BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

Drucksache 12/197

12. Wahlperiode

15.01.87

Der Hamburgische Datenschutzbeauftragte

An den
Herrn Präsidenten der Bürgerschaft

Betr.: Fünfter Tätigkeitsbericht
des Hamburgischen Datenschutzbeauftragten zum 1. Januar 1987

Gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen fünften Tätigkeitsbericht, den ich zum 1. Januar 1987 erstellt habe.*

Dem Senat leite ich meinen Tätigkeitsbericht gleichzeitig zu.

Schapper

* Verteilt nur an die Abgeordneten der Bürgerschaft

Bürgerschaftsdrucksachen — außer Senatsvorlagen — sind zu beziehen bei:
Druckerei Warlenberg & Söhne GmbH, Theodorstraße 41 w, 2000 Hamburg 50, Telefon 89 39 48

Fünfter Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten

Zugleich
Tätigkeitsbericht der Aufsichtsbehörde
für den nicht-öffentlichen Bereich

vorgelegt zum 1. Januar 1987
Redaktionsschluß: 8. Dezember 1986

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Claus Henning Schapper
Karl-Muck-Platz 1 · 2000 Hamburg 36 · Tel.: 34 97 40 20

Druck: Lütcke & Wulff, Hamburg 1

GLIEDERUNG

Seite

Abkürzungsverzeichnis

ADV	= Automatische Datenverarbeitung
APIS	= Arbeitsdatei PIOS Innere Sicherheit
AVAD	= Auskunftsstelle über den Versicherungsaußendienst e.V.
BAG	= Bundesarbeitsgericht
BAföG	= Bundesausbildungsförderungsgesetz
BAJS	= Behörde für Arbeit, Jugend und Soziales
BaKred	= Bundesaufsichtsamt für das Kreditwesen
BauGB	= Baugesetzbuch
BAV	= Bundesaufsichtsamt für das Versicherungswesen
BB	= Betriebsberater
BBauG	= Bundesbaugesetz
BBG	= Bundesbeamtengesetz
bDSB	= betrieblicher Datenschutzbeauftragter
BetrVG	= Betriebsverfassungsgesetz
BDSG	= Bundesdatenschutzgesetz
BfD	= Bundesbeauftragter für den Datenschutz
Bfl	= Behörde für Inneres
BGB	= Bürgerliches Gesetzbuch
BGBl	= Bundesgesetzblatt
BGH	= Bundesgerichtshof
BGS	= Bundesgrenzschutz
BKA	= Bundeskriminalamt
BKK	= Betriebskrankenkasse
BND	= Bundesnachrichtendienst
BSB	= Behörde für Schule und Berufsbildung
BseuchG	= Bundesseuchengesetz
BT	= Bundestag
BTM	= Betäubungsmittel
Btx	= Bildschirmtext
BV	= Berufsunfähigkeitsversicherung
BVerfG	= Bundesverfassungsgericht
BVerfSchG	= Bundesverfassungsschutzgesetz
BZRG	= Bundeszentralregister
CR	= Computer und Recht
DB	= Der Betrieb
DRS	= Drucksache

DS	= Datenschutz
DSB	= Datenschutzbeauftragter
DTV	= Deutscher Transportversicherer-Verband
DV	= Datenverarbeitung
DVO	= Durchführungsverordnung
DVZ	= Datenverarbeitungszentrale
EC-Karte	= Eurocheque-Karte
EDV	= Elektronische Datenverarbeitung
GDV	= Gesamtverband der Versicherungswirtschaft
GewO	= Gewerbeordnung
GG	= Grundgesetz
GVBl	= Gesetz- und Verordnungsblatt
HBauO	= Hamburgische Bauordnung
HEW	= Hamburgische Electricitäts-Werke GmbH
HGW	= Hamburger Gaswerke GmbH
HHA	= Hamburger Hochbahn AG
HmbBG	= Hamburgisches Beamtengesetz
HmbDSB	= Hamburgischer Datenschutzbeauftragter
HmbDSG	= Hamburgisches Datenschutzgesetz
HmbPersVG	= Hamburgisches Personalvertretungsgesetz
HmbSOG	= Hamburgisches Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
HmbVerfSchG	= Hamburgisches Verfassungsschutzgesetz
HUK-Verband	= Verband der Haftpflicht-, Unfall-, Auto- und Rechtsschutzversicherer e.V.
HVV	= Hamburger Verkehrsverbund
HWW	= Hamburger Wasserwerke GmbH
IMK	= Konferenz der Innenminister
IuK	= Information und Kommunikation
JVA	= Justizvollzugsanstalt
KAN	= Kriminalaktennachweis
KBA	= Kraftfahrtbundesamt
KGSt	= Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KpS	= Kriminalpolizeiliche personenbezogene Sammlung
LDSG	= Landesdatenschutzgesetz
LID	= Lehrerindividualdatei
MAD	= Militärischer Abschirmdienst

ME	= Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder
MiStra	= Mitteilungen in Strafsachen
MittVw	= Mitteilungen für die hamburgische Verwaltung
MiZi	= Mitteilungen in Zivilsachen
NADIS	= Nachrichtendienstliches Informationssystem
NJW	= Neue Juristische Wochenschrift
NRW	= Nordrhein-Westfalen
OECD	= Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	= Oberfinanzdirektion
OWiG	= Ordnungswidrigkeitengesetz
PB	= Polizeiliche Beobachtung
PC	= Personal Computer
PIN	= Identifizierungsnummer
PIOS	= Inpol-Anwendungen Personen, Institutionen, Objekte und Sachen
PIS	= Personalinformationsystem
POLAS	= Polizeiliches Auskunftssystem
POS	= Point of Sale
RVO	= Reichsversicherungsordnung
RZ	= Rechenzentrum
SCHUFA	= Schutzgemeinschaft für allgemeine Kreditsicherung
SGB	= Sozialgesetzbuch
SOG	= s. HmbSOG
SPUDOK	= Spurendokumentation
StGB	= Strafgesetzbuch
StPO	= Strafprozeßordnung
StV-Btx	= Staatsvertrag über Bildschirmtext
StVG	= Straßenverkehrsgesetz
StVollzG	= Strafvollzugsgesetz
TB	= Tätigkeitsbericht
TEMEX	= Telemetry Exchange
VDVM	= Verband der Versicherungsmakler
VE	= Vorentwurf
VV	= Verwaltungsvorschrift
VZ-Urteil	= Volkszählungsurteil

WoBindG	= Wohnungsbindungsgesetz
WRV	= Weimarer Reichsverfassung
ZAG	= Gesetz über die Zusammenarbeit der Dienste und der Polizei
ZAW	= Zentralausschuß der Werbewirtschaft e.V.
ZEVIS	= Zentrales Verkehrsinformations-System
ZKA	= Zentraler Kreditausschuß
ZPO	= Zivilprozeßordnung

Paragraphenangaben ohne Zusatz beziehen sich auf das
Hamburgische Datenschutzgesetz (HmbDSG)

1. Zur Lage des Datenschutzes

1.1 Zur Kritik am Datenschutz und an den Datenschützern

Die Regierenden meinen offenbar, die Rolle, welche die Datenschutzbeauftragten zu spielen hätten, erschöpfe sich darin, durch ihre bloße Existenz und gelegentlich durch konstruktive Kritik beruhigend auf die Bürger einzuwirken. Wenn die Datenschutzbeauftragten diesen Erwartungen nicht entsprechen, dann ist ihr Rat nicht mehr gefragt.

Die Datenschutzbeauftragten hätten sich mit ihrer Kritik an den Sicherheitsgesetzen von ihren eigentlichen Aufgaben entfernt und in den tagespolitischen Kampf begeben, so lautete der Vorwurf des innenpolitischen Sprechers der CDU/CSU-Fraktion, als sich die Datenschutzbeauftragten im Januar zum Gesetzespaket der Koalition äußerten. In einem Interview mit dem SPIEGEL im März bezeichnete der Bundesinnenminister die Datenschutzbeauftragten als Sondergremium von Oberkontrolleuren, die ihre Rolle verkannt hätten. Im April präzisierte die CDU/CSU-Fraktion ihre Kritik: Die Datenschützer seien nicht bereit, das Prinzip der wehrhaften Demokratie, zu dem sich unser Grundgesetz ausdrücklich bekenne, ernst zu nehmen. Ihnen fehle in Fragen der inneren Sicherheit die notwendige Fachkenntnis. Die Unionsparteien seien deshalb nicht bereit, alles höchst einseitig durch die Brille der Datenschutzbeauftragten zu sehen, um nicht sträflich die Belange unseres Landes in Fragen äußerer und innerer Sicherheit zu vernachlässigen. Der Bundesinnenminister hat uns leider im unklaren darüber gelassen, wen er gemeint hat, als er von einem Datenschutz sprach, der zum Teil von Kräften massiv betrieben werde, die damit den Staat und seine Abwehrkräfte schwächen wollten (in einem Interview mit der WELT am 15. Oktober 1986).

Die Tendenz, dem Datenschutz — wer oder was immer damit gemeint sein mag — die Schuld zuzuschieben, wenn eine von der Öffentlichkeit stark beachtete Straftat verübt wurde und bei den Ermittlungen Erfolge ausblieben, hat sich verstärkt. Wenn es darum geht, von Fahndungspannen oder organisatorischen Versäumnissen abzulenken — als Buhmann scheint sich der Datenschutz vorzüglich zu eignen. Manchmal ist dann auch von überzogenem oder mißverstandenem Datenschutz die Rede, gelegentlich wird die Angst der Amtsträger vor den strengen Anforderungen des Datenschutzes als Ursache von Fehlleistungen bezeichnet. Am deutlichsten hat es wieder einmal der innerhalb der Bundesregierung für den Datenschutz verantwortliche Innenminister gesagt — in dem schon erwähnten Interview mit der WELT —, was vom Datenschutz zu halten ist: „Dies hat dann zu der irrigen These geführt, daß der Schutz des Bürgers vor dem Staat — Stichwort: Datenschutz — Vorrang habe vor dem Schutz des Bürgers vor Kriminalität und Terror. In Wirklichkeit schützt man durch solche Hemmnisse nicht den Bürger, sondern im Gegenteil die Terroristen und ihr Umfeld."

Zu der Behauptung, der Datenschutz behindere die Bekämpfung des Terrorismus, ja leiste ihm gewissermaßen sogar Vorschub, sei folgendes angemerkt: Es ist infam, wenn in einer Zeit verständlicher Bestürzung über terroristische Gewalttaten und Morde bei den Bürgern der Eindruck erweckt werden soll, der Datenschutz und die Datenschutzbeauftragten seien die Ursache für fehlende Fahndungserfolge. In Wirklichkeit steht der Datenschutz einer effektiven polizeilichen Datenverarbeitung nicht entgegen.

- Richtig ist vielmehr, daß die Rasterfahndung kaum mehr angewandt wird, weil sie offenbar wenig Erfolg verspricht. Den Terroristen sind die polizeitaktischen Mittel inzwischen bekannt. Sie hinterlassen kaum noch Spuren in Dateien, die Fahndungsansätze bieten.
- Richtig ist, daß es nicht am fehlenden Zugriff auf Fahrzeugdateien gelegen hat, wenn die Polizei von Terroristen benutzte Fahrzeuge nicht schneller gefunden hat.
- Erhebliche Skepsis ist auch gegenüber der Behauptung geboten, mit einer Mobilisierung aller verfügbaren Computer sei dem Terrorismus entschiedener beizukommen. Diese Skepsis wird auch von Sicherheitsbehörden geteilt.

Die Datenschutzbeauftragten verschließen sich nicht der Notwendigkeit, die Befugnisse der Sicherheitsbehörden und ihre Informationstechnik neuen Anforderungen anzupassen. Sie warnen jedoch davor, terroristische Anschläge zum Anlaß für weitreichende Einschränkungen des Datenschutzes zu nehmen, die zur wirksamen Bekämpfung des Terrorismus nicht einmal geeignet sind. Das Spannungsverhältnis zwischen Datenschutz und Sicherheit darf nicht einseitig zu Lasten der verfassungsmäßig garantierten Bürgerrechte aufgelöst werden. Die Situation verbietet oberflächliche Polemik und verlangt differenzierte Lösungsansätze, die die Bekämpfung des Terrorismus verbessern, ohne wesentliche Elemente des freiheitlichen Rechtsstaates in Frage zu stellen.

1.2 Zum Stand der Gesetzgebung

Drei Jahre sind vergangen, seit das Bundesverfassungsgericht sein Volkszählungsurteil verkündet hat. Die für die Vorbereitung von Gesetzen zuständigen Stellen, die Bundesregierung und die Landesregierungen, haben sich einige Zeit gelassen für die Analyse des Urteils, haben dann aber eingeräumt, daß die Entscheidung sich nicht nur mit der zwangsweisen Erhebung personenbezogener Daten zu statistischen Zwecken befasse, daß sie vielmehr grundsätzliche rechts- und verfassungspolitisch bedeutsame Aussagen zum allgemeinen Persönlichkeitsrecht enthalte und mithin für alle Bereiche der Verwaltung, in denen personenbezogene Daten erhoben und verarbeitet würden, zu beachten sei (Zitat aus der Begründung zu dem von der Bundesregierung zusammen mit den Koalitionsfraktionen eingebrachten Paket der sogenannten Sicherheits- und Datenschutzgesetze). Doch haben die Verantwortlichen Taten kaum folgen lassen, abgesehen von der hessischen Koalition, die im November eine Novellierung des Datenschutzgesetzes verabschiedet hat — ein neues Gesetz, das den Datenschutz ein gutes Stück voran gebracht hat —, und abgesehen von der nordrhein-westfälischen Landesregierung, die Anfang Dezember einen Entwurf zur Novellierung des Datenschutzgesetzes im Landtag eingebracht hat — einen Entwurf, der sich ebenfalls in erfreulicher Weise von dem Entwurf der Bundesregierung zur Novellierung des Bundesdatenschutzgesetzes abhebt.

Der Hamburger Senat hat mehrfach — zum Beispiel in seiner Stellungnahme zu meinem 3. Tätigkeitsbericht und in seiner Antwort auf ein Ersuchen der Bürgerschaft zu meinem 2. Tätigkeitsbericht — hervorgehoben, daß nach seiner Auffassung die seit Jahren vielfach geforderte Verbesserung des Datenschutzes — insbesondere durch eine Novellierung des Bundesdatenschutzgesetzes, aber auch durch bereichsspezifische Regelungen — durch das Volkszählungsurteil unübersehbare Dringlichkeit erhalten habe. Er hat mit Kritik an der Bundesregierung und den sie tragenden Fraktionen nicht gespart, durch deren Säumnis, nicht eingelöste Ankündigungen und Uneinigkeit zunehmend ein unhaltbarer Zustand eingetreten sei. Gleichzeitig hat der Senat jedoch deutlich gemacht, daß es ihm empfehlenswert erscheine, zunächst das Ergebnis von Beratungen auf Bundesebene abzuwarten, ehe er eigene Initiativen zur Novellierung von Landesgesetzen ergreifen und Gesetzentwürfe in der Bürgerschaft einbringen wolle. Sollte der Bund jedoch seiner Verantwortung und der von ihm beanspruchten Schrittmacherfunktion auf dem Gebiet des Datenschutzes nicht alsbald gerecht werden, könnten die Länder nicht unbegrenzt länger warten — so der Senat Anfang 1985. Ich meine, daß der Senat in der Tat nicht länger warten kann und auf vielen Aufgabengebieten, für die ich schon in meinen früheren Tätigkeitsberichten Gesetzesinitiativen angemahnt habe (Polizei, Verfassungsschutz, Gesundheitswesen, Statistik usw.), tätig werden muß.

Dabei gehe ich von der Rechtsprechung des Bundesverfassungsgerichts aus, welche sich schon wiederholt mit der Situation beschäftigt hat, daß für einen Grundrechtseingriff Rechtsgrundlagen entweder ganz fehlen oder daß sie unzureichend sind. In diesen Fällen hat das Bundesverfassungsgericht die Notwendigkeit von Übergangsfristen anerkannt, in welchen der Gesetzgeber Gelegenheit zu einer verfassungsgemäßen Regelung haben muß. Für die Dauer derartiger Übergangsfristen hat es keine allgemeingültigen Maßstäbe gesetzt. Verschiedentlich hat es darauf abgestellt, daß eine ge-

setzliche Regelung in der laufenden Legislaturperiode des Parlaments erfolgen müsse. Eine Übergangsfrist könne dann nicht länger anerkannt werden, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert habe. Wenn ich nun die Intensität der Auseinandersetzung um die Bewertung des Volkszählungsurteils, die Fülle und Komplexität des zu regelnden Stoffes, den Stand der Vorbereitungen der Gesetzgebung und die seit der Entscheidung verstrichene Zeit berücksichtige, so komme ich zu dem Ergebnis, daß die Frist spätestens mit dem Ende der neuen Wahlperiode der Bürgerschaft abläuft.

Auf Bundesebene haben die Koalitionsfraktionen im Januar das bereits erwähnte Paket der Sicherheits- und Datenschutzgesetze eingebracht. Vier der Gesetzentwürfe sind nicht mehr im Bundestag beraten worden und werden der Diskontinuität anheim fallen, in der neuen Legislaturperiode des Bundestages müssen also neue Entwürfe eingebracht werden. Ich hatte mich schon im vorigen Tätigkeitsbericht zu den Gesetzesvorhaben geäußert und war zu dem Ergebnis gekommen, daß die Entwürfe deutlich hinter den verfassungsrechtlichen Anforderungen zurückgeblieben seien und wir es nicht zu bedauern hätten, wenn es nicht mehr zu Gesetzesbeschlüssen käme. Diese Bewertung bleibt bestehen.

Drei Entwürfe hatte der Bundestag mit geradezu atemberaubender Geschwindigkeit beraten und sie schon im Februar verabschiedet. Die Gesetze sollen am 1. April 1987 in Kraft treten. Es handelt sich um

— eine Änderung des Personalausweisgesetzes, durch die — nunmehr endgültig — der maschinenlesbare Personalausweis eingeführt werden soll,

— eine Änderung des Paßgesetzes, durch die der maschinenlesbare Reisepaß eingeführt werden soll und

— eine Änderung des Strafprozeßordnung, durch die die sogenannte Schleppnetzfahndung ermöglicht werden soll.

Anfang Dezember ist — plötzlich als eines der sogenannten Anti-Terror-Gesetze — eine Änderung des Straßenverkehrsgesetzes hinzugekommen, die vor allem den direkten Zugriff der Polizei auf die Datenbestände des Kraftfahrtbundesamtes (ZEVIS) rechtlich absichern soll.

Diese vier Gesetze haben eines gemeinsam: Sie sollen die Einführung neuer Informations- und Kommunikationssysteme, die Nutzung modernster Technik ermöglichen. Mit ihnen wird hingegen ganz offensichtlich nicht die Absicht verfolgt, die nötigen Konsequenzen aus dem Volkszählungsurteil zu ziehen und tragfähige Rechtsgrundlagen für solche Grundrechtseingriffe zu schaffen, die sich aus der schon heute praktizierten Informationstätigkeit des Staates ergeben. D.h., die Polizei etwa oder der Verfassungsschutz, deren automatisierte Verfahren schon längst einen hohen Standard erreicht haben und immer weiter ausgebaut werden, dürfen bis auf weiteres den Übergangsbonus strapazieren.

Dies ist um so bedenklicher, als jedes der vier verabschiedeten Gesetze der Polizei neue technische Kontrollmöglichkeiten gibt, ohne daß zugleich geregelt ist — in den Polizeigesetzen oder der Strafprozeßordnung —, welches Ausmaß an Kontrolle den Bürgern zugemutet werden soll. Konkret: Bei Einführung des computerlesbaren Personalausweises werden die Voraussetzungen nicht festgelegt sein, unter denen die Polizei — mit Hilfe des neuen Ausweissystems — Personenkontrollen durchführen und Personalien feststellen darf. Bei Eröffnung der H-Anfrage für diejenigen Polizeidienststellen, die bislang noch nicht an ZEVIS angeschlossen waren, und Einführung der P-Anfrage für alle Polizeibehörden werden die Befugnisse der Polizei zur Halterfeststellung und zur Nutzung der Halterdaten nicht geklärt sein. § 163d StPO schließlich schafft eine isolierte und allein auf § 111 StPO (Einrichtung von Kontrollstellen) abgestimmte Regelung für bestimmte Fahndungsmaßnahmen, während die Strafprozeßordnung im übrigen keine Vorschriften enthält, aus denen sich Zulässigkeit und Gren-

zen der Informationsverarbeitung zu Zwecken der Strafverfolgung ergeben, so daß spätestens bei der Verwertung von Zufallsfunden nach § 163d Abs. 4 Zweifelsfragen auftreten.

Es gibt also keine Maßstäbe, um die Verhältnismäßigkeit von Informationseingriffen beurteilen zu können, für die sich die Polizei des computerlesbaren Ausweises bedienen oder auf ZEVIS zurückgreifen darf. Desgleichen fehlt es an einer präzisen Bestimmung des Zweckes, für den die so gewonnenen Daten verwendet werden dürfen. Die verfassungsrechtlichen Bedenken, die ich in meinem letzten Tätigkeitsbericht gegen das Sicherheitspaket und insbesondere gegen die vorgezogene Inkraftsetzung des Personalausweisgesetzes und des ZEVIS-Gesetzes vorgebracht habe, bleiben mithin in vollem Umfang bestehen.

2. Entwicklung der Dienststelle

2.1 Personal

In meinem 4. TB (2.1, S. 6) hatte ich die Erwartung ausgesprochen, daß mir die Bürgerschaft je eine neue Stelle des höheren und des gehobenen Dienstes für das Haushaltsjahr 1986 bewilligt. Das ist geschehen. Allerdings durfte ich — aus haushaltswirtschaftlichen Gründen — die Stellen erst zum 1. Dezember 1986 ausschreiben, so daß sie bis Ende des Jahres noch nicht besetzt werden konnten. Ich hoffe allerdings, daß mir dies im Laufe des 1. Quartals des nächsten Jahres gelingen wird. Dann werden mehr als 3 Jahre verstrichen sein, ehe diese erstmals im 2. TB geforderte Personalverstärkung verwirklicht werden kann.

Wie ich in meinem 3. TB (2.1, S. 5) ausführlich begründet habe, ist eine weitere Verbesserung des Personalbestandes unabdingbar, damit die Dienststelle des Hamburgischen Datenschutzbeauftragten den Anforderungen einer effektiven Datenschutzkontrolle einigermaßen gerecht werden kann. Für die Prüfung und Überwachung der gesamten hamburgischen Verwaltung und sonstigen öffentlichen Stellen stand mir bislang neben 2 Sachbearbeitern des gehobenen Dienstes und einem „Techniker" nur ein einziger Jurist zur Verfügung, der aber durch Beratung und Mitarbeit an bereichsspezifischen Datenschutzregelungen ausgelastet war. Wenn jetzt ein 2. Jurist hinzukommt, der auch im nichtöffentlichen Bereich mit aushelfen muß, werden es die personellen Kapazitäten der Dienststelle auch weiterhin nicht zulassen, daß unmittelbare Prüfungen „vor Ort" in nennenswertem Umfang stattfinden. Demgegenüber belegen auch die Tätigkeitsberichte von Kollegen mit teilweise unvergleichlich besserer Personalausstattung, wie wichtig Datenschutzprüfungen — wenn möglich Querschnittsprüfungen — etwa bei den Sicherheitsbehörden sind. In diesem Zusammenhang verweise ich als nur ein Beispiel auf den 8. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz vom November 1986.

Die Notwendigkeit, die Dienststelle über den bisher bewilligten Rahmen hinaus zu verstärken, wird durch zwei Entscheidungen von Senat und Bürgerschaft unterstrichen:

— Nach den Vorfällen auf dem Heiligengeistfeld am 8. Juni 1986, zu denen ich mich unter 5.8.2 dieses Berichtes äußere, wird die Polizei um 292 neue Mitarbeiterinnen und Mitarbeiter verstärkt; das sind 292 zusätzliche Datenerheber und -verarbeiter.

— Der Senat hat mit seinen Beschlüssen über die Anwendung der neuen IuK-Technik in der Hamburger Verwaltung (4. TB, 3.1, S. 9) die Weichen für einen verstärkten Technikeinsatz in den Behörden gestellt. Das wird nicht nur zu einer stärkeren Nutzung der Angebote der Datenverarbeitungszentrale führen, sondern richtet sich gerade auf die Einführung von immer mehr dezentralen DV-Einrichtungen (Personal-Computer usw.). Damit wird eine immer größere Anzahl von Mitarbeitern der Hamburger Verwaltung an die Datenverarbeitung herangeführt. Diese neuen DV-Anwender verfügen häufig nicht über spezielle DV-Kenntnisse (die sie zur Nutzung der neuen Systeme auch nur noch in geringem Maße benötigen); ihnen fehlt darüber hinaus häufig auch das Problembewußtsein für Belange des Datenschutzes und der Datensicherung (das sehr wohl von ihnen gefordert werden muß, siehe 3.1 dieses Berichtes). Der Datenschutzbeauftragte hat also nicht nur eine immer größer werdende Zahl von DV-Anwendungen zu überwachen, er hat darüber hinaus eine zunehmende Zahl von Anwendern bei der Bewältigung für sie neuer Probleme des Datenschutzes zu unterstützen. Damit nicht genug: In Fortführung der IuK-Beschlüsse von 1985 hat der Senat mit dem Entwurf des Stellenplans 1987 46 zusätzliche Stellen für IuK-Fachkräfte (nach einer Aufstockung um eine mir nicht genau bekannte Zahl von IuK-Fachleuten schon im Jahre 1986) eingeworben.

Durch diese Stellenvermehrungen werden gerade die Teile der Hamburger Verwaltung, denen ich meine besondere Aufmerksamkeit zu widmen habe, in quantitativer wie in qualitativer Hinsicht so verstärkt, daß Konsequenzen für die personelle Ausstattung

meiner Dienststelle unvermeidlich sind. Entsprechende Stellenanträge werde ich für die kommenden Haushaltsjahre stellen.

Schließlich bin ich der Meinung, daß die Bewertung einiger vorhandener Dienstposten nicht den Anforderungen entspricht, die an die Stelleninhaber zu stellen sind. Sie hält auch den Vergleich mit entsprechenden Tätigkeiten in anderen Behörden nicht stand. Ich werde deshalb zum Stellenplan 1988 die von mir als vordringlich erachteten Stellenhebungen beantragen und hoffe, daß ich trotz der angespannten Haushaltslage vom Senat hierin unterstützt werde.

2.2 Eingaben

Bis zum 3. Dezember 1986 gingen 299 Eingaben ein. Sie betrafen folgende Bereiche:

A	Öffentlicher Bereich	129
	davon Sicherheitsbereich	46
	Gesundheits- und Sozialbereich	34
	übrige Bereiche	49
B	Nicht-öffentlicher Bereich	170
	davon Versandhandel	13
	Versicherungswirtschaft inkl. Auskunftsstelle über den Versicherungsaußendienst	31
	Kreditwirtschaft	29
	Sonstige des 3. Abschnitts	59
	Auskunfteien	35
	Sonstige des 4. Abschnitts	3

3. Beobachtung der automatisierten Datenverarbeitung (ADV)

3.1 Dezentrale Datenverarbeitung

Angesichts der schnellen Entwicklung der Datenverarbeitungstechnik und des anhaltenden Preisverfalls vor allem im Bereich der Computer-Hardware halten auch in der Verwaltung kleinere und kleinste DV-Systeme verstärkt Einzug. Das Erscheinungsbild der eingesetzten Geräte und Anlagen ist außerordentlich vielfältig. Das Spektrum reicht von den sog. „Abteilungsrechnern" über Mehrplatzsysteme bis zu Personalcomputern verschiedener Leistungsklassen. Bei der Software gewinnen „Anwendersysteme" (z. B. Textverarbeitungs- und Datenbankverwaltungssysteme) an Einfluß. Diese Systeme ermöglichen es auch Mitarbeitern ohne tiefere ADV-Kenntnisse, nach nur verhältnismäßig kurzer Einarbeitungszeit Verfahren zu entwickeln und abzuwickeln.

Neben den „autonomen" Anlagen mit eigener Verarbeitungskapazität verbessert sich auch die Ausstattung mit Bildschirmterminals, die im Rahmen umfangreicher Verfahren im On-line-Betrieb mit der Datenverarbeitungszentrale (DVZ) betrieben werden. Neben und anstelle von zentral betriebenen „Stapelverfahren" treten zunehmend Dialogverfahren, die einen direkten Zugriff auf benötigte Daten vom Arbeitsplatz aus ermöglichen.

Auf längere Sicht ist zu erwarten, daß die Entwicklung der Datenendgeräte, der Vermittlungs- und der Übertragungstechnik zur verstärkten Vernetzung zentraler und dezentraler Datenverarbeitung führt und die heutige Trennung zwischen „autonomer" DV, On-line-Verfahren mit „dummen Terminals" und nur zentral betriebener DV schrittweise aufgehoben wird. Hierfür spricht nicht nur die von der Post geplante Dienstintegration

im Rahmen eines „dienste-integrierenden digitalen Netzes" — ISDN — (vergleiche hierzu auch Nr. 3.2 des vorliegenden Berichts), sondern auch das zunehmende Angebot von multifunktionalen Datenendgeräten, die für verschiedene bislang getrennte Dienste (z.B. Telefonieren, Bildschirmtext, individuelle Daten- und Textverarbeitung) benutzt werden können.

Allgemein ist schon heute festzustellen, daß die ADV stärker an die fachlich zuständigen Mitarbeiter der Verwaltung heranrückt und damit nicht mehr allein oder auch nur vorrangig die Domäne der dafür speziell ausgebildeten ADV-Fachkräfte bleibt.

Der zunehmende Einsatz dezentraler Technik eröffnet nicht nur neue Anwendungsmöglichkeiten, sondern bringt auch neuartige Risiken mit sich. Dies will ich durch folgende Beispiele aus der Praxis hamburgischer Behörden illustrieren:

(1) Zur Bewältigung einer befristeten terminabhängigen Aufgabe setzte eine öffentliche Stelle einen PC ein. Mit dem PC wurden personenbezogene Daten verarbeitet. Außer der Bedienungskraft hatte keine der an der Aufgabenerfüllung beteiligten Personen ADV-Erfahrung oder Kontakt zu einer ADV-Gruppe. Bei der Prüfung der betreffenden DV-Anwendung mußte ich feststellen, daß von den verantwortlichen Personen genau genommen überhaupt keine Maßnahmen getroffen worden waren, um die Ausführung der Vorschriften des HmbDSG zu gewährleisten. Die für die PC-Bedienung zuständige Kraft hatte lediglich von sich aus einige Vorkehrungen getroffen, um die unbefugte Benutzung des PC zu verhindern und um den Datenbestand bei eventuellem Verlust oder Beschädigung rekonstruieren zu können. Ich will an diesem Beispiel nicht aufzählen, was alles versäumt worden ist und welche Maßnamen bei dieser konkreten Anwendung hätten getroffen werden können und müssen, um nur den erforderlichen und angemessenen Sicherungs- und Organisationsaufwand zu erfüllen. Ich habe diesen Fall geschildert, um deutlich zu machen, daß mit der Verbreitung der PC's in der Verwaltung immer mehr Personen automatisierte Datenverarbeitung betreiben, die „von Haus aus" keine „Datenverarbeiter" sind, d.h. keine Ausbildung als ADV-Organisationssachbearbeiter o.ä. erhalten haben. Diese Personen sind in der Regel, wenn sie mit der PC-Datenverarbeitung beginnen, nicht über Fragen des Datenschutzes und der Datensicherung informiert, ihnen fehlt ein entsprechendes Problembewußtsein. Sie kennen meist weder die Richtlinien, die das Senatsamt für den Verwaltungsdienst hierzu erlassen hat (ADV-Handbuch Teil 4.1), noch die einschlägigen Datenschutzbestimmungen. Selbst wenn diese Mitarbeiter — mehr oder minder zufällig — auf die Richtlinien und Bestimmungen aufmerksam werden, sind sie meist schon allein deshalb nicht in der Lage, die Bestimmungen richtig anzuwenden, weil ihnen die Fachbegriffe nicht geläufig sind.

    Die Ursache für die fehlenden Datenschutz- und Datensicherungskenntnisse der „nichtprofessionellen" Datenverarbeiter liegt meines Erachtens in folgendem: Bisher waren in den Behörden nur ganz bestimmte Mitarbeiter Adressaten für Datenverarbeitungs- und damit auch für Datenschutz- und Datensicherungsfragen, nämlich die Mitarbeiter in den Organisations- und Datenverarbeitungsreferaten (ADV-Gruppen). Der Informationsfluß zwischen dem Senatsamt und diesen Gruppen funktioniert. So ist z.B. jedes ADV-Gruppen-Mitglied im Verteiler für die ADV-Handbücher registriert und erhält vom Senatsamt die Handbücher und eventuelle Ergänzungen. Nicht geregelt ist hingegen, wie die PC-Anwender, die nicht zu einer ADV-Gruppe gehören, mit den entsprechenden Informationen versorgt werden.

(2) Eine andere Stelle setzte einen PC ein, um damit den Datex-P-Dienst der Deutschen Bundespost nutzen zu können. Die Stelle beabsichtigte, mit einer Gegenstelle im Ausland zu kommunizieren. Da ein Verbindungsaufbau nur in abgehender Richtung möglich sein mußte, brauchte die Stelle keinen Datex-P-Hauptanschluß, sondern entschloß sich aus Kostengründen zu der Lösung, nur einen Wählzugang über das Fernsprechnetz zum Datex-P-Netz (Datex-P20F-Betrieb) in Anspruch zu nehmen.

Für die Inanspruchnahme des Dienstes Datex-P20 über einen Wählzugang wurde der Stelle von der Post eine Teilnehmerkennung zugeteilt, die, worauf die Post deutlich hinweist, geheimzuhalten ist. An technischen Einrichtungen ist für die Nutzung des Dienstes nur ein Telefonanschluß, ein Akustikkoppler (oder ein Modem) und ein Start/Stop-Gerät (zeichenorientierte asynchrone Datenendeinrichtung, z. B. ein PC) erforderlich. Eine Verbindung kann mit einer gültigen Teilnehmerkennung von jedem beliebigen Telefonanschluß (auch von öffentlichen Telefonzellen) aus aufgebaut werden.

Einige Zeit nach Einrichtung des Anschlusses wurde aufgrund einer ungewöhnlich hohen Rechnung (DM 22 000,— statt ca. DM 100,— für einen Abrechnungszeitraum) festgestellt, daß die Teilnehmerkennung der betreffenden Stelle unbefugt benutzt worden war. Aus den Protokollen der Bundespost über die Verbindungen im fraglichen Zeitraum konnte nur festgestellt werden, daß Verbindungen zu Gegenstellen in aller Welt (z. B. Japan) aufgebaut worden waren, zu denen die betreffende öffentliche Stelle keine Verbindung hatte. Zum Teil war versucht worden, Verbindung zu Gegenstellen aufzubauen, die durch eigene Programmroutinen den Zugang abblocken konnten, weil den Eindringlingen die Zugangsinformationen offenbar nicht bekannt waren.

Bei der Untersuchung dieses Falles habe ich festgestellt, daß die Stelle, die mit ihrem PC am Datex-P-Dienst teilnahm, sich über die Risiken des Dienstes Datex-P20F und über die Bedeutung der Teilnehmerkennung nicht im klaren war. Nur so konnte es dazu kommen, daß zwar alle betroffenen Mitarbeiter „im Grunde" wußten, daß die Teilnehmerkennung geheimzuhalten ist, daß die erforderlichen und dieser Tatsache angemessenen organisatorischen Maßnahmen jedoch nicht getroffen wurden. Das Schriftstück, in dem die Post die vollständige Teilnehmerkennung mitgeteilt hatte, war zu der den Datex-P-Anschluß betreffenden Akte genommen worden, die im Schrank der Sekretärin aufbewahrt wurde. Die Teilnehmerkennung war im übrigen „allen Mitgliedern der Abteilung (ca. 5-10 Personen)" bekanntgegeben worden. Der Personenkreis wurde nicht schriftlich festgehalten. Wer die Teilnehmerkennung tatsächlich kannte — z. B. arbeiteten in der Stelle häufig in der Ausbildung befindliche Personen —, war nicht bekannt. Dies war angesichts der Bedeutung und der Wirkungsweise der Teilnehmerkennung für Datex-P unverantwortlich. Die Teilnehmerkennung hat nämlich im Datex-P-Dienst die Funktion eines Kontos oder „Kostenträgers" für die Inanspruchnahme des Dienstes. Ihr werden die Gebühren zugeordnet, die bei Verbindungen unter ihrer Angabe auflaufen. Wer eine Teilnehmerkennung kennt, kann von jedem beliebigen Telefonanschluß aus unter Angabe dieser Kennung Datex-P auf Kosten des rechtmäßigen Inhabers der Kennung nutzen, ohne daß beim Verbindungsaufbau geprüft wird, von welchem Telefonanschluß aus der Verbindungsaufbau betrieben wird. Daher existiert natürlich auch in keinem Protokoll ein Hinweis auf den Verwender der Teilnehmerkennung. Selbstverständlich hätte der Personenkreis, der die Teilnehmerkennung benutzen durfte, so klein wie möglich gehalten werden müssen, er hätte schriftlich dokumentiert werden müssen, und die Kennung hätte häufiger verändert werden müssen.

Mit diesem Beispiel wird deutlich, daß technische Maßnahmen der Datensicherung nur dann wirksam greifen, wenn sowohl die organisatorischen Bedingungen (hier: Geheimhaltung der Teilnehmerkennung) entsprechend gestaltet sind als auch das Problembewußtsein der betroffenen Mitarbeiter entwickelt wird.

Die dezentralen Anlagen, insbesondere PC's sind zwar nicht in der Lage, die Groß-ADV zu ersetzen, ihre Leistungsfähigkeit reicht jedoch bereits heute in einen Bereich hinein, der noch vor wenigen Jahren in Rechenzentren betriebenen Großrechnern vorbehalten war.

Da die kleinen Geräte in der Regel mit Diskettenlaufwerken ausgerüstet sind und die dazugehörenden Disketten das Westentaschenformat kaum überschreiten, ist die „Abgangskontrolle", d. h. die Kontrolle darüber, daß keine Datenträger entfernt werden, problematisch. Diese in den gängigen Formaten in jedem Kaufhaus käuflich zu erwerben-

den Disketten können dazu verwendet werden, mittels eines Kopierprogramms Daten unbemerkt zu übertragen und aus dem Bereich des Rechners zu entfernen.

Neben den durch „Unbefugte" hervorgerufenen Datensicherungsrisiken erlangt mit der Ausbreitung dezentraler DV auch das Risiko des Mißbrauchs von Daten durch „Befugte", d.h. zur Dienststelle gehörende Mitarbeiter, eine zunehmende Bedeutung. Da moderne auf PC's ablauffähige Datenbankverwaltungssysteme die variable Auswertung und Verknüpfung von Datenbeständen ermöglichen, ohne daß zuvor langwierige Programmierarbeiten notwendig sind, ergibt sich hier ein zusätzliches Risiko für die Gewährleistung des informationellen Selbstbestimmungsrechts für diejenigen, deren Daten mit solchen Systemen gespeichert und verarbeitet werden.

Die auf die „klassische", nur zentral betriebene ADV abstellenden Maßnahmen zur Datensicherung sind nicht ohne Schwierigkeiten auf die neue Technik und ihre Einsatzfelder übertragbar.

Ich habe diese Entwicklung zum Anlaß genommen, im Frühsommer des Jahres eine Umfrage bei Behörden und Ämtern über die Datensicherung bei dezentralen DV-Anlagen und -Geräten zu starten. Dezentrale DV-Geräte oder -Anlagen sind

— DV-Anlagen und -Geräte, die außerhalb der Rechenzentren betrieben werden, unabhängig davon, ob sie von spezialisiertem ADV-Fachpersonal oder durch die für die jeweilige Fachaufgabe zuständigen Personen bedient werden,

— Bürocomputer (auch Minicomputer oder mittlere Datentechnik genannt) und Personalcomputer, unabhängig davon, ob sie selbständig arbeiten, miteinander vernetzt sind oder über Leitungen mit einem Rechenzentrum verbunden sind,

— sämtliche Geräte, über die die Benutzer mit (räumlich entfernten) DV-Anlagen kommunizieren können.

Ziel der Erhebung war es, einen Überblick über die in der hamburgischen Verwaltung bei der Verarbeitung personenbezogener Daten eingesetzten Anlagen und -geräte zu bekommen (an zentraler Stelle der Hamburger Verwaltung gibt es einen solchen Überblick bislang nicht) und den Stand der Datensicherung im Sinne von § 8 Abs. 1 HmbDSG zu überprüfen.

Aus den meisten Behörden liegen mir inzwischen zwar Rückmeldungen vor, eine systematische und vollständige Auswertung der eingegangenen Fragebögen war in der Kürze der bis zur Fertigstellung des Tätigkeitsberichts zur Verfügung stehenden Zeit jedoch noch nicht möglich. Gleichwohl kann ich hier über erste Ergebnisse berichten:

3.1.1 Umfang und Art der dezentralen Datenverarbeitung

Bis zum heutigen Tage liegen mir über 160 Rückmeldungen vor. Diese Meldungen beziehen sich zum Teil jedoch auf mehrere Geräte des gleichen Typs bzw. auf ganze ADV-Verfahren, bei denen eine Vielzahl von Einzelgeräten zum Einsatz kommt.

Nach Mitteilung des Senats sind zur Zeit mehr als 1100 Arbeitsplätze allein im Rahmen von On-line-Verfahren mit Verbindung zur DVZ mit Bildschirmterminals ausgestattet. Die Installation von weiteren 600 Bildschirm-Terminals ist kurzfristig geplant. Im Rahmen der großen realisierten Verfahren (Polizei, Steuerverwaltung, Besoldungs- und Versorgungsstelle) werden personenbezogene Daten verarbeitet.

Bei den autonomen Anlagen, die unabhängig von der DVZ und dem Rechenzentrum der Universität Hamburg betrieben werden, beläuft sich die Zahl der bei der Verarbeitung personenbezogener Daten eingesetzten Anlagen auf über 150, wobei zum Teil eine größere Anzahl von Bildschirmarbeitsplätzen an eine Zentraleinheit angeschlossen sind (PC-Mehrplatzsysteme und „Abteilungsrechner"). Aus den Meldungen geht hervor, daß es sich zum Teil um Pilotprojekte handelt und eine Ausweitung der dezentral betriebenen Verfahren vorgesehen ist.

3.1.2 Stand der Datensicherung

Die Erhebung gibt über den Stand der technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes ein uneinheitliches Bild, denn die eingesetzten Anlagen verfügen über sehr unterschiedliche technische Voraussetzungen hinsichtlich effektiver Benutzungs- und Zugriffskontrollen und die Einsatzfelder und das organisatorische Umfeld sind außerordentlich vielfältig.

Gleichwohl schälen sich verschiedene Problemkomplexe heraus, die bislang von den Anwendern nicht oder nur unzureichend berücksichtigt werden:

— Technik: Die zum Einsatz kommenden Geräte und die eingesetzte Software verfügen zum Teil nicht über die in der Groß-ADV üblichen Sicherungsmöglichkeiten wie z.B. einen durch das Betriebssystem gewährleisteten Paßwortschutz und eine entsprechende Benutzeridentifikation und die Führung eines automatisierten Protokolls der über die Anlage abgewickelten Aktivitäten.

— Raumsicherung: Ein besonderer Gebäudeschutz, ja sogar eine räumliche Abschottung der ja auch zutreffend „Arbeitsplatzcomputer" genannten Personalcomputer stößt angesichts der Raumausstattung vieler Dienststellen auf Probleme.

— Organisation: Die neue Technik wird häufig im Rahmen vorhandener Organisationsstrukturen eingeführt, ohne daß die hiermit verbundenen neuen Probleme und Risiken und die notwendig werdenden Maßnahmen angemessen berücksichtigt werden.

— Personelle Ausstattung: Die Verfahren werden zum Teil von Mitarbeitern ohne spezielle ADV-Kenntnis entwickelt und bedient. Diesem Personenkreis mangelt es häufig nicht nur an einschlägigen Kenntnissen sondern auch an einem entwickelten Problembewußtsein für Datenschutz und Datensicherung. Diese Mitarbeiter sind auch nicht — wie die ADV-Gruppen — in die entsprechenden Strukturen eingebunden, die für den zwischenbehördlichen Erfahrungsaustausch über ADV-Probleme bestehen.

3.1.3 Forderungen

Auch wenn die vom Senatsamt für den Verwaltungsdienst erlassenen Regelungen (Richtlinie zum Verfahren der Datensicherung im Rahmen der automatisierten Datenverarbeitung — DS-Richtlinie —, Rahmenregelungen zur Datensicherung für automatisierte Verfahren — DS-Rahmenregelungen —, Richtlinie zur Freigabe von automatisierten Verfahren — Freigaberichtlinie —, Richtlinie für die Verfahrensdokumentation — Dokumentationsrichtlinie) zum Teil nicht unmittelbar auf die neuen technischen Möglichkeiten angewandt werden können, da sie von der klassischen Organisationsform der zentralen Datenverarbeitung in einer gesonderten Rechenstelle ausgehen, und zudem bestimmte Entwicklungen auf dem Gebiet der Software-Entwicklung nicht berücksichtigen, entbindet dieser Tatbestand die zuständigen Fachbehörden nicht von ihrer Verpflichtung zur Sicherstellung des Datenschutzes gemäß § 16 HmbDSG (Eigenverantwortung).

Angesichts der Vielfalt der eingesetzten Techniken, der stürmisch voranschreitenden technischen Entwicklung und der Vielgestaltigkeit der mit dezentralem Gerät wahrgenommenen Aufgaben fällt es nicht leicht, einheitliche detaillierte Forderungen nach Maßnahmen zur Gewährleistung des Datenschutzes zu stellen. Gleichwohl würde ich es — wie ich schon in meinem 4. TB unter Nr. 3.3 ausgeführt habe — sehr begrüßen, wenn von zentraler Stelle Rahmenregelungen für den Einsatz dezentraler DV-Anlagen aufgestellt würden. Die Fachbehörden müßten einen solchen Rahmen ausfüllen:

— Es sind klare Regelungen (möglichst in Form von Dienstanweisungen) aufzustellen, die die Verantwortlichkeiten der einzelnen Anwender und (bei autonomen Anlagen) der Betreiber festschreiben. Diese Regelungen müssen auf die konkreten Umstände in den Behörden abstellen und geeignete Datenschutz- und Datensicherungsmaßnahmen festlegen.

— Die zuständigen Stellen haben Sorge dafür zu tragen, daß revisionsfähige Unterlagen (Logprotokoll bzw. Logbuch, Inventarisierung der Datenträger, Zuordnung von Benutzern zu Benutzergruppen, Art und ggf. zeitliche Befristung ihrer Berechtigungen, Programmdokumentation) geführt werden.

— Die Aufbau- und Ablauforganisation muß datenschutzfreundlich gestaltet werden. Dazu gehören — sofern realisierbar — die Funktionstrennung zwischen Entwickler, Systemverantwortlichen und Benutzer. Schon beim Systemdesign muß geklärt werden, welcher Benutzer welche Daten für die von ihm wahrzunehmenden Aufgaben benötigt. Gerade wenn eine Funktionstrennung nicht oder nur unzureichend zu gewährleisten ist, besteht die Notwendigkeit der Schaffung einer internen Datenschutzkontrollinstanz, die von den Anwendern getrennt ist.

— Die organisatorischen Maßnahmen müssen von technischen Mitteln der Datensicherung flankiert werden. Dazu gehören sowohl die Raumsicherung als auch die technische Ausstattung der Geräte. Entscheidend ist nicht die einzelne getroffene Maßnahme sondern das Gesamtkonzept. Dabei ist sowohl der Schutzzweck — Art der verarbeiteten Daten — als auch das Gefährdungsrisiko — z. B. Kenntnisnahme durch Publikum — zu berücksichtigen. Zumindest bei Verarbeitung von Daten, die einem besonderen Amts- oder Dienstgeheimnis unterliegen — z. B.. Gesundheitsdaten —, ist die Verwendung von Geräten mit Benutzeridentifikation, Paßwortschutz und automatischer Führung eines Logprotokolls erforderlich.

Für die Aufstellung entsprechender Regelungen und Maßnahmenkataloge wäre es hilfreich, wenn für alle eingesetzten Anlagen Schwachstellenanalysen durchgeführt würden, um die sich konkret abzeichnenden Risiken (z. B. unbefugter Zugang zur Anlage, unbefugtes Entfernen von Datenträgern, unbefugte Eingabe, Benutzung und Übermittlung) zu erkennen und zu bewerten. Die Ergebnisse dieser Analyse können Voraussetzung für spezielle auf den Einzelfall zugeschnittene Maßnahmen sein. Häufig sind es schon kleine Veränderungen (Einbau von Sicherheitsschlössern, Herausnahme des Rechnerraumes aus der allgemeinen Schließanlage, Auslagerung von Sicherungskopien in einen verschlossenen Schrank außerhalb des Rechnerraumes usw.), die den Standard der Datensicherung deutlich verbessern. Voraussetzung hierfür ist jedoch, daß die mit der Datenverarbeitung befaßten Mitarbeiter hinsichtlich der mit der Datenverarbeitung verbundenen Risiken sensibilisiert werden.

Die bei den Prüfungen in verschiedenen Bereichen zutage getretenen Mißstände sind zum Teil darauf zurückzuführen, daß schon bei der Projektentwicklung die Belange des Datenschutzes nicht oder nur unzureichend berücksichtigt wurden und die solcherart konzipierten fertigen Systeme hier schwere Mängel aufweisen.

Wenn die Berücksichtigung von mir erhobener Forderungen zur Sicherstellung des Datenschutzes zum Teil tiefe Einschnitte in die organisatorische und technische Ausgestaltung der Verfahren bedeutet, so hätte sich dies vielfach vermeiden lassen, wenn die Gewährleistung des informationellen Selbstbestimmungsrechtes schon in der Planungsphase in den Zielkatalog der Projekte eingegangen wäre. Die Eigenverantwortung der Datenverarbeitung betreibenden Stellen setzt nicht erst am fertigen Produkt, sondern bereits bei der Konzeption an. Dementsprechend begrüße ich es ausdrücklich, daß ich von einigen Behörden, namentlich der Behörde für Inneres bei dem Online-Verfahren Einwohnerwesen und von der Behörde für Schule und Berufsbildung bei dem Projekt „Modernisierung der Lehrerindividualdatei" frühzeitig beteiligt wurde.

3.1.4 Prüfungergebnisse

3.1.4.1 Einsatz dezentraler DV-Anlagen in einem Krankenhaus

(1) Für das Krebsregister werden sämtliche in diesem Krankenhaus behandelten Krebspatienten dateimäßig erfaßt. Die Dateien beinhalten sowohl Name, Anschrift und Geburtsdatum als auch diverse Informationen über den Krankheitsverlauf und

Therapiemaßnahmen. Diese Daten unterliegen der ärztlichen Schweigepflicht. An die zu treffenden Maßnahmen zur Sicherstellung des Datenschutzes ist deshalb ein strenger Maßstab anzulegen.

Die Verarbeitung dieser Daten erfolgt auf einer Anlage der Mittleren Datentechnik mit angeschlossenen 10 Bildschirmterminals. Als Speichermedium werden Wechselplatten mit hoher Speicherkapazität und Magnetbänder benutzt. Die Zentraleinheit befindet sich in einem speziellen Rechnerraum, die Bildschirmterminals sind über das Institut verteilt.

Der Rechnerraum befindet sich im Tiefparterre eines Gebäudes und ist nicht in ausreichendem Maß gegen Einbruch gesichert. Weil der Raum in eine allgemeine Schließanlage integriert ist, haben mehr Personen Zugang, als für die Aufrechterhaltung des Betriebs notwendig ist. Magnetplatten und -bänder werden in großer Zahl ausschließlich im Rechnerraum aufbewahrt. Ein Bestandsverzeichnis über die Datenträger wird nicht geführt. Eine Auslagerung von Sicherungskopien findet nicht statt. Sowohl die Zugangskontrolle als auch die Abgangskontrolle (Kontrolle, daß keine Datenträger unbefugt entfernt werden) ist unzureichend.

Die Systembenutzung geschieht über die im Haus verteilten Bildschirmterminals. Die Benutzer erhalten Zugang zum System durch Eingabe einer Benutzeridentifikation und durch ein vom Systemadministrator zugeteiltes Paßwort. Alle Paßwörter werden in unverschlüsselter Form gespeichert und können durch ein entsprechendes Programm dem Administrator angezeigt werden. Dadurch hat der Systemverwalter die Möglichkeit, auf alle in der Anlage gespeicherten Daten zuzugreifen, ohne daß dies für seine Aufgabe erforderlich ist.

Hingegen ist der Zugriff auf die Daten bei den einzelnen Benutzern auf die für ihre Arbeiten erforderlichen Daten beschränkt. Der Zugriff auf die Daten wird jedoch nicht protokolliert — ebensowenig wie die Eingabe der Daten.

Es existieren keinerlei schriftliche Regelungen über
— Aufgaben
— Verantwortlichkeiten
— Befugnisse des Systemverantwortlichen bzw. der Benutzer
— Maßnahmen zur Sicherstellung des Datenschutzes.

Eine Programmdokumentation der ausschließlich in Assembler geschriebenen Programme ist ebenfalls nicht vorhanden, so daß die Betriebssicherheit nicht gewährleistet ist.

(2) In der Hämatologischen Abteilung desselben Krankenhauses werden für die Dokumentation, für die Erstellung von Arztbriefen und für die Statistik von Therapieergebnissen Gesundheitsdaten von Patienten gespeichert. Bei dem Verfahren handelt es sich um ein integriertes Datenbank- und Textverarbeitungssystem.

Das System wird von einem Arzt in Zusammenarbeit mit Informatikstudenten entwickelt und befindet sich noch in der Versuchsphase. Es wird mit echten Daten getestet, zu denen auch die beauftragten Informatikstudenten Zugang haben. Dies ist im Hinblick darauf, daß es sich dabei um Gesundheitsdaten handelt, die der ärztlichen Schweigepflicht unterliegen, besonders bedenklich.

Die personenbezogenen Daten befinden sich auf einer Festplatte und auf speziellen Streamer-Cassetten, die in einem Schrank im Rechnerraum aufbewahrt werden. Dieser Schrank ist lediglich durch ein einfaches Schloß gesichert. Da der Raum an ein Labor anschließt, und die Tür während der Dienstzeit nicht verschlossen ist, reicht diese Sicherung nicht aus.

Die Benutzung des Gerätes wird in ausreichendem Maße durch Benutzeridentifikation und Paßwörter geschützt. Die Paßwörter werden vom Benutzer selbst gewählt und in verschlüsselter Form gespeichert.

Die Zugriffskontrolle scheint nach den mir vorgelegten Informationen in ausreichendem Maße gewährleistet zu sein, da die Zugriffsberechtigungen begrenzt sind und der Zugriff protokolliert wird.

Zur Zeit existieren keine schriftlichen Regelungen über Berechtigungen und Verantwortlichkeiten. Es ist aber vorgesehen, entsprechende Regelungen zu erlassen.

3.1.4.2 Gruppengeschäftsstellen beim Amtsgericht Hamburg

Bei den Gruppengeschäftsstellen Zivil/Miete und Straf/Jugend werden unter Einsatz zweier integrierter Text- und Dateiverarbeitungssysteme verschiedene Verwaltungsaufgaben (u.a. Verwaltung von Stammdaten, Erledigung von Schreibwerk und Protokollführung, Fertigung von Terminrollen usw.) unterstützt bzw. abgewickelt.

Die Systeme bestehen jeweils aus einer Zentraleinheit und den daran angeschlossenen neun (Zivil/Miete) bzw. acht (Straf/Jugend) Bildschirmarbeitsplätzen. Die Zentraleinheiten verfügen über jeweils ein Fest- und ein Wechselplattenlaufwerk. Die on-line mit den Zentraleinheiten verbundenen Bildschirmarbeitsplätze verfügen über eigene Verarbeitungskapazität („Intelligenz") und jeweils zwei Diskettenlaufwerke.

In den Erhebungsbögen wurde angegeben, bei den eingesetzten Verfahren würden keine Dateien im Sinne von § 4 Abs. 4 Nr. 3 HmbDSG verarbeitet. Die Dateien sind auch nicht zum Datenschutzregister gemeldet. Die Prüfung hat ergeben, daß die Stammdaten der Prozeßbeteiligten eindeutig in Dateienform gespeichert und verarbeitet werden. Die Dateien können mittels menugesteuerter Sortierverfahren nach verschiedenen Schlüsselbegriffen umgeordnet und ausgewertet werden.

Die bei den Gruppengeschäftsstellen Zivil/Miete und Straf/Jugend eingesetzten Verfahren sind nahezu identisch; sie unterscheiden sich lediglich hinsichtlich der Struktur der aufgenommenen Stammdaten. Der Stammdatensatz im Bereich Straf/Jugend enthält auch den entsprechenden Paragraphen des Strafgesetzbuches bzw. anderer Rechtsvorschriften, gegen die verstoßen zu haben dem Beschuldigten vorgeworfen wird. Die hier gespeicherten Daten sind dementsprechend als sensibler einzuschätzen als die im Bereich Zivil/Miete gespeicherten Stammdaten.

Die Zentraleinheiten, Bildschirmarbeitsplätze und Drucker sind in den Gruppengeschäftsstellen und in einigen Gerichtssälen untergebracht. Bei den Gruppengeschäftsstellen handelt es sich um größere Büroräume, in denen die Sachbearbeitung, aber auch der Publikumsverkehr abgewickelt wird. Die Zahl der Zugangsberechtigten innerhalb der Dienstzeiten ist somit nicht beschränkt.

Die Zugangstüren sind unverschlossen (Publikumsverkehr!). Die Türen sind mit einfachsten Schlössern ausgestattet, die sich mit einem einfachen Generalschlüssel oder durch einen Dietrich leicht öffnen lassen. Da die Öffnungszeiten — zumindest des Ziviljustizgebäudes (6.00 - 21.00 Uhr) weit über die üblichen Dienstzeiten hinausgehen, ist ein unbefugter Zutritt außerhalb der Dienstzeiten zu den entsprechenden Räumen weitgehend unkontrolliert möglich. Da in den Geschäftsräumen auch sämtliche Prozeßakten hängen, kann somit auch auf diese manuell geführten Datensammlungen ohne weiteres unbefugt zugegriffen werden.

Die Geräte sind zum Teil im Erdgeschoß untergebracht. Die nur einfach verglasten Fenster sind nicht gesondert gesichert.

Daten werden sowohl auf den Fest- und Wechselplattenlaufwerken als auch auf Disketten gespeichert. Die für die Datensicherung eingesetzten Wechselplatten werden in einem nicht weiter gesicherten Fach der Zentraleinheit untergebracht. Ein Verzeichnis der Datenträger, insbesondere der Disketten, existiert nicht. Entsprechend dürfte das Abhandenkommen einzelner Floppydisks kaum bemerkt werden. Die eingesetzte Software ermöglicht es den Sachbearbeitern, unbemerkt sämtliche Daten (z. B. die Stammdatei) auf Disketten zu kopieren und diese Disketten zu entfernen.

Die Benutzer erhalten Zugang zum System durch Eingabe einer Benutzeridentifikation und durch ein Paßwort. Das Paßwort ist bei der Eingabe nicht sichtbar. Zur Vereinfachung des Geschäftsbetriebes hat man darauf verzichtet, verschiedene Paßwörter zu vergeben, so daß nur eine Benutzeridentifikation und ein Paßwort zum Einsatz kommen. Die Bildschirme bleiben für die ganze Dienstzeit aktiviert, so daß ein unbefugt Hinzutretender auch ohne Kenntnis des Paßwortes die Möglichkeit hat, das System zu benutzen, sofern er über entsprechende Kenntnisse verfügt. Da es sich um ein komfortables menugesteuertes und somit sehr benutzerfreundliches System handelt, sind die dazu erforderlichen Vorkenntnisse nur gering. Im Hinblick auf die nur unzureichende Zugangskontrolle und die Tatsache, daß in den Gruppengeschäftsstellen zwangsläufig auch Publikumsverkehr abgewickelt wird, reichen die getroffenen Maßnahmen zur Benutzerkontrolle bei weitem nicht aus. Dieser Eindruck wird noch verstärkt durch die Tatsache, daß die Systemaktivitäten nicht aufgezeichnet werden.

Alle Benutzer haben das gleiche Recht, auf alle Datenbestände zuzugreifen. Differenzierte Zugriffsberechtigungen (Benutzerprofile) sind nicht vorgesehen und gäben auch nur dann einen Sinn, wenn unterschiedliche Benutzeridentifikationen und verschiedene Paßwörter zum Einsatz kämen. Eine Protokollierung des Datenzugriffs findet nicht statt.

Der Transport von Datenträgern findet in der Weise statt, daß von den einzelnen Sachbearbeitern erstellte und bearbeitete Disketten von einem Bildschirmarbeitsplatz an einen anderen Bildschirmarbeitsplatz getragen werden. Dabei werden sogenannte Diskettentaschen benutzt. Jeder Sachbearbeiter verfügt über eine solche Tasche. Es besteht die Gefahr, daß beim Transport Disketten abhanden kommen und dann unbefugt gelesen, verändert oder gelöscht werden.

Zwei Mitarbeiter der Gruppengeschäftsstellen sind für das Funktionieren der Systeme zuständig. Sie haben dabei Zugriff auf sämtliche Datenbestände, obwohl sie sonst nicht sachbearbeitend tätig sind.

Es gibt keine schriftlichen Regelungen über Verantwortlichkeiten und Zuständigkeiten. Datenschutzregelungen sind ebenfalls nicht erlassen worden.

Bei der Prüfung ist deutlich geworden, daß bei der Konzeption des Anfang 1986 in Betrieb gegangenen Verfahrens Datenschutzüberlegungen nicht oder nur sehr unzureichend angestellt wurden. Dies hat dazu beigetragen, daß das Gesamtsystem den Anforderungen nach § 8 Abs. 1 HmbDSG (wonach die technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten) nicht genügt.

Die in meinem Prüfungsbericht aufgestellten Forderungen mögen im Nachhinein nur unter Schwierigkeiten zu realisieren sein; die auftretenden Probleme hätten sich jedoch vermeiden bzw. verringern lassen, wenn schon bei der Systemkonzeption Datenschutzerwägungen angestellt worden wären. Dagegen kann auch nicht ins Feld geführt werden, daß beim Amtsgericht in nicht-automatisierter Form verarbeitete Daten (Akten) ebenfalls nicht ausreichend gesichert werden. Beispielhaft sei hier auf das antiquierte Schließsystem hingewiesen, das generell als unzureichend bezeichnet werden muß, sofern in den betreffenden Räumen personenbezogene oder sonstige sensible Daten verarbeitet werden.

3.2 Neue Medien

Die Neuen Medien haben bereits in meinen bisherigen Tätigkeitsberichten einen breiten Raum eingenommen. Im Berichtszeitraum hat die Reichweite dieser Medien zugenommen und die Pläne zur Realisierung neuer Dienste haben sich konkretisiert. Datenschutzspezifische Probleme ergeben sich in diesem Zusammenhang durch die Digitalisierung der eingesetzten Technik und durch die Dienstintegration (auf die medienpolitischen Aspekte soll an dieser Stelle nicht eingegangen werden).

Das Stichwort „Digitalisierung" beschreibt

— den Ersatz elektromagnetischer Vermittlungstechnik durch programmgesteuerte Vermittlungssysteme,

— den Übergang von analogen Formen der Nachrichtenübertragung (dabei werden akustische Schwingungen in elektromagnetische Schwingungen umgesetzt und beim Empfänger wieder in akustische Schwingungen rückgeformt) zur digitalisierten Übertragung (bei der Sprachübertragung werden die akustischen Schwingungen abgetastet und codiert, die so digitalisierten Signale werden übertragen und beim Empfänger wieder in analoge Schwingungen übersetzt), und

— den verstärkten Einsatz digitaler Endgeräte, z.B. Computer, die die digitalen Signale ohne „Übersetzung" verstehen können.

Durch die Digitalisierung fallen in großem Umfang Verbindungs-, Abrechnungs- und Benutzungsdaten an. Da immer größere Bereiche der menschlichen Kommunikation nicht mehr anonym abgewickelt werden, entsteht die Gefahr, daß die anfallenden Daten länger als erforderlich gespeichert und mit dem Ziel ausgewertet werden, Persönlichkeitsprofile über den Teilnehmer zu gewinnen, die sich beziehen auf

— die Art und den Umfang der Inanspruchnahme der einzelnen Dienste,

— die Anbieter von abgerufenen Informationen und die jeweiligen Kommunikationspartner, mit denen eine Verbindung hergestellt wurde,

— den Inhalt der Kommunikation.

Durch die Zusammenfassung bisher getrennt betriebener Netze zu einem dienste-integrierenden digitalen Netz (Integrated Services Digital Network — ISDN —) und den Übergang zu einem alle Dienste (auch die Verteildienste Rundfunk und Fernsehen) umfassenden dienste-integrierenden, digitalisierten breitbandigen Netz (Integriertes Breitbandiges Fernmelde-Netz — IBFN —) in den 90er Jahren könnte die Gefahr entstehen, daß die zwangsläufig anfallenden Verbindungs- und sonstigen Daten zu immer tiefenschärferen Persönlichkeitsbildern zusammengeführt werden. Da die Dienste mit einer einheitlichen Technik über hierarchisch aufgebaute Netze von nur einem einzigen Betreiber (Deutsche Bundespost) abgewickelt werden, wird mit den neuen Techniken — neben den zu begrüßenden zusätzlichen Möglichkeiten für die Benutzer — auch die technische Infrastruktur geschaffen, die sich für die Kontrolle des Kommunikationsverhaltens der Bürger eignen würde, wenn ein entsprechender Vorsatz vorhanden wäre und die entsprechenden rechtlichen Schranken versagten.

Vor dem Hintergrund eines stark gestiegenen Angebots und der zu erwartenden verstärkten Nutzung von Informations- und Kommunikationsdienstleistungen und der zunehmenden Ausstattung von Betrieben, Behörden und Haushalten mit entsprechendem technischen Gerät erscheinen die beschriebenen Gefahren besonders gravierend. Ihnen kann im Prinzip auf verschiedenen Wegen entgegengetreten werden:

— durch Nicht-Teilnahme,

— durch datenschutzfreundliche technische Ausgestaltung der Dienste,

— durch rechtliche Regelungen.

Auf die Möglichkeit einer individuellen Nichtteilnahme an Diensten soll an dieser Stelle nicht weiter eingegangen werden. Gleichwohl ist darauf hinzuweisen, daß die mangelnde Akzeptanz bestimmter Angebote (z.B. Bildschirmtext) auch darauf zurückzuführen ist, daß die getroffenen Datensicherungsmaßnahmen nicht ausreichen oder Dienstbetreiber nicht immer mit der gebotenen Offenheit über den Stand der Datensicherung und insbesondere über vermeintliche oder tatsächliche Mängel in der Datensicherheit des Systems und die daraufhin getroffenen Maßnahmen berichten (vgl. hierzu insbesondere meine Ausführungen im 4. TB, Nr. 4.1.1.3).

3.2.1 Telekommunikationsordnung der Post (TKO)

Die Bundespost hat es mit der Verordnung über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Fernmeldewesens (Telekommunikationsordnung — TKO —) unternommen, die unübersichtlichen das Fernmeldewesen betreffenden Vorschriften zusammenzufassen und zu vereinheitlichen und bislang ungeregelte Tatbestände durch Rechtsvorschrift zu regeln. Insbesondere ist darauf hinzuweisen, daß die TKO auch klare, wenn auch nicht immer ausreichende Datenschutzbestimmungen enthält. Dies ist gerade in Anbetracht der beschriebenen Gefahren für das informationelle Selbstbestimmungsrecht bedeutsam, die sich aus der Digitalisierung der Telekommunikation ergeben. Gleichwohl sind hier kritische Bemerkungen angebracht:

(1) Die Regelungen der TKO haben zum Teil grundrechtseinschränkenden und zum Teil grundrechtssichernden Charakter. Der Entscheidung über die künftige Struktur der Telekommunikationsdienste kommt für die Lebensverhältnisse der Bevölkerung — die immer stärker von den entsprechenden Dienstleistungen tangiert werden — große Bedeutung zu. Ich bin deshalb der Auffassung, daß für die Regelung solcher, wesentliche Bereiche des öffentlichen Lebens bestimmender Sachverhalte die Verordnungsermächtigung aus § 14 Postverwaltungsgesetz für die in der TKO zusammengefaßten Sachverhalte nicht ausreicht und daß vielmehr der Gesetzgeber die wesentlichen Entscheidungen selbst in der Weise treffen muß, daß den verfassungsgerichtlichen Vorgaben folgende gesetzliche Regelungen gefunden und dabei die Belange des Datenschutzes in angemessener Weise berücksichtigt werden.

(2) Die von den Datenschutzbeauftragten von Bund und Ländern formulierten Forderungen sind vom Bundesministerium für das Post- und Fernmeldewesen zum Teil nicht oder nur unzureichend in der TKO berücksichtigt worden. Lediglich beim Bildschirmtext-Dienst entsprechen die Datenschutzbestimmungen im wesentlichen den geforderten Standards. Dagegen sind folgende Forderungen der Datenschutzbeauftragten nicht erfüllt worden:

— Jeder Kommunikationsdienst birgt auch technisch bedingte Risiken in sich, die vom Teilnehmer nicht ohne weiteres erkennbar sind. Deshalb sollte die Deutsche Bundespost zur Information der Teilnehmer über die grundlegenden technischen Bedingungen der jeweiligen Dienste und die damit verbundenen unvermeidlichen Risiken bei der Datensicherung verpflichtet werden. Dadurch würde den Teilnehmern auch ein sicherheitsförderndes Nutzungsverhalten erleichtert.

— Eine präzise Umschreibung der öffentlichen Telekommunikationsdienste einschließlich der Festlegung der jeweils gespeicherten und weiterverarbeiteten Verbindungs-, Abrechnungs- und Benutzungsdaten sind notwendig, damit der Bürger die durch die Dienstinanspruchnahme resultierenden Einschränkungen seines informationellen Selbstbestimmungsrechts klar erkennen kann. Aus dem gleichen Grund sind auch klarere Regelungen über die Zulassung der Benutzung des öffentlichen Netzes für „sonstige Kommunikationszwecke" erforderlich.

— Die TKO sieht vor, daß personenbezogene Daten von der Deutschen Bundespost für keine anderen als „Telekommunikationszwecke" verwendet werden. Anstelle dieser sehr unscharfen Formulierung muß eine klare und nachvollziehbare Nutzungsbegrenzung für die anfallenden personenbezogenen Daten treten.

— Die TKO gestattet es der Deutschen Bundespost, personenbezogene Daten, die der Bereitstellung der Verbindung dienen, zu speichern oder sonst zu verarbeiten, soweit dies für die jeweilige Kommunikationsdienstleistung erforderlich ist oder der Teilnehmer eine andere Art der Verarbeitung beantragt hat. Angesichts der Tatsache, daß Verbindungsdaten Auskunft über das Kommunikationsverhalten der einzelnen Teilnehmer geben, müssen diese von jeglicher Übermittlung ausgeschlossen werden. Ein solches Verbot ist auch deshalb notwendig, weil sich die Verbindungsdaten zumeist nicht allein auf den „Anrufer" beziehen, sondern auch auf seine Kommunikationspartner (z.B. Telefon-Zielnummer).

— Auf den Zwangseintrag im Telefonbuch muß — gerade auch im Hinblick auf das bereits realisierte „elektronische Telefonbuch", das über Bildschirmtext abzurufen ist — verzichtet werden. Anders als das konventionelle, gedruckte Telefon-

buch könnte das elektronische Telefonbuch (durch Einsatz intelligenter Btx-Endgeräte) als bundesweites Adreßregister der Telefonkunden benutzt werden. Die Zwangseintragung stellt in diesem Zusammenhang eine wesentliche Beeinträchtigung des Rechts auf informationelle Selbstbestimmung dar.

— Die von der Post angebotene Dienstleistung „Feststellen ankommender Wählverbindungen" sollte auf begründete Einzelfälle beschränkt werden, da dem Anrufer nicht bekannt ist, inwieweit der angerufene Teilnehmer von dieser Betriebsmöglichkeit Gebrauch macht, die es ermöglicht, die Ausgangspunkte aller ankommenden Gespräche zu registrieren und dem Angerufenen zur Kenntnis zu bringen. Die in der TKO vorgesehene Möglichkeit, diese Dienstleistung jedem Teilnehmer ohne Begründung gegen Zahlung einer Gebühr einzuräumen, birgt die Gefahr in sich, daß hier eine mißbräuchliche Kontrolle der Anrufer bzw. der Inhaber der Anschlüsse — die ja nicht unbedingt mit den Anrufern identisch sind — erfolgt.

(3) Durch eine datenschutzfreundlichere Dienstgestaltung ließe sich die Speicherung von Daten und die Beeinträchtigung von Belangen der Betroffenen vermeiden:

— Die „Vergleichszählung" durch die Post, bei der alle abgehenden Verbindungen mit Zielnummer zum Zwecke des Gebührennachweises registriert werden, birgt ebenfalls Gefahren für das informationelle Selbstbestimmungsrecht in sich, wenn z.B. ein Anschluß von mehreren Benutzern gebraucht wird und der Anschlußinhaber so von den Kommunikationspartnern der „Mitbenutzer" Kenntnis erhält. Vorzuziehen und unter Datenschutzgesichtspunkten unbedenklich wäre hier die Schaffung der Möglichkeit der komfortablen und ausführlichen Gebührenzählung beim Teilnehmer selbst.

— Die Daten werden in der Regel unverschlüsselt über die von der Deutschen Bundespost unterhaltenen Fernmeldenetze übertragen. Dadurch ergibt sich das Risiko des Abhörens. Dies könnte durch ein Angebot eines Dienstes für die Verschlüsselung von Nachrichten vermindert werden. In Anbetracht der künftig und zum Teil schon heute eingesetzten Technik dürften dem Einsatz eines solchen Dienstes auch Kapazitätsrestriktionen kaum im Wege stehen.

3.2.2 TEMEX

In meinen früheren Tätigkeitsberichten (2. TB S. 41, 3. TB S. 22, 4. TB S. 28) habe ich über Wirkungsweise und datenschutzrechtlich relevante Aspekte von TEMEX berichtet. Die bei abstrakter Betrachtung möglicher Anwendungen gesehenen Gefahren haben sich bisher nicht konkretisiert.

Hamburg gehört zu den elf Städten, in denen die Deutsche Bundespost sogenannte Betriebsversuche durchführt, um nach der Entwicklung der postseitig (z.B. in den TEMEX-Zentralen) benötigten Technik, die mit der im Mai 1986 durch die Post getroffenen Auswahlentscheidung für zwei Systeme vorerst zu einem Abschluß gekommen ist, auch die Entwicklung der anwenderseitig erforderlichen Technik (z.B. in den TEMEX-Leitstellen) zu ermöglichen und zu fördern. Die Post erwartet, aus der als Betriebsversuch deklarierten Einführungs- und Erprobungsphase des Dienstes Informationen und Erkenntnisse für die endgültige Entscheidung über die Technik zu gewinnen, die später (ab 1987) im Regelbetrieb eingesetzt werden soll. In Hamburg sind inzwischen zwar die vier Fernsprechanschlußbereiche (eventuell kommt ein fünfter hinzu) festgelegt worden, in denen die TEMEX-Hauptzentrale und die TEMEX-Zentralen eingerichtet werden sollen, an die potentielle Anbieter von TEMEX-Dienstleistungen ihre TEMEX-Leitstellen und die TEMEX-Netzanschlüsse ihrer Kunden anschließen können. Mit dem Betriebsversuch ist jedoch noch nicht begonnen worden.

Die Post hat den Termin für die Bereitstellung der postseitigen Technik mehrmals hinausgeschoben und zuletzt angekündigt, daß TEMEX-Anbieter frühestens ab Dezember 1986 die Möglichkeit zum Anschluß von TEMEX-Leitstellen haben werden. Die potentiellen Anbieter von TEMEX-Dienstleistungen sind aber — jedenfalls in Hamburg — selbst noch nicht bereit und aufgrund fehlender Technik und Software auch noch nicht

in der Lage, mit dem Test einer Fernwirkdienstleistung zu beginnen. Bei einer Informationsveranstaltung der Post für die Teilnehmer aller Betriebsversuche im August dieses Jahres wurde deutlich, daß außerhalb Hamburgs vorwiegend kommunale Anwender Interesse an TEMEX zeigen, und zwar zur Realisierung recht spezieller technischer Projekte (z.B. Park-Leit-System o.ä.). In Hamburg sind unter den Interessenten eine Reihe privater Anwender. Die Anwendungen, mit denen sich Interessenten in Hamburg an dem Betriebsversuch beteiligen wollen, betreffen

— die Überwachung der Funktionsfähigkeit von technischen Geräten und Anlagen (z.B. Automatenfüllstand, Störungsfreiheit von Kühlanlagen, Rolltreppen usw., Temperaturregelung von Heizungsanlagen, Ein- und Ausschalten von Beleuchtungen),

— die klassischen Dienstleistungen der Wach- und Sicherungsunternehmen (Überwachung von Brand- und Einbruchsmeldern in öffentlichen und privaten Objekten wie Produktionsstätten, Behördengebäuden, Privathäusern),

— das Ablesen von Verbrauchsmeßgeräten (Zählerstände).

Während die Angebote von Dienstleistungen der unter dem ersten Spiegelstrich genannten Art keinerlei datenschutzrechtliche Relevanz haben, weil keine personenbezogenen Daten anfallen können, können bei den unter den anderen Spiegelstrichen genannten Dienstleistungen personenbezogene Daten in begrenztem Umfang anfallen. Die Datenschutzbeauftragten haben deshalb bestimmte Anforderungen an die technische und vertragliche Ausgestaltung der Angebote gestellt. Diese Anforderungen habe ich in meinem 4. Tätigkeitsbericht (Seite 29) genannt. An ihnen wird festgehalten.

Insbesondere hat kein potentieller Anwender Pläne angekündigt, sich an dem Betriebsversuch mit einer Dienstleistung zu beteiligen, bei der mittels besonderer Technik Personen im privaten Bereich überwacht und dabei anfallende Daten über das TEMEX-Netz an die TEMEX-Zentrale des Anbieters weitergeleitet werden. Denkbar wäre z.B. eine Dienstleistung, bei der Personen, die aus Altersgründen (Säuglinge, Kinder, alte Menschen) oder wegen akuter Erkrankung oder dauernder Hilfsbedürftigkeit unter Aufsicht oder in Kontakt zu Pflegediensteinrichtungen bleiben müssen, von einer Pflegedienstzentrale (privater Anbieter, karitative Einrichtung, Krankenhaus) aus „überwacht" und bei Bedarf durch von der Zentrale aus eingesetzte Hilfskräfte betreut werden. Die Eigenart des TEMEX-Dienstes, der gekennzeichnet ist durch Datenübertragungen geringen Umfangs (1 digitales Zeichen = Bit, Gruppen von 8 Bits oder — bei nicht zeitkritischen Anwendungen — bis zu 48 Bitgruppen zu 8 Bits je Meldung und eine begrenzte Anzahl von Meldungen pro Monat), schließt die ständige Übertragung von Geräuschen oder gar von bewegten Bildern einer Videokamera aus. Die Überwachung als TEMEX-Dienstleistung kann immer nur auf die Meldung von Zustandsänderungen (Säugling fängt an zu schreien, im Krankenzimmer ist das Licht eingeschaltet worden, eine Klingel wurde betätigt), die durch Kameras und andere technische Geräte festgestellt wurden, oder auf das Ausbleiben eines angeforderten oder verabredeten Signals gerichtet sein.

Zur Zeit sehen ich keine konkreten Gefahren für die Persönlichkeitsrechte von Bürgern. Ich werde die Entwicklung jedoch weiter aufmerksam verfolgen und zu gegebener Zeit Anwendungen daraufhin überprüfen, ob die aus datenschutzrechtlicher Sicht geforderten Vorkehrungen getroffen worden sind.

4. Grenzüberschreitender Datentransfer und Datenschutz

4.1 Einleitung

Ebenso wie man heute in den entlegensten Teil der Welt telefonieren kann, ist es auch möglich geworden, Computer Informationen austauschen zu lassen und Daten von einem Land der Erde in jedes beliebige andere Land zu senden — mit einer Leichtigkeit und Schnelligkeit, die die Möglichkeiten des Telefons bei weitem übertreffen.

So kann die Feststellung nicht verwundern, daß seit Beginn der siebziger Jahre der internationale Datentransfer ständig steigende Zuwachszahlen zu verzeichnen hat. Zunehmender Informationshunger und technische Neuerungen in der Möglichkeit des Datentransports haben dieses Wachstum genährt und treiben es immer schneller voran. Informationsbedarf und das technisch Machbare steigern sich gegenseitig.

Den Vorteilen stehen dabei nicht zu unterschätzende Gefahren gegenüber: Kunden, Geschäftspartnern und besonders Arbeitnehmern — auch Führungskräfte sind da nicht verschont — droht die Verdatung der persönlichen Integrität in entlegenen, kaum zu kontrollierenden und anonymen Massenspeichern. Während Waren und Personen an der Grenze gestoppt und geprüft werden können, fließen Datenströme unsichtbar und in aller Stille über die Ländergrenzen, und es ist unerheblich, wie viele Grenzen die Daten passieren. Aus diesem Grunde können zum Umfang des grenzüberschreitenden Datenverkehrs auch keine konkreten Zahlen festgestellt werden; es lassen sich lediglich Schätzungen anstellen und die nehmen sich gewaltig aus: Eine Untersuchung der Vereinten Nationen geht davon aus, daß die Zahl der Anschlußstellen an Datenübertragungsnetze allein in Westeuropa von 393 000 im Jahre 1979 auf über 1,5 Millionen im Jahre 1987 angestiegen sein wird. Die Zahl der Datenstationen wird nach dieser Schätzung im gleichen Zeitraum von 625 000 auf beinahe vier Millionen angewachsen sein und die Anzahl der täglichen internationalen Transaktionen sich nahezu verneunfacht haben.

Wie sieht es da mit dem Schutz des Bürgers vor „Verdatung" aus? Können wirtschaftliche Interessen und grenzüberschreitender Datenschutz zusammenfinden? Verliert das Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht abgeleitet hat, im grenzüberschreitenden Datenverkehr seinen Sinn? Der Begriff der „Datenoase" — angelehnt an den Begriff der Steueroase — macht die Runde: hiermit sind Länder bezeichnet, die nur einen geringen Standard des Datenschutzes aufweisen oder überhaupt nicht über datenschutzrechtliche Vorschriften verfügen. Welche Regelungen trifft das BDSG für den grenzüberschreitenden Datenverkehr? Bietet das BDSG einen ausreichenden Schutz vor den Gefahren eines weltweit möglichen Datentransfers? Sind Verbesserungen oder Änderungen notwendig?

4.2 Merkmale des grenzüberschreitenden Datentransfers und seine Risiken für die Betroffenen

Als erstes sind drei Fragen zu klären: wer sind die am Datentransfer beteiligten Stellen; wie setzen sich die Daten zusammen, die übermittelt werden, und auf welchen Übertragungswegen vollzieht sich der internationale Datenverkehr?

Vorwiegend sind es Unternehmen, die im Interesse ihrer wirtschaftlichen Ziele Daten mit ausländischen Stellen austauschen. Aber auch staatliche Institutionen und supranationale Einrichtungen wie z.B. INTERPOL empfangen und versenden Daten.

Im nichtöffentlichen Bereich läßt sich eine Unterscheidung der datenverarbeitenden Stellen zunächst nach dem Zweck der Datenverarbeitung treffen. Hier sind es die Servicerechenzentren, Marktforschungsinstitute und gewerblichen Wirtschaftsauskunfteien, die Daten regelmäßig nicht für eigene, sondern für fremde Zwecke verarbeiten. Die Möglichkeiten der ADV haben es mit sich gebracht, daß die Dienstleistung „Datenverarbeitung" nicht mehr an den Ort des Auftraggebers gebunden ist. Abends das Datenmaterial versenden, nachts bearbeiten lassen und morgens fertig zurückerhalten — das ist eine Form der Datenverarbeitung, die heute sogar über den Atlantik hinweg praktiziert wird.

In der großen Mehrzahl der Fälle betreiben die Unternehmen die Datenverarbeitung im eigenen Interesse zur Realisierung ihrer eigenen Geschäftsziele. Zum einen sind es hier deutsche Unternehmen, die Daten an eigene Betriebsstätten oder Niederlassungen im Ausland übersenden. Daneben besteht der Datenverkehr zwischen deutschen und ausländischen Unternehmen, sei es, daß die Unternehmen als Konzerne miteinan-

der verbunden sind oder in anderer Form, z. B. durch joint-venture-Verträge zusammenwirken oder sei es, daß sie grundsätzlich unabhängig voneinander arbeiten, wie etwa regelmäßig Zulieferer und Subunternehmen.

Die Art der übermittelten Daten ergibt sich weitgehend aus den wirtschaftlichen oder sonstigen Zielen der am Datentransfer beteiligten Stellen, z. B.: Zahlen und Fakten der Produktion, Rechnungslegung, Lagerverwaltung, Lieferbarkeit, Beschaffung, Forschung usw. bewegen sich zwischen Geschäftsstellen, Fabriken, Zentralen und Niederlassungen hin und her. Ein Teil dieser Daten ist aus datenschutzrechtlicher Sicht ohne Interesse, soweit es sich etwa um ausschließlich unternehmensbezogene Daten handelt oder um technisch-wissenschaftliche Angaben.

Nicht selten geht es aber um die Übermittlung von Informationen, die mit personenbezogenen Angaben durchsetzt sind, wie z. B. Lieferdaten oder Angaben über Auftragslisten. Teilweise werden sogar ausschließlich personenbezogene Daten übermittelt, z. B. Kundenlisten oder Personaldaten. Die Schätzungen, wie hoch der Anteil personenbezogener Daten am Gesamtumfang des internationalen Datenverkehrs sein mag, müssen Spekulation bleiben — auf die genaue Kenntnis kommt es aber auch nicht an: bei einigen hundert Millionen Datentransaktionen pro Arbeitstag geht der Anteil personenbezogener Daten selbst bei der Annahme von 0,1 % immer noch in die Hunderttausende.

Ebenso vielfältig wie die am internationalen Datentransfer beteiligten Stellen und die Art der übermittelten Informationen zeigen sich die unterschiedlichen Wege des Datentransports: die traditionellen Arten der Übermittlung — per Bote und per Post — lassen sich zur Übertragung größerer Datenmengen nutzen, indem die Daten entweder als Listen, Mikrofiches, Akten oder in direkt maschinenlesbarer Form auf Datenträgern — etwa Magnetbändern, Magnetplatten, Kassetten, Disketten usw. — verschickt werden. Da ein wesentlicher Vorteil der EDV, nämlich Schnelligkeit und Aktualität dabei verlorengeht, dürfte diese Art der Datenübertragung immer mehr zurückgehen. Fernschreibnetze weisen zwar eine größere Geschwindigkeit auf, aber auch sie sind gemessen an modernen Datennetzen eher als langsam zu bezeichnen. Vor allem aber werden die Daten nicht in maschinenlesbarer Form übermittelt, so daß eine direkte Verbindung von Computer zu Computer nicht möglich ist. Hier liegt der wichtigste Unterschied zu den Datennetzen: sie ermöglichen einen Datenaustausch zwischen verschiedensten EDV-Geräten, also zwischen mehreren Rechenanlagen, zwischen Terminal und Datenbank, zwischen Computer und weit entfernt aufgestellten Peripheriegeräten wie z. B. Hochleistungsdruckern. Dabei vollzieht sich der Datenaustausch mit immer größer werdenden Übertragungsgeschwindigkeiten. Bei den Datennetzen bedient man sich der gesamten Palette neuester technischer Möglichkeiten, angefangen bei verschiedenen Arten der Kabeltechnik bis hin zu Satelliten als Übertragungsweg. Träger von Datennetzen sind sowohl öffentliche Stellen — wie etwa die Deutsche Bundespost, die das Netz für jeden Benutzer gegen Entgelt bereitstellt — als auch private Unternehmen sowie Unternehmens- oder Organisationsgemeinschaften.

Eine Bewertung des Datenflusses hat Vorteile und Gefahren gegeneinander abzuwägen. Erst so kann bestimmt werden, welche datenschutzrechtlichen Regelungen notwendig sind, um die zumeist wirtschaftlichen Interessen einerseits und dem Schutz der persönlichen Integrität andererseits gerecht zu werden.

Die Vorteile für verarbeitende Stellen ergeben sich weitgehend aus der Möglichkeit, EDV-Anlagen jederzeit und weltweit verbinden und nutzen zu können. Expertenwissen muß nicht teuer eingekauft werden, sondern ist weltweit abrufbar. Branchensoftware kann über das Datennetz geliefert werden und muß nicht teuer auf den üblichen Verkehrswegen zugestellt werden. Unterschiedliche Zeitzonen lassen sich zur Kostensenkung ausnutzen, indem nachts Daten dort verarbeitet werden, wo zur gleichen Zeit Tag ist. Niederlassungen können unabhängig von der Entfernung zum Stammhaus kontrolliert und geführt werden. Der allgemeine Warenaustausch wird erleichtert, da ein jederzeitiger Überblick über Bestand und Verbleib von Waren möglich ist, und die Produk-

tion läßt sich besser steuern, wenn Termine mit den Zulieferern je nach Bedarf abgestimmt werden können.

Die allgemeinen Gefahren der automatisierten Datenverarbeitung drohen in besonderem Maße dann, wenn personenbezogene Daten im Ausland verarbeitet werden. Sind die Daten erst aus dem Geltungsbereich des BDSG hinausgelangt, hat der Betroffene nur wenig Möglichkeiten, etwas gegen die Beeinträchtigung seiner persönlichen Integrität zu unternehmen. Selbst wenn das ausländische Recht datenschutzrechtliche Vorschriften enthält und sogar ebenso weitreichende Rechte eröffnet wie das BDSG, ist die Durchsetzung dieser Rechte im Ausland problematisch. Soweit der Betroffene von der Übermittlung überhaupt erfährt, ist für ihn nicht leicht zu erkennen, an welche Stelle im Ausland er sich wenden soll. Hinzu kommen sprachliche Probleme: wer ist schon in der Lage, datenschutzrechtliche Ansprüche in einer Fremdsprache zu formulieren? Im übrigen ist zu bedenken, daß die meisten Länder nicht über ein Datenschutzrecht verfügen, das sich am BDSG messen ließe.

4.3 Lösungsversuche durch internationale Zusammenarbeit

Idealziel des grenzüberschreitenden Datenschutzes wäre ein weltweit gleich hohes Niveau datenschutzrechtlicher Bestimmungen. Angesichts des Datenschutzgefälles selbst in Westeuropa mutet dieses Idealziel utopisch an. Diesem Ziel kann man allerdings durch völkerrechtliche Vereinbarungen näherkommen, indem in verschiedenen Staaten international zumindest ein ähnlich hoher Standard des Datenschutzes herbeigeführt wird. Dementsprechend hat die OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) 1980 Richtlinien zum Schutz der Privatsphäre und zum grenzüberschreitenden Fluß personenbezogener Daten verabschiedet. In ihrer Präambel wird einerseits auf den notwendigen Schutz der Privatsphäre hingewiesen, andererseits aber auch besonders die Notwendigkeit eines Datenaustausches betont, indem festgelegt wird, daß die Errichtung ungerechtfertigter Hindernisse für die Entwicklung der wirtschaftlichen und sozialen Beziehungen zwischen den Mitgliedstaaten verhindert werden soll. Der erste Abschnitt legt u.a. den Anwendungsbereich fest; er umfaßt die Verarbeitung personenbezogener Daten natürlicher Personen unabhängig davon, ob die Verarbeitung in automatisierten Verfahren erfolgt. Im zweiten Abschnitt finden sich Grundsätze für die einzelnen Phasen der Datenverarbeitung im nationalen Bereich. Abschnitt drei beschäftigt sich mit dem grenzüberschreitenden Datenverkehr, ohne jedoch Regelungen von wünschenswerter Klarheit zu treffen. Auch der vierte Abschnitt, der die Umsetzung der Richtlinien durch Verfahren und Institutionen zum Inhalt hat, bietet keine griffigen Normen. Entsprechendes gilt für die Bestimmungen des fünften Abschnitts zur internationalen Zusammenarbeit in Datenschutzfragen. Da die Richtlinien in der Form einer Empfehlung ergangen sind, werden die Mitgliedstaaten durch sie nicht gebunden.

Eine völkerrechtlich verbindliche Abmachung dagegen stellt die Datenschutz-Konvention des Ministerrates des Europarats vom 17. September 1980 dar. Sie ist als „Meilenstein zum internationalen Datenschutz" bezeichnet worden. Zwar sind die Regeln des Übereinkommens nicht automatisch Teil des Rechtssystems der Vertragsstaaten, die das Übereinkommen ratifiziert haben. Aber die Vertragsstaaten verpflichten sich mit der Unterzeichnung der Konvention, spätestens mit dem Inkrafttreten die in ihr niedergelegten Grundsätze zu verwirklichen. Für die Bundesrepublik, die das Übereinkommen Anfang 1985 ratifiziert hat, ergibt sich daraus kein unmittelbarer Änderungsbedarf, weil die Konvention in weiten Bereichen unserem Verständnis von datenschutzrechtlichen Normen folgt. Die Begriffe personenbezogene Daten und Datenverarbeitung etwa sind an die entsprechenden Definitionen des BDSG angelehnt. Trotz der notwendigen Vereinheitlichung des Datenschutzes in verschiedenen Ländern ist die Konvention dennoch flexibel. Den Unterzeichnerstaaten ist freigestellt, an weitergehenden innerstaatlichen Bestimmungen festzuhalten. Die Konvention versteht sich als Normierung von Mindestanforderungen für den Datenschutz. Für den Betroffenen bringt die Konvention den Vorteil, das Verfahren zur Erteilung von Auskünften und zur Durchsetzung von Rechten gegenüber datenverarbeitenden Stellen der Unterzeichnerstaaten

geregelt zu finden, ebenso die Frage der Kosten und der Stellen, an die sich der Betroffene wenden kann. Die Konvention bestimmt, daß jeder Unterzeichnerstaat eine oder mehrere Behörden anzugeben hat, die als Verbindungsstelle zu den Datenschutzbehörden des eigenen Landes und der anderen Staaten fungieren. Für die Bundesrepublik sind dies das Bundesinnenministerium sowie jeweils eine Behörde der Länder. Ein beratender Ausschuß, der aus Vertretern der Unterzeichnerstaaten besteht, trägt zur Harmonisierung des Datenschutzrechts in den Unterzeichnerländern bei. Ein weiterer Vorteil der Konvention besteht darin, daß sie sich nicht auf Mitgliedstaaten des Europarats beschränkt, sondern unter bestimmten formellen Voraussetzungen auch den Beitritt anderer Staaten — hier ist vor allem an Mitgliedstaaten der OECD, an die USA, Kanada und Japan gedacht — ermöglicht.

Die Konvention stellt ein allgemeines Regelungswerk dar, das durch bereichsspezifische Regelungen ergänzt wird. So hat der Europarat u.a. Empfehlungen über Bestimmungen für automatische medizinische Datenbanken, zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik und für den Bereich des Direktmarketing einschließlich des Adressenhandels verabschiedet.

Rechtsvorschriften der Europäischen Gemeinschaft zum Datenschutz bestehen bisher nicht, obwohl sich das Europäische Parlament wiederholt mit Datenschutzfragen befaßt hat. In seiner Sitzung vom 8. und 9. März 1982 verabschiedete das Europäische Parlament eine Entschließung, in der es zwar eine Gemeinschafts-Richtlinie für erwägenswert hält, eigene gesetzgeberische Tätigkeit aber nur für den Fall vorsieht, daß sich die Europaratskonvention als unzureichend erweisen sollte.

Trotz der Konvention des Europarats, mit der jetzt Erfahrungen zu sammeln sein werden, sind nicht alle Probleme des grenzüberschreitenden Datenverkehrs gelöst, dies schon deshalb nicht, weil die Zahl der nicht beigetretenen Länder die Zahl der Unterzeichnerländer bei weitem überwiegt. Daher stellt sich die Frage, wie im Hinblick auf eine Datenübermittlung in diese Länder ein hinreichender Schutz personenbezogener Daten zu verwirklichen ist. Da ohne internationale Vereinbarungen das BDSG nicht über seinen Geltungsbereich hinausreichen kann, läßt sich der Schutz nur durch besondere Zulässigkeitsregeln für den Datenexport erreichen.

4.4 Die Regelung des grenzüberschreitenden Datenverkehrs im BDSG

Eine abschließende Regelung der mit dem grenzüberschreitenden Datenverkehr verbundenen Probleme hält das BDSG nicht bereit, einen Abschnitt „grenzüberschreitender Datentransfer" sucht man im BDSG vergeblich. Das heißt allerdings weder, daß ein grenzüberschreitender Datenversand ausgeschlossen ist, noch daß er unbegrenzt möglich ist. Vielmehr bestimmt sich die Zulässigkeit grenzüberschreitender Datenübermittlungen nach den allgemeinen Regelungen, die das BDSG für die Verarbeitung von Daten trifft. Allein für den Bereich der Auftragsdatenverarbeitung trifft das Gesetz (für den nichtöffentlichen Bereich) eine spezielle Regelung: Datenverarbeiter, die Daten nicht für eigene, sondern für fremde Zwecke verarbeiten, sieht das Gesetz im Verhältnis zu ihren Auftraggebern nicht als Dritte an (§ 2 Abs. 3 Nr. 2 BDSG), da sie bei der Datenverarbeitung ausschließlich im Interesse des Auftraggebers handeln. Auftraggeber und Datenverarbeiter, in der Regel ein Servicerechenzentrum, behandelt das BDSG also als eine Einheit. Dies gilt aber nur, solange sich das Servicerechenzentrum im Inland befindet. Das Gesetz stellt ausdrücklich klar, daß ein ausländischer Auftrags-Datenverarbeiter in jedem Fall als „Dritter" im Sinne des BDSG anzusehen ist. Mit der Folge: weil das BDSG auf den Datenverarbeiter im Ausland nicht mehr anwendbar ist und den Schutz des Betroffenen nicht mehr sicherstellen kann, ist eine Übermittlung von Daten nur unter den allgemeinen Zulässigkeitsvoraussetzungen möglich. Die rechtliche Situation ist damit für die grenzüberschreitende Auftragsdatenverarbeitung in eindeutiger Weise und durchaus zufriedenstellend geklärt.

Die allgemeinen Vorschriften des BDSG bestimmen, daß die Datenverarbeitung — also das Speichern, Übermitteln, Verändern oder Löschen von Daten — nur dann zu-

lässig ist, wenn entweder das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder eine wirksame Einwilligung des Betroffenen vorliegt. Das unbefugte Übermitteln von personenbezogenen Daten ist nach § 41 BDSG mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht.

4.5 Bewertung der Übermittlungsvorschriften des BDSG

Auf den ersten Blick hat es den Anschein, als könne das BDSG die persönliche Integrität des einzelnen auch ohne ausdrückliche Regelung des grenzüberschreitenden Datenverkehrs gewährleisten, indem es den Export personenbezogener Daten nur im Rahmen der allgemeinen Vorschriften zuläßt. Bei genauerem Hinsehen aber zeigt sich, daß dieser Schutz nur scheinbar so exakt und wirkungsvoll ist, wie es im Interesse des einzelnen wünschenswert wäre. Schon die Zulässigkeit der Übermittlung im Inland selbst ist nicht selten eine schwierige Auslegungsfrage.

Der Wortlaut des § 24 Abs. 1 Satz 1 BDSG etwa läßt offen, ob die Voraussetzung, daß „schutzwürdige Belange des Betroffenen nicht beeinträchtigt" werden dürfen, allein auf die dritte Alternative (Übermittlung zur Wahrung berechtigter Interessen) zu beziehen ist oder auch auf die ersten beiden Alternativen (im Rahmen eines Vertragsverhältnisses oder vertragsähnlichen Verhältnisses). Für die Zulässigkeit einer Übermittlung ins Ausland kann es auf diese umstrittene Frage entscheidend ankommen: fehlt es in dem Land, in das personenbezogene Daten im Rahmen eines Vertragsverhältnisses — wie etwa im Rahmen eines Arbeitsvertrages — übermittelt werden sollen, an einem dem BDSG vergleichbaren Datenschutzgesetz, so sind schutzwürdige Belange des Betroffenen beeinträchtigt, da keinerlei Schutz mehr möglich ist. Würde die Voraussetzung, daß schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden dürfen, also nicht auch auf die ersten beiden Alternativen des § 24 Abs. 1 Satz 1 BDSG bezogen, wäre eine Übermittlung ins Ausland trotz der Beeinträchtigung schutzwürdiger Belange möglich.

In § 32 BDSG fehlt der Hinweis auf „schutzwürdige Belange" des Betroffenen im Wortlaut des Gesetzes völlig. Es ist umstritten, ob für eine Übermittlung nicht dennoch die schutzwürdigen Belange des Betroffenen zu beachten sind. Die Meinungen gehen darüber auseinander, ob mit dem Hinweis auf das „berechtigte Interesse" des Empfängers an der Übermittlung neben den Interessen des Empfängers auch die Interessen des Betroffenen zu berücksichtigen sind. Eine Auffassung geht dahin, daß das „berechtigte Interesse" des Empfängers immer ins Verhältnis zu setzen ist mit den schutzwürdigen Belangen des Betroffenen, daß also das „berechtigte Interesse" des Empfängers und die Belange des Betroffenen miteinander abzuwägen sind, obwohl im Wortlaut des § 32 Abs. 2 BDSG ein ausdrücklicher Hinweis auf die schutzwürdigen Belange des Betroffenen fehlt. Dieser Meinung schließe ich mich an. Demnach ist eine Auslandsübermittlung auch nach § 32 Abs. 2 BDSG ausgeschlossen, wenn das Empfängerland keinen dem BDSG ähnlichen Standard des Datenschutzes aufweist.

Das BDSG weist weitere Streitpunkte auf: „Übermittlung" ist die Weitergabe von personenbezogenen Daten an einen von speichernder Stelle und Betroffenem verschiedenen „Dritten". Im Zusammenhang mit der Frage, wer nun als „Dritter" anzusehen ist i.S. des BDSG, gehen die Auffassungen darüber auseinander, ob die im Ausland tätige unselbständige Zweigstelle eines deutschen Unternehmens als Unternehmensteil zum deutschen Unternehmen zu rechnen ist (wie dies für inländische Zweigstellen allgemein bejaht wird), oder ob die ausländische Zweigstelle etwa als „Dritter" im Sinne des BDSG einzustufen ist. Die Antwort auf diese Frage entscheidet darüber, ob z.B. die Weitergabe von personenbezogenen Arbeitnehmerdaten eines deutschen Unternehmens an eine Baustelle im Ausland eine Datenübermittlung im Sinne des BDSG darstellt und damit nur unter den Voraussetzungen der allgemeinen Zulässigkeitsvorschriften möglich ist, oder ob es sich um einen internen Datenaustausch innerhalb eines Unternehmens handelt, der grundsätzlich keinen Schranken unterliegt. Für beide Seiten gibt es gewichtige Argumente: einerseits beruft man sich auf die rechtliche Einheit, die Unternehmen und Zweigstelle bilden und betont, daß die Qualifizierung der

Zweigstelle als „Dritter" zu einer unzulässigen Ausdehnung der Strafdrohung gem. § 41 BDSG führe, daß sie auf einer „verfassungsrechtlich äußerst bedenklichen" Gesetzesanalogie beruhe. Die Gegenauffassung betont die Ausgestaltung des BDSG als Auffanggesetz, das einen lückenlosen Schutz des einzelnen vor der Verdatung gewährleisten soll, was ohne die Einstufung der unselbständigen Zweigstelle im Ausland als „Dritter" schlechthin nicht möglich wäre, da sonst personenbezogene Daten ohne jede weitere Prüfung den Geltungsbereich des BDSG verlassen könnten. Der Streit soll hier nicht in seiner ganzen Breite dargestellt werden, es genügt die Feststellung, daß verschiedene Auslegungen des Gesetzes möglich sind und auch vertreten werden.

Betrachtet man den umgekehrten Fall, daß ein ausländisches Unternehmen in der Bundesrepublik eine unselbständige Zweigstelle unterhält, dann ist sogar ein handfester Mißbrauch mit personenbezogenen Daten denkbar: sieht man hier ebenfalls die Zweigstelle nicht als „Dritten" an und sammelt diese Zweigstelle Daten, um sie an das ausländische Unternehmen weiterzugeben, ohne sie selbst in einer Datei zu speichern, dann unterliegt der Datenexport keinerlei Schranken, weil die Erhebung von Daten nicht unter den Begriff der „Datenverarbeitung" fällt, die durch das BDSG geregelt wird, und die Speicherung vom BDSG nur erfaßt wird, wenn sie in einer Datei erfolgt. Mit entsprechender Auslegung könnte der Datenexport ungehemmt florieren.

Als Fazit läßt sich für die Bewertung der allgemeinen Vorschriften des BDSG zur Übermittlung von Daten ins Ausland festhalten:

Ein hinreichender Schutz der persönlichen Integrität läßt sich erreichen, wenn die einzelnen Vorschriften des BDSG im Lichte des Volkszählungsurteils gesehen werden und entsprechend den vom Bundesverfassungsgericht benannten Grundsätzen zum Recht auf informationelle Selbstbestimmung interpretiert werden. Aus der Sicht des Datenschutzes erscheint das als Selbstverständlichkeit. Die besondere Schwierigkeit mit den Generalklauseln und den unbestimmten Rechtsbegriffen des BDSG liegt nun allerdings darin, daß eine bestimmte Auslegung nicht verbindlich vorgegeben werden kann. Das ist allenfalls in wenigen Ausnahmefällen möglich, wenn etwa das Bundesverfassungsgericht eine bestimmte verfassungskonforme Auslegung vorschreibt. Das ist mit dem Volkszählungsurteil aber nicht geschehen. Hier hat das Bundesverfassungsgericht zwar den verfassungsrechtlichen Rang des Rechts auf informationelle Selbstbestimmung herausgestellt, damit aber nicht etwa streitige Auslegungsfragen verbindlich entschieden, ganz abgesehen davon, daß sich das Urteil zunächst einmal auf den öffentlichen Bereich bezieht und es natürlich auch Stimmen gibt, die eine Übertragung der Grundsätze auf den nichtöffentlichen Bereich ablehnen. Die Streitfrage etwa, ob die im Ausland tätige, unselbständige Zweigstelle eines deutschen Unternehmens als „Dritter" im Sinne des BDSG anzusehen ist, bleibt durch das Urteil unentschieden. Es zeigt sich, daß im Hinblick auf den grenzüberschreitenden Datentransfer weniger die Gerichtsbarkeit als vielmehr der Gesetzgeber gefordert ist. Die Meinungsvielfalt in so entscheidenden Fragen wie den Zulässigkeitsvoraussetzungen von Datenübertragungen ins Ausland offenbart, daß der Materie mit der Auslegung der bestehenden Normen nicht sachgerecht beizukommen ist, daß vielmehr der Gesetzgeber nach besseren Regelungen suchen muß. Solange ein Gesetz nicht eindeutige Regelungen trifft, sondern Auslegungen zuläßt, die zu unterschiedlichen Ergebnissen führen, so lange wird es auch Stimmen geben, die einer großzügigen Auslegung das Wort reden und datenschutzrechtliche Bedenken in den Wind schlagen.

5. Einzelprobleme im öffentlichen Bereich

5.1 Sozialwesen

5.1.1 Bearbeitung von Wohngeldanträgen

In meinem 4. TB (4.14.2, S. 110) hatte ich über die Prüfung der Wohngelddienststelle Eimsbüttel berichtet. Die Prüfung hat dazu geführt, daß einige Vordrucke, insbesondere das Antragsformular, unter meiner Beteiligung überarbeitet wurden.

Zu der von mir im 4. TB kritisierten Praxis der Datenübermittlungen für statistische Zwecke hat mir inzwischen das Statistische Landesamt versichert, daß für die laufende Statistik keine Kopien von Magnetbändern an das Statistische Bundesamt übersandt werden. Es werden vielmehr spezielle Magnetbänder zur Fertigung der nach § 35 WoGG vorgeschriebenen Statistiken erstellt und dem Statistischen Bundesamt zugeleitet. Dies geschieht ohne Verwendung der Wohngeldnummer, so daß aus datenschutzrechtlicher Sicht nichts zu beanstanden ist.

5.1.2 Informationsverarbeitung im Bereich der Jugendbehörden Hamburgs

Im Berichtsjahr habe ich die Prüfung der Informationsverarbeitung im Bereich der Jugendbehörden Hamburgs abschließen können. Die bereits in meinem 4. TB (4.14.3, S. 111) erwähnte Überarbeitung der Vordrucke ist unter meiner Mitwirkung inzwischen vollzogen worden. In den zahlreichen Sitzungen des Vordruckausschusses ist es m.E. gelungen, die von mir kritisierten Vordrucke im Bereich der Jugendverwaltung den datenschutzrechtlichen Anforderungen entsprechend neu zu gestalten.

In den Gesprächen mit den Behördenvertretern wurden die inhaltlichen Ergebnisse meiner Prüfung und die daraus resultierenden Vorschläge zumeist angenommen bzw. es wurde zugesagt, sie künftig in der Praxis zu beachten. Über die in einigen Bereichen bestehenden unterschiedlichen Rechtsauffassungen habe ich mit den Jugendbehörden mit folgendem Ergebnis verhandelt:

1. Gem. § 78 Abs. 4 Nr. 1 Jugendwohlfahrtsgesetz (JWG) hat der Träger eines Heimes dem Landesjugendamt die Personalien und Art der Ausbildung des Leiters und der Erzieher dieser Einrichtung zu melden. Ich hatte im Prüfbericht kritisiert, daß das Amt für Jugend auch die Meldung von Personaldaten der Pflege- und Hauswirtschaftskräfte verlangt.

   Das Amt für Jugend hat in seiner Stellungnahme darauf hingewiesen, daß zwischen Vollheimen und Kindertagsheimen unterschieden wird. Bei Vollheimen hält das Amt für Jugend daran fest, auch Personaldaten von Pflege- und Hauswirtschaftskräften zu erheben; lediglich Familienstand und Staatsangehörigkeit seien verzichtbar. Die anderen Personaldaten seien notwendig, weil die Pflege- und Hauswirtschaftskräfte in die pädagogische Arbeit mit den Minderjährigen unmittelbar einbezogen seien und die Angaben für die Erfüllung der gesetzlichen Aufsichtspflicht über die Vollheime benötigt würden.

   Bei Kindertagesheimen sei auch das Abfragen der Staatsangehörigkeit sowohl von Erziehern als auch von Pflege- und Hauswirtschaftskräften notwendig, um Kenntnis über mehrsprachiges Personal und dessen Einsatzmöglichkeiten in Gebieten mit hohem Ausländeranteil zu erlangen. Das Amt für Jugend hat meinen Vorschlag, wonach dieses Ziel auch mit der Frage nach Fremdsprachenkenntnissen erreicht werden könne, akzeptiert.

   Alle weiteren Angaben sind nach den Erläuterungen des Amtes für Jugend auch m.E. gem. § 78 bzw. 84 JWG erforderlich.

2. Im Prüfbericht wird u.a. kritisiert, daß bei Anträgen auf Ausstellung eines Jugendgruppenleiterausweises auch der Beruf des Antragstellers erfragt wird. Das Amt für Jugend hielt diese Angabe für erforderlich, um bei pädagogischer Qualifikation des Bewerbers den Ausweis auch ohne weitere Ausbildungsmaßnahmen ausstellen zu können. Meiner Anregung entsprechend wird künftig lediglich nach einer erzieherischen Ausbildung gefragt.

3. Die Vertrauensstelle für Verlobte und Eheleute führt eine Kartei über ihre Klienten. Daneben werden noch Registerkarten geführt mit den Personalien und der Unterschrift des Klienten, worauf die für die Beratung zu lösenden Gebührenmarken geklebt werden. Bisher wurden diese Karten 5 Jahre aufbewahrt. Da nach meinen Feststellungen im Rahmen von Ehescheidungen eine Bestätigung über die Beratung innerhalb der dreijährigen Trennungsfrist benötigt wird, reicht m.E. eine dreijährige Aufbewahrungsfrist aus. Das Amt für Jugend hat dies akzeptiert und wird künftig entsprechend verfahren.

4. Aus Anlaß von Kurverschickungen Jugendlicher werden dem zuständigen Bezirksgesundheitsamt formularmäßig eine Reihe von Daten übermittelt. Der Vordruck wurde inzwischen mit meiner Beteiligung datenschutzrechtlichen Erfordernissen angepaßt, so daß z.B. künftig nicht mehr nach dem Beruf der Eltern gefragt wird.

5. Bisher wurden die Unterlagen über Adoptionsbewerber 2 bzw. 3 Jahre aufbewahrt. Ich habe mich mit dem Amt für Jugend dahingehend verständigt, daß diese Frist auf 6 Monate zu verkürzen ist, sofern die Bewerber abgelehnt werden.

6. Im Prüfbericht habe ich auch die Weitergabe gesamter Fürsorgeakten des Jugendamtes an andere Jugendbehörden, z.B. an die Jugendbewährungshilfe, kritisiert. Dieses grundsätzliche Problem der Aktenführung ist inzwischen durch den Entwurf einer Dienstvorschrift der BAJS zum Schutz der Sozialdaten weitgehend entschärft worden. Darin soll die Akteneinsicht und -übersendung wie folgt geregelt werden:

   Bei einer Aktenanforderung durch eine Sozialdienststelle ergibt sich das Problem, daß oftmals nicht alle in der Akte befindlichen Daten für die Aufgabenerfüllung der Dienststelle erforderlich sind und daß für bestimmte Daten über die Voraussetzungen des § 69 SGB-X hinaus weitere Offenbarungseinschränkungen z.B. aus § 203 Abs. 1 und 3 StGB und § 76 SGB-X folgen.

   Die Frage, ob die Kenntnis aller Daten aus einer Akte erforderlich ist, wird in der Regel von der ersuchten Stelle nicht ohne weiteres prüfbar sein. Das Ersuchen ist daher zu begründen. Fehlt eine Begründung, ist das Akteneinsichtsersuchen bzw. die Aktenanforderung abzulehnen.

   Ergibt sich aus der begründeten Anfrage, daß nicht alle in der Akte befindlichen Daten benötigt werden, sind die Unterlagen entsprechend zu selektieren oder die Aktenübersendung zu verweigern. An die Prüfungspflicht der ersuchten Stelle dürfen jedoch keine überhöhten Anforderungen gestellt werden, denn grundsätzlich trägt die ersuchende Stelle die Verantwortung dafür, da die Akteneinsicht zur Erfüllung ihrer Aufgaben nötig ist. Die ersuchte Stelle muß daher Akteneinsichts- bzw. Aktenübersendungsbegehren nur dann zurückweisen, wenn aus der Begründung des Ersuchens erkennbar ist, daß nicht alle in der Akte befindlichen Daten benötigt werden. Bei Verweigerung der Aktenübersendung ist auf alle Einzelfragen insoweit zu antworten, als dies im Rahmen des § 69 SGB-X zulässig ist.

   Eine Aktenübersendung an eine nicht entscheidungsbefugte Stelle, z.B. durch eine Sozialdienststelle an den Bundesminister für Arbeit oder durch die Bezirksämter an die Rechtsabteilung der BAJS zur Klärung einer abstrakten Rechtsfrage, ist nicht zulässig. Hierbei werden in der Regel personenbezogene Daten zur Aufgabenerfüllung nicht benötigt, da es nicht um die Klärung eines konkreten Sachverhalts, sondern um anonymisiert darstellbare Probleme geht. Eine Anfrage ist daher im allgemeinen nur in anonymisierter Form zulässig.

   Befinden sich in der Akte medizinische oder sonstige Daten, die der Geheimhaltungspflicht nach § 203 Abs. 1 und 3 StGB unterliegen, können sie in der Regel ohne Einwilligung des Betroffenen gemäß § 69 Abs. 1 Nr. 1 nur offenbart werden, wenn diese Daten im Zusammenhang mit der Begutachtung wegen der Erbringung von Sozialleistungen oder wegen der Aufstellung einer Bescheinigung zugänglich gemacht worden sind (§ 76 Abs. 2 SGB-X).

   Wegen dieser Einschränkung sollen die der Geheimhaltungspflicht nach § 203 Abs. 1 und 3 StGB in Verbindung mit § 76 SGB-X unterliegenden Daten in einer besonderen Heftung der Akte geführt werden, so daß dieser Teil bei einem Aktenübersendungsantrag insgesamt herausgenommen werden kann.

   Eine Aktenübersendung an das Staatsarchiv ist bis zum Erlaß eines hamburgischen Archivgesetzes und einer gesetzlichen Ermächtigung im SGB-X (letztere ist z.Z. in Vorbereitung) nicht zulässig, soweit die Akten Sozialdaten enthalten.

5.1.3 Prüfung einer Betriebskrankenkasse (BKK)

Die in meinem 4. TB (4.14.4, S. 112) erwähnte Prüfung einer BKK habe ich im Berichtszeitraum abgeschlossen. Ich habe festgestellt, daß bei der geprüften BKK eine große Aufgeschlossenheit gegenüber den Belangen des Datenschutzes vorhanden ist.

Das Prüfergebnis, dessen wesentliche Punkte ich hier noch einmal zusammenfassen möchte, beruht natürlich auf Feststellungen, wie ich sie bei der geprüften BKK getroffen habe. Allerdings gelten die gesetzlichen Grundlagen, nach denen sich die geprüfte BKK zu richten hat, für alle Betriebskrankenkassen und darüber hinaus für sämtliche gesetzlichen Krankenkassen. Deshalb werde ich bei Gelegenheit prüfen, ob sich die Informationsverarbeitung bei anderen gesetzlichen Krankenkassen nachhaltig von der Praxis der geprüften BKK unterscheidet. Dabei wird mich auch interessieren, ob andere gesetzliche Krankenkassen ebenfalls nach einem ebenso überzeugenden Datenschutzkonzept arbeiten, wie ich es bei dieser Prüfung vorgefunden habe.

Bei der geprüften BKK habe ich weder konkrete Verletzungen des Sozialgeheimnisses noch eine mißbräuchliche Verwendung von Sozialdaten erkennen können. Ich hatte allerdings datenschutzrechtliche Bedenken gegen die Organisation des Datenschutzes innerhalb der BKK geäußert. So ist die zu Beginn der Prüfung festgestellte, nicht unproblematische Doppelfunktion des stellvertretenden Geschäftsführers, der gleichzeitig Leiter der Melde- und Beitragsabteilung, Innenrevisor und betrieblicher Datenschutzbeauftragter war, von mir kritisiert worden. Dies ist gegen Ende der Prüfung geändert worden.

Weitere Datenschutzprobleme ergeben sich als Folge von Gesetzesbestimmungen, nach denen die gesetzlichen Krankenkassen insgesamt zu arbeiten haben. So erscheinen mir einige Regelungen der RVO, durch die die Krankenkassen veranlaßt werden, umfangreiche Erhebungen bis in den privaten Lebensbereich hinein anzustellen, reformbedürftig. Hier denke ich insbesondere an die Regelungen des § 185b RVO über die Gewährung einer Haushaltshilfe sowie des § 205 über die Gewährung von Familienhilfe:

— Nach § 185b RVO müssen die Krankenkassen eine Vielzahl von Daten (z. B. sämtliche im Haushalt lebende Personen, Verwandtschaftsgrad, Alter, Berufstätigkeitszeiten, Fahrzeiten zum Arbeitsplatz) erheben, die aus meiner Sicht in diesem Umfang nicht in jedem Fall erforderlich sind.

— In § 205 RVO ist geregelt, daß der Familienangehörige keinen eigenen Anspruch gegen die Krankenkasse hat; vielmehr ist nur das Mitglied für seine Angehörigen anspruchsberechtigt. Dies hat zur Folge, daß die erforderlichen Daten von der Krankenkasse nicht bei den Angehörigen selbst erfragt, sondern vom Mitglied der Krankenkasse mitgeteilt werden. Die Daten werden dann, wie es nach § 319 RVO vorgesehen ist, unter der Versicherungsnummer des Mitgliedes bei der Krankenkasse gespeichert. Auf diese Weise können der Krankenkasse Daten von Familienangehörigen offenbart werden, auch wenn diese nichts davon wissen und schon gar nicht damit einverstanden sind. Dies ist datenschutzrechtlich bedenklich. Deshalb sollte § 205 RVO dahingehend neu gefaßt werden, daß den Familienangehörigen unter bestimmten Voraussetzungen ein eigener Anspruch gegen die Krankenkasse eingeräumt wird.

Die BKK hat zugesagt, daß sie die von ihr selbst erarbeiteten Vordrucke mit dem — in § 9 Abs. 2 BDSG — vorgeschriebenen Hinweis auf die Rechtsvorschrift der Datenerhebung bzw. Freiwilligkeit der Angaben versehen wird. Ich hoffe, daß auch die bundeseinheitlich verwendeten Formulare entsprechend überarbeitet werden. Im übrigen werden in den Erhebungsbogen von vornherein möglichst viele Daten über die Anspruchsberechtigten erfaßt, obwohl nach den gesetzlichen Vorschriften oft nur die Kenntnis eines Merkmals ausreicht, um eine Anspruchsberechtigung zu prüfen. Dann ist das Erfragen weiterer Voraussetzungen nicht mehr erforderlich. Werden aber solche nicht erforderlichen Angaben gespeichert, so sind sie gem. § 84 SGB-X zu löschen.

Schließlich wiederhole ich an dieser Stelle die in meinem 4. TB (a.a.O.) aufgestellte Forderung, dafür zu sorgen, daß medizinische Daten der Mitglieder von Krankenkassen grundsätzlich nur in der Beziehung Arzt/Patient bzw. Vertrauensarzt/Patient bleiben. Nur in Ausnahmefällen darf von diesem Prinzip abgewichen werden und erst nach Überprüfung, ob detaillierte medizinische Angaben auch tatsächlich zur Aufgabenerfüllung der Krankenkassen erforderlich sind, eine Weitergabe erfolgen. Zwar nimmt die Krankenkasse auch Aufgaben der Rehabilitation wahr, doch dies reicht nicht aus, um generell einen umfassenden Austausch medizinischer Daten zwischen Arzt und Krankenkasse zu rechtfertigen. Dies kann lediglich in bestimmten Einzelfällen zugelassen werden, in denen dann die Einwilligung des Mitgliedes einzuholen ist, zumindest müßte das Mitglied vorher über einen solchen Datenaustausch informiert werden.

5.1.4 Offenbarung von Sozialdaten auf Überweisungsträgern

Durch mehrere Bürgerbeschwerden bin ich darauf aufmerksam geworden, daß die Hamburgischen Sozialhilfedienststellen bei der Übersendung von Sozialhilfeleistungen auf Konten der Empfänger als Verwendungszweck „Sozialamt" auf dem Überweisungsträger angeben. Damit wird gegenüber dem Geldinstitut offenbart, daß der Kontoinhaber Sozialhilfe erhält. Es handelt sich hierbei um ein Sozialgeheimnis, das von den Leistungsträgern gem. § 35 SGB I gewahrt werden muß. Eine Offenbarung kommt nur in Betracht, wenn

— der Betroffene gem. § 67 SGB X eingewilligt hat oder

— dies nach den Bestimmungen der §§ 68 bis 77 SGB-X zulässig ist.

Nach den mir vorliegenden Informationen werden die Hilfeempfänger von den Sozialdienststellen nicht um eine entsprechende Einwilligungserklärung gebeten. Da auch die weiteren gesetzlichen Offenbarungsbefugnisse der §§ 68 bis 77 SGB-X eine derartige Offenbarung nicht abdecken, ist sie aus meiner Sicht rechtswidrig.

In meinen Gesprächen mit der Verwaltung habe ich darauf hingewiesen, daß nach einer Entscheidung des Verwaltungsgerichts Düsseldorf in einem ähnlich gelagerten Fall als Absender lediglich die jeweilige Stadtkasse genannt werden soll. Weiterhin dürften bei Zahlungen nach dem BSHG außer der Angabe des Empfängers, des Datums des Leistungsbescheides, des Leistungszeitraumes und eines anonymisierten Aktenzeichens keine weiteren Angaben auf dem Überweisungsträger enthalten sein. In Nordrhein-Westfalen wird inzwischen entsprechend verfahren. Auch für die Hamburgischen Leistungsträger müßte aus meiner Sicht ein solches Verfahren ausreichend sein, um ggf. den Nachweis über die von ihm geschuldete Leistung erbringen zu können, da ein anonymisiertes Aktenzeichen den Hilfeempfänger für den Leistungsträger hinreichend präzise bestimmt.

Die Vorschrift des § 55 SGB I, wonach eine Geldleistung, die von einem SGB-Leistungsträger gewährt wird, für die Dauer von 7 Tagen unpfändbar ist, gebietet ebenfalls nicht die Mitteilung des Sozialhilfebezugs an ein Geldinstitut. Es sind keine Gründe ersichtlich, die es gebieten, daß der Sozialleistungsträger generell bei allen Sozialhilfeempfängern, ohne daß eine Pfändung vorliegt oder auch nur droht, dem Geldinstitut gegenüber die überwiesenen Geldmittel als Sozialleistungen kenntlich macht. Gem. § 55 Abs. 2 SGB I ist es nämlich Sache des Empfängers, gegebenfalls den Zweck der Überweisung nachzuweisen. Dies dürfte in der Regel ohne weiteres durch die Vorlage des Leistungsbescheides oder des Schreibens, mit dem die Leistung angekündigt wird, möglich sein.

Die Behörde für Arbeit, Jugend und Soziales konnte sich bisher meinen rechtlichen Bedenken nicht anschließen und sieht deshalb auch keine Veranlassung, die gegenwärtige Praxis zu ändern. Die Diskussion ist noch nicht abgeschlossen.

5.1.5 Automation in der Abteilung Schwerbehindertengesetz des Versorgungsamtes

Im Berichtszeitraum ist ein Bildschirm-Dialog-Verfahren in der Abteilung Schwerbehindertengesetz des Versorgungsamtes für die Durchführung der Aufgaben nach dem Schwerbehindertengesetz (SchwbG) eingeführt worden, um das Verwaltungsverfahren zur Anerkennung der Vergünstigungen nach dem SchwbG zu beschleunigen und sicherer zu gestalten. Außerdem soll die Automation der Statistik in diesem Bereich sichergestellt werden. Der Datensatz umfaßt neben den für die Statistik aufgrund § 51 SchwbG erforderlichen Angaben Hinweise auf den Bearbeitungsstand des Verfahrens (u.a. Anforderung von Unterlagen beim Antragsteller, Anforderung bzw. Eingang von Berichten, Aktenabgabe an Gerichte oder Gutachter, Widerspruch, Klage, Erinnerungen, Ablage). Entscheidungen über die gestellten Anträge sind allein aufgrund der im automatisierten Bestand gespeicherten Daten nicht möglich, sondern sie müssen auch künftig anhand des Bearbeitungsstandes in den Akten getroffen werden.

Wie ich feststellen konnte, ist eine Übermittlung personenbezogener Daten aus der Datei an Dritte ausgeschlossen. Auch die Weitergabe zu statistischen Zwecken erfolgt in hinreichend anonymisierter Form.

Zwischen der BAJS und dem Personalrat der BAJS wurde nach § 83 des Hamburgischen Personalvertretungsgesetzes eine Dienstvereinbarung zur Anwendung des ADV-Verfahrens geschlossen. Darin wird u.a. geregelt,

- bei welchen Arbeiten das ADV-Verfahren die Mitarbeiter unterstützen soll,
- welche Systemausstattung vorgesehen ist,
- in welcher Form das Verfahren dokumentiert werden soll,
- welche Überlegungen zum Schutz vor der Überwachung einzelner Bediensteter vorgesehen sind.

Ich habe aufgrund der mir vorliegenden Informationen keine datenschutzrechtlichen Bedenken gegen das beschriebene ADV-Verfahren erhoben.

5.1.6 Weitergabe von Adoptionsdaten

Einen besonders krassen Fall der Verletzung datenschutzrechtlicher Belange der Betroffenen habe ich im Berichtsjahr beim Versorgungsamt feststellen müssen, der mich zu einer Beanstandung gegenüber dem Senat gem. § 21 Abs. 1 Satz 1 HmbDSG veranlaßt hat. Dabei ging es nicht darum, einzelne Mitarbeiter von Dienststellen wegen ihres Fehlverhaltens „an den Pranger" zu stellen. Wenn ich den Eindruck hätte, dem Datenschutz könnte etwa mit disziplinarrechtlichen Maßnahmen Genüge getan werden, weil es sich um isoliertes, nur einen Einzelfall betreffendes individuelles Fehlverhalten handelte, würde ich dies nicht zum Gegenstand einer Beanstandung machen. Ein solcher Sachverhalt lag nach meinem Eindruck jedoch nicht vor.

Im Laufe des vergangenen Jahres habe ich mich mit einer Reihe von Eingaben und Vorgängen beschäftigen müssen, die eine auffällige Unbekümmertheit von Mitarbeitern der hamburgischen Verwaltung im Umgang mit personenbezogenen Daten aufgedeckt haben. Mir scheint, das — insbesondere nach Bekanntwerden des Volkszählungsurteils des Bundesverfassungsgerichts — zeitweilig festzustellende erfreuliche Verständnis für datenschutzrechtliche Erfordernisse droht in weiten Bereichen wieder verlorenzugehen.

Dem Beanstandungsfall liegt folgender Sachverhalt zugrunde:

Ein Ehepaar hatte vor einigen Jahren ein Kind adoptiert, dessen leibliche Mutter von dem mutmaßlichen Vater des Kindes getötet worden war. Dieser wurde wegen der Tat zu einer mehrjährigen Freiheitsstrafe verurteilt, die er z.Z. verbüßt. Wahrscheinlich wegen dieser Umstände wurde eine nach § 1747 BGB zugelassene sog. „Inkognito-Adoption" durchgeführt.

Für das Kind wurde vom Versorgungsamt eine Waisenrente gewährt. Deshalb informierte das Jugendamt als früherer Vormund des Kindes das Versorgungsamt über die Adoption und teilte den Namen der Adoptiveltern mit, damit die Waisenrente an diese ausgezahlt werden konnte. Das Schreiben des Jugendamtes enthält folgenden Hinweis:

„Achtung: Es handelt sich um eine Inkognito-Adoption."

Gleichwohl hat das Versorgungsamt in voller Kenntnis aller Umstände den neuen — nach der Adoption vergebenen — Namen des Kindes dem Mann mitgeteilt, der für den Tod der Mutter des Kindes verantwortlich ist, als es diesem gegenüber Schadensersatzansprüche geltend machte.

Da der Täter ernsthaft gedroht hat, das Kind an sich zu nehmen und mit ihm gemeinsam aus dem Leben zu scheiden, ergeben sich für die neue Familie weitreichende Konsequenzen. Nicht nur das Kind, sondern auch die Adoptiveltern müssen ihre bisherigen Lebensumstände radikal verändern und trotzdem weiterhin mit einer ständigen Angst leben. Schlimmere Folgen einer unsachgemäßen Behandlung personenbezogener Daten sind kaum denkbar.

Dieser Vorfall ist um so gravierender, als — unabhängig von Datenschutzbestimmungen — das Adoptionsrecht selbst von Schutzvorschriften für Adoptivkinder und -eltern bestimmt wird, und zwar nicht beschränkt auf sog. „Inkognito-Adoptionen". § 1758 BGB verbietet generell für alle Adoptionen die Offenbarung von Tatsachen, die geeignet sind, die Annahme und ihre Umstände aufzudecken, es sei denn die Betroffenen stimmten zu oder besondere Gründe des öffentlichen Interesses erforderten es. Diese Regelung gilt besonders gegenüber den leiblichen Eltern des Kindes, denn nach den gesetzgeberischen Vorstellungen ist es für die ungestörte Entwicklung eines Kindes in der neuen Familie unerläßlich, daß Störungen aus der alten Familie unterbleiben (vgl. Amtl. Begr., BT-Drucks. 7/3061, S. 19, vom 7. Januar 1975). Deshalb sollten Fälle unterbunden werden, in denen die leiblichen Eltern oder andere frühere Verwandte Jahre nach der Adoption versuchen, Kontakt zu dem Kind aufzunehmen (a.a.O., S. 46). Darüber hinaus bestimmt § 1758 Abs. 2 S. 1 BGB, daß das Offenbarungs- und Ausforschungsverbot schon von der Erteilung der erforderlichen elterlichen Einwilligung an gilt. Das Vormundschaftsgericht kann sogar die Wirksamkeit des Verbotes von dem Zeitpunkt an anordnen, zu dem ein Antrag auf Ersetzung der Einwilligung gestellt worden ist (vgl. Bericht und Antrag des Rechtsausschusses, BT-Drucks. 7/5087, S. 18/19, vom 27. April 1976). Schließlich wird das Offenbarungs- und Ausforschungsverbot durch § 61 Abs. 2 Personenstandsgesetz und § 34 Abs. 2 Gesetz über Angelegenheit der freiwilligen Gerichtsbarkeit abgesichert.

Dem Versorgungsamt hätte sich deshalb förmlich aufdrängen müssen, daß dem wegen der Tötung der Mutter des Kindes verurteilten Täter unter keinen Umständen die neue Identität des Kindes hätte preisgegeben werden dürfen. Dies muß dem Senat sicher Veranlassung geben, die mit Adoptionsdaten befaßten Mitarbeiter der Verwaltung über spezielle datenschutzrechtliche Konsequenzen in Adoptionsfällen zu belehren.

Wegen des von mir zuvor beschriebenen allgemeinen Nachlassens der Aufmerksamkeit von Mitarbeitern der hamburgischen Verwaltung für datenschutzrechtliche Erfordernisse halte ich es darüber hinaus für geboten, daß der Senat den vorliegenden besonders schwerwiegenden Sachverhalt zum Anlaß nimmt, sämtliche Mitarbeiter der hamburgischen Verwaltung erneut darauf hinzuweisen, daß die Erhebung und Offenbarung personenbezogener Daten und Umstände grundsätzlich nur

— mit Einwilligung der Betroffenen oder

— aufgrund gesetzlicher Befugnis

erfolgen darf.

Ich habe dem Senat gem. § 21 Abs. 3 HmbDSG vorgeschlagen, dies in Form einer Beilage bei der Versendung der nächsten Besoldungs-/Gehaltsmitteilungen durchzuführen und meine Bereitschaft erklärt, an der Formulierung eines solchen Hinweises mitzuwirken.

Mit einer Stellungnahme des Senats zu der Beanstandung und zu meinem Vorschlag rechne ich im Februar 1987.

5.1.7 Sorgloser Umgang mit personenbezogenen Daten durch das Jugendamt Wandsbek

Durch zwei Eingaben wurde ich darauf aufmerksam gemacht, daß einige Mitarbeiter des Jugendamtes Wandsbek eine bemerkenswerte Sorglosigkeit beim Umgang mit ihnen anvertrauten personenbezogenen Daten an den Tag legten. In beiden Fällen wurden bei der Bearbeitung eines Antrages auf Gewährung eines Zuschusses zum Tagespflegegeld unbefugt Sozialdaten Dritten offenbart. Im einzelnen hatte sich folgendes ereignet:

Die beiden Petenten hatten einen Zuschluß zum Tagespflegegeld beantragt, um damit die Kosten der Unterbringung ihrer Kinder in einer Tagespflegestelle zu senken. Das Jugendamt Wandsbek kam nach der Prüfung beider Anträge jeweils zum Ergebnis, daß die Voraussetzungen für die Bewilligung eines solchen Zuschusses nicht erfüllt seien, und erläuterte das den Petenten in schriftlichen Bescheiden sehr ausführlich. Diese Bescheide enthielten u.a. genaue Angaben über das Brutto- und Nettogehalt, die Höhe der Steuerabgaben und der Beiträge zur Sozialversicherung, Krankenkasse und sonstigen Versicherungen sowie die Fahrtkosten zum Arbeitsplatz der Petenten. Das Jugendamt Wandsbek übersandte Durchschriften der Bescheide ohne Zustimmung der Petenten an die Tagespflegemütter.

Wie mir das Bezirksamt Wandsbek inzwischen mitgeteilt hat, hat sich das Jugendamt bei der Weitergabe der in Rede stehenden personenbezogenen Daten an einer von der Behörde für Arbeit, Jugend und Soziales erlassenen Verwaltungsvorschrift (Fachliche Weisung AJ 6/84) orientiert. Hierin wird bestimmt, daß die Pflegepersonen eine Durchschrift der Mitteilung erhalten sollen, die die Sorgeberechtigten über die Bewilligung der Leistung bekommen. Persönliche Daten soll diese Mitteilung nicht enthalten. Die Pflegepersonen bekommen diese Informationen, damit sie wissen, welches Pflegegeld das Jugendamt und welchen Betrag die Eltern an sie zahlen. Für den Fall einer Ablehnung reicht es auch nach Auffassung des Bezirksamtes Wandsbek aus, der Tagespflegemutter eine kurze Mitteilung, daß das Jugendamt kein Pflegegeld zahlt, zuzuleiten. Dem stimme ich zu.

Aus datenschutzrechtlicher Sicht ist zu der Angelegenheit folgendes anzumerken:

Das Jugendamt ist gem. § 27 Sozialgesetzbuch I (SGB I) zuständig für die Gewährung von Leistungen der Jugendhilfe, wozu auch Pflegegeldzahlungen gehören. Als Sozialleistungsträger ist das Jugendamt jedoch gem. § 35 SGB I verpflichtet, ihm anvertraute personenbezogene Daten geheim zu halten bzw. nicht unbefugt zu offenbaren. Nach § 35 Abs. 2 SGB X ist eine Offenbarung nur unter den Voraussetzungen der §§ 67 bis 77 SGB X zulässig.

Da es in diesen Fällen eine spezielle gesetzliche Grundlage für die in Frage stehenden Übermittlungen nicht gibt und auch die Offenbarungstatbestände der § 68 bis 77 SGB X nicht greifen, käme allein die Einwilligung gem. § 67 SGB X als Offenbarungsbefugnis in Betracht. Eine solche Einwilligung ist von den Petenten allerdings nicht erteilt worden. Somit war die Offenbarung ihrer Daten an die Tagespflegemutter rechtswidrig.

5.2 Personalwesen

5.2.1 Speicherung der Wählbarkeitsfälle von Beamten und Angestellten der FHH

Das Senatsamt für den Verwaltungsdienst — Personalamt — hat bislang an zentraler Stelle Daten aller Wahlbewerber aus dem öffentlichen Dienst der Freien und Hansestadt Hamburg, die für die Bürgerschaft oder die Bezirksversammlungen kandidieren, karteimäßig erfaßt. Die Kartei diente folgenden Zwecken:

— Prüfung der Wählbarkeitsvoraussetzung bei Beamten und Angestellten im öffentlichen Dienst der Freien und Hansestadt Hamburg nach § 15 des Gesetzes über die

Wahl zur Hamburgischen Bürgerschaft und § 15 des Gesetzes über die Wahl der Bezirksversammlungen,

— Aufbereitung der Wahlbewerber im öffentlichen Dienst der FHH nach Parteizugehörigkeit der Betroffenen für die politische Leitung des Senatsamtes,

— Informationsgrundlage für die Auskunftserteilung über den Bearbeitungsstand der Wählbarkeitsfälle gegenüber den Behörden und Ämtern, bei denen die Betroffenen beschäftigt sind.

Darüber hinaus wurde den Beschäftigungsbehörden Mitteilung gemacht, wenn Bewerber auf Listen von als verfassungsfeindlich eingestuften Parteien kandidieren. Das Senatsamt für den Verwaltungsdienst — Personalamt — hat dargelegt, daß die Übermittlung von Daten an andere Stellen aus den Sachakten über die Wählbarkeitsfälle durchgeführt werde. Da es sich bei der Wählbarkeitskartei demnach um eine nicht automatisierte Datei handele, deren Daten nicht zur Übermittlung an Dritte bestimmt seien, hat das Senatsamt für den Verwaltungsdienst — Personalamt — darum gebeten, die Kartei aus dem Datenschutzregister zu streichen.

Zu prüfen war, ob

— es sich bei der Kartei — wie in dem Bezugsschreiben vom 9. Oktober 1986 behauptet — um eine „interne Datei" im Sinne von § 1 Abs. 2 Satz 2 HmbDSG handelt,

— die Speicherung der in der Kartei enthaltenen Merkmale für die Aufgabenerfüllung gemäß § 15 des Gesetzes über die Wahl zur Hamburgischen Bürgerschaft und § 15 des Gesetzes über die Wahl zu Bezirksversammlungen erforderlich ist,

— die Verarbeitung für „interne Zwecke" (Aufbereitung der Wahlbewerber nach Parteizugehörigkeit für den Staatsrat des Senatsamtes) und

— die Übermittlung von Daten über Bewerber auf mutmaßlich verfassungsfeindlichen Listen an die Beschäftigungsbehörden zulässig ist.

5.2.1.1 Handelt es sich um eine „interne Datei"?

Nach § 1 Abs. 2 Satz 1 HmbDSG gilt für personenbezogene Daten, die nicht zur Übermittlung an Dritte bestimmt sind und in nicht-automatisierten Verfahren verarbeitet werden, von den Vorschriften des HmbDSG nur § 8 (Datensicherung). Nach Auskunft des Personalamtes sollen bestimmte Angaben, die dem Landeswahlleiter und anderen Stellen in der Vergangenheit aus der Kartei übermittelt wurden, in Zukunft aus dem Sachvorgang mitgeteilt werden. Dadurch wird die Kartei jedoch nicht zur „internen Datei", die nicht zum Datenschutzregister gemeldet werden muß. Bei gleichzeitiger Speicherung von Sachverhalten in Akten- und in Dateiform ist im Interesse der Gewährleistung des Rechts auf informationelle Selbstbestimmung der Betroffenen in der Regel davon auszugehen, daß das Hamburgische Datenschutzgesetz voll anzuwenden ist und die Einschränkung von § 1 Abs. 2 Satz 1 HmbDSG nicht greift, unabhängig davon, ob im Einzelfall aus der Akte oder aus der Datei übermittelt wird. Andernfalls wäre es den Behörden ohne weiteres möglich, durch Änderung der Übermittlungsquelle bestimmte Daten dem Schutz des Hamburgischen Datenschutzgesetzes zu entziehen (vgl. 2. Tätigkeitsbericht, 2.5.2, S. 13).

Da der rechtmäßige Zweck der Datei (s. u.) auf eine Übermittlung der Wählbarkeitsentscheidung an den Landeswahlleiter, die Bezirksversammlungen und die Beschäftigungsbehörde angelegt war, mußte davon ausgegangen werden, daß die hierbei zum Einsatz kommende Kartei — die ja einen Auszug aus der Sachakte darstellt — auch für die Übermittlung herangezogen wurde.

5.2.1.2 Sind die gespeicherten Daten für die Aufgabenerfüllung erforderlich?

Nach § 15 Abs. 1 des Gesetzes über die Wahl zur Hamburgischen Bürgerschaft (im wesentlichen sinngleich mit § 15 des Gesetzes über die Wahl zu den Bezirksversammlungen) haben Beamte und Angestellte, die in einem beim Landeswahlleiter eingereichten Wahlvorschlag benannt sind, dies ihrem Dienstherren unverzüglich anzuzeigen. Der

Dienstherr hat daraufhin unverzüglich darüber zu entscheiden, ob der Beamte oder Angestellte Hoheitsbefugnisse unter den Voraussetzungen des § 13 Abs. 1 ausübt und somit nicht wählbar ist.

Die Wahlordnung für die Wahlen zur Hamburgischen Bürgerschaft und zu den Bezirksversammlungen (HmbWO) regelt das entsprechende Verfahren. Gemäß § 27 Abs. 2 HmbWO haben die Dienstvorgesetzten die Anzeige des Bewerbers mit einer Beschreibung der von ihm ausgeübten Tätigkeit an die oberste Dienstbehörde — das ist das Senatsamt für den Verwaltungsdienst — Personalamt — weiterzuleiten. Nach § 27 Abs. 4 HmbWO wird die von der obersten Dienstbehörde getroffene Entscheidung dem Dienstvorgesetzten und — bei Bewerbern zur Bürgerschaft — auch dem Landeswahlleiter zur Kenntnis gegeben.

Die im Personalamt geführte Datei der Wählbarkeitsfälle enthielt neben den Identifikationsangaben im engeren Sinne (Name, Vorname, Geburtsdatum) die Beschäftigungsdienststelle, die Amts-/Dienstbezeichnung, die Art der Kandidatur (Bürgerschaft/Bezirksversammlung) die Parteizugehörigkeit, das Aktenzeichen des Personalamtes, das Datum der Wählbarkeitsentscheidung und ggf. einen Vermerk, falls negativ entschieden wurde. Zu prüfen war insbesondere, aus welchem Grund die Parteizugehörigkeit dateimäßig erfaßt wurde. Da es sich hierbei um ein Merkmal handelt, das bei der eigentlichen Wählbarkeitsentscheidung keine Rolle spielen darf, ist eine Speicherung fragwürdig.

Nach § 9 Abs. 1 HmbDSG ist das Speichern von Daten an die Erforderlichkeit für die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gebunden. Die Speicherung des Merkmals „Parteizugehörigkeit" war für die Erfüllung der Aufgaben nach § 15 des Gesetzes über die Wahl zur Hamburgischen Bürgerschaft und des Gesetzes über die Wahl der Bezirksversammlungen nicht erforderlich, da die allein vom Senatsamt zu beantwortende Frage, ob von dem Bewerber Hoheitsbefugnisse ausgeübt werden, unabhängig von der Parteizugehörigkeit entschieden werden muß.

5.2.1.3 Ist die Aufbereitung für „interne Zwecke" des Senatsamtes für den Verwaltungsdienst — Personalamt — zulässig?

Bei der Aufbereitung für „interne Zwecke" handelt es sich um die Erstellung von Listen, in denen die in der Kartei erfaßten Wahlbewerber aus dem öffentlichen Dienst der Freien und Hansestadt Hamburg nach Parteizugehörigkeit geordnet zusammengefaßt wurden. Diese Listen wurden dem für das Senatsamt zuständigen Staatsrat vorgelegt. Dieser Zweck läßt sich nicht aus den Wahlgesetzen oder der Hamburgischen Wahlordnung herleiten. Da es sich bei dem Senatsamt für den Verwaltungsdienst — Personalamt — um eine zentrale Stelle handelt, die für die Planung der Personalentwicklung der hamburgischen Verwaltung zuständig ist und die auch an der Stellenbesetzung mitwirkt, sind derartige Auswertungen besonders problematisch. Es darf nicht der Verdacht aufkommen, als sei die Parteizugehörigkeit ein Kriterium bei Personalentscheidungen.

Da diese Aufbereitungen nicht für die Aufgabenerfüllung im Rahmen der Wählbarkeitsentscheidungen erforderlich sind, gilt hier § 10 Abs. 2 HmbDSG. Danach dürfen personenbezogene Daten, die für eine bestimmte Aufgabe gewonnen wurden, für andere Aufgaben nur unter Maßgabe der Bestimmungen des § 10 Abs. 1 HmbDSG verwendet werden. D.h., die listenmäßige Aufbereitung der Bewerber nach Parteizugehörigkeiten ist nur dann zulässig, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers (hier: Staatsrat des Senatsamtes für den Verwaltungsdienst) gelegenen Aufgaben erforderlich ist und die Zulässigkeit mehrfacher Verwendung dem Bewerber bekannt ist. Sich einen Überblick über die Parteizugehörigkeit der Wahlbewerber zu verschaffen, ist selbst keine vom Staatsrat des Senatsamtes wahrzunehmende Aufgabe und ist auch nicht für andere von ihm rechtmäßig wahrzunehmende Aufgaben erforderlich. Die bisherige Praxis ist deshalb unzulässig; bereits erstellte Listen müssen vernichtet werden.

5.2.1.4 Ist die Übermittlung von Bewerberdaten an die Beschäftigungsbehörden bei Kandidatur auf einer als verfassungsfeindlich eingestuften Liste rechtmäßig?

Diejenigen Bewerber, die auf Listen kandidieren, die — von wem auch immer — als verfassungsfeindlich eingestuft wurden, wurden den Beschäftigungsbehörden mitgeteilt. Diese entscheiden daraufhin, ob und ggf. wie gegen die Betreffenden disziplinarrechtlich vorgegangen wird. Ich halte diese Praxis für problematisch, da die entsprechenden Angaben dem Personalamt nur im Rahmen seiner Kompetenzen gemäß § 15 der Wahlgesetze bekanntgeworden sind.

Gemäß § 27 Abs. 4 HmbWO ist der Dienstvorgesetzte des Bewerbers von der Entscheidung über die Wählbarkeitsvoraussetzungen zu informieren, nicht jedoch über anläßlich des Entscheidungsprozesses dem Personalamt bekanntgewordene Tatsachen. Die Verquickung der Wählbarkeitsentscheidung mit der Übermittlung von Zweifeln über die Verfassungstreue von Wahlbewerbern aus dem öffentlichen Dienst an die Beschäftigungsbehörden verstößt gegen das Zweckbindungsgebot der Datenverarbeitung durch öffentliche Stellen. Sie ist zudem weder durch die Wahlgesetze noch durch sonstige Rechtsvorschriften vorgesehen.

Kurz vor Redaktionsschuß hat mir das Senatsamt für den Verwaltungsdienst — Personalamt — mitgeteilt, daß die Kartei über die Fälle der Wählbarkeit von Beamten und Angestellten der Freien und Hansestadt Hamburg zur Bürgerschaft und zu den Bezirksversammlungen nach der Wahl am 9. November 1986 vernichtet worden sei. Ob zur nächsten Wahl nochmals eine entsprechende Kartei angelegt werde, sei offen und werde zur gegebenen Zeit entschieden werden. Die Parteizugehörigkeit der Wahlbewerber werde in eine neue Kartei jedenfalls nicht mehr aufgenommen werden.

Ich begrüße diese Entscheidung des Senatsamtes für den Verwaltungsdienst. Zu den weiteren — über die karteimäßige Speicherung der Parteizugehörigkeit hinausgehenden — von mir vorgebrachten Kritikpunkten — insbesondere zur Aufbereitung der Daten für „interne Zwecke" und zur Datenübermittlung — hat sich das Senatsamt nicht geäußert. Ich gehe jedoch davon aus, daß die nicht zulässigen von mir monierten Auswertungen und Übermittlungsvorgänge in Zukunft unterbleiben, unabhängig davon, ob die entsprechenden Daten einer Datei, einer Akte oder sonstigen Erkenntnisquellen entnommen werden.

5.2.2 Modernisierung der Lehrerindividualdatei (LID)

Ich habe bereits in meinen vorangegangenen Tätigkeitsberichten ausführlich zu dem Verfahren Lehrerindividualdatei Stellung genommen (3. Tätigkeitsbericht, 3.2.2.6, S. 26 und 4. Tätigkeitsbericht, 4.2.4, S. 32). Im Zusammenhang mit der verstärkten Nutzung neuer IuK-Techniken in der Hamburgischen Verwaltung wurde von der Behörde für Schule und Berufsbildung eine Projektgruppe zur „Modernisierung der LID" eingesetzt.

Bei der LID handelt es sich um ein verhältnismäßig betagtes ADV-Verfahren, das in der Form der Stapelverarbeitung abgewickelt wird. Als Mangel wurde — neben dem umständlichen Verfahrensablauf und der mangelnden Aktualität des Datenbestandes — angesehen, daß die Personalabteilung der BSB kaum von der LID profitiert, obwohl hier die meiste dabei anfallende Arbeit zu leisten ist.

Die „Modernisierung" der LID verfolgt folgende Ziele:

— Dialogisierung des Verfahrens (direkter Zugriff auf Personaldaten durch die Personalsachbearbeiter und Schulaufsichtsbeamten vom Arbeitsplatz aus),

— Integration in ein schrittweise von der BSB aufzubauendes Informationssystem, das z. B. auch die statistischen Informationen über Schüler und Klassen umfaßt,

— Schaffung eines aktuellen Datenbestandes, der sich für vielfältige planerische und dispositive Aufgaben verwenden läßt.

Wegen der strategischen Bedeutung für die Gesamtverwaltung wird das Projekt vom Senatsamt für den Verwaltungsdienst — Organisationsamt — personell unterstützt.

Die zeitgleich mit der Projektgruppe eingesetzte Lenkungsgruppe, an der ich beteiligt bin, hat die Projektgruppe beauftragt, bei ihren Arbeiten den Aspekten Datenschutz, Abgrenzung gegenüber Personalinformationssystemen und Übertragbarkeit auf andere Behörden besonderes Augenmerk zu widmen.

Die Projektarbeit konzentrierte sich bislang auf die Durchführung einer „Daten-Strukturanalyse" (DSA). Dabei handelt es sich um ein modernes Instrument für die systematische Vorbereitung des Einsatzes von Datenbanksystemen, das in Großorganisationen eingesetzt wird (in der Hamburger Verwaltung kam die DSA z. B. beim Projekt „Automatisierung des Einwohnerwesens" erfolgreich zum Einsatz — vgl. 5.7.1). Die Datenstrukturanalyse führt zur Entwicklung eines logischen Datenmodells, in dem die Informationsbedarfe unabhängig von der technischen Realisierung (Hardware, Programmiersprache, Datenbank) dargestellt werden.

Die Unterlagen der Datenstrukturanalyse sollen eine auch für ADV-Laien nach kurzer Einführung verständliche Darstellung des Datenbestandes sein. Sie bilden die Grundlage für

— die Beurteilung der Übertragbarkeit des Verfahrens auf andere Behörden;
— die detaillierte Funktionenanalyse (ablauforientierte Beschreibung der fachlichen Funktionen);
— den Entwurf eines provisorischen Bestandes für das Prototyping und des endgültigen Bestandes und
— die Pflege des künftigen Verfahrens.

Bisher sind folgende Arbeiten geleistet worden:

— Erstellen der Aufgabengliederung der Personalabteilung. Die Aufgaben der Personalabteilung wurden bis zu den Einzelangaben gegliedert, die es erlauben, die verwendeten und produzierten Daten zu nennen. Die Aufgabengliederung bildet die Grundlage für die Beschreibung des Datenflusses zwischen den Aufgaben (graphisch und verbal).
— Entwicklung eines Datenmodells.

  Die bisherige LID bot einen guten Ausgangspunkt für ein vorläufiges Datenmodell. Die bestehenden Schlüsselverzeichnisse wurden überprüft und teilweise umstrukturiert. Soweit Schlüsselverzeichnisse der BVSt vorliegen, sollen diese für die neue LID verwendet werden. Bereits in dieser Phase wurden bestimmte datenschutzrechtliche Belange berücksichtigt. So wurde z. B. der Grund der Schwerbehinderungen als Datenelement gestrichen und die Aufnahme der Krankenstandsmeldungen in die neue LID abgelehnt.

  Das Datenmodell wird durch Untersuchung des Datenflusses zwischen den Aufgaben ständig weiterentwickelt. Zur Zeit läßt sich das Datenmodell in folgende größere Bereiche gliedern:

  — Aktuelle Lehrerindividualdatei;
  — Historik;
  — Veränderungen mit Zukunftsdatum;
  — Unterrichtsverteilung und
  — Schlüsselverzeichnisse.
— Definition des Dateninhalts.

  Für jedes Datenelement wurde die Bedeutung seines Inhalts verbal beschrieben und in der Arbeitsgruppe abgestimmt.
— Ermittlung von Redundanzen.

  Zur Ermittlung von Redundanzen (mehrfach vorhandene Informationen) wurden die Schlüsselverzeichnisse der alten LID und der Besoldungs- und Versorgungsstelle verglichen und angepaßt.

Neben dem hier dargestellten systematischen Ansatz wird ein „Pilotprojekt" vorbereitet, mit dessen Hilfe z.B. die Benutzerfreundlichkeit des zu entwickelnden Verfahrens gewährleistet werden soll.

Bei der Bewertung der „Modernisierung der LID" knüpfe ich an meine Ausführungen zu Personalinformationssystemen im 3. Tätigkeitsbericht (3.2.1, S. 23) an. Zwar ist die Abgrenzung von „Personalinformationssystemen" explizit formuliertes Ziel des beschriebenen Projektes. Ich habe jedoch Zweifel, ob sich die Aussage, die modernisierte LID sei kein Personalinformationssystem, halten läßt.

Trotz aller terminologischen Schwierigkeiten bei der Definition des Begriffs „Personalinformationssystem" handelt es sich ohne Zweifel dann um ein solches System, wenn ein Verfahren folgende Merkmale aufweist:

— Zusammenführung von Daten über das Personal aus verschiedenen Datenbeständen, die für ganz unterschiedliche Aufgaben angelegt worden sind,

— Verknüpfung über ein gemeinsames eindeutiges Kennzeichen,

— vielseitige Verwendung der gespeicherten Daten für verschiedenste Zwecke (z.B. Organisation, Disposition, Planung, Statistik, Beurteilung, Bezahlung).

Selbst dedizierte (d.h. auf eine spezielle Aufgabe zugeschnittene) Systeme können — z.B. durch Zukauf oder Entwicklung weiterer Module — zu umfassenden Personalinformationssystemen ausgebaut werden. Die umfassende Zielsetzung des beschriebenen Projekts „Modernisierung der LID" lassen, auch wenn die entsprechenden Arbeiten noch nicht abgeschlossen sind, den Schluß zu, daß hier ein in Teilen auf andere Behörden übertragbares Personalinformationssystem entsteht.

5.2.3 Überprüfung von Anspruchsvoraussetzungen für die Gewährung des Ortszuschlages (OZ)

Beamten und Angestellten im öffentlichen Dienst steht — neben der Grundvergütung — ein Ortszuschlag zu, der nach sozialen Gesichtspunkten gestaffelt ist. Ledige und Geschiedene (mit bestimmten Ausnahmen) erhalten den Ortszuschlag der Stufe 1, Verheirateten steht der (höhere) Ortszuschlag der Stufe 2 zu. Die Zuordnung zu Stufe 3 und zu den folgenden Stufen erfolgt gemäß der Zahl der Kinder, für die gemäß Bundeskindergeldgesetz Kindergeld gezahlt wird.

Steht der Ehegatte des Bediensteten ebenfalls als Beamter, Richter, Soldat oder Angestellter im öffentlichen Dienst oder in einem Dienst- oder Beschäftigungsverhältnis bei einem anderen dem öffentlichen Dienst gleichgestellten Arbeitgeber und ist dort ebenfalls aufgrund des BAT oder anderer Tarifverträge ortszuschlagsberechtigt, so vermindert sich der zu gewährende Ortszuschlag um die Hälfte des Differenzbetrages zwischen Stufe 1 und Stufe 2. Damit soll vermieden werden, daß die Sozialkomponente des OZ an beide im öffentlichen Dienst beschäftigte Ehepartner (d.h. doppelt) bezahlt wird. Rechtsgrundlagen für die OZ-Gewährung sind die §§ 39 bis 41 Bundesbesoldungsgesetz und § 29 BAT. Die Anspruchsberechtigung auf OZ der Stufe 2 wird von den Behörden bei der Einstellung und danach in unregelmäßigen Abständen mit einem einheitlichen Formular (P 10.025) überprüft. Darauf wurde — um eine Doppelzahlung des auf die Ehe bezogenen OZ-Anteils zu vermeiden — folgende Frage gestellt:

> „2.1 Steht Ihr Ehegatte in einem Beschäftigungsverhältnis im öffentlichen Dienst?
> Ja/Nein/Unbekannt
> Beschäftigungsstelle des Ehegatten (nur auszufüllen, wenn „Ja" oder „Unbekannt" angekreuzt ist): . . ."

Es folgen Fragen, die sich auf den Beschäftigungsumfang (Voll-/Teilzeitbeschäftigung), evtl. Beurlaubungen, die Art des Beschäftigungsverhältnisses und die „Kennziffer, Personalnummer" des Ehegatten beziehen, die ebenfalls nur dann zu beantworten waren, wenn der Ehegatte im öffentlichen Dienst tätig ist.

Diese detaillierten Angaben werden erhoben, um dem öffentlichen Arbeitgeber des Ehegatten eine „Vergleichsmitteilung" über die Meldung des zu Überprüfenden zukommen zu lassen. Der Rechnungshof hat die Begrenzung der Frage nach dem Arbeitgeber des Ehegatten auf den Fall, daß der Erklärende die Zugehörigkeit des Ehegatten zum öffentlichen Dienst bejaht, moniert. Irre sich der Erklärende bei der Verneinung dieser Frage, bleibe der Personalverwaltung regelmäßig verborgen, daß die Anwendung von Konkurrenzregelungen in Betracht komme und ggf. nur verminderte Bezüge zustünden. Die Gefahr des Irrtums ist nach Einschätzung des Rechnungshofes deshalb groß, weil zum öffentlichen Dienst im Sinne des § 40 Abs. 7 BBesG oder entsprechender tariflicher Bestimmungen auch Einrichtungen gehören, die gemeinhin nicht zum öffentlichen Dienst gezählt werden. Die Gefahr des Irrtums wird im übrigen auch in einem Erlaß des Bundesinnenministeriums in der Weise berücksichtigt, daß von einer unverbindlichen Auffassung auszugehen ist, wenn die Frage nach der Zugehörigkeit zum öffentlichen Dienst verneint wurde, die Überprüfung durch die Personalverwaltung aber das Gegenteil ergeben sollte.

Das Senatsamt für den Verwaltungsdienst — Personalamt — vertritt eine ähnliche Auffassung:

Der Verzicht auf die Angabe des Arbeitgebers des Ehegatten in den Fällen, in denen seine Beschäftigung im öffentlichen Dienst verneint wurde, habe wiederholt zu Fehlzahlungen geführt, weil für die Beschäftigten häufig nicht erkennbar gewesen sei, ob es sich bei der Beschäftigung des Ehegatten um eine Tätigkeit im öffentlichen Dienst im Sinne des § 29 Abschnitt B BAT bzw. des Besoldungsrechts handele.

Hier habe auch die Begriffsbestimmung des öffentlichen Dienstes auf der Rückseite des Vordrucks keine Abhilfe schaffen können.

Es sei für die Antragsteller insbesondere nicht klar zu erkennen, ob der Arbeitgeber des Ehegatten

— die für den öffentlichen Dienst geltenden Tarifverträge

— oder Tarifverträge wesentlich gleichen Inhalts

— oder die darin oder in Besoldungsgesetzen über Ortszuschläge oder Sozialzuschläge getroffenen Regelungen

— oder vergleichbare Regelungen

anwende und ob der Bund, ein Land, eine Gemeinde oder andere Körperschaft des öffentlichen Rechts oder ihre Verbände durch Zahlung von Beiträgen oder Zuschüssen oder in anderer Weise beteiligt seien. Für Einrichtungen von Religionsgesellschaften gebe es weitere Besonderheiten.

In allen nicht in einem umfangreichen Verzeichnis aufgeführten Fällen müsse im Einzelfall geprüft werden, ob die Voraussetzungen für eine Gleichstellung mit dem öffentlichen Dienst (Gewährung von Ortszuschlag, Sozialzuschlag oder einer vergleichbaren Leistung, finanzielle Beteiligung des Bundes usw.) gegeben seien.

Das Senatsamt hat aus diesen Gründen dem Rechnungshof zugesagt, bei einer Neuauflage des Vordrucks unter Nr. 2.1 den Klammerzusatz zu streichen. Die z.Z. anstehende Neuauflage wird daher diesen Klammerzusatz nicht mehr enthalten.

Auch wenn ich zugestehe, daß sich die Zuordnung von Institutionen zum Bereich des „öffentlichen Dienstes" im Einzelfall schwierig gestalten kann, erscheint mir der eingeschlagene Weg — Streichung des einschränkenden Klammerzusatzes — als problematisch, da nun in jedem Fall neben der Angabe der Beschäftigungsstelle auch der Umfang der Beschäftigung (Voll- bzw. Teilzeitbeschäftigung), die Art des Beschäftigungs-, Dienst- oder Ausbildungsverhältnisses und die Kennziffer bzw. Personalnummer des Ehegatten erfragt werden.

Da — wie das Senatsamt für den Verwaltungsdienst — Personalamt — bestätigt — nicht vorgesehen ist, nunmehr auch die privaten Arbeitgeber in das ohnehin problematische Vergleichsmitteilungsverfahren einzubeziehen, ist es nicht einzusehen, weshalb

nunmehr bei allen Bediensteten diese differenzierten Daten erhoben werden sollen. Auch wenn — wie in diesem Fall — darüber nachgedacht werden muß, ob die den Bediensteten gestellten Fragen von diesen aufgrund der ihnen gegebenen Erläuterungen zutreffend und vollständig beantwortet werden können, rechtfertigt dies nicht die vollzogene und allem Anschein nach nicht voll durchdachte Änderung des Fragebogens mit der Folge, daß nun regelmäßig z.B. die Personalnummer des Ehegatten auch dann erhoben wird, wenn dieser bei einem privaten Arbeitgeber beschäftigt ist.

Während einige Behörden noch den alten Fragebogen benutzen und sich mit den den Arbeitgeber des Ehegatten betreffenden Fragen auf den öffentlichen Dienst beschränken, beharrt die Behörde für Schule und Berufsbildung auf einer vollständigen Beantwortung des neugefaßten Formulars.

Einer Bediensteten der BSB, die sich mit der Bitte um Überprüfung der Angelegenheit an mich gewandt hatte, wurde mit der Begründung: „Änderung des Ortszuschlages wegen Berufung auf Datenschutz" der Ortszuschlag um die Hälfte des Differenzbetrages zwischen Stufe 1 und Stufe 2 gekürzt. Ich halte die mit dieser Begründung vorgenommene Kürzung der Bezüge für einen Verstoß gegen das in § 23 Hamburgisches Datenschutzgesetz enthaltene Benachteiligungsverbot. Danach darf niemand wegen der Mitteilung von Tatsachen, die geeignet sind, den Verdacht aufkommen zu lassen, das Hamburgische Datenschutzgesetz sei verletzt worden, gemaßregelt oder benachteiligt werden. Dieses Vorgehen läßt zudem den Eindruck entstehen, als würde eine Mitarbeiterin, die von ihrem Recht auf Anrufung des Hamburgischen Datenschutzbeauftragten (§ 22 HmbDSG) Gebrauch macht, aus diesem Grunde diszipliniert. Dies ist um so bedauerlicher, als das Senatsamt für den Verwaltungsdienst mich erst aufgrund dieser Eingabe über seine Absichten und Beweggründe zur Änderung der Überprüfung der Anspruchsvoraussetzungen der OZ-Gewährung informiert hat.

Zwar hat die Schulbehörde zugestanden, daß der Vermerk auf der Änderungsanzeige falsch sei und hat die Begründung für die Gehaltskürzung zurückgezogen. Sie war aber nicht bereit, die erfolgte Kürzung des OZ bei der betroffenen Mitarbeiterin rückgängig zu machen, obwohl die Frage, welche Angaben bei den Bediensteten zur Überprüfung der OZ-Voraussetzungen erhoben werden dürfen, noch nicht abschließend geklärt ist. Da die Behörde an Stelle der fehlerhaften Begründung keine neue — stichhaltigere — Begründung für ihr Vorgehen geliefert hat, halte ich dies für eine fragwürdige Ausnutzung der Machtposition des Dienstherren gegenüber einer Bediensteten. Die BSB hätte durchaus die Möglichkeit gehabt, die in Frage stehenden Gehaltsbestandteile zunächst — evtl. „unter Vorbehalt" — zu zahlen und ggf. nach abgeschlossener Prüfung zurückzufordern.

Ich werde dem Komplex „Überprüfung der Voraussetzungen für die Zahlung von Ortszuschlägen" auch im kommenden Jahr meine Aufmerksamkeit widmen; das praktizierte Verfahren ist noch unter anderen Gesichtspunkten problematisch (Kreis der Befragten, Vergleichsmitteilungsverfahren, Spezialfragebögen für bestimmte Personengruppen).

5.3 Statistik

5.3.1 Volkszählung 1987

Die Vorbereitungen für die für das Jahr 1987 angesetzte Volkszählung liefen im Berichtsjahr an. Die Rechtsgrundlage — das Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1987 — VZG 1987 —) hatte der Deutsche Bundestag bereits 1985 verabschiedet (vgl. meinen 4. TB, 4.3.1, S. 35). Auch wenn zur Zeit nicht abzusehen ist, ob die Diskussion über die Volkszählung 1987 wieder die gleiche Intensität erreicht und mit vergleichbarer Schärfe geführt wird, wie die vom Bundesverfassungsgericht zunächst ausgesetzte und dann in wesentlichen Punkten als nicht mit der Verfassung vereinbar erklärten Volkszählung 1983, möchte ich an dieser Stelle einige Bemerkungen zur geplanten Volkszählung 1987 anbringen:

— Das VZG 1987 berücksichtigt im wesentlichen die vom Bundesverfassungsgericht aufgestellten Forderungen.

— Die allem Anschein nach vorhandene Reserve eines nicht unbedeutenden Anteils der Bevölkerung gegen eine Totalerhebung mit Auskunftszwang und die nicht auszuschließende Möglichkeit, daß kein vollständiges und richtiges Ergebnis zustande kommt, lassen die Frage entstehen, ob der Gesetzgeber nicht besser daran getan hätte, die mit Auskunftspflicht versehenen Merkmale auf ein Mindestmaß zu begrenzen, statt wie im VZG 1987 vorgesehen alle Angaben zwangsweise zu erheben.

— Sollte es zu Auskunftsverweigerungen (harter Boykott) oder zu bewußt unrichtigen Angaben (weicher Boykott) in größerem Ausmaße kommen, sind die daraufhin zu ergreifenden Zwangsmaßnahmen nur unter erheblichem Zeit- und Geldaufwand durchzusetzen. Es ist geplant, in den Erhebungsstellen zur Vorbereitung und Durchsetzung solcher Maßnahmen auch moderne Datenverarbeitungstechnik einzusetzen, wobei neben Dateien mit ausdrücklich durch Gesetz erlaubten Merkmalen (Hilfs- und Erhebungsmerkmale) auch automatisiert geführte „Verweigererdateien" entstehen können, die neue datenschutzrechtliche Probleme aufwerfen (vgl. 5.3.1.2).

— Das VZG 1987 sieht vor, daß die Erhebungsstelle bestimmte ihr von der Meldebehörde übermittelte Daten (Gemeinde, Straße, Hausnummer, Haupt- oder Nebenwohnung, Geburtsjahr und -monat, Geschlecht, Staatsangehörigkeit) für die Vervollständigung der Angaben der Volks- und Berufszählung verwenden darf, soweit im Einzelfall eine Auskunft innerhalb von sechs Wochen nach dem Zählungsstichtag beim Auskunftspflichtigen nicht zu erreichen ist. Diese „Ersatzvornahme" würde lediglich bei diesem Kernbestand von Merkmalen eine vollständige Erhebung garantieren. Die darüber hinaus erhobenen Angaben wären, sollte die Verweigerung — sei sie nun hart oder weich — größeres Ausmaß annehmen, nur noch mit Einschränkung aussagefähig. Eine „Hochrechnung" dieser Merkmale auf den Gesamtbestand wäre nur dann möglich, wenn die Verweigerer die gleiche Struktur hätten wie die Gesamtbevölkerung. Dies ist aber nicht anzunehmen.

Die vom Bundestag am 4. Dezember 1986 verabschiedete Novelle eines Bundesstatistikgesetzes ermächtigt die Bundesregierung, durch Rechtsverordnung die Erhebung einzelner Merkmale auszusetzen und von einer Befragung mit Auskunftspflicht zu einer Befragung ohne Auskunftspflicht überzugehen (§ 5 (4) BStatG).

Angesichts der vorgebrachten Probleme wäre zu erwägen, ob die Bundesregierung hiervon bei der Volkszählung 1987 in der Weise Gebrauch machen sollte, daß nur noch die in § 11 (1) VZG 1987 für die Ersatzvornahme zugelassenen Merkmale und darüber hinaus ggf. einige weitere Merkmale, sozusagen als „unverzichtbarer Kernbestand" zwangsweise erhoben werden. Die Beantwortung der übrigen Fragen sollte freiwillig sein. Eine solche Vorgehensweise würde befriedend wirken und ein Scheitern der gesamten Volkszählung und damit Fehlinvestitionen in Höhe vieler Hundert Millionen DM vermeiden. Ich bin mir der Tatsache bewußt, daß eine Umsetzung dieses Vorschlages auch organisatorische Probleme mit sich brächte, die jedoch — im Verhältnis zu den sich abzeichnenden Problemen bei Durchführung der Volkszählung wie geplant — durchaus zu bewältigen und hinzunehmen wären.

5.3.1.1 Hamburger Verordnung zur Durchführung des Volkszählungsgesetzes 1987

Der Senat hat auf Grund von § 9 Abs. 3 Volkszählungsgesetz 1987 am 2. September 1986 eine Rechtsverordnung erlassen, die gewährleisten soll, daß — bezogen auf die Bedingungen in Hamburg — die notwendigen technischen und organisatorischen Maßnahmen getroffen werden, die einen Datenmißbrauch ausschließen.

Die Verordnung

— bestimmt das Statistische Landesamt zur einzigen Erhebungsstelle und regelt die Abschottung der für die Volkszählung vorgesehenen Räumlichkeiten des Statistischen Landesamtes,

— regelt — unter Konkretisierung der Vorschriften von § 10 VZG 1987 — die Auswahl und die Pflichten der Zähler (kein Einsatz als Zähler im unmittelbaren Nachbarschaftsbereich und bei möglichen Konflikten zwischen beruflicher Tätigkeit und Wahrung des Statistikgeheimnisses — z. B. bei Polizisten, Mitarbeitern der Finanzämter),

— verbietet die Koppelung der Volkszählung 1987 mit anderen — auch freiwilligen — statistischen Erhebungen,

— verpflichtet den Leiter des Statistischen Landesamtes zum Erlaß weiterer organisatorischer und technischer Anordnungen.

Obwohl mit der Gebäudevorerhebung bereits begonnen wurde, lagen mir bis Redaktionsschluß die nach § 8 der Verordnung vom Leiter des Statistischen Landesamtes zu erlassenen ergänzenden Anordnungen noch nicht einmal als Entwurf vor. Ich möchte an dieser Stelle darauf hinweisen, daß es höchste Zeit wird, Regelungen über

— die Funktionen und Verantwortlichkeiten der im Statistischen Landesamt mit der Durchführung der Volkszählung betrauten Bediensteten,

— die Sicherung der für die Aufbewahrung und Bearbeitung der Erhebungsunterlagen bereitgestellten Räume,

— die Berechtigung des Zugangs zu den Räumen und die Überwachung dieser Berechtigung,

— die Sicherung der für die Erhebungsstelle bestimmten Posteingänge,

— die laufende Überwachung der zur Wahrung des Statistikgeheimnisses und des Datenschutzes getroffenen Maßnahmen

zu erlassen. Ihnen kommt aber im Sinne der Sicherstellung des Datenschutzes große Bedeutung zu.

5.3.1.2 ADV-Einsatz in der Erhebungsstelle

Es ist vorgesehen, bei der Volkszählung 1987 erstmals für die Unterstützung der Erhebungsstellen bei der Durchführung der Erhebung moderne Datenverarbeitungstechnik einzusetzen (dagegen sind die Zählungsergebnisse schon bei den vorangegangenen Volkszählungen in automatisierten Verfahren anonymisiert gespeichert und ausgewertet worden). Anders als einige andere Bundesländer will das Statistische Landesamt Hamburg die Vollständigkeitskontrolle der Erhebungsbögen, die „Ersatzvornahme" nach § 11 Abs. 1 VZG 1987 und die Vorbereitung von Zwangsmaßnahmen gegen diejenigen, die ihrer Auskunftspflicht nicht nachkommen, über ein On-line-Verfahren abwickeln. Dabei sollten zunächst 24, inzwischen sogar 48 (s.u.) in der Erhebungsstelle aufgestellte Terminals mit der Datenverarbeitungszentrale der Hamburger Verwaltung (DVZ) verbunden werden. Ein solches Verfahren hat gegenüber dem in Erhebungsstellen anderer Bundesländer alternativ vorgesehenen PC-Einsatz den Vorteil, daß standardmäßig die bei einem solchen Dialogverfahren eingebauten Datensicherungsmaßnahmen über das Betriebssystem gewährleistet werden.

Fraglich könnte allerdings sein, ob die Verarbeitung von im Rahmen der Volkszählung gespeicherten Daten auf demselben Rechner, auf dem auch andere Verwaltungsverfahren abgewickelt werden, dem vom Bundesverfassungsgericht formulierten Abschottungsgebot von Statistik und Verwaltung genügt. Da mir das Statistische Landesamt jedoch bislang kein ADV-Konzept für das geplante Verfahren vorgelegt hat, kann ich hierzu noch nicht abschließend Stellung nehmen.

Es hat mich verwundert, daß der Senat Mitte November bei der Bürgerschaft unter Berufung auf ein „verändertes Konzept" Mittel für 24 weitere Datensichtstationen beantragt hat. Damit sollen „die Zählungsdienststellen für jede denkbare Kontroll- und Prüftätigkeit technisch ausreichend ausgestattet werden" (Drs. 11/7116). Da nach Auskunft des Statistischen Landesamtes bislang noch gar kein ADV-Konzept für den ADV-Einsatz in der Erhebungsstelle erstellt wurde, stellt sich die Frage, auf welcher Grundlage

die Beschaffungsentscheidungen gefällt wurden. Nicht „jede denkbare Kontroll- und Prüftätigkeit" ist im Rahmen der Durchführung der Volkszählung auch zulässig. Im übrigen muß ich feststellen, daß die Drucksache, die sich auch mit den für das Statistische Landesamt vorgesehenen Sicherungsmaßnahmen befaßt, mit mir nicht abgestimmt wurde.

Für den ADV-Einsatz in den Erhebungsstellen gibt es keine spezialgesetzliche Rechtsgrundlage. Andererseits ist der Einsatz von ADV-Anlagen für diesen Zweck auch nicht untersagt. Gleichwohl muß ich feststellen, daß die Speicherung von Identifikationsangaben von Auskunftspflichtigen eine zusätzliche Gefahrenquelle für das informationelle Selbstbestimmungsrecht werden kann, dies deshalb, weil nunmehr die Identifikationsdaten und die statistischen Daten mit Hilfe der ADV ohne großen Aufwand miteinander verknüpft werden könnten. Auch wenn dies hier nicht vorgesehen ist und das VZG 1987 eine Reidentifizierung verbietet, so kann bei der Speicherung der weiter unten beschriebenen Merkmale auf elektronischen Datenträgern nicht mit letzter Sicherheit nachgeprüft werden kann, ob die entsprechenden Daten tatsächlich gelöscht werden (oder ob nicht etwa eine Kopie des Datenbestandes doch noch irgendwo existiert) und somit die im VZG 1987 vorgesehenen Trennungs- und Löschungsregelungen umgangen werden. Zwar gewährleisten moderne DV-Anlagen, daß ein unkontrollierter Zugriff auf gespeicherte Daten stark erschwert wird und alle Aktivitäten auf der Anlage durch automatische Einrichtungen protokolliert werden. Sobald jedoch Datenträger aus der Anlage entfernt und auf einer anderen Anlage ausgewertet oder kopiert werden, wäre ein solcher Eingriff weder zu verhindern (es sei denn, die Daten wären verschlüsselt gespeichert) noch nachzuweisen. Aus diesem Grund sind an die Sicherheit der Datenträgerverwaltung, insbesondere an einen lückenlosen Nachweis des Datenträgerumlaufs (einschließlich Sicherungskopien) besonders strenge Maßstäbe anzulegen.

Es ist geplant, im Rahmen der Durchführung der Zählung durch die Erhebungsstelle folgende Merkmale zu speichern:

(1) Vor- und Familiennamen,
(2) Gemeinde, Straße, Hausnummer,
(3) Haupt- und Nebenwohnung,
(4) Geburtsjahr und -monat,
(5) Geschlecht,
(6) Staatsangehörigkeit,
(7) Bearbeitungsmerkmale.

Bei den Merkmalen (1) und (2) handelt es sich um Hilfsmerkmale gem. § 8 (1) Nr. 1 VZG 1987. Die Merkmale (3) bis (6) sind eindeutig Erhebungsmerkmale (§ 5 Nr. 1 und Nr. 3 VZG 1987). Die Bearbeitungsmerkmale (7) sind weder Erhebungs- noch Hilfsmerkmale.

Die Übermittlung der Merkmale (1) bis (6) durch die Einwohnerdienststellen aus der Einwohnerkartei an die Erhebungsstelle (Statistisches Landesamt) ist nach § 11 Abs. 1 Satz 1 VZG 1987 und die Nutzung der Daten zur Gewährleistung der Vollständigkeit der Zählung und zur „Ersatzvornahme" nach § 11 Abs. 1 Satz 2 VZG 1987 zulässig. Bei der Verarbeitung dieser Daten durch die Erhebungsstelle ist zu unterscheiden, ob es sich um Hilfs- oder um Erhebungsmerkmale handelt: Die Hilfsmerkmale nach § 8 (1) Nr. 1 VZG 87 sind Identifikationsangaben, die zur Organisation und Durchführung der Zählung erforderlich sind. Zu den Hilfsmitteln bei der Organisation der Volkszählung zählen auch Namens- und Adressenlisten, die dem Zähler mitgegeben werden. Diese Listen dürfen nur diejenigen Angaben enthalten, die zur Identifikation der Befragten unbedingt notwendig sind. Angaben zu Erhebungsmerkmalen gewinnen im Zusammenhang mit der Kenntnis von Hilfsmerkmalen eine neue Qualität, da die Hilfsmerkmale als Identifikatoren eine eindeutige Zuordnung zu bestimmten Personen ermöglichen. Aus diesem Grund hat der Gesetzgeber in § 15 VZG 87 Trennungs- und Löschungsvorschriften erlassen, die von den Erhebungsstellen einzuhalten sind. Dar-

über hinaus hat er in § 13 (1) und (4) VZG 87 dem Auskunftspflichtigen die Möglichkeit eingeräumt, die Erhebungsvordrucke der Erhebungsstelle zuzuleiten, ohne daß der Zähler von den Antworten Kenntnis erhält.

Ursprünglich war geplant, die Merkmale (1) bis (5) mit der sogenannten „Namensliste" dem Zähler zur Kenntnis zu bringen. Dagegen hatte ich Bedenken erhoben. Dadurch wäre nämlich die dem Befragten eingeräumte Möglichkeit unterlaufen worden, am Zähler vorbei seine Angaben der Erhebungsstelle zuzuleiten (§ 13), da der Zähler durch die Angaben in der Namensliste auf jeden Fall Kenntnis von einigen Erhebungsmerkmalen erlangen könnte. Das Statistische Landesamt hat sich daraufhin bereit erklärt, in der Namensliste die zur Identifikation der Auskunftspflichtigen notwendigen Angaben auf ein Minimum (Anschrift, Familien- und Vornamen) zu reduzieren und keine weiteren Angaben zur Person auszudrucken.

Bei den „Bearbeitungsmerkmalen" handelt es sich weder um Erhebungs- noch um Hilfsmerkmale. Folgende Merkmalsausprägungen sollten hier ursprünglich gespeichert werden:

— nicht angetroffene Personen/Haushalte,

— Personen/Haushalte, die per Post zurückschicken wollen,

— Personen/Haushalte, die von vornherein verweigern,

— Veränderungen von Personen/Haushalten zwischen dem Zeitpunkt der Erstellung der Namensliste und dem Zählungsstichtag (Geburten, Sterbefälle, Zu- und Wegzüge),

— Personen/Haushalte, die auch zum Zeitpunkt der Erstellung der Namensliste dort nicht gewohnt haben („Karteileichen").

Eine Erhebung derart differenzierter „Bearbeitungsmerkmale", die zudem auf subjektiven Wahrnehmungen der Zähler beruht, hätte einer gesetzlichen Grundlage bedurft, die jedoch nicht besteht. Da die vom Statistischen Landesamt geplante Datei im wesentlichen der Vollständigkeitskontrolle dienen soll, darf allenfalls gespeichert werden, ob eine Person oder ein Haushalt den Bogen per Post zurücksendet oder ob aus anderen Gründen der Zähler keine ausgefüllten Erhebungsvordrucke zurückbringt. Ich habe gegenüber dem Statistischen Landesamt erklärt, daß ich eine weitere, über die genannten zwei Fallgruppen hinausgehende Differenzierung (etwa die gesonderte Markierung von Personen/Haushalten, die erklärt haben, verweigern zu wollen) für nicht zulässig halte. Das Statistische Landesamt hat sich mit der Reduktion der „Bearbeitungsmerkmale" auf die zwei angeführten Ausprägungen einverstanden erklärt.

5.3.1.3 Hinweise auf dem Haushaltsmantelbogen

Auf dem dem Innenausschuß bei seiner Beschlußfassung über das Volkszählungsgesetz 1987 vorgelegten Haushaltsmantelbogen befand sich folgender Hinweis:

> „Der Haushaltsmantelbogen mit seinen Angaben dient allein der Organisation der Zählung. Ihr Name wird nicht elektronisch gespeichert. Er dient lediglich dazu, die Vollzähligkeit der Erhebung zu gewährleisten . . ."

Im Hinblick auf den in vielen Erhebungsstellen — auch in Hamburg (vgl. Nr. 5.3.1.2) — vorgesehenen Einsatz von automatisierter Datenverarbeitung bei der Abwicklung der Zählung, entsprach dieser Passus nicht der tatsächlichen Praxis. Daraufhin hat das Statistische Bundesamt den Hinweis wie folgt geändert:

> „. . . Ihr Name hilft lediglich, die Vollzähligkeit der Erhebung zu gewährleisten; er wird nicht zusammen mit Ihren Angaben aus dem Personenbogen oder dem Wohnungsbogen auf elektronischen Datenträgern gespeichert . . ."

Zwar stellt die Neufassung — v.a. zusammen mit den vom Statistischen Bundesamt erstellten „Informationen zur Volkszählung 1987" — eine Annäherung an die geplante Praxis dar; voll befriedigen kann sie jedoch nicht: Ich hätte es für besser gehalten,

wenn die Formulierungen auf dem Haushaltsmantelbogen so gefaßt worden wären, daß sie dem Informationsanspruch des Bürgers nach § 16 VZG 1987 genügen. Sie hätten über Zweck, Art und Umfang der Datenverarbeitung zutreffend, vollständig und verständlich Auskunft geben müssen. Ich habe Zweifel, ob dies durch die vorgesehene Formulierung („Ihr Name wird . . . nicht zusammen mit Ihren Angaben aus dem Personenbogen oder dem Wohnungsbogen auf elektronischen Datenträgern gespeichert") tatsächlich erreicht wird.

5.3.1.4 Zählergewinnung

Für die Durchführung der Volkszählung werden allein in Hamburg mehr als 13 000 Zähler benötigt. Die ehrenamtlichen Zähler sind von der Erhebungsstellen (in Hamburg vom Statistischen Landesamt) auszuwählen (§ 10 Abs. 1 VZG 1987). Bund, Länder und Gemeinden sind nach § 10 Abs. 3 VZG 1987 verpflichtet, den Erhebungsstellen auf Anforderung Bedienstete für die Zählertätigkeit zu benennen.

Um möglichst viele Freiwillige als Zähler zu gewinnen, haben sich die in Hamburg vertretenen öffentlichen Arbeitgeber, insbesondere die Freie und Hansestadt Hamburg, zunächst an der Werbung freiwilliger Zähler beteiligt. Die Bediensteten der FHH wurden in einem Brief dazu aufgefordert, sich freiwillig als Zähler zu melden. Für die Werbeaktion wurde auf die zentral geführten Datenbestände der Besoldungs- und Versorgungsstelle zurückgegriffen. Da es im Interesse der reibungslosen Durchführung der Zählung ist, einen möglichst großen Anteil der Zähler auf freiwilliger Basis zu gewinnen und bei der zunächst durchgeführten Werbeaktion auch keine Datenübermittlung an Dritte stattgefunden hat (der Brief richtete sich direkt an die Bediensteten), habe ich an dem praktizierten Verfahren allenfalls auszusetzen, daß die zum Zwecke der Besoldungszahlung gespeicherten Daten verstärkt auch für andere — wenn auch in diesem Falle nicht zu beanstandende — Zwecke gebraucht werden.

Da befürchtet wird, daß sich freiwillige Zähler nicht in genügender Zahl finden lassen, wurde parallel zu der „Werbeaktion" die zwangsweise Verpflichtung von Zählern vorbereitet. Nach § 10 Abs. 2 VZG 1987 ist zur Übernahme der Zählertätigkeit jeder Deutsche vom vollendeten 18. bis zum vollendeten 65. Lebensjahr verpflichtet. Zu befreien ist, wem eine solche Tätigkeit aus gesundheitlichen oder anderen wichtigen Gründen nicht zugemutet werden kann (§ 10 Abs. 2 Satz 2 VZG 1987). Um die Verpflichtungsaktion vorzubereiten, hat das Senatsamt für den Verwaltungsdienst — Personalamt — die Namen, Vornamen, Anschriften und Beschäftigungsbehörden aller 40 000 Beamten und Angestellten der FHH, die

— ihren Hauptwohnsitz in Hamburg haben,

— nicht zu den Bereichen Polizei, Steuerverwaltung, Staatsanwaltschaft, Einwohner-Zentralamt und Verfassungsschutz und

— nicht zu den Schichtdiensten

gehören, aus den Dateien der Besoldungs- und Versorgungsstelle dem Statistischen Landesamt übermittelt. Dieses hat diese Daten an der Datei der Baublöcke vorbeigeführt, um den Einsatzbereich als Zähler außerhalb der unmittelbaren Nachbarschaft der Betroffenen festzulegen (nach § 5 Abs. 3 der Verordnung zur Durchführung des VZG 1987 dürfen Zähler nicht in dem Baublock, in dem sie wohnen und in den ihn unmittelbar umschließenden Baublöcken eingesetzt werden). Die so ergänzten Daten hat das Statistische Landesamt in Listenform an die Beschäftigungsbehörden gegeben mit der Maßgabe, ein Drittel der aufgelisteten Personen als Zähler zu benennen. Besondere Auflagen, etwa über die räumliche Verteilung der von den Behörden auszuwählenden Zähler wurden vom Statistischen Landesamt nicht gestellt.

Ich halte die Übermittlung der Daten von insgesamt 40 000 Bediensteten durch das Senatsamt für den Verwaltungsdienst an das Statistische Landesamt bei insgesamt nur 13 000 zu bestellenden Zählern für nicht verhältnismäßig und auch nicht vom Volkszählungsgesetz 1987 gedeckt. Korrekt wäre es gewesen, wenn die Benennung der notwendigen Zahl der Zähler direkt durch die Beschäftigungsdienststellen evtl. in

Zusammenarbeit mit dem Personalamt, aber ohne vorherige Übermittlung einer so großen Zahl von Personaldaten an das Statistische Landesamt erfolgt wäre. Im übrigen hat die Einschaltung des Statistischen Landesamtes in diesem frühen Stadium die Zählergewinnung in keiner Weise gefördert, zumal die vom Statistischen Landesamt vorgenommene Zuordnung der Bediensteten zu Baublöcken zweckmäßigerweise erst nach der Benennung von 13 000 in Frage kommenden Zählern erfolgt wäre, weil die Baublockzugehörigkeit kein Auswahlkriterium für die Behörden darstellt.

Ich halte das gewählte Verfahren auch aus einem anderen Grund für bedenklich: In einem vom Statistischen Landesamt vorbereiteten „Benachrichtigungsschreiben" werden die Bediensteten, deren Benennung als Zähler vorgesehen ist, dazu aufgefordert, Gründe, aus denen ihnen die Zählertätigkeit nicht zugemutet werden kann, gegenüber ihrer Beschäftigungsdienststelle geltend zu machen. Die Behörden verfahren mit diesen Einwendungen unterschiedlich. Während einige Dienststellen die vom Statistischen Landesamt geforderte Anzahl der Bediensteten benennen und auch eventuelle Einwendungen gegen eine Zählerbestellung ungeprüft weiterleiten, prüfen andere Behörden inhaltlich, ob den Betroffenen der Zählerdienst zugemutet werden kann. Dabei werden nicht nur dienstliche Belange (z.B. Dienstzeiten am Nachmittag oder Abend) sondern auch gesundheitliche und soziale Gründe (Betreuung pflegebedürftiger Angehöriger, Alkoholgefährdung, alleinerziehender Elternteil usw.) geprüft. In den Fällen, in denen die Gründe für stichhaltig befunden werden, verzichten diese Behörden auf die Zählerbenennung. Andernfalls werden die Betroffenen benannt und die gegenüber der Beschäftigungsbehörde geäußerten Einwendungen an das Statistische Landesamt weitergeleitet. Es ist nicht sichergestellt, daß die von den Behörden auf diese Weise erlangten — z.T. sehr sensiblen — Informationen über das Privatleben und die Gesundheit ihrer Bediensteten nicht — gewollt oder ungewollt — in personalpolitische Entscheidungen einfließen. So ist es nicht auszuschließen, daß Kenntnisse über gesundheitliche Beeinträchtigungen oder besondere soziale Belastungen von Bediensteten, die die Behörde durch Einwendungen gegen die Zählerbenennung erlangt hat, bei der Besetzung von Beförderungsstellen eine Rolle spielen können. Diese Gefahr besteht, da die Entscheidungen über die Zählerbenennung in der Regel in den Personalabteilungen fallen, die auch bei der Personaldisposition mitwirken, obwohl die entsprechenden Unterlagen natürlich nicht in die Personalakten gelangen dürfen,

Gemäß § 10 Abs. 1 VZG 1987 sind Auswahl und Bestellung der Zähler Aufgaben der Erhebungsstelle. Dementsprechend wäre es auch vorzuziehen gewesen, wenn die persönlichen Gründe, die von als Zähler vorgesehenen Bediensteten gegen eine Zählerbestellung vorgebracht werden, direkt gegenüber dem Statistischen Landesamt vorgebracht und von diesem auch geprüft und bei der Zählerauswahl berücksichtigt worden wären. Aus den Vorschriften des Volkszählungsgesetzes läßt sich lediglich ableiten, daß die Behörden bei der Zählerbenennung dienstliche Gründe, die gegen einen Zählereinsatz sprechen, erheben und bei ihrer Entscheidung über die Benennung berücksichtigen, damit „lebenswichtige Tätigkeiten öffentlicher Dienste. . . nicht unterbrochen werden" (§ 10 Abs. 3 VZG 1987). Neben dem beschriebenen Benennungsverfahren ist auch die Information der für die Benennung vorgesehenen Bediensteten durch die Behörden zu beanstanden. In dem vom Statistischen Landesamt entworfenen Muster eines Benachrichtigungsschreibens und den mir vorliegenden tatsächlich an die Bediensteten verschickten Schreiben fehlt eine klare und vollständige Information über das Verfahren der Zählerauswahl und in diesem Zusammenhang vorgesehene Datenübermittlungen. So wird nicht deutlich, daß die Behörden die ihnen gegenüber geäußerten Hinderungsgründe gegen die Bestellung zum Zähler an eine andere Stelle — das Statistische Landesamt — weiterleiten. Im Gegenteil: über den Verbleib der Einwendungen — auch darüber, daß diese nicht zur Personalakte genommen werden — fehlt jede Aussage.

Obwohl im Rahmen der Zählerverpflichtung Daten von mehr als 40 000 Bediensteten der FHH mehrfach übermittelt und von den zur Zählerbenennung vorgesehenen Mitarbeitern z.T. — wie beschrieben — sehr sensible Daten erhoben und ebenfalls übermit-

telt wurden, bin ich über das gewählte Verfahren weder vom Statistischen Landesamt noch vom Senatsamt für den Verwaltungsdienst — Personalamt — vorab informiert worden und hatte somit auch keine Gelegenheit, meine Bedenken geltend zu machen.

5.3.2 Mikrozensus

In meinem 4. TB (3.5, S. 19) bin ich auf das Problem der Deanonymisierung von für Statistiken erhobenen und anonymisierten Daten eingegangen. Dabei ging es u.a. um die Frage, welche Merkmale wenigstens bekannt sein müssen, um eine Deanonymisierung durchführen zu können.

Insgesamt werden bei der jedes Jahr durchgeführten Mikrozensus-Befragung etwa 60 Fragen gestellt, die von allen Mitgliedern der zu einer 1%-Stichprobe gehörenden Haushalte zu beantworten sind.

Dabei wird unterschieden zwischen Hilfs- und Erhebungsmerkmalen. Die Hilfsmerkmale dienen allein der Durchführung der Zählung. Es handelt sich dabei um

— Vor- und Familienname,
— Telefonnummer,
— Straße, Hausnummer, Lage der Wohnung im Gebäude,
— Vor- und Familienname des Wohnungsinhabers
— Name der Arbeitsstätte.

Die Hilfsmerkmale, die eine eindeutige Identifizierung der Auskunftspflichtigen ermöglichen, dürfen nur getrennt von den Erhebungsmerkmalen auf gesonderte für die maschinelle Weiterverarbeitung bestimmte Datenträger übernommen werden. Die Erhebungsvordrucke einschließlich der Hilfsmerkmale sind spätestens vier Jahre nach Durchführung der Erhebung zu löschen. Durch diese Regelungen soll gewährleistet werden, daß auf Dauer lediglich die anonymisierten, d.h. den einzelnen Befragten nicht mehr zuzuordnenden Erhebungsdaten gespeichert und für statistische, planerische und wissenschaftliche Zwecke ausgewertet werden. Da die erhobenen Datenbestände tief in die Intimsphäre der Betroffenen hineinreichen (die beim Mikrozensus gestellten Fragen gehen weit über die im Rahmen der Volkszählung erhobenen Merkmale hinaus), kommt dem Schutz der Auskunftspflichtigen davor, daß ihre Daten anderen Personen bekannt werden, große Bedeutung zu.

Eine Reidentifizierung des Auskunftspflichtigen (oder sinngleich: Deanonymisierung der Daten) bezeichnet in diesem Zusammenhang die Möglichkeit, die Daten, obwohl sie ohne die Hilfsmerkmale gespeichert sind, wieder einzelnen Personen oder Haushalten zuzuordnen.

Damit eine Reidentifizierung möglich ist, müssen folgende Bedingungen erfüllt sein:

(1) Es müssen bestimmte Merkmale der Person oder des Haushalts, der festgestellt werden soll, bekannt sein.

(2) Derjenige, der einen Reidentifizierungsversuch unternimmt, muß Zugang zu den gespeicherten Daten haben.

Erkenntnisziel einer Reidentifizierung könnte es sein,

— die noch nicht bekannten Merkmale der Zielperson zu erfahren oder

— Erkenntnisse über andere Personen, die in demselben Haushalt oder in derselben Wohnung leben wie die Zielperson, zu gewinnen (da die Zugehörigkeit zu einem Haushalt selbst ein auf Dauer gespeichertes Erhebungsmerkmal darstellt, könnten durch Reidentifizierung nur eines Haushaltsmitgliedes auch die übrigen Mitglieder festgestellt werden).

Für eine Reidentifzierung besonders geeignet sind v.a. solche Merkmale, bei denen es eine große Zahl möglicher Merkmalsausprägungen gibt (z.B. Geburtsjahr oder Einkommen). Schon die Kenntnis sehr weniger Merkmale (z.B. Alter, Berufsbereich und

Miethöhe) ermöglicht mit großer Wahrscheinlichkeit die Reidentifizierung des die gesuchte Person betreffenden Datensatzes und damit auch die individuelle Zuordnung der übrigen Merkmalsausprägungen (also z. B. Schulbildung, Familienstand, Angaben zur Erwerbstätigkeit). Dies wird auch vom Statistischen Landesamt eingeräumt. Eine dort durchgeführte Modellrechnung kommt zu folgendem Ergebnis:

„Wir unterstellen, daß von einer Person das Alter, der Berufsbereich (aus einer Systematik von 39 Berufen) und die Miethöhe nach einer von elf Gruppen jeweils in Schritten von DM 100,— bekannt sind.

Im Mikrozensus 1985 wurden z. B. 200 Personen im Alter von 55 Jahren erfaßt. Nimmt man an — was wahrscheinlich nicht der Realität entspricht —, daß diese Personen über die Kategorien Beruf und Miethöhe sich gleichmäßig verteilen, wäre zu erwarten, daß in jedem Feld der nach den genannten Merkmalen gegliederten Tabelle im Durchschnitt

$$\frac{200}{39 \times 11} = 0{,}47 \text{ Personen}$$

anzutreffen wären. Die meisten Tabellenfelder blieben also leer, da die entsprechenden Merkmalskombinationen auf keine Person zutreffen. Damit ist die Identifizierungsmöglichkeit einzelner Personen wahrscheinlich. Selbst wenn man in dieser Altersgruppe von der gleichen Verteilung der Miethöhe wie bei der Gesamtbevölkerung ausgeht und die betreffende Person der am stärksten besetzten Mietklasse zuordnet (nach dem Mikrozensus 1982 fallen 28 % der Wohnungen in die Kategorie DM 300,— bis DM 400,—), würde die Verteilung der sich daraus ergebenden 56 Personen über die 39 Berufe zu einem Erwartungswert von

$$\frac{56}{39} = 1{,}44 \text{ Personen}$$

pro Tabellenfeld führen. Bei zusätzlicher Nutzung der Angabe des Geschlechts läge der Erwartungswert wieder deutlich unter 1. Die Identifizierung der meisten Personen dieser Gruppe wäre damit hochwarscheinlich."

Wenn bei Mehrpersonenhaushalten ein Deanonymisierungsversuch unternommen wird, genügt sogar die Kenntnis von noch weniger Merkmalen als in der Modellrechnung beschrieben für die Erzielung eines „Treffers". Angesichts dieser Ergebnisse kommt der Datensicherung (dem Schutz der Daten vor unberechtigtem Zugriff) und vor allem der strikten Trennung von Statistik und Verwaltung größte Bedeutung zu. In diesem Zusammenhang verweise ich auf meine Ausführungen zur Notwendigkeit eines Landesstatistikgesetzes (vgl. 5.3.3).

5.3.3 Landesstatistikgesetz

Ich habe bereits in meinem 4. TB (4.3.5, S. 43) darauf hingewiesen, daß mir ein Landesstatistikgesetz notwendig erscheint. Die Notwendigkeit ergibt sich vor allem aus folgendem:

Das Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz — BStatG —) bindet das Statistische Landesamt nur insoweit, als es bei der Durchführung von Bundesstatistiken mitwirkt. Das Bundesstatistikgesetz regelt das Verwaltungsverfahren für Bundesstatistiken (Art. 73 Nr. 11 GG), und das abschließend, ist aber kein (Rahmen-) Gesetz, das Vorgaben für den Landesgesetzgeber enthält.

Da entsprechende landesrechtliche Regelungen fehlen, sind die im Statistischen Landesamt abgewickelten Landesstatistiken ohne ausreichende gesetzliche Grundlage.

Das Bundesverfassungsgericht hat mit seinem Volkszählungsurteil besondere Anforderungen an die Erhebung und Verarbeitung personenbezogener Daten für statistische Zwecke formuliert, die auch bei Landesstatistiken einzuhalten sind:

„Ist die Vielfalt der Verwendungs- und Verknüpfungsmöglichkeiten damit bei der Statistik von der Natur der Sache eher nicht im voraus bestimmbar, müssen der Informationserhebung und -verarbeitung innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen. Es müssen klar definierte Verarbeitungsvoraussetzungen geschaffen werden, die sicherstellen, daß der einzelne unter den Bedingungen einer automatischen Erhebung und Verarbeitung der seine Person betreffenden Angaben nicht zum bloßen Informationsobjekt wird. Beides, die mangelnde Anbindung an einen bestimmten, jederzeit erkennbaren und nachvollziehbaren Zweck sowie die multifunktionale Verwendung der Daten, verstärkt die Tendenzen, welche durch die Datenschutzgesetze aufgefangen und eingeschränkt werden sollen, die das verfassungsrechtlich gewährleistete Recht auf informationelle Selbstbestimmung konkretisieren." (Urteilstext S. 50 f.)

Gerade weil Statistiken Datensammlungen auf Vorrat darstellen, denen eine konkrete Zweckbindung zumeist abgeht, ist besonderer Wert auf die Normenklarheit der anordnenden Rechtsvorschriften (Art der Daten, Verarbeitungsform, Trennungs- und Löschungsgebote usw.) und auf die strikte organisatorische und personelle Abschottung der die Statistiken durchführenden Stellen von der übrigen Verwaltung zu legen. Es bietet sich an, die in diesem Zusammenhang zu regelnden allgemeinen Sachverhalte in einem Landesstatistikgesetz zusammenzufassen und darüber hinaus spezialgesetzliche Rechtsgrundlagen für die einzelnen Statistiken zu schaffen, wie dies auch bei den Bundesstatistiken der Fall ist.

Das Statistische Landesamt hat in der Vergangenheit wiederholt erklärt, es gäbe keine hamburgischen Landesstatistiken. Dies trifft nicht zu. Richtig ist nur, daß es in Hamburg keine Landesstatistiken anordnenden Landesgesetze gibt.

Unter Landesstatistiken sind zu verstehen:

— Statistiken für Landeszwecke, für die Daten bei den Betroffenen unmittelbar mit oder ohne Auskunftspflicht erhoben werden (Primärstatistiken),

— Statistiken für Landeszwecke, die sich aus dem Geschäftsgang der Behörden ergeben bzw. aus automatisierten Verwaltungsdateien abgeleitet werden (Sekundärstatistiken) und

— Statistiken, die aufgrund von Vereinbarungen der Bundesländer durchgeführt werden (sog. koordinierte Landesstatistiken).

Nach dem Verzeichnis der im Statistischen Landesamt der Freien und Hansestadt Hamburg bearbeiteten Statistiken gibt es eine Fülle von Statistiken, die für hamburgische Zwecke oder als koordinierte Länderstatistiken durchgeführt werden und bei denen zu vermuten ist, daß hierbei personenbezogene Daten erhoben oder verarbeitet werden.

Die Behörde für Inneres hat sich bislang noch nicht abschließend zu der Notwendigkeit eines Landesstatistikgesetzes geäußert. Ich möchte indes darauf hinweisen, daß die bislang geübte Praxis, Statistiken mit personenbezogenen Daten auch ohne gesetzliche Grundlage durchzuführen, nicht fortgesetzt werden darf.

5.3.4 Verwendung von personenbezogenen Kennzeichen in Sekundärstatistiken

Ein besonderes, ebenfalls durch ein Landesstatistikgesetz (vgl. 5.3.3) und in Einzelgesetzen zu regelndes Problem bildet die Verwendung von Aktenzeichen oder vergleichbaren Identifikationsangaben im Rahmen von Sekundärstatistiken.

Es handelt sich dabei z. Z. um 26 Statistiken, für die das Statistische Landesamt Einzeldaten über natürliche Personen mit Geschäftszeichen oder ähnlichen Kennzeichen von verwaltungsinternen Auskunftsstellen erhält. Die entsprechenden Daten (sowohl die Erhebungsmerkmale im eigentlichen Sinne als auch die Aktenzeichen o. ä.) stammen sämtlich aus dem Verwaltungsvollzug. Der Personenbezug ist über das Identifikationsmerkmal herstellbar. Aufgrund ihres Inhalts lassen sich Kennzeichen, die identifi-

zierenden Charakter haben (Namensbestandsteile mit Geburtsdatum und andere Namenssurrogate), Kennzeichen, die unverschlüsselte oder verschlüsselte Informationen über die Person des Betroffenen oder die Herkunft der Daten enthalten (z. B. Sitz der Verwaltungsbehörde, Steuerart), die im speziellen Fall einer besonderen Geheimhaltung unterliegen können (z. B. nach der AO oder dem SGB), und neutrale Kennzeichen, die keinen Aufschluß über den Betroffenen geben, unterscheiden.

Eine gesetzliche Ermächtigung zur Verwendung eines Kennzeichens für bundesstatistische Zwecke ist bisher in § 35 Abs. 3 Wohngeldgesetz für die „Kennummer" der Wohngeldstatistik enthalten. Darüber hinaus regelt der Regierungsentwurf eines Hochschulstatistikgesetzes die Nutzung der Matrikelnummer bei der Studentenstatistik.

Die Notwendigkeit der Verwendung der Kennzeichen wird von Statistikern damit begründet, daß ein Teil der kaum zu vermeidenden Fehler und Unklarheiten nur durch einen Rückgriff auf das Datenmaterial, aus dem die Angaben gewonnen werden, zu bereinigen ist.

Problematisch ist die Erhebung und Verwendung dieser Kennzeichen unter folgenden Gesichtspunkten:

— Eine durch nicht plausible Angaben motivierte Rückfrage bei einer auskunftgebenden Stelle könnte bei dieser Zweifel aufkommen lassen, ob ihre eigenen Unterlagen (Verwaltungsvorgänge) der Wahrheit entsprechen. Dadurch entsteht die Gefahr, daß unter Verletzung des Grundsatzes der Trennung von Statistik und Verwaltungsvollzug Angaben, die für statistische Zwecke erhoben wurden, für Verwaltungszwecke (Sachverhaltsermittlungen, Korrektur von Verwaltungsdaten) genutzt werden.

— Kennzeichen bieten die Möglichkeit, Verknüpfungen mit Datenbeständen aus anderen Bereichen vorzunehmen. Sie können zudem den Charakter eines auf Dauer angelegten bereichsspezifischen Personenkennzeichens haben (Steuernummer).

— Kennzeichen sind zum Teil frei zugänglich oder zumindest Verfahrensbeteiligten und am Verfahren Interessierten bekannt bzw. ohne große Mühe zugänglich (z. B. Geschäftszeichen der Gerichte).

— Ein erhöhtes Reidentifizierungsrisiko besteht, wenn Kennzeichen nicht auf statistische Funktionen beschränkt bleiben. Zudem bestehen nur geringe Chancen zur Aufklärung eines Mißbrauchs, wenn Kennzeichen vielen Mitarbeitern in den Verwaltungsbehörden und nicht nur den Statistiksachbearbeitern bekannt sind.

— Die Verarbeitung von Kennzeichen, die die Betroffenen unmittelbar identifizieren oder verschlüsselte oder unverschlüsselte Informationen enthalten, bedeutet einen unmittelbaren Eingriff in das Recht auf informationelle Selbstbestimmung. Ein solcher Eingriff ist nach dem Volkszählungsurteil nur aufgrund einer gesetzlichen Erlaubnis zulässig.

Aus der dargestellten Problemlage ergibt sich die Notwendigkeit, in den die jeweiligen Statistiken anordnenden Rechtsvorschriften die Art des Kennzeichens, die zulässigen Nutzungsmöglichkeiten, die Trennung von den Erhebungsmerkmalen, das Verbot der Weitergabe und die Löschung festzulegen.

Als Alternative zu der Verwendung der Akten- und Geschäftszeichen bieten sich an:

— Plausibilitätskontrollen für Zwecke der Statistik werden verstärkt in den auskunftgebenden Stellen durchgeführt.

— Bei Daten, die maschinell verarbeitet werden, kann eine Umschlüsselung der Kennzeichen vor Übermittlung der Daten an die Statistischen Ämter erfolgen.

— Das Statistische Landesamt kann verstärkt nur für Statistikzwecke benutzte laufende Nummern vergeben (Aufdruck auf Erhebungsunterlagen).

Auf Kennzeichen, die nicht nur dem Zweck der Durchführung einer einzelnen Sekundärstatistik dienen, sollte generell verzichtet werden, wenn dadurch nicht ihre Durchführung gefährdet wird.

5.4 Landesarchivgesetz

Unter Datenschutzaspekten bringt das Fehlen eines Archivgesetzes vor allem für die zeitgeschichtliche Forschung Probleme mit sich, da die Zeithistorik wegen ihres Bezugs auf die jüngere Vergangenheit auch auf personenbezogene Dokumente von noch lebenden, bzw. erst vor kurzer Zeit verstorbenen Personen zurückgreifen will.

Das Interesse an der Erforschung der jüngeren Vergangenheit, insbesondere an der Aufklärung von Vorgängen während der Periode des Nationalsozialismus, gerät in Konflikt mit der Wahrung des Rechts auf informationelle Selbstbestimmung von in Archivalien erwähnten Personen. Es ist keineswegs Ziel des Datenschutzes, zeithistorische Forschung zu erschweren oder gar zu verhindern, indem den Forschenden die für ihre Arbeit notwendigen Dokumente vorenthalten werden. Gleichwohl bedarf es einer klaren gesetzlichen Grundlage für die Herausgabe personenbezogenen Archivgutes.

Da der von der Bundesregierung 1984 eingebrachte Entwurf eines Bundesarchivgesetzes mit Sicherheit in dieser Wahlperiode nicht mehr verabschiedet wird und nicht absehbar ist, ob, wann und in welcher Gestalt die Bundesregierung einen neuen Entwurf einbringen und der Bundestag ihn verabschieden wird, ist es nicht mehr hinnehmbar, daß der Senat eine Bundesregelung abwartet. Vielmehr muß er hier die Initiative ergreifen, um das bestehende Regelungsdefizit zu beseitigen und der Bürgerschaft ein Landesarchivgesetz vorlegen, wie dies in anderen Bundesländern bereits geschehen ist. Nur durch ein Gesetz lassen sich Grundrechtsbeschränkungen — darum handelt es sich bei der Weitergabe personenbezogenen Archivgutes von lebenden Personen — auf eine verfassungsrechtlich einwandfreie Grundlage stellen.

Die Benutzung des Staatsarchivs und damit auch die Weitergabe personenbezogenen Archivgutes ist bislang in einer Benutzerordnung geregelt, die vom Direktorium des Archives erlassen wurde. Darin wird zwischen für die allgemeine Benutzung gesperrtem und nicht gesperrtem Archivgut unterschieden. Sperrfristen wurden durch Senatsbeschluß vom 20. Juli 1977 festgelegt. Der Senatsbeschluß lautet:

„1. Das Staatsarchiv kann nichtpersonenbezogenes staatliches Archivgut mit Ablauf des dreißigsten und personenbezogenes staatliches Archivgut mit Ablauf des sechzigsten Jahres nach seiner Schließung für wissenschaftliche und sonstige nichtamtliche Zwecke zugänglich machen, soweit nicht von den Behörden, aus deren Zuständigkeitsbereich das Archivgut stammt, längere Sperrfristen festgesetzt sind.

2. Ausnahmegenehmigungen zur Benutzung von staatlichem Archivgut, das Benutzungsbeschränkungen nach Nummer 1 unterliegt, kann der mit der Dienstaufsicht über das Staatsarchiv beauftragte Staatsrat im Einvernehmen mit der betroffenen Behörde in begründeten Fällen erteilen."

Am 1. Juli 1980 haben die Staatsräte ergänzend hierzu den Beschluß gefaßt, bei der Prüfung des Einzelfalles und bei der Abwägung der Interessen solle auf jeden Fall der Persönlichkeitsschutz Vorrang haben.

Zwar führt das Staatsarchiv keine Statistik über die erteilten Ausnahmegenehmigungen, doch ist in letzter Zeit eine deutliche Zunahme der Anträge und auch der Ausnahmegenehmigungen für die Nutzung personenbezogenen Archivgutes vor Ablauf der regulären Sperrfristen zu verzeichnen (1986 ca. 2 Fälle pro Monat). Das Staatsarchiv verfährt dabei folgendermaßen: Für jeden Fall von Archivalienbenutzung wird eine Akte angelegt, die gegebenenfalls den Vorgang betreffende Ausnahmegenehmigungen enthält. Jeder Einzelfall wird nach seinen besonderen Umständen geprüft: Forscher, Thema, methodische Notwendigkeit der Benutzung personenbezogenen Archivgutes, Art und Inhalt der gewünschten Archivalien, Möglichkeit einschränkender Auflagen wie Kopierverbot und Anonymisierung in der geplanten Veröffentlichung. In jedem Einzelfall ist zwischen den Grundsätzen des Schutzes der Menschenwürde (Art. 1,1 GG) und der informationellen Selbstbestimmung einerseits und der Wissenschaftsfreiheit (Art. 5,3 GG) andererseits abzuwägen. Dabei ist auch der Gesichtspunkt von Bedeutung, daß Daten aus dem familiären und Intimbereichen einer Person unter stärkerem Schutz stehen als Informationen aus dem öffentlichen, d.h. politischen, amtli-

chen oder wissenschaftlichen Tätigkeitsbereich. In jedem Fall ist Voraussetzung der Einsichtnahme in personenbezogenes Archivgut, daß der Benutzer sich schriftlich verpflichtet, die berechtigten Interessen Dritter zu berücksichtigen und die Verantwortung und Haftung gegenüber Dritten anzuerkennen, die eine Verletzung ihrer Interessen durch die Archivalienauswertung behaupten. Sofern dem Staatsarchiv bekannt ist oder sofern das Staatsarchiv mit seinen Hilfsmitteln feststellen kann, daß die Betroffenen leben, werden personenbezogene Archivalien nur mit Zustimmung der Betroffenen vorgelegt.

Auch wenn ich keine gravierenden materiellen Bedenken gegen die dargestellte Praxis des Staatsarchivs habe, muß ich doch darauf hinweisen, daß der zitierte Senatsbeschluß und der Beschluß der Staatsräte nur noch für eine begrenzte Übergangszeit eine tragfähige Grundlage für die Weitergabe personenbezogenen Archivgutes abgeben können. Senat und Bürgerschaft sind aufgefordert, hier tätig zu werden und eine landesgesetzliche Regelung vorzulegen, die den datenschutzrechtlichen Anforderungen genügt und den von den Archiven wahrzunehmenden Aufgaben Rechnung trägt. In diesem Zusammenhang verweise ich auf den von den Datenschutzbeauftragten von Bund und Ländern vorgelegten Musterentwruf für ein bundeseinheitliches Gesetz über die Sicherung und Nutzung von Archivgut (vgl. auch meinen 2. TB, 3.2.1.2, S. 42).

5.5 Bauwesen

5.5.1 Hamburgische Bauordnung (HBauO)

Die Hamburgische Bauordnung ist am 1. Juli 1986 verkündet worden. Das Gesetz, das am 1. Januar 1987 in Kraft tritt, ist überwiegend auf der Grundlage der von der Ministerkonferenz der Arbeitsgemeinschaft der für das Bau-, Wohnungs- und Siedlungswesen zuständigen Minister und Senatoren der Länder (ARGEBAU) verabschiedeten Musterbauordnung erstellt worden. Inwiefern ein Gesetz zur Regelung des Bauordnungsrechts datenschutzrechtliche Belange der am Bauordnungsverfahren Beteiligten berührt, ist für die mit dem Gesetzentwurf befaßten Stellen offenbar nicht auf Anhieb erkennbar gewesen. Jedenfalls ist in dem Entwurf keine Regelung über die Erhebung und Verarbeitung der in einem Bauordnungsverfahren anfallenden personenbezogenen Daten enthalten, und ich konnte die datenschutzrechtlich gebotenen Anforderungen an das neue Gesetz erst so spät in die Diskussion einbringen, daß diese erst in die Ausschußberatungen eingeflossen sind. In Anbetracht der praktischen und zeