz über eigene Wahrnehmungen von sich aus zu unterrichten, auf Erkenntnisse aus den Bereichen Spionage und Terrorismus. Die allen Behörden eingeräumte Befugnis, dem Verfassungsschutz auch Informationen über gewaltfreie extremistische Bestrebungen zuzuleiten, birgt in dieser uneingeschränkten Form die Gefahr in sich, einem Klima allgemeinen Denunziantentums Vorschub zu leisten. Auch vermag der Bürger, der in Kontakt mit einer Verwaltungsbehörde tritt, nicht zu erkennen, was diese wann und bei welcher Gelegenheit an die Verfassungsschutzbehörde übermittelt. Schließlich fehlt in der Vorschrift die Verpflichtung, Veränderungen des Sachverhaltes der Verfassungsschutzbehörde nachzuberichten.

Die in § 9 des Entwurfes festgelegte Verpflichtung für alle übrigen öffentlichen Stellen, der Verfassungsschutzbehörde die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen, geht zu weit. Dies gilt gleichermaßen für die vorgesehene pauschale Ermächtigung der Verfassungsschutzbehörde, in alle amtlich geführten Register Einsicht zu nehmen. Schließlich fehlt es auch an einer Regelung für die Übermittlung von Informationen durch andere Stellen, die diese aufgrund besonderer Eingriffsbefugnisse erlangt haben. Die in § 9 Abs. 2 vorgesehene Befreiung der Verfassungsschutzbehörde von der Verpflichtung, ihre Auskunftsersuchen zu begründen, kann nur für die Fälle hingenommen werden, in denen Sicherheitsinteressen oder schutzwürdige Belange des Betroffenen nicht entgegenstehen.

Angesichts des umfassenden Sammlungsauftrages der Verfassungsschutzbehörden bedürfen die dort angefallenen Erkenntnisse einer besonders strengen Abschottung nach außen. Dem trägt § 10 Abs. 1 des Entwurfs nicht hinreichend Rechnung, der es für eine Weiterleitung verfassungsschutzbehördlicher Erkenntnisse an andere öffentliche Stellen genügen läßt, daß die Daten dort im Rahmen der Aufgabenerfüllung für Zwecke der öffentlichen Sicherheit benötigt werden.

Die in § 10 Abs. 2 zugelassene Übermittlung von Daten der Verfassungsschutzbehörde an Dienststellen der Stationierungsstreitkräfte muß angesichts der unübersehbaren Folgewirkungen an besonders enge Voraussetzungen geknüpft werden. Zumindest ist eine Abwägung der schutzwürdigen Belange der Betroffenen vorzuschreiben.

Die Weitergabe von Erkenntnissen an private Stellen, § 10 Abs. 3, muß auf die Fälle der Sicherheitsüberprüfung und der Spionage bzw. Terrorismusabwehr beschränkt werden. Die Abgrenzung zwischen Bundesamt und Landesämter für Verfassungsschutz bezüglich des Geheimschutzes in der Wirtschaft ist nicht präzise geregelt.

4. **Trennungsgebot**

Das Trennungsgebot ist durch die Alliierten im Polizeibrief eingeführt worden. Es resultiert aus der Erfahrung des Dritten Reiches mit der Gestapo, in dem es ein solches Trennungsgebot nicht gab. Diese Hintergründe zeigen, daß insbesondere aufgrund unserer historischen Erfahrung die strikte Trennung von Polizei und Nachrichtendiensten verfassungsrechtlich unverzichtbar ist. Das Trennungsgebot bestimmt deshalb die rechtsstaatlichen Grenzen der Zusammenarbeit von Nachrichtendiensten und Polizei. Das Trennungsgebot erschöpft sich nicht in einer bloßen organisatorischen Trennung zwischen Nachrichtendiensten und Polizei. Gerade wegen der automatisierten Datenverarbeitung kommt es mindestens ebenso auf eine strikte Trennung der Informationsbestände an. Das Trennungsgebot darf nicht durch einen umfassenden Informationsaustausch unterlaufen werden. Ein Verständnis, daß die Trennung nur auf organisatorischer Ebene anzusiedeln wäre, wird den Informationsverarbeitungsprinzipien und den damit verbundenen Auswirkungen auf die Persönlichkeitsrechte in keinster Weise gerecht.

Würden die vorliegenden Entwürfe des Verfassungsschutzgesetzes und des MAD-Gesetzes verabschiedet, so würde das Trennungsgebot nicht vollständig gewahrt

bleiben. § 10 Abs. 1 läßt beispielsweise die Übermittlung personenbezogener Informationen durch das Bundesamt für Verfassungsschutz, die es durchaus auch mit nachrichtendienstlichen Mitteln gewonnen haben kann, an Behörden des Bundes und bundesunmittelbare juristische Personen des öffentlichen Rechts zu. Der Einsatz nachrichtendienstlicher Mittel durch die Verfassungsschutzbehörden ist aber eine Sonderbefugnis, die in dieser Form anderen Behörden nicht zur Verfügung steht. Um Verkürzung der Rechte der Bürger auszuschließen, bedarf es auch in diesem Fall einer Beschränkung der Übermittlung auf bestimmte Katalogdaten, so sieht z. B. das Bremische Verfassungsschutzgesetz an dieser Stelle den Katalog des § 7 Abs. 3 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vor.

5. **Nachrichtendienstliche Mittel**

Der Grundsatz der Normenklarheit gebietet es, die in § 5 vorgesehene Befugnis, nachrichtendienstliche Mittel einzusetzen, durch eine Aufzählung der wichtigsten Mittel zu präzisieren. Daneben sollte die Festlegung der zulässigen Mittel in einer Verwaltungsvorschrift vorgeschrieben werden. Angesichts der Schwere des mit der Anwendung nachrichtendienstlicher Mittel verbundenen Eingriffs in das Persönlichkeitsrecht muß ihr Einsatz grundsätzlich auf konkret verdächtige Personen beschränkt werden. Entsprechend den Regelungen über die Post- und Telefonüberwachung sind ein Verwertungsverbot und eine Verpflichtung zur nachträglichen Unterrichtung des Betroffenen vorzusehen. Ferner ist gesetzlich klarzustellen, daß auch bei der Anwendung nachrichtendienstlicher Mittel die allgemeinen Rechtsvorschriften zu beachten sind.

6. **Rechtsweggarantie, Klagemöglichkeiten und Auskunftsrechte des Bürgers**

Zur Sicherung des Rechtsstaates zählen neben der Gewaltenteilung und der Gewährung justizieller Grundrechte (Artikel 101, 103, 104 GG) auch die Gewährleistung der Unabhängigkeit der Gerichte (Artikel 97 GG) wie auch die Garantie gerichtlicher Kontrolle staatlichen Handelns durch Artikel 19 Abs. 4 GG. Artikel 19 Abs. 4 GG garantiert allgemein auch die Zugänglichkeit des Rechtsweges.

Die Regelungen des vorliegenden Entwurfes enthalten insoweit keine Ausschlußregelungen, so daß dem betroffenen Bürger zunächst einmal grundsätzlich der Rechtsweg offen steht. Er kann also Maßnahmen der Verfassungsschutzämter, von denen er sich getroffen fühlt, wie Bescheide der Verfassungsschutzämter gerichtlich (in der Regel durch die Verwaltungsgerichte) überprüfen lassen.

Probleme ergeben sich aber in anderer Hinsicht. Sie werden zwar nicht durch Regelungen des Entwurfes erzeugt, bei einer entsprechenden Aufnahme von Regelungen in die Entwürfe könnten sie aber beseitigt oder eingedämmt werden. Ein Mangel zur Überprüfung staatlicher Maßnahmen, den Schutz der Gerichte in Anspruch nehmen zu können, liegt für den Bürger darin begründet, daß ihm weder im Vorfeld noch im gerichtlichen Verfahren genügend Informationen zur Verfügung stehen, um mögliche Verstöße der Verfassungsschutzbehörden gegen Grundrechte oder Gesetze hinreichend darlegen zu können.

Zu beachten ist hier aber, daß Artikel 19 Abs. 4 GG kein allgemeines Begründungsgebot für staatliche Akte enthält. Begründungspflichten sind vielmehr speziell für belastende Verwaltungsmaßnahmen aus dem Rechtsstaatsprinzip abzuleiten (vergleiche Maunz-Düring-Herzog Art. 19 Rdnr. 253 mit weiteren Nachweisen). Die Ausgestaltung der Begründungspflichten ist daher Aufgabe des Gesetzgebers, der unter Berücksichtigung der Beeinträchtigung der Grundrechte des Bürgers und unter Berücksichtigung des Regelungsgegenstandes differenziert zu entscheiden hat und dabei auch Ausnahmen und Einschränkungen festlegen darf.

Soweit daher in den Entwürfen keine Aussage etwa über Auskunftsrechte der Bürger gegenüber dem Verfassungsschutz oder dem MAD getroffen wird, gelten für die Datenspeicherungen bei den Ämtern und den damit verbundenen Eingriffen in das Recht auf informationelle Selbstbestimmung die allgemeinen Regelungen des § 13 Abs. 2 und 3 BDSG. Diese schreiben vor, daß die Behörden des Verfassungsschutzes sowie Behörden des Bundesministers der Verteidigung, soweit die Sicherheit des Bundes berührt wird, auf Antrag dem Betroffenen keine Auskunft zu erteilen haben. Eine Auskunftserteilung unterbleibt, soweit die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde, die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, die personenbezogenen Daten oder die Tatsache ihrer Spei-

cherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen, die Auskunft sich auf die Übermittlung personenbezogener Daten an die in § 12 Abs. 2 Nr. 1 BDSG genannten Behörden bezieht.

Der Gesetzentwurf der Bundesregierung zu § 13 BDSG enthält insoweit keine Verbesserung der Rechtsstellung des Betroffenen, vielmehr werden auch noch die Kontrollmöglichkeiten des Bundesbeauftragten für den Datenschutz in Abs. 5 eingeschränkt.

Ohne auf den Ort einer solchen Regelung einzugehen, wäre meines Erachtens zu prüfen, ob nicht in Abhängigkeit zum Interesse des Betroffenen an einer Auskunft und seinen Darlegungen hierzu ein differenziertes Auskunftsrecht gesetzlich garantiert werden kann. Zu unterscheiden sind dabei im wesentlichen drei Möglichkeiten:

— In den Fällen, in denen ein Bürger nicht weiß, daß er Maßnahmen von seiten der Ämter, wie z. B. Beobachtung und den damit verbundenen entsprechenden Datenspeicherungen unterliegt, wird er auch keinen Anlaß haben, ein Auskunftsbegehren zu stellen. Soweit ein Bürger dennoch einen Antrag auf Auskunft stellt oder aber, wenn er nur einen vagen Verdacht äußert und deshalb eine Auskunft verlangt, so wäre diesem in der Regel aus überwiegendem Geheimhaltungsinteresse nicht zu entsprechen.

— Anders hingegen könnte mit Anträgen auf Auskunft verfahren werden, aus denen ersichtlich wird, daß dem Betroffenen entweder sämtliche oder doch weitgehend alle Maßnahmen der Ämter gegen ihn bekannt sind, in diesem Falle wäre ein Geheimhaltungsinteresse nicht zu erkennen.

— Schließlich ist die Konstellation noch denkbar, daß der Betroffene glaubhaft darlegt, daß er durch verschiedene Ereignisse und Umstände sich in seiner Lebensqualität in erheblichem Maße eingeschränkt fühlt, die Ämter aber diesen Zustand in keiner Weise verursacht oder mit zu vertreten haben. Auch in diesem Falle wäre zu überlegen, ob nicht dem Betroffenen eine, gegebenenfalls auch eingeschränkte Auskunft erteilt werden könnte, um ihm so die Möglichkeit zu eröffnen, die Ursachen für seine Beeinträchtigung an anderer Stelle zu suchen.

Über die allgemeinen rechtsstaatlichen Anforderungen hinaus verlangt Artikel 19 Abs. 4 GG, daß die Gründe einer angegriffenen Verwaltungsentscheidung in gerichtlichen Verfahren mitgeteilt werden, es sei denn, diese prozessuale Begründungspflicht ist wegen eines überwiegenden Geheimhaltungsinteresses eingeschränkt. Eine Beschränkung des Auskunfts- als auch des Akteneinsichtsrechts, z. B. gegen Ausforschung, verstößt jedenfalls nicht gegen den Rechtsschutzgedanken des Artikels 19 Abs. 4 GG.

7. Gegenseitige Unterrichtung der Verfassungsschutzämter

§ 4 des Entwurfes zum Verfassungsschutzgesetz sieht Unterrichtung der verschiedenen Landes- und Bundesämter untereinander vor. Er differenziert zwischen

— Datenübermittlungen des Bundesamtes an die Landesämter

— Datenübermittlungen eines Landesamtes an andere Landesämter

— Datenübermittlungen eines Landesamtes an das Bundesamt.

Die „Erforderlichkeit" der Daten für Zwecke des Verfassungsschutzes ist als einziges Kriterium für die Zulässigkeit einer Datenübermittlung im Gesetzentwurf vorgesehen. Eine inhaltliche Eingrenzung dessen, was jeweils erforderlich ist, wird nicht vorgenommen. Insbesondere läßt die Vorschrift offen, welches Recht denn für den Übermittlungsvorgang anzuwenden ist, das der übermittelnden oder das der empfangenden Stelle.

Der im Entwurf vorgesehene umfassende Informationsaustausch der Verfassungsschutzbehörden untereinander bedarf einer Verdeutlichung, welche Datenübermittlungen zugelassen werden sollen. Erstrebenswert wäre es, eine aufgabenbezogene Einschränkung vorzusehen. Datenschutzrechtlich relevant wird dies insbesondere auch, weil der Entwurf in § 4 Abs. 1 letzter Satz eine Regelung vorsieht, wonach die Unterrichtung der Verfassungsschutzbehörden die Übermittlung personenbezogener Informationen einschließt. Aus der Stellung könnte man zwar

entnehmen, daß grundsätzlich die Unterrichtung in Angelegenheiten des Verfassungsschutzes ohne die Übermittlung personenbezogener Daten stattfinden soll und nur in der Ausnahme auch diese Mitteilungen personenbezogene Daten enthalten sollen; fraglich ist aber bei Beachtung der Begründung zu § 4 des Entwurfes, ob der Gesetzgeber dies tatsächlich so gewollt hat. An dieser Stelle ist daher eine normenklare Regelung erforderlich, die sich nicht nur am Erforderlichkeitsgrundsatz orientiert. Es sollten engere Kriterien geschaffen werden, die die Rechte und Pflichten zur Übermittlung personenbezogener Daten konkretisieren.

Bedenklich ist auch, wenn in der Begründung zu § 4 hervorgehoben wird, daß erforderlich im Sinne des Absatzes 1 nicht nur die Kenntnis von Informationen sei, die den Bund als Gebietskörperschaft betreffen, sondern daß er Kenntnis über alle Angelegenheiten des Verfassungsschutzes erhalten müsse, die das Bundesamt für Verfassungsschutz zentral sammelt und auswertet. An dieser Stelle wird deutlich, daß der gesamte Aufgabenbereich, wie er in § 3 des Entwurfes geregelt ist, mit in die Unterrichtungspflicht hinsichtlich der Übermittlung personenbezogener Angaben einbezogen werden muß. Dies bedeutet in der Praxis, daß alleine unter dem Vorbehalt des Erforderlichkeitsgrundsatzes alle einmal in den Bereich einer Verfassungsschutzbehörde gelangten personenbezogenen Informationen im Zuge der gegenseitigen Unterrichtung weitergegeben werden können.

Die Regelung dieser Vorschrift führt daher nicht zu einer präziseren Beschreibung der personenbezogenen Datenübermittlung und wird daher weder kalkulierbarer noch kontrollierbarer.

8. Gemeinsame Datenbestände und Textzusätze

Besondere Bedenken bestehen gegen die vorgesehene automatische Abrufbarkeit von Textzusätzen, weil die Textinformation, bevor sie abgerufen wird, nicht inhaltlich überprüft werden kann (Wahrheitsgehalt, Aktualität, Verwertungsverbote, Quellenschutz etc.). Es besteht deshalb die Gefahr, daß ein Sachverhalt, verkürzt wiedergegeben, in jederzeit automatisch abrufbaren Informationssystemen erhältlich ist und den Bürger diese somit politisch und strafrechtlich nachteilig qualifizieren kann, ohne daß der Bürger dies überprüfen könnte. Diese qualitative Erweiterung des nachrichtendienstlichen Informationssystems (NADIS) ist für die Arbeit des Verfassungsschutzes nicht erforderlich; weiterhin bestehen verfassungsrechtliche Bedenken, so daß die Erweiterung auch aus rechtlichen Gründen nicht zulässig ist.

Das Prinzip muß sein, so wenig Informationen wie möglich im NADIS aufzunehmen; Einzelentscheidungen sind nur durch Einsicht in die Akte zu treffen. Die Mehrzahl der Probleme entsteht durch Verkürzungen von Texten. So kennt jeder Politiker die Problematik verkürzter Redezitate in der Presse. Die Feststellung eines geparkten Pkws in der Nähe eines extremistischen Objektes gerinnt in der Verkürzung zur Teilnahme des Halters, obwohl es verschiedene Sachverhalte geben kann, warum der Halter dort sein Fahrzeug geparkt hat.

9. Wird die föderale Ordnung durch den Entwurf beeinträchtigt?

Nach § 9 Abs. 1 des Entwurfes BVerfSchG kann das Bundesamt von jeder Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, die Übermittlung von Daten verlangen und amtlich geführte Register einsehen. Nach § 16 des Entwurfes können die Verfassungsschutzbehörden der Länder bei Behörden des Bundes die Übermittlung personenbezogener Informationen verlangen und amtlich geführte Register einsehen. Nach § 15 hat die Bundesregierung ein Weisungsrecht gegenüber den obersten Landesbehörden, die für die Zusammenarbeit der Länder mit dem Bund auf dem Gebiet des Verfassungsschutzes zuständig sind. Nach § 2 Abs. 2 wird bestimmt, daß die Länder eine Behörde zu bestimmen und zu unterhalten haben, die Angelegenheiten des Verfassungsschutzes bearbeitet. Die Regelung in § 15 steht zudem in einem besonderen Verhältnis zu Artikel 37 GG. Nach Artikel 37 GG (Bundeszwang) kann die Bundesregierung mit Zustimmung des Bundesrates die notwendigen Maßnahmen treffen, um das Land im Wege des Bundeszwanges zur Erfüllung seiner Pflichten anzuhalten. Sicherlich besitzt § 15 nicht die gleiche Qualität, doch muß erkannt werden, daß § 15 mehr als die Koordinierung bzw. Zusammenarbeit regelt, denn er sieht ein direktes Weisungsrecht des Bundes vor. Insgesamt beeinträchtigen die dargestellten Regelungen die föderale Ordnung.

10. Sicherheitsüberprüfungen

Angesichts der in § 3 Abs. 2 des Entwurfes zum Verfassungsschutzgesetz getrof-

fenen Regelung der Sicherheitsüberprüfung sind im Schwerpunkt die folgenden Gesichtspunkte anzusprechen:

— Die Regelung im Entwurf sieht keine klare Zuständigkeitsabgrenzung zwischen den Bundes- und Landesämtern bei der Durchführung der Sicherheitsüberprüfung vor.

  — Hinsichtlich der Anfragen öffentlicher Stellen läßt sich eine Trennung der Zuständigkeiten zwischen den Bundes- und den Landesämtern für Verfassungsschutz noch leicht entsprechend der Anstellungsbehörde der zu überprüfenden Personen realisieren.

  — Die Überprüfung im privaten Bereich sollte von den Landesämtern durchgeführt werden. Dieses Verfahren hätte für den privaten Bereich zwei Vorteile, zum einen könnte ein Landesamt wegen des Näher-dran-Prinzips in effektiverer Weise auch die jeweilige Sicherheitssituation des Betriebes mit berücksichtigen. Beachtet man darüber hinaus, daß Sicherheitsüberprüfungen bei Betrieben im wesentlichen auf Anordnung des Bundeswirtschaftsministeriums bei Vertragsvergabe gefordert werden, ist zu befürchten, daß die Betriebe aus der Angst heraus, sonst die Auftragserteilung nicht zu bekommen, gegenüber dem Bundesamt vorsichtigere Angaben machen würden, als sie dies tun würden, wenn das Landesamt eine Überprüfung durchführen würde.

— Die Entscheidung über die Einstufung eines Betriebes in die Kategorie eines sicherheitsempfindlichen Betriebes wie auch die Differenzierungen zwischen einzelnen Sicherheitsstufen ist legislatorisch festzulegen. Notwendig ist es, die Prozedur, wie der Bundesminister für Wirtschaft Betriebe zu Geheimbetrieben benennt, festzulegen. Neben dem Interesse der Sicherheit steht das Interesse der Arbeitnehmer, beschäftigt zu sein.

  Notwendig ist es, für diesen Bereich der Geheimschutzregelung in der Wirtschaft klare Bestimmungen sowohl der Aufgaben und der Befugnisnormen als auch des Verfahrens in Abstimmung mit dem Bundeswirtschaftsminister zu finden. Dazu gehört z. B. die exakte Festlegung, welche Stellen lebens- und verteidigungswichtige Einrichtungen darstellen, die verantwortliche und überprüfbare Festlegung von Sperrzonen, um so exakt zu erkennen, welche Arbeitnehmer in Sperrzonen arbeiten sollen und welche zum Umgang mit Verschlußsachen verpflichtet werden sollen.

— Nach derzeitiger Praxis machen die Landesämter für Verfassungsschutz eine Vorprüfung, indem die Stellen zunächst in den Bereichen „Zugang erhalten sollen", § 3 Abs. 2 Nr. 2 BVerfSchG-E, und „beschäftigt werden sollen" § 3 Abs. 2 Nr. 2 BVerfSchG-E (und die entsprechenden landesrechtlichen Regelungen), eine Anfrage stellen, ob überhaupt eine Aussicht auf Erfolg besteht, daß die Sicherheitsüberprüfung positiv verläuft. In einem zweiten Verfahren mit Wissen und unter Mitwirkung des Betroffenen wird dann die tatsächliche Sicherheitsüberprüfung über das Bundesministerium für Wirtschaft durch das Bundesamt für Verfassungsschutz durchgeführt. Diese, ihrem Wesen nach einheitliche Prüfung durch verschiedene Stellen des Bundes und der Länder durchführen zu lassen, halte ich für wenig zweckmäßig.

— Für die Verfassungsschutzämter bedeutet die Mitwirkungspflicht, daß die anfragende Stelle selbst die Entscheidung darüber trifft, ob die entsprechende Person eingestellt wird und mit einer sicherheitsrelevanten Aufgabe betraut wird oder nicht. Daher muß der Verfassungsschutz der Stelle inhaltliche Daten bekanntgeben, damit diese selbst in die Lage versetzt wird, eine Entscheidung zu treffen (hinsichtlich der hiermit einhergehenden Probleme der Zweckentfremdung vgl. meine Ausführungen unter „12. Zweckbindung" dieser Stellungnahme). Die Verfassungsschutzämter handeln bei der Durchführung der Sicherheitsüberprüfung quasi im Auftrage anderer Stellen, sie können daher auch die Verfahrensvoraussetzungen für die Einleitung einer Sicherheitsüberprüfung nicht in jedem Einzelfall würdigen. Dieser Zustand führt dazu, daß insbesondere im privaten Bereich, abgedeckt durch die Regelung in § 4 Abs. 2 Nr. 1 des Entwurfes BVerfSchG „die Zugang ... sich verschaffen können", auch die letzte Ersatzraumpflegerin noch einer Sicherheitsüberprüfung unterworfen wird. Die Regelungen des Entwurfes bringen auch diesen Teil des Verfahrens nicht klar genug zum Ausdruck und bedürften einer Überarbeitung.

Es empfiehlt sich daher, die Mitwirkung der Verfassungsschutzbehörden an der Sicherheitsüberprüfung von Personen durch andere Stellen im Verfassungsschutzgesetz umfassender zu regeln. Eine solche Regelung müßte neben klaren Zuständigkeitsregelungen eine präzise Beschreibung der mitwirkungspflichtigen Umstände ausweisen und die damit in Zusammenhang stehende Datenverarbeitung präziser regeln.

Sofern über die Sicherheitsüberprüfung (§ 3 Abs. 2) hinaus eine Mitwirkung an anderen Verfahren wie etwa bei Einbürgerungen, Asylverfahren, Ordensverleihung oder der Überprüfung von Bewerbern für den öffentlichen Dienst für unabdingbar gehalten wird, sind diese im Gesetz ausdrücklich zu nennen. Die im Zusammenhang damit stehende Datenverarbeitung ist im Verfassungsschutzgesetz präzise zu regeln.

Unabhängig davon ist für die Sicherheitsüberprüfung und jedes andere Verfahren zur Überprüfung von Personen eine bereichsspezifische Regelung erforderlich.

Für die Mitwirkung des Verfassungsschutzes bei Personenüberprüfungen (§ 3 Abs. 2) sind im übrigen weitere Prinzipien zu beachten (vgl. im einzelnen unter Nr. V des Beschlusses der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 1985 — 8. Jahresbericht, Anlage 2)

11. **Zweckbindung**

Das Prinzip der Zweckbindung leitet sich verfassungsrechtlich aus Artikel 2 Abs. 1 GG in Verbindung mit Artikel 1 Abs. 1 GG ab. Die Rechtsprechung des Bundesverfassungsgerichts spricht den Gedanken der Zweckbindung im Scheidungsaktenbeschluß (BVerfGE 27, 244, 250 ff.), in dem das Recht auf private Lebensgestaltung und die Integrität der menschlichen Person in der geistig-seelischen Beziehung und das Verhältnismäßigkeitsgebot herangezogen werden, im Mikrozensusbeschluß (BVerfGE 27, 1), in dem die grundsätzliche Möglichkeit freier und selbstverantwortlicher Entfaltung der Persönlichkeit angenommen wurde, und auch im Lebach-Urteil (BVerfGE 35, 202), in dem dem Einzelnen das Recht zugesprochen wurde, seine Individualität zu entwickeln und zu wahren, an. Die Rechtsprechung zum Recht auf autonome Selbstdarstellung (BVerfGE 32, 373 und 34, 238) verweist auch auf ein Schutzgut, das dem einzelnen die Möglichkeit gewährt, über sein Bild selbst bestimmen zu können. Die Gewährleistung des Grundsatzes der Zweckbindung setzt aber eine rechtliche Trennung, eine verwaltungsorganisatorische Beachtung und eine ADV-organisatorische Berücksichtigung voraus. Hierauf habe ich bereits in meinem 6. Jahresbericht auf den Seiten 78 ff. hingewiesen.

Insbesondere wegen der vom Verfassungsschutz angewendeten Methoden der geringen Transparenz der Datenverarbeitung bei den Ämtern wie auch die eingeschränkten Kontrollmöglichkeiten gegenüber den Ämtern zwingen den Gesetzgeber, in besonders starkem Maße die Einhaltung des Zweckbindungsgrundsatzes durch rechtliche Regelungen zu gewährleisten.

Die Befugnisse zur Verarbeitung und sonstigen Nutzung personenbezogener Daten dürfen daher nicht nur in Generalklauseln beschrieben und sehr weit gefaßt werden, sie sind vielmehr zu differenzieren nach Art und Zweck der Datenerhebung. Die Anwendung nachrichtendienstlicher Mittel stellt eine besondere Form personenbezogener Datenerhebung dar, so daß Begriff und damit Inhalt, Zweck und Ausmaß präzisiert werden müssen.

Auch die Befugnisse des Bundesamtes für Verfassungsschutz zur Übermittlung von Daten an andere Behörden ist sehr vage und unpräzise formuliert. Angesichts der umfassenden Datensammlung der Verfassungsschutzbehörden müßte eine besonders strenge Abschottung nach außen gegenübergestellt werden. Dem trägt § 10 Abs. 1 des Entwurfs nicht hinreichend Rechnung, der es für eine Weiterleitung verfassungsschutzbehördlicher Kenntnisse an andere öffentliche Stellen genügen läßt, daß die Daten dort im Rahmen der Aufgabenerfüllung für Zwecke der öffentlichen Sicherheit benötigt werden. Auch die in § 10 Abs. 2 zugelassene Übermittlung von Daten der Verfassungsschutzbehörden an Dienststellen der Stationierungsstreitkräfte müßte an besonders enge Voraussetzungen geknüpft werden, um eine Zweckentfremdung der Daten weitgehend auszuschließen. Die Gefahr einer zweckentfremdeten Verwendung von Mitteilungen besteht auch bei Mitteilungen, die im Rahmen einer Sicherheitsüberprüfung gegenüber privaten Stellen vorgenommen werden. Die Praxis der telefonischen Nachfrage im Rahmen von Bewerbungen beim früheren Arbeitgeber ist allgemein bekannt. Eine Mitteilung

von Daten durch den früheren Arbeitgeber, die ihm aus Anlaß einer Sicherheitsüberprüfung bekannt geworden sind, ist zu unterbinden. Deswegen bedürfte es gerade in diesem Bereich neben dem Zweckbindungsgebot ergänzender sanktionierter Vorschriften bei einem Verstoß gegen das Zweckbindungsgebot, um so die Einhaltung sicherzustellen.

Eine zweckveränderte Nutzung von Daten könnte auch dann gegeben sein, wenn Verfassungsschutzbehörden Datenangaben von im Zuge einer Sicherheitsüberprüfung benannten Vertrauenspersonen, die diese über sich und über den Überprüfenden gegenüber den Verfassungsschutzämtern gemacht haben, um die Sicherheitsüberprüfung durchzuführen, plötzlich für andere Aufgaben der Verfassungsschutzämter genutzt würden.

Schließlich stellt auch die in § 9 des Entwurfes vorgesehene Verpflichtung für alle öffentlichen Stellen, den Verfassungsschutzbehörden die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen, einen Verstoß gegen den Zweckbindungsgrundsatz dar. Eine derartige Ermächtigung ist zu weit. Dies gilt auch für die im Entwurf vorgesehene Befugnis der Verfassungsschutzbehörden, in jedes amtliche Register einsehen zu können.

Zusammenfassend läßt sich daher feststellen, daß die im Entwurf vorgesehenen Regelungen dem Zweckbindungsgrundsatz nicht in ausreichendem Maße Rechnung tragen.

12. Veröffentlichung von personenbezogenen Daten

Das Sachwortregister der bisher veröffentlichten Verfassungsschutzberichte enthält neben der Aufführung der Organisationen einen vollständigen alphabetisch geordneten Katalog aller im Bericht namentlich genannten Personen. Schon das zufällige Nachschlagen einiger Namen, die im Text durch Sperrschrift hervorgehoben sind, verdeutlicht, daß der Bericht an vielen Stellen auch ohne die Nennung der Namen nicht an Qualität oder Aussagekraft verlieren würde. Die in § 11 Abs. 2 gefundene Formel „wenn schutzwürdige Belange des Betroffenen nicht vorliegen oder die Interessen der Allgemeinheit überwiegen", hat im Grunde genommen auch heute Geltung. Daher ist anzunehmen, daß diese Formulierung lediglich die gängige Praxis in den Berichten abdecken soll.

Soweit Personen der Zeitgeschichte namentlich erwähnt werden, bestehen keine Bedenken hinsichtlich einer Veröffentlichung. Dies gilt insbesondere für Personen, die auf Bundesebene tätig sind. Anders stellt sich das Verhältnis dar, wenn Personen nur auf regionaler oder lokaler Ebene agieren. Die vom Entwurf zugelassene Unterrichtung der Öffentlichkeit über personenbezogene Daten der Verfassungsschutzbehörden muß die Ausnahme bleiben; § 11 Abs. 2 sollte daher enger gefaßt werden.

13. Schaffen Verfahrensvorschriften neue Datenschutzrisiken?

Regelungen, wie sie der gegenwärtige Entwurf des Verfassungsschutzgesetzes vorsieht, sind in ähnlicher Form im bremischen Verfassungsschutzgesetz bereits seit 1981 geregelt. Die Erfahrung zeigt, daß es kein unverhältnismäßiger Verwaltungsaufwand ist, solche verschiedenen Verfahrens- und Datenschutzvorschriften aufrechtzuerhalten. Zur Gewährleistung eines Mindestmaßes an Kontrolle sind bestimmte Verfahrens- und Datenschutzvorschriften unverzichtbar. Vermieden werden muß, daß durch die Protokollierung neue Datenschutzrisiken für den Bürger entstehen. So bietet sich im Einzelfall durchaus an, sog. Verdichtungsprotokollierungen zu erarbeiten, um entsprechende Stichproben und Zufallskontrollen (nur zu Zwecken der Datenschutzkontrolle) durchzuführen, ohne daß dabei die entsprechenden Datenschutzrisiken für den Bürger auftreten.

14. Anmerkungen zum Entwurf des MAD-Gesetzes und der Abgrenzung zum Verfassungsschutz

Die in Artikel 73 Nr. 1 und Nr. 10, Artikel 87 und 87 a GG getroffene Entscheidung sieht keine spezielle Organisationsform des Militärischen Abschirmdienstes vor. Zwar könnte man Teilaufgaben des Verfassungsschutzes eigenständigen Stellen übertragen, fraglich ist aber, ob es einen Verstoß gegen die Verfassung bedeutet, wenn man den MAD als Abteilung dem Bundesamt für Verfassungsschutz angliedern würde. Im Bereich der Bundeswehr mag zwar ein besonders hoher Sicherheitsbedarf bestehen, grundsätzlich könnte aber praktisch der Bereich mit Sicherheitsbeauftragten genauso betraut werden wie Betriebe oder Behörden. Für die

Differenzierungsüberlegung spricht meines Erachtens Artikel 87 Abs. 1 Satz 2, der aufzählt, daß durch Bundesgesetz für unterschiedliche Aufgaben verschiedene Stellen eingerichtet werden können.

Wegen der Besonderheiten und Eigenheiten im Bereich der Bundeswehr scheint es erforderlich, eigene rechtliche Regelungen für die Informationsverarbeitung zu statuieren. Auch die Aufgabenwahrnehmung in kleineren Organisationseinheiten entspricht durchaus dem Datenschutzrechtsgedanken der Funktionstrennung.

Wichtig ist daher unter Berücksichtigung der vom Gesetzgeber getroffenen Entscheidung zur Einrichtung zweier Dienste nur, daß die Tätigkeitsfelder des Verfassungsschutzes und des MAD vom Gesetzgeber genau gegeneinander abgegrenzt werden, so daß keine sich überschneidenden Bereiche entstehen. Ein sinnvolles Kriterium scheint dabei zu sein, daß sowohl der Täter als auch das Objekt oder Opfer im Bereich der Bundeswehr liegen müssen. Das würde bedeuten, daß z. B. ein Soldat, der sich in einer lokalen neonazistischen Gruppe organisiert oder umgekehrt, soweit eine solche Gruppe Soldaten vor dem Kasernentor agiert, eine Beobachtung dieser Bestrebung dem Verfassungsschutz obliegen würde. Damit wäre gleichzeitig sichergestellt, daß keine Sicherheitslücken entstehen. Diese trennscharfe Abgrenzung der Tätigkeitsfelder erscheint in § 1 Abs. 2 nicht ganz geglückt.

16. Regelung für die Datenverarbeitung in Akten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz haben in ihrer Erklärung zur Novellierung des Bundesdatenschutzgesetzes vom 4. November 1983 bereits darauf hingewiesen, daß die Entscheidung des Gesetzgebers, bei der Anwendung des Bundesdatenschutzgesetzes von der Verarbeitung personenbezogener Daten in Dateien auszugehen, für den Bürger kaum verständlich ist und daß dies in der Praxis zu Unzuträglichkeiten führen und die Wirksamkeit des Datenschutzes mindern wird. Solange eine solche Anknüpfung besteht, muß der Dateibegriff wenigstens so definiert werden, daß ein Höchstmaß an Schutz für den Betroffenen erreicht wird. Dazu gehört, daß alle automatisierten Verfahren und alle Akten und Aktensammlungen einbezogen werden, die mit Hilfe automatisierter Verfahren erschlossen werden können.

Die Frage muß daher auch unter dem Gesichtspunkt der aufgrund des Bundesdatenschutzgesetzes bzw. der Novelle des Bundesdatenschutzgesetzes vorgesehenen Kontrollmöglichkeiten für die Datenverarbeitung in Akten gesehen werden. Hier schränkt § 19 Abs. 6 der Novelle zum BDSG i. V. m. Abs. 4 Nr. 1 BDSG-E die Kontrollmöglichkeit unter dem Vorbehalt ein, daß im Einzelfall nicht von der zuständigen obersten Behörde festgestellt wird, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Das Gesetz sollte eine Überprüfungsmöglichkeit dieser Entscheidung durch ein anderes Gremium vorsehen.

Angesichts der bereits jetzt bestehenden Möglichkeiten, mit Hilfe des automatisierten Verfahrens (NADIS) auch komplexe Aktensammlungen gezielt zu erschließen, ist nicht zu erkennen, warum nicht die Vorschriften über die Speicherung, Veränderung und sonstige Nutzung personenbezogener Daten nicht auch auf Akten Anwendung finden sollen.

17. Speicherung von Daten unverdächtiger Bürger

Für die Zulässigkeit der Speicherung gilt § 7 des Entwurfes. Keine der in Nrn. 1 bis 3 getroffenen Regelungen gibt hinreichend deutlich zu erkennen, daß damit auch eine Speicherung unverdächtiger Bürger beabsichtigt ist. So ist allgemein bekannt, daß sicherheitsüberprüfte Personen, die ja zunächst einmal per se unverdächtig sind, in Datensammlungen personenbezogen gespeichert sind. Die Regelung des § 7 Abs. 1 Nr. 3 macht dies nicht hinreichend deutlich, obwohl es sowohl dem Betroffenen einsichtig sein würde, daß so verfahren wird, wie auch kein Grund ersichtlich ist, dies nicht in einer Regelung deutlich zu machen.

Weitere denkbare Möglichkeiten der Speicherung von Daten unverdächtiger Bürger sind etwa im Bereich der Opfer und der Hinweisgeber zu sehen. Auch hier sind die in § 7 getroffenen Regelungen nicht hinreichend deutlich. Es wird daher empfohlen, die Anforderungen an die Speicherung solcher Personenkreise gesetzlich näher zu regeln und dabei nach Personenkreisen und Anlässen zu differenzieren.

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 24./25. November 1986

Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren

Das Strafprozeßrecht enthält in wesentlichen Bereichen noch keine den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügenden Vorschriften über den Umgang mit personenbezogenen Daten. Die nachfolgenden Überlegungen haben eine Zusammenstellung der Themenbereiche zum Gegenstand, in denen die Schaffung geeigneter Rechtsgrundlagen zum Schutze des Persönlichkeitsrechts der Betroffenen geboten erscheint und formulieren zugleich auch inhaltliche Kriterien, an denen die neuen Vorschriften zu messen sein werden. Die Regelungsvorschläge sollen den Strafverfolgungsorganen die verfassungsrechtlich gebotenen Rechtsgrundlagen verschaffen, die sie für eine wirksame Aufgabenerfüllung benötigen.

Die jetzige Rechtssituation verlangt eine Ergänzung der Strafprozeßordnung um Vorschriften, die bei ihren Regelungen die Datenverarbeitung sowohl in Akten als auch in Dateien berücksichtigen. Bislang bestehende Unsicherheiten bei der Datenverarbeitung im Strafverfahren, die darauf beruhen, daß in der Paxis der Informationsverarbeitung eine deutliche Abgrenzung zwischen den Befugnissen und Verantwortlichkeiten der Justizverwaltung, der Richter, der Staatsanwaltschaft und der Polizei nicht immer möglich ist, müssen beseitigt werden.

Darüber hinaus sollten langfristig weitere Überlegungen angestellt werden, wie der Strafprozeß dem modernen Rechts- und Verfassungsverständnis angepaßt werden kann. Die Datenschutzbeauftragten begrüßen in diesem Zusammenhang die neuen Regelungen zur besseren Wahrung der schutzwürdigen Belange des Verletzten im Strafverfahren. Sie verweisen ferner auf die seit langem geführte Diskussion über eine Umgestaltung der Hauptverhandlung in Strafsachen nach den Grundsätzen des sog. Schuldinterlokuts. Unter dem Gesichtspunkt des Persönlichkeitsschutzes wäre es z. B. sehr zu begrüßen, wenn Feststellungen, die den persönlichen Lebensbereich des Angeklagten berühren, erst dann getroffen und insbesondere in öffentlicher Verhandlung erörtert würden, wenn klar wird, daß sie für die richterliche Entscheidung auch erforderlich sind.

Besondere Aufmerksamkeit verdient die Überlegung, eine Generalklausel zur Datenverarbeitung in die Strafprozeßordnung einzuführen. Im Hinblick auf die Risiken einer extensiven Auslegung derartiger Befugnisnormen sollte grundsätzlich am sicher gehaltenen Prinzip des gesetzlich präzise beschriebenen Einzeleingriffs festgehalten und die Strafprozeßordnung auch zukünftig von Generalklauseln freigehalten werden. Eine solche Vorschrift kann allenfalls als engbegrenzte Auffangregelung in Betracht kommen.

1. Befugnisse im Ermittlungsverfahren

Die verschiedenen Phasen der Informationsgewinnung und -verarbeitung durch die Staatsanwaltschaft und die Polizei zu Zwecken der Strafverfolgung bedürfen einer grundlegenden Überarbeitung und ergänzender gesetzlicher Regelungen.

1.1 Befugnisnormen für die Informationserhebung

Voraussetzungen und Umfang der Erhebung von Daten bei der Vernehmung von Beschuldigten und Zeugen im Rahmen des Strafverfahrens sind im Gesetz zu präzisieren. Dabei ist zwischen der Erhebung der Personalien (Identitätsfeststellung) und der Vernehmung zur Sache und zur Person im übrigen zu unterscheiden. Entsprechende Korrekturen sind daher in den §§ 68, 69, 136 und 163 b StPO vorzunehmen (vgl. z. B. Ziffer 2.3).

1.2 Gesetzliche Regelungen der Fahndungsmaßnahmen im Strafverfahren

Bei der Fahndung nach Beschuldigten und Zeugen werden personenbezogene Daten erhoben, gespeichert und übermittelt. Hierfür sind normenklare Rechtsgrundlagen zu schaffen. § 131 StPO ist entsprechend zu ergänzen. Die Anordnung einer Fahndungsmaßnahme ist grundsätzlich dem Staatsanwalt vorzubehalten.

a) Ausschreibung des Beschuldigten zur Festnahme

Die Fahndung nach dem Beschuldigten zum Zwecke der Festnahme kann grundsätzlich nur zugelassen werden, wenn ein vollziehbarer Haft- oder Unterbrin-

gungsbefehl vorliegt. Ausnahmen werden über § 131 Abs. 2 StPO hinaus nur möglich sein, wenn zumindest die Voraussetzungen eines Haft- oder Unterbringungsbefehls vorliegen und wenn Gefahr im Verzug besteht (vgl. § 127 Abs. 2 StPO). In diesen Fällen ist stets unverzüglich eine Entscheidung über den Erlaß eines Haft- oder Unterbringungsbefehls herbeizuführen. Wird der Antrag abgelehnt oder kann über den Antrag kurzfristig nicht entschieden werden, ist die Fahndungsmaßnahme sofort wieder aufzuheben.

Art und Umfang der zulässigen Fahndungsmaßnahmen nach dem Beschuldigten sind auf der Grundlage des Verhältnismäßigkeitsprinzips gesetzlich festzulegen.

Im einzelnen sind hierbei insbesondere zu unterscheiden:

— örtliche Fahndung

— überörtliche Fahndung

— internationale Fahndung.

Auf überörtliche Fahndungsmaßnahmen nach dem Beschuldigten ist zu verzichten, wenn eine gezielte Fahndung vor Ort mit hoher Wahrscheinlichkeit zum Erfolg führen wird. Eine internationale Fahndung nach dem Beschuldigten ist nur anzuordnen, wenn und soweit gesichert ist, daß die Staatsanwaltschaft im Falle einer Festnahme des Beschuldigten ein Auslieferungsersuchen anregen wird. Im übrigen sind bei der Abwägung nach dem Verhältnismäßigkeitsgrundsatz hier die voraussichtliche Dauer der Auslieferungshaft des Beschuldigten im Festnahmeland sowie die dort herrschenden Haftbedingungen angemessen zu berücksichtigen.

Der Inhalt des Fahndungsersuchens ist gesetzlich zu beschreiben. Maßstab für die Erforderlichkeit der Datenübermittlung ist § 131 Abs. 3 StPO.

b) Ausschreibung des Beschuldigten zur Aufenthaltsermittlung

Die Fahndung nach dem Beschuldigten zum Zwecke der Aufenthaltsermittlung kann zugelassen werden, wenn der Beschuldigte unbekannten Aufenthalts ist und das Ermittlungsverfahren nicht auch ohne seine Anhörung abgeschlossen werden kann (§ 163 a Abs. 1 StPO).

Art und Umfang der zulässigen Fahndungsmaßnahmen sind nach dem Grundsatz der Verhältnismäßigkeit gesetzlich festzulegen. Der Inhalt des Fahndungsersuchens ist auf eine Bezeichnung und Beschreibung des Beschuldigten zu begrenzen.

c) Ausschreibung von Zeugen zur Aufenthaltsermittlung

Die Fahndung nach einem Zeugen zum Zwecke der Aufenthaltsermittlung kann zugelassen werden, wenn der Zeuge unbekannten Aufenthalts ist und die Maßnahme in einem angemessenen Verhältnis zur Bedeutung der Angelegenheit, insbesondere zur Bedeutung seiner möglichen Aussage und der Möglichkeit einer Aussageverweigerung steht.

Art und Umfang der zulässigen Fahndungsmaßnahmen sind unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich festzulegen.

Das Fahndungsersuchen kann neben einer Bezeichnung und Beschreibung des Zeugen auch einen Hinweis auf die Umstände (Straftat) enthalten, zu denen der Zeuge vernommen werden soll. Eine Benennung des Beschuldigten ist in diesem Zusammenhang nicht zulässig.

d) Öffentlichkeitsfahndung

Die Fahndung nach Beschuldigten oder Zeugen unter Inanspruchnahme von Publikationsorganen darf angesichts des damit verbundenen intensiven Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen nicht auf die allgemeinen Rechtsgrundlagen für die Fahndung gestützt werden, sondern bedarf einer eigenständigen gesetzlichen Regelung.

e) Befugnisnormen für besondere Fahndungsmethoden und den Einsatz technischer Mittel

Die nachfolgend genannten Fahndungsmethoden sind mit erheblichen Gefahren für das informationelle Selbstbestimmungrecht der Betroffenen verbunden. Die Voraussetzungen für eine Datenerhebung sowie für die weitere Verwertung

der gewonnenen Daten sind deshalb besonders präzise und unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Einige der aufgeführten Fahndungsmethoden sollten von vornherein nur zur Verfolgung besonders schwerer, enumerativ zu bezeichnender Straftaten zugelassen werden.

Im einzelnen sind folgende Grundsätze zu beachten:

aa) Rasterfahndung

Der Abgleich mit öffentlichen und privaten Datenbeständen zum Zwecke der Rasterfahndung bedarf einer gesetzlichen Grundlage. Dabei sind die verschiedenen zulässigen Möglichkeiten von Datenabgleichen zu beschreiben und unter Berücksichtigung der dabei verwendeten Verfahren getrennt zu regeln.

Der Umfang der für den Abgleich vorgesehenen Daten sollte auf Name, Anschrift, Geburtsdatum und auf im Einzelfall besonders festzulegende Merkmale begrenzt werden. Die Vorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

Die Herausgabe von Datenbeständen darf nur verlangt werden, wenn Tatsachen die Annahme rechtfertigen, daß der Datenabgleich zur Ergreifung des Täters oder zur Aufklärung der Straftaten führt und die Aufklärung ohne diese Maßnahme aussichtslos oder wesentlich erschwert wäre.

Der Datenabgleich findet grundsätzlich bei der zur Herausgabe verpflichteten Stelle unter Aufsicht der Staatsanwaltschaft statt. Von der zur Herausgabe verpflichteten Stelle ist hierzu ein separierter Datenbestand zu erstellen, der nur die vorgenannten Daten enthalten darf. Beim Abgleich müssen technische Verfahren verwendet werden, die sicherstellen, daß eine unberechtigte Kenntnisnahme durch Dritte verhindert wird.

Der Einsatz der Rasterfahndung ist auf die Strafverfolgung bei besonders schwerwiegenden Straftaten, die enumerativ aufzuführen sind, zu beschränken.

Die Rasterfahndung sollte wegen ihrer weitreichenden Wirkung nur durch ein Gericht angeordnet werden. Ein Antrag auf richterliche Anordnung sollte nur gestellt werden dürfen, wenn der Generalstaatsanwalt diesem zugestimmt hat.

Zeigt sich, daß der Zweck eines Abgleiches nicht erreicht werden kann, ist die Rasterfahndung abzubrechen und alle im Zusammenhang mit der Maßnahme angefallenen Unterlagen sind sofort zu vernichten. Nach Durchführung des Abgleichs sind angefallene Unterlagen, die für die weiteren Ermittlungen nicht mehr benötigt werden, umgehend zu vernichten. Daten und Unterlagen über Betroffene, gegen die nach konventioneller Ermittlung der gewonnenen Hinweise keine weiteren Verdachtsmomente festgestellt werden können, sind ebenfalls unverzüglich zu vernichten.

Die durch die Rasterfahndung gewonnenen Daten dürfen nur für Zwecke der Strafverfolgung genutzt werden; eine Nutzung in anderen Strafverfahren ist nur zulässig, wenn es sich dabei um Straftaten handelt, für die die Anordnung der Rasterfahndung ebenfalls möglich wäre. Diese Nutzung für ein anderes Verfahren darf nach Zustimmung des Generalstaatsanwaltes nur durch ein Gericht angeordnet werden.

Die nach Durchführung des Datenabgleiches von gezielten Ermittlungsmaßnahmen betroffenen Personen sind hiervon zu unterrichten, sobald dies ohne Gefährdung des Untersuchungszweckes geschehen kann.

Der jeweils zuständige Datenschutzbeauftragte des Bundes oder des Landes ist nach Beendigung der Maßnahme zu unterrichten.

bb) Spurendokumentationssysteme (SPUDOK) und andere entsprechende automatisierte Sammlungen und Suchsysteme

Automatisierte Dateien, die zur Unterstützung strafrechtlicher Ermittlungsverfahren durch temporäre Dokumentation und Recherche von Hinweisen, Ermittlungsergebnissen oder Spuren im weitesten Sinne in beliebiger Datenstruktur geführt werden (z. B. SPUDOK-Datei), dürfen bei der Polizei längstens bis zum Abschluß der Ermittlungen aufbewahrt werden; sie sind

nach Abschluß der Ermittlungen der Staatsanwaltschaft als Beweismittel zu übergeben und dürfen danach nur noch für die Zwecke des betreffenden Strafverfahrens verwendet werden.

Durch die Automatisierung darf keine unangemessene Verkürzung oder Verzerrung des Sachverhalts entstehen.

Personenbezogene Informationen in SPUDOK-Dateien sind in regelmäßigen Abständen, mindestens jedoch alle 6 Monate auf ihre Erforderlichkeit zu überprüfen. Die Daten sind zu löschen, wenn sich die Spur als falsch herausgestellt hat. Die Daten in diesen Dateien dürfen nur für die Zwecke verwendet werden, zu denen sie angelegt wurden. Es ist festzulegen, ob und inwieweit die gewonnenen Daten zur Verfolgung anderer Straftaten verwendet werden dürfen. Personenbezogene Daten von Anzeigeerstattern, Hinweisgebern, Zeugen und Geschädigten sowie von „anderen Personen" sind als solche zu kennzeichnen. Jede Speicherung in einer SPUDOK ist aktenmäßig zu belegen.

Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, daß der Abruf der Daten nur den Bediensteten möglich ist, die hierfür im Einzelfall zuständig sind.

cc) Informationserhebung im Rahmen polizeilicher Beobachtung

Die polizeiliche Beobachtung, die planmäßige Observation und die Überwachung mit technischen Mitteln sollten in getrennten Vorschriften geregelt werden.

Der einer Straftat Verdächtige darf zur polizeilichen Beobachtung in einem Informationssystem mit Direktabrufverfahren ausgeschrieben werden, wenn bestimmte Tatsachen den Verdacht begründen, daß eine besonders schwerwiegende enumerativ bezeichnete Straftat begangen oder ihre Begehung in strafbarer Weise verursacht worden ist. Die Ausschreibung ist nur zulässig, wenn Tatsachen die Annahme rechtfertigen, daß die Zusammenführung und Sammlung der aufgrund der Ausschreibung erlangten Erkenntnisse über das Antreffen der Person und etwaiger Begleitpersonen sowie mitgeführter Sachen zur Aufklärung der Straftat oder zur Ergreifung des Täters führen und die Aufklärung ohne diese Maßnahme aussichtslos oder wesentlich erschwert wäre. Eine Anordnung der polizeilichen Beobachtung gegen Unverdächtige ist auszuschließen. Die Wirksamkeit der Anordnung ist gesetzlich zu befristen.

Eine Verwertung der im Rahmen polizeilicher Beobachtung gewonnenen Daten in anderen Verfahren ist nur zur Verfolgung von solchen Straftaten zulässig, die ebenfalls die Anordnung dieser Fahndungsmaßnahmen rechtfertigen können.

Die Anordnung darf nur durch die Staatsanwaltschaft getroffen werden. Eine Anordnungsbefugnis für Hilfsbeamte der Staatsanwaltschaft ist wegen der Langfristigkeit der Maßnahme nicht vorzusehen. Die Verlängerung der Maßnahme einer polizeilichen Beobachtung ist unter den Vorbehalt generalstaatsanwaltschaftlicher Genehmigung zu stellen.

Auch die Informationserhebung im Rahmen der planmäßigen Observation bedarf einer besonderen gesetzlichen Grundlage. Sie darf nur angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, daß besonders schwerwiegende Straftaten, die enumerativ aufzuführen sind, oder Straftaten der organisierten Kriminalität begangen oder ihre Begehung in strafbarer Weise versucht worden ist und Tatsachen die Annahme rechtfertigen, daß die aufgrund der Observation erlangten Erkenntnisse zur Aufklärung der Straftat oder zur Ergreifung des Täters führen und die Aufklärung ohne diese Maßnahme aussichtslos oder wesentlich erschwert wäre. Eine Anordnung gegen Personen, die der Straftat nicht verdächtig sind, ist auszuschließen. Die planmäßige Observation darf nur vom Richter angeordnet werden. Es ist gesetzlich festzulegen, daß die Wirksamkeit der Anordnung zu befristen ist. Eine Verwertung der gewonnenen Daten ist nur zum Zwecke der Verfolgung von Straftaten zulässig, die die Anordnung der Fahndungsmaßnahme rechtfertigen können.

Bei der Anordnung einer Überwachung mit technischen Mitteln sind neben den Vorschriften für die planmäßige Observation auch die Vorschriften über den Einsatz technischer Mittel zu beachten.

dd) Befugnis zur erkennungsdienstlichen Behandlung

§ 81 b 1. Alternative StPO ist zu präzisieren, und sein Verhältnis zu § 163 b StPO ist normenklar abzugrenzen. § 81 b 2. Alternative StPO ist zu streichen; eine entsprechende Regelung ist in den Polizeigesetzen vorzusehen.

Erkennungsdienstliche Unterlagen, die für den Zweck der Durchführung des Strafverfahrens notwendig sind, sind zu vernichten, sobald die Identität des Betroffenen festgestellt ist und die Unterlagen nicht mehr für das jeweilige Strafverfahren erforderlich sind, sofern die Aufbewahrung nicht aufgrund anderer Rechtsvorschriften zulässig ist.

In § 111 Abs. 3 StPO (Straßenkontrollen) ist deutlicher darauf hinzuweisen, daß für § 111 StPO die Regelung von § 163 b Abs. 2 StPO gilt, wonach Nichtverdächtige nicht gegen ihren Willen erkennungsdienstlich behandelt werden dürfen.

ee) Informationserhebung in Versammlungen zu Zwecken der Strafverfolgung

Die Datenerhebung in Versammlungen ist wegen des Eingriffs in die Grundrechte der Versammlungsfreiheit und der freien Meinungsäußerung besonders zu regeln. Als Ansatzpunkte differenzierter Regelungen sind der Ort der Versammlung (geschlossener Raum oder im Freien) und die Art der Erhebung (offene oder verdeckte Ermittlung) zu beachten. Die Teilnahme an Versammlungen ist durch geeignete gesetzliche Regelungen vor allgemeinen Datenerhebungen zu schützen; soweit zunächst nicht zu verhindern ist, daß Daten Unbeteiligter oder Unverdächtiger gespeichert werden, sind diese unverzüglich zu löschen.

ff) Einsatz lesender oder mithörender technischer Geräte und Bildaufzeichnungen/Video

Der Einsatz technischer Mittel zu Zwecken der Strafverfolgung bedarf einer gesonderten rechtlichen Behandlung. Der Einsatz technischer Mittel stellt in der Regel einen zusätzlichen Eingriff in das informationelle Selbstbestimmungsrecht dar. Wie die Regelung z. B. in § 100 a StPO zeigt, darf nicht jede Straftat mit jedem technischen Mittel verfolgt werden. Soweit bei Nutzung des Btx-Systems der Bundespost oder anderer sog. Neuer Medien angefallene Daten in die Fahndung mit einbezogen werden sollen, bedarf es hierfür eigener enger gesetzlicher Regelungen.

Die Verwendung von Abhörgeräten und die heimliche Aufnahme des in der Öffentlichkeit gesprochenen Wortes auf Tonträger ist nur zulässig, wenn dies zur Aufklärung einer der (in Anlehnung an § 100 a StPO) enumerativ aufzuführenden Straftaten erforderlich ist. Die heimliche Aufzeichnung beweglicher Bilder ist ebenfalls gesetzlich zu begrenzen. Die Verwertung der gewonnenen Daten zur Verfolgung anderer Straftaten ist entsprechend gesetzlich zu beschränken.

Das Erheben von Daten mit technischen Hilfsmitteln aus oder in Wohnungen berührt Artikel 13 GG und ist nur unter engeren Voraussetzungen als die Anordnung der Hausdurchsuchung vorzusehen. Soweit Daten mit technischen Mitteln aus oder in Wohnungen erhoben werden sollen, sind nicht nur Verfahrensregelungen zu treffen, vielmehr sind im Gesetz die in Betracht kommenden Fälle genau zu beschreiben. Anhaltspunkte dafür können die besondere Schwere oder die besondere technische Begehungsform einer Straftat sein. Eine solche Datenerhebung mit technischen Mitteln ist darüber hinaus nur dann angemessen, wenn Tatsachen die Annahme rechtfertigen, daß durch Einsatz solcher Geräte die Tat nachgewiesen werden kann.

gg) Informationserhebung durch Inanspruchnahme von Informanten oder durch den Einsatz von V-Personen und verdeckten Ermittlern

Werden im Zuge der Strafverfolgung Informationen durch Informanten gegen die Zusicherung der Vertraulichkeit oder durch den Einsatz von V-Personen und verdeckten Ermittlern erhoben, so ist hierfür wegen der Gefahren für die Rechte des Beschuldigten, insbesondere wegen seines Anspruchs auf rechtliches Gehör, ebenfalls eine normenklare gesetzliche Regelung erforderlich. Zum Schutze des Betroffenen sind Voraussetzungen und Inhalt des verdeckten Tätigwerdens der Ermittlungsorgane gesetzlich genau zu beschreiben. Außerdem ist im Gesetz ein angemessener Ausgleich

zwischen dem Recht des Informanten (Datenlieferanten) auf Vertraulichkeit oder Geheimhaltung und dem Recht des Betroffenen auf ein faires, rechtsstaatliches Verfahren (Artikel 2 Abs. 1 GG i. V. m. Artikel 20 Abs. 3 GG) zu finden.

— Die Informationserhebung durch Einsatz von V-Personen und die Inanspruchnahme von Informanten kann im Bereich der Schwerkriminalität, der organisierten Kriminalität und der schweren Staatsschutzdelikte zugelassen werden. Im Bereich der mittleren Kriminalität ist eine besonders gründliche Prüfung des Einzelfalles geboten.

— Die Informationserhebung durch den Einsatz von verdeckten Ermittlern bedarf ebenfalls einer besonders sorgfältigen Einzelfallprüfung. Die Informationserhebung ist auf enumerativ aufgeführte Tatbestände der Schwerkriminalität zu begrenzen. Es sollte überprüft werden, ob für diese Fälle ggf. ein Verwertungsverbot eingeführt werden sollte.

Die Informationserhebung durch Inanspruchnahme von Informanten und Einsatz von V-Personen sowie verdeckten Ermittlern sollte nur zugelassen werden, wenn die Aufklärung der Straftat sonst aussichtslos wäre.

Die Entscheidung über den Einsatz von V-Personen sowie verdeckten Ermittlern trifft die Staatsanwaltschaft. Bei Gefahr im Verzuge kann die Anordnung auch von ihren Hilfsbeamten (§ 152 Gerichtsverfassungsgesetz) getroffen werden; die Genehmigung der Staatsanwaltschaft ist in diesem Falle unverzüglich nachzuholen. Beim Einsatz von verdeckten Ermittlern ist wegen des Ausnahmecharakters die Zustimmung des Leiters der Staatsanwaltschaft vorzusehen.

Um rechtswidrige Praktiken von V-Leuten und verdeckten Ermittlern zu unterbinden, sind im Gesetz die Grenzen des zulässigen Einsatzes festzulegen. Es ist ferner klarzustellen, daß alle gesammelten Informationen (§ 163 StPO) schriftlich festgehalten werden. Werden im Zuge der weiteren Ermittlungen die durch Informanten, V-Personen und verdeckte Ermittler gewonnenen Ersterkenntnisse (sog. „Basisermittlungen") durch eigene weitere Ermittlungen (Maßnahmen) der Polizei zum Beweis verdichtet, der an sich einen Rückgriff auf diese Personen erübrigt, so sind gleichwohl die Basisinformationen (Ermittlungsansatz) schriftlich niederzulegen. Eine Abtrennung dieser Informationserhebungen bei der Polizei ist auszuschließen.

Die geheimzuhaltenden Tatsachen und Erkenntnisse sind der Staatsanwaltschaft zu übermitteln und dabei deutlich als solche zu kennzeichnen. Solange die Zusicherung der Vertraulichkeit/Geheimhaltung nicht weggefallen ist, hat die Staatsanwaltschaft diese Informationen in gesonderten Akten aufzubewahren. Hierauf sind das Gericht bei Vorlage der Akten und die Verteidigung nach Abschluß der Ermittlungen unverzüglich hinzuweisen.

1.3 Allgemeine Befugnisnorm für die Speicherung und sonstige Verwendung von Daten

Die Staatsanwaltschaft darf grundsätzlich personenbezogene Daten speichern und sonst nutzen, die rechtmäßig erhoben worden sind und deren Speicherung zur Erfüllung ihrer durch Rechtsnorm zugewiesenen Aufgaben erforderlich ist. Die Verwertung von Daten, die unter Verstoß gegen ein Beweiserhebungsverbot erlangt worden sind, ist nur aufgrund einer ausdrücklichen gesetzlichen Bestimmung zulässig.

1.4 Gesetzliche Regelungen für die Nutzung und die Weitergabe von Daten

a) Allgemeine Regelungen für die Datenweitergabe im Verhältnis Staatsanwaltwaltschaft/Polizei

aa) Weitergabe von Daten durch die Polizei an die Staatsanwaltschaft:

Die Polizei gibt alle Daten, die sie zur Aufklärung von Straftaten im Wege des ersten Zugriffs oder aufgrund eines staatsanwaltschaftlichen Ermittlungsauftrages erhoben hat, ohne Verzug an die Staatsanwaltschaft weiter (§§ 161 Satz 2, 163 Abs. 2 StPO). Im übrigen hat die Polizei Daten an die Staatsanwaltschaft weiterzugeben, die zur rechtmäßigen Erfüllung staatsanwaltschaftlicher Aufgaben vor Einleitung des Ermittlungsverfahrens erforderlich sind. Eine entsprechende gesetzliche Grundlage ist zu schaffen. Hierin ist auch zu regeln, ob und ggf. welche der im Rahmen der Strafverfolgung angefallenen Unterlagen bei der Polizei verbleiben dürfen.

Gibt die Polizei Erkenntnisse, die nicht im konkreten Ermittlungsverfahren gewonnen worden sind, an die Staatsanwaltschaft weiter, ist sie für die Zulässigkeit der Weitergabe verantwortlich. Geschieht die Weitergabe auf Veranlassung der Staatsanwaltschaft, trifft diese die Verantwortung für die Zulässigkeit.

Die Tatsache der Weitergabe ist zu dokumentieren. Ergibt sich später eine Änderung wesentlicher Gesichtspunkte, so ist die Staatsanwaltschaft unverzüglich hiervon zu unterrichten.

bb) Weitergabe von Daten durch die Staatsanwaltschaft an die Polizei

Soweit dies zur rechtmäßigen Erfüllung ihrer Aufgaben als Ermittlungs- und Vollstreckungsbehörde, insbesondere im Rahmen der Erteilung von Ermittlungsaufträgen erforderlich ist, kann die Staatsanwaltschaft personenbezogene Einzeldaten an die Polizei weitergeben. Die Weitergabe bedarf einer normenklaren Rechtgrundlage.

Die Erteilung von Ermittlungsaufträgen kann mit der Übersendung bisher angefallener Akten oder von Aktenteilen verbunden werden, soweit die Kenntnis der Sachzusammenhänge zur Erledigung des Auftrages notwendig erscheint und dadurch nicht im Einzelfalle schutzwürdige Belange Betroffener unverhältnismäßig beeinträchtigt werden.

Die Verantwortung für die Zulässigkeit der Datenweitergabe trägt die Staatsanwaltschaft, die den Vorgang auch zu dokumentieren hat.

b) Weitergabe von Daten zwischen Staatsanwaltschaften

Die Staatsanwaltschaft kann personenbezogene Einzeldaten an eine andere Staatsanwaltschaft weitergeben, soweit dies zur rechtmäßigen Erfüllung ihrer Aufgaben als Ermittlungs- und Vollstreckungsbehörde oder zur rechtmäßigen Erfüllung der entsprechenden Aufgaben der anderen Staatsanwaltschaft erforderlich ist. Hierfür ist eine gesetzliche Grundlage zu schaffen.

Die Weitergabe der Daten kann auch durch Übersendung der Akten oder von Aktenteilen erfolgen, soweit zur Erfüllung der Aufgaben die Kenntnis der Sachzusammenhänge nötig erscheint und dadurch nicht im Einzelfalle schutzwürdige Belange Betroffener unverhältnismäßig beeinträchtigt werden.

Das Ersuchen um Datenweitergabe ist von der anfordernden Staatsanwaltschaft schriftlich zu begründen. Die Verantwortung für die Zulässigkeit der Weitergabe trägt die abgebende Staatsanwaltschaft.

Die Tatsache der Datenweitergabe ist zu dokumentieren. Über Änderungen wesentlicher Gesichtspunkte ist die Empfängerbehörde unverzüglich zu unterrichten.

c) Informationssysteme zur Strafverfolgung, zentrale Namensdateien und Aktennachweissysteme

Die Errichtung und Nutzung von Informationssystemen zur Strafverfolgung bedürfen einer gesetzlichen Regelung, die den verfassungsrechtlichen Grundsätzen der Verhältnismäßigkeit und Normenklarheit entspricht. Dabei hat der Gesetzgeber auch sicherzustellen, daß der Polizei und der Staatsanwaltschaft nur die Datenbestände zur Verfügung stehen, die für ihre jeweiligen Aufgaben erforderlich sind. In diesem Zusammenhang ist es notwendig, die vorhandenen polizeilichen und die geplanten staatsanwaltschaftlichen Informationssysteme im Hinblick auf die Erforderlichkeit, Datenstrukturierung und die verschiedenen Verantwortlichkeiten zu überprüfen. Die Datenschutzbeauftragten werden hierzu gesondert Stellung nehmen.

Anders als bei umfangreichen Informationssystemen ist bei zentralen Namensdateien und vergleichbaren behördeninternen Aktennachweissystemen eine Regelung hinreichend, die sicherstellt, daß nur Daten verwendet werden, die aus innerhalb dieser Behörde geführten Akten entnommen wurden. Eine Entscheidung der Staatsanwaltschaft darf nicht allein auf der Grundlage des Dateinhaltes getroffen werden.

Die Speicherung weiterer Daten und eine Nutzungserweiterung bedürfen einer spezifischen gesetzlichen Ermächtigung. Im übrigen wird an den Beschluß der

Konferenz der Datenschutzbeauftragten vom 28./29. September 1981 zu den Mindestanforderungen für den Datenschutz bei zentralen Namenskarteien der Staatsanwaltschaften erinnert.

d) Berichtspflichten in Strafsachen (BeStra)

Die Staatsanwaltschaften sind verpflichtet, im allgemeinen oder im Einzelfall bestimmte Strafsachen dem Justizminister/-senator des Landes einen Bericht zu erstatten.

Aus datenschutzrechtlicher Sicht ist zweifelhaft, ob die politische Verantwortlichkeit des Justizministers/-senators und § 147 Nr. 2 GVG eine ausreichende Grundlage für die hier vorgesehenen personenbezogenen Datenübermittlungen sind.

Es ist daher normenklar zu regeln, welche Anlässe Gegenstand einer Meldung sein sollen, wen die Verpflichtung trifft und wie nach Abschluß eines Verfahrens der Vorgang bei den Justizministern/-senatoren zu behandeln ist.

2. Wahrnehmung der Rechte des Beschuldigten, anderer am Verfahren Beteiligter, Dritter und der Öffentlichkeit

2.1 Akteneinsichtsrechte

Die in § 147 StPO getroffenen Regelungen sind ergänzungsbedürftig. Auch die Nummern 185, 185 a der Richtlinien über das Strafverfahren und das Bußgeldverfahren (RiStBV) genügen nicht den Anforderungen der Verfassung, da sie keine Rechtsvorschrift sind; darüber hinaus sind sie nicht normenklar.

Die gesetzliche Neuregelung der Auskunfts- und Akteneinsichtsrechte sollte sich auf die gesamte Strafakte (Verfolgung und Vollstreckung) beziehen.

Strafakten von Staatsanwaltschaften und Gerichten enthalten regelmäßig zahlreiche, z. T. sehr sensitive Daten über eine Vielzahl von Personen. Dementsprechend hat das Bundesverfassungsgericht auch schon in seiner älteren Rechtsprechung (E 27, 344; 34, 206) einer Einsichtnahme von Dritten in Prozeßakten enge Grenzen gezogen.

In keinem Fall dürfen über eine Einsichtnahme in Strafakten besondere Geheimhaltungsbestimmungen unterlaufen werden. Die Einsichtnahme in beigezogene Akten kann in der Regel nur mit Genehmigung der Ausgangsbehörde gestattet werden.

a) Akteneinsicht für öffentliche Stellen

Gerichte, Staatsanwaltschaften, Behörden und andere öffentliche Stellen sollten Akteneinsicht oder -vorlage nur bei Darlegung eines rechtlichen Interesses und nur für gesetzlich präzise umschriebene, eigene Zwecke beanspruchen können. Der Wertungsmaßstab des Bundeszentralregistergesetzes ist zu berücksichtigen.

Die hierbei erlangten Informationen dürfen nur zu dem Zweck verwendet werden, zu dem sie befugt offenbart worden sind (vgl. § 78 Satz 1 SGB X). Eine Weitergabe an dritte Stellen ist auszuschließen.

In der Regel ist eine Einzelauskunft ausreichend; für eine Übersendung der gesamten Akten ist ein besonderes rechtliches Interesse erforderlich.

b) Akteneinsicht durch die Verteidigung

Das Akteneinsichtsrecht des Verteidigers (§ 147 StPO) ist durch eine genauere Regelung der Nutzung und der Informationsweitergabe aus den Strafakten zu ergänzen. Eine Weitergabe von Informationen an den Beschuldigten ist unzulässig, wenn dadurch der Untersuchungszweck gefährdet wird. Eine Aushändigung der Originale von Aktenbestandteilen an den Beschuldigten ist stets unzulässig. Der Verteidiger ist namentlich bei der Herausgabe von Kopien für die Wahrung der Persönlichkeitsrechte Dritter verantwortlich.

c) Akteneinsicht durch den verteidigerlosen Beschuldigten

Dem verteidigerlosen Beschuldigten sollte zu einer wirksamen Verteidigung ein gesetzlicher Auskunftsanspruch zuerkannt werden, wenn er sich ohne Aktenkenntnis nicht angemessen verteidigen kann und der Untersuchungszweck durch die Auskunft nicht gefährdet wird.

Nach rechtskräftigem Abschluß des Hauptverfahrens oder der Einstellung des Ermittlungsverfahrens sollte jeder Beschuldigte auch ohne Vertretung durch einen Rechtsanwalt Einsicht in seine Strafverfahrensakte erhalten. Hierbei hat die einsichtgewährende Stelle die berechtigten Interessen des Beschuldigten gegen die schutzwürdigen Belange betroffener Dritter abzuwägen. Auf jeden Fall ist dem Beschuldigten Auskunft aus den zentralen Namensdateien und Aktennachweissystemen zu erteilen.

d) Akteneinsicht durch Privat- und Nebenkläger oder durch Rechtsanwälte zur Geltendmachung von Ansprüchen Dritter

Auch im Fall des Privat- und Nebenklägers sollte grundsätzlich am Anwaltszwang bei der Akteneinsicht (§§ 385, 397 StPO) festgehalten werden, da der Rechtsanwalt eine größere Gewähr für die Wahrung der Persönlichkeitsrechte Dritter bietet.

Die Gewährung von Akteneinsicht für Rechtsanwälte, die mit der Geltendmachung zivil- oder öffentlich-rechtlicher Ansprüche oder der Wahrnehmung sonstiger rechtlicher Interessen beauftragt sind, greift in das Recht auf informationelle Selbstbestimmung ein. Die Akteneinsicht ist deshalb gesetzlich streng zu regeln und darf sich nicht auf den gesamten Akteninhalt erstrecken, sondern nur auf den Teil, dessen Kenntnis für die Prüfung der geltend gemachten Ansprüche erforderlich ist. Der Rechtsanwalt ist für die Wahrung der Persönlichkeitsrechte Dritter verantwortlich; er hat die Zweckbindung der Daten bei Dritten sicherzustellen.

Selbst dem Rechtsanwalt darf bei der Geltendmachung von Ansprüchen oder im Fall der Privat- bzw. Nebenklage keine Akteneinsicht gewährt werden, wenn eine Beeinträchtigung überwiegender Interessen Dritter nicht ausgeschlossen werden kann.

Zur Wahrung anderer als rechtlicher Interessen darf keine Akteneinsicht gewährt werden.

e) Akteneinsicht für wissenschaftliche Zwecke

Auch die Verwendung von Informationen zu Zwecken wissenschaftlicher Forschung, die in Strafakten und Dateien gespeichert werden, bedarf einer normenklaren Eingriffsermächtigung in der Strafprozeßordnung.

Bei einer gesetzlichen Regelung ist grundsätzlich von folgendem auszugehen:

— Personenbezogene Angaben dürfen für ein Forschungsvorhaben nur offenbart werden, wenn dieses Forschungsvorhaben nicht auf andere Weise durchgeführt werden kann.

— Eine Einsichtnahme in Akten- bzw. eine Weitergabe personenbezogener Daten — ohne Einwilligung der Betroffenen — kommt nur in Betracht, wenn die Einholung von Einwilligungen unmöglich oder nur unter unverhältnismäßigem Aufwand möglich ist und das Allgemeininteresse an der Durchführung eines bestimmten Forschungsvorhabens das Geheimhaltungsinteresse der Betroffenen erheblich überwiegt. Die Entscheidung dieser Frage ist dem zuständigen Gerichtspräsidenten bzw. dem Leiter der Staatsanwaltschaft vorzubehalten; die Genehmigung kann mit Auflagen versehen werden.

— Die erlangten personenbezogenen Informationen sind von dem Forscher sobald wie möglich zu anonymisieren und dürfen nur zum Zweck eines bestimmten Forschungsvorhabens verwendet werden. Auswertungsergebnisse dürfen nur in anonymisierter Form weitergegeben und veröffentlicht werden.

— Eine Einsichtnahme bzw. Übermittlung ist auf Informationen aus rechtskräftig abgeschlossenen Verfahren zu beschränken.

— Die Einsichtnahme in Akten sollte nur in den Räumen der aktenführenden Dienststelle erfolgen.

2.2 Die Wahrung der Rechte des vom Strafverfahren Betroffenen und am Strafverfahren Beteiligter bei Mitteilungen personenbezogener Angaben durch die Staatsanwaltschaft und Gerichte

Die Strafprozeßordnung und das Jugendgerichtsgesetz enthalten eine Reihe von Vorschriften, die Mitteilungspflichten gegenüber Dritten begründen. Diese Mit-

teilungspflichten bedürfen ebenfalls einer Überprüfung unter datenschutzrechtlichen Gesichtspunkten.

Zur Klarstellung wird darauf hingewiesen, daß die nachfolgend erwähnten prozeßrechtlichen Vorschriften ausschließlich Mitteilungen an solche Personen oder Stellen zum Gegenstand haben, die mittelbar oder unmittelbar vom jeweiligen Verfahren betroffen sind. Es wird daran erinnert, daß die derzeit noch in Verwaltungsvorschriften geregelten Mitteilungen an Personen oder Stellen, die nicht in dieser Form von Strafverfahren betroffen sind (MiStra), ebenfalls der gesetzlichen Regelung bedürfen.

a) Mitteilungen an Anzeigeerstatter

Auf Mitteilungen über die Einstellung eines Ermittlungsverfahrens an den Anzeigeerstatter kann nicht verzichtet werden. Der Umfang der Mitteilung bedarf jedoch der Einschränkung und Präzisierung.

Hinsichtlich des Umfangs der Mitteilungen nach § 171 StPO ist danach zu differenzieren, ob der Anzeigeerstatter gleichzeitig auch Verletzter der Straftat ist oder ob dies nicht der Fall ist. Zur Vermeidung unnötiger Offenbarungen personenbezogener Daten des vom Strafverfahren Betroffenen ist die Mitteilung im zweiten Fall möglichst allgemein zu halten. Der Anzeigeerstatter, der gleichzeitig Verletzter ist, kann dagegen eine weitergehende Mitteilung erhalten, soweit diese zur Wahrnehmung von Beschwerdemöglichkeiten notwendig ist. Im Falle der Einstellung des Ermittlungsverfahrens nach § 154 Abs. 1 StPO darf der dem Anzeigeerstatter von der Staatsanwaltschaft zugehende Bescheid keine näheren Hinweise auf die „andere Tat" enthalten. Unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit kann es im Einzelfall aus Gründen des Persönlichkeitsschutzes erforderlich sein, den Namen des Beschuldigten dem Anzeigeerstatter nicht mitzuteilen.

b) Mitteilungen anläßlich der Überwachung des Post- und Fernmeldeverkehrs

Gemäß § 101 Abs. 1 StPO sind die Beteiligten von Maßnahmen, die zur Überwachung des Postverkehrs (§§ 99, 100 StPO) und des Fernmeldeverkehrs (§§ 100 a, 100 b StPO) getroffen wurden, zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks geschehen kann. § 101 StPO bedarf insoweit der Präzisierung. Der Umfang der Benachrichtigung Dritter ist unter Abwägung der Interessen des Beschuldigten an der Geheimhaltung des gegen ihn gerichteten Strafvorwurfs und der Interessen der betroffenen Dritten an der Überprüfung der gegen sie gerichteten Maßnahme gesetzlich festzulegen. In die Strafprozeßordnung aufzunehmen sind hierzu ferner Löschungsbestimmungen und Verwertungsverbote. Die bei der Gelegenheit der Telefonüberwachung gewonnenen Erkenntnisse können nicht uneingeschränkt, sondern nur zur Verfolgung von Katalogstraftaten nach § 100 a StPO verwertet werden. Die Voraussetzungen von Zweckdurchbrechungen sind gesetzlich zu regeln. In diesem Zusammenhang wird daran erinnert, daß die Weitergabe und Nutzung von Erkenntnissen, die durch Strafverfolgungsmaßnahmen erlangt wurden, für Zwecke außerhalb der Strafverfolgung nur in Ausnahmefällen zugelassen werden darf. Besondere Bedeutung kommt dabei der Regelung der Weitergabe für nachrichtendienstliche Zwecke zu.

c) Mitteilungen bei Durchsuchungen

Gemäß § 103 StPO kann eine Durchsuchung unter bestimmten Voraussetzungen auch bei Dritten vorgenommen werden. Den von einer solchen Maßnahme betroffenen Dritten ist auf Verlangen „der Grund der Durchsuchung" mitzuteilen (§ 107 StPO). Der Umfang der Mitteilung hat sich am Grundsatz der Güterabwägung zu orientieren.

Die Bestimmung des § 108 StPO ist um Verwertungsverbote für sogenannte Bagatelldelikte zu erweitern; insbesondere sollte gesetzlich klargestellt werden, daß eine Weitergabe von Erkenntnissen für Zwecke der Nachrichtendienste, denen die Durchsuchung und Beschlagnahme verwehrt ist, ausgeschlossen wird.

d) Mitteilungen an Behörden und sonstige öffentliche Stellen

Verschiedene Vorschriften (z. B. §§ 138 c Abs. 2, 138 d Abs. 2 StPO, § 70 JGG) sehen Mitteilungen an Behörden und andere öffentliche Stellen vor. Solche Mitteilungen an Verfahrensbeteiligte sind gesetzlich zuzulassen, soweit sie zur

Aufgabenerfüllung erforderlich sind. Umfang, Zweck und Voraussetzungen solcher Mitteilungen sind dabei präzise zu bestimmen.

Soweit Behörden und andere öffentliche Stellen unterrichtet werden sollen, denen am jeweiligen Verfahren keine eigenen Beteiligungsrechte zustehen, ist dies im Zuge der Schaffung gesetzlicher Regelungen zu MiStra (Justizmitteilungsgesetz) zu berücksichtigen.

2.3 Öffentlichkeit und Schutz der Persönlichkeit (§§ 169 ff. GVG); Nennung des Angeklagten durch Aushang im Gericht; Verzicht auf das Verlesen von Papieren in geeigneten Fällen (§ 249 StPO)

Die öffentliche Bekanntgabe der persönlichen Daten eines Angeklagten durch Aushang der Terminsankündigung im Gericht bedarf der gesetzlichen Grundlage. Die Bekanntgabe ist in der Regel auf Vor- und Zuname des Angeklagten und das Aktenzeichen des Verfahrens zu beschränken. Die Angabe persönlicher Daten von Zeugen und Sachverständigen auf der im Gericht aushängenden Terminsankündigung sollte unterbleiben. Die Mitglieder des Gerichts sollten nur mit dem Zunamen aufgeführt werden.

Bei der öffentlichen Zustellung an einen Beschuldigten gemäß § 40 StPO sollen nur die Daten angegeben werden, die für eine ausreichende Identifizierung der Person des Betroffenen und des Gegenstandes der Verhandlung unabdingbar sind. Zu weiteren Einzelheiten ist auf das in der Geschäftsstelle des Gerichts niederzulegende Schriftstück zu verweisen.

Die Pflicht des Zeugen gemäß § 68 Abs. 1 Satz 1 StPO, bei der Vernehmung zur Person stets das „Alter", den „Stand" oder das „Gewerbe" anzugeben, sollte aufgehoben werden.

§ 249 StPO sollte in Fortsetzung der mit dem Strafverfahrensänderungsgesetz 1979 begonnenen Reform dahingehend geändert werden, daß die Verlesung von Urkunden und anderen Beweismitteln im Regelfall unterbleibt und statt dessen der wesentliche Inhalt mitgeteilt wird. Die Verlesung bleibt zulässig, sofern es im Einzelfall das Gericht für erforderlich hält oder die Staatsanwaltschaft, der Nebenkläger, der Angeklagte oder sein Verteidiger es beantragen. Dabei ist die Möglichkeit einer teilweisen Verlesung zu prüfen.

Auch in den Fällen des § 251 Abs. 3 StPO sollte die Verlesung von Urkunden stärker eingeschränkt werden. Für den Regelfall sollte genügen, daß das Gericht den wesentlichen Inhalt der Urkunden für die Entscheidungsfindung wiedergibt.

§ 256 Abs. 1 Satz 1 StPO gesteht seinem Wortlaut nach dem Gericht nur die generelle Abwägung zu, ob es ein Zeugnis oder ein Gutachten verlesen will oder nicht. Dem Gericht sollte auch hier im Gesetz die Möglichkeit eingeräumt werden, bei überwiegendem Persönlichkeitsschutz bestimmte Teile von der Verlesung auszunehmen und sich ggf. auf eine inhaltliche Wiedergabe zu beschränken.

2.4 Auskünfte an die Medien

Für Auskünfte an die Medien durch die Justiz und die Polizei sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen. Vor einer Veröffentlichung sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Insbesondere um eine unnötige Bloßstellung zu vermeiden, sollte festgelegt werden, daß Namen und sonstige Angaben (auch Abkürzungen), die Opfer von Straftaten, Beschuldigte und Angeklagte bestimmbar machen, in Auskünften nicht aufgeführt werden, es sei denn, daß das Verfahren gerade im Hinblick auf die Person des Betroffenen für die Öffentlichkeit von erheblicher Bedeutung ist. Entsprechend sollte auch im Hinblick auf andere Verfahrensbeteiligte (wie Zeugen und Sachverständige) verfahren werden. Besonderer Schutz sollte den Angehörigen gelten, die mit der Straftat nichts zu tun haben. Ein Anspruch der Presse auf Bildherausgabe besteht nicht. Im Strafverfahren gegen Jugendliche und Heranwachsende überwiegt in der Regel das schutzwürdige private Interesse der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten.

2.5 Kontrolle von Gerichtsbesuchern und Speicherung der Daten durch andere Behörden

Die bestehenden gesetzlichen Vorschriften über die Öffentlichkeit der Verhandlung (§§ 169 ff. GVG) sollten klarstellend ergänzt werden:

Der freie Zugang zum Ort der Verhandlung (Verhandlungsraum, Verhandlungsbereich, Verhandlungsgebäude) kann durch Personen- und Ausweiskontrollen beschränkt werden, wenn dies im Einzelfall zur Abwehr von Gefahren für Leib und Leben oder Sachen von erheblicher Bedeutung geboten erscheint. Die erhobenen Daten dürfen nur der zuständigen Polizeidienststelle und nur für den vom Gericht genannten Überprüfungszweck übermittelt und weder dort noch bei anderen Stellen gespeichert werden.

Eine Speicherung durch das Gericht ist nur zulässig, solange noch von den Besuchern eine konkrete Gefahr der genannten Art für das Gerichtsverfahren ausgeht. Nach Beendigung des Besuchs hat das Gericht die Daten zu löschen.

3. Aufbewahrungs- und Löschungsbestimmungen

Die Aufbewahrung und Löschung der Daten sowohl in den Akten als auch in den Dateien muß gesetzlich geregelt werden. Die jetzt geltenden Aufbewahrungsbestimmungen bedürfen einer Überprüfung insbesondere im Hinblick auf die Aufbewahrungsdauer. Die maßgebenden Fristen sollten gekürzt, in jedem Falle aber unter Berücksichtigung des Verfahrensausganges und der Schwere der Tat noch stärker abgestuft werden. Gesondert zu regeln sind die Löschungsbestimmungen für automatisierte Aktennachweissysteme einerseits und für Daten, die in automatisierten Dateien zu Fahndungszwecken (z. B. SPUDOK) geführt werden andererseits.

4. Aussage- und Zeugnisverweigerungsrechte

4.1 Zeugnisverweigerungsrechte für Wissenschaftler

Es ist zu prüfen, ob und inwieweit der besondere Schutz von Berufs- und Amtsgeheimnissen erweitert werden muß, der in der Strafprozeßordnung bislang durch Zeugnisverweigerungsrechte und Beschlagnahmeverbote für die Träger von Berufsgeheimnissen abgesichert ist. Zu berücksichtigen ist dabei insbesondere der Schutz solcher Informationen, die Wissenschaftlern zu Forschungszwecken offenbart worden sind.

4.2 Aussageverweigerung der Datenschutzbeauftragten

Um eine unabhängige Datenschutzkontrolle zu gewährleisten und das Vertrauensverhältnis zwischen dem Bürger und den Datenschutzbeauftragten zu schützen, sollte ein Zeugnisverweigerungsrecht für den Datenschutzbeauftragten (und seine Bediensteten) aufgenommen werden. Dem Datenschutzbeauftragten muß auch in § 96 StPO die Möglichkeit eröffnet werden, selbst über das Herausgabeverlangen von Akten und Unterlagen zu entscheiden und diese zu versagen, soweit dadurch die Erfüllung seiner Aufgaben gefährdet oder erschwert wird. Es ist zu prüfen, ob für die Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich vergleichbare Regelungen getroffen werden müssen.

5. Organisatorische Maßnahmen

Für die Anlage neuer und für die Überprüfung vorhandener personenbezogener Sammlungen muß der Erlaß von Errichtungsanordnungen gesetzlich vorgesehen werden, die Regelungen enthalten über

1. die Bezeichnung, den Zweck und die Rechtsgrundlage der Sammlung,
2. den in die Sammlung aufzunehmenden Personenkreis,
3. die Art und den Umfang der zu speichernden Informationen, die der Erschließung dienen können,
4. die Übermittlung von Informationen,
5. die Dauer der Aufbewahrung der Informationen,
6. die zuständige Stelle für die Anlage und Führung der Sammlung sowie die Zugriffsberechtigten,
7. bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung und Löschung und
8. die getroffenen technischen und organisatorischen Maßnahmen (vgl. § 6 BDSG).

SCHUFA-Klausel für Kontoeröffnungsanträge

Ich/Wir willige(n) ein, daß die Bank der für meinen/unseren Wohnsitz zuständigen SCHUFA-Gesellschaft (Schutzgemeinschaft für allgemeine Kreditsicherung) Daten über die Beantragung, die Aufnahme und Beendigung dieser Kontoverbindung übermittelt.

Unabhängig davon wird die Bank der SCHUFA auch Daten aufgrund nicht vertragsgemäßen Verhaltens (z. B. Scheckkartenmißbrauch durch den rechtmäßigen Karteninhaber, Scheckrückgabe mangels Deckung, Wechselprotest, beantragter Mahnbescheid bei unbestrittener Forderung sowie Zwangsvollstreckungsmaßnahmen) melden. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der Bank, eines Vertragspartners der SCHUFA oder der Allgemeinheit erforderlich ist und dadurch meine/unsere schutzwürdigen Belange nicht beeinträchtigt werden.

Soweit hiernach eine Übermittlung erfolgen kann, befreie(n) ich/wir die Bank zugleich vom Bankgeheimnis.

Die SCHUFA speichert die Daten, um den ihr angeschlossenen Kreditinstituten, Leasinggesellschaften, Einzelhandels-, Versandhandels- und sonstigen Unternehmen, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben, Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Sie stellt diese Daten ihren Vertragspartnern nur zur Verfügung, wenn diese ein berechtigtes Interesse an der Datenübermittlung glaubhaft darlegen. Die SCHUFA übermittelt nur objektive Daten ohne Angabe des kontoführenden Instituts; subjektive Werturteile, persönliche Einkommens- und Vermögensverhältnisse sind in SCHUFA-Auskünften nicht enthalten.

Ich kann/Wir können Auskünfte bei der SCHUFA über die mich/uns betreffenden gespeicherten Daten erhalten. Die Adresse der SCHUFA lautet:

Ich/Wir willige(n) ein, daß im Falle eines Wohnsitzwechsels die vorgenannte SCHUFA die Daten an die dann zuständige SCHUFA übermittelt.

Weitere Informationen über das SCHUFA-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird.

SCHUFA-Klausel für Kreditanträge

Ich/Wir willige(n) ein, daß die Bank der für meinen/unseren Wohnsitz zuständigen SCHUFA-Gesellschaft (Schutzgemeinschaft für allgemeine Kreditsicherung) Daten über die Beantragung, die Aufnahme (Kreditnehmer, Mitschuldner, Kreditbetrag, Laufzeit, Ratenbeginn) und vereinbarungsgemäße Abwicklung (z. B. vorzeitige Rückzahlung, Laufzeitverlängerung) dieses Kredits übermittelt.

Unabhängig davon wird die Bank der SCHUFA auch Daten aufgrund nicht vertragsgemäßer Abwicklung (z. B. Kündigung des Kredits, Inanspruchnahme einer vertraglich vereinbarten Lohnabtretung, beantragter Mahnbescheid bei unbestrittener Forderung sowie Zwangsvollstreckungsmaßnahmen) melden. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der Bank, eines Vertragspartners der SCHUFA oder der Allgemeinheit erforderlich ist und dadurch meine/unsere schutzwürdigen Belange nicht beeinträchtigt werden.

Soweit hiernach eine Übermittlung erfolgen kann, befreie(n) ich/wir die Bank zugleich vom Bankgeheimnis.

Die SCHUFA speichert die Daten, um den ihr angeschlossenen Kreditinstituten, Leasinggesellschaften, Einzelhandels-, Versandhandels- und sonstigen Unternehmen, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben, Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Sie stellt diese Daten ihren Vertragspartnern nur zur Verfügung, wenn diese ein berechtigtes Interesse an der Datenübermittlung glaubhaft darlegen. Die SCHUFA übermittelt nur objektive Daten ohne Angabe des Kreditgebers; subjektive Werturteile, persönliche Einkommens- und Vermögensverhältnisse sind in SCHUFA-Auskünften nicht enthalten.

Ich kann/Wir können Auskunft bei der SCHUFA über die mich/uns betreffenden gespeicherten Daten erhalten. Die Adresse der SCHUFA lautet:

Ich/Wir willige(n) ein, daß im Falle eines Wohnsitzwechsels die vorgenannte SCHUFA die Daten an die dann zuständige SCHUFA übermittelt.

Weitere Informationen über das SCHUFA-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird.

SCHUFA-Klausel für Bürgschaftserklärungen

Ich/Wir willige(n) ein, daß das Kreditinstitut der für meinen/unseren Wohnsitz zuständigen SCHUFA-Gesellschaft (Schutzgemeinschaft für allgemeine Kreditsicherung) Daten über die vorgesehene Bürgschaft, ihre Übernahme (Bürge, Kreditnehmer, Betrag, Laufzeit, Ratenbeginn des Kredits) und Erledigung übermittelt.

Unabhängig davon wird das Kreditinstitut der SCHUFA auch Daten aufgrund nicht vertragsgemäßer Erfüllung dieser Bürgschaft (z. B. beantragter Mahnbescheid bei unbestrittener Forderung sowie Zwangsvollstreckungsmaßnahmen) melden. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies zur Wahrung berechtigter Interessen des Kreditinstituts, eines Vertragspartners der SCHUFA oder der Allgemeinheit erforderlich ist und dadurch meine/unsere schutzwürdigen Belange nicht beeinträchtigt werden.

Soweit hiernach eine Übermitltung erfolgen kann, befreie(n) ich/wir das Kreditinstitut zugleich vom Bankgeheimnis.

Die SCHUFA speichert die Daten, um den ihr angeschlossenen Kreditinstituten, Leasinggesellschaften, Einzelhandels-, Versandhandels- und sonstigen Unternehmen, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben, Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Sie stellt diese Daten ihren Vertragspartnern nur zur Verfügung, wenn diese ein berechtigtes Interesse an der Datenübermittlung glaubhaft darlegen. Die SCHUFA übermittelt nur objektive Daten ohne Angabe des Kreditgebers; subjektive Werturteile, persönliche Einkommens- und Vermögensverhältnisse sind in SCHUFA-Auskünften nicht enthalten.

Ich kann/Wir können Auskunft bei der SCHUFA über die mich/uns betreffenden gespeicherten Daten erhalten. Die Adresse der SCHUFA lautet:

Ich/Wir willige(n) ein, daß im Falle eines Wohnsitzwechsels die vorgenannte SCHUFA die Daten an die dann zuständige SCHUFA übermittelt.

Weitere Informationen über das SCHUFA-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird.

Druck: Anker-Druck Bremen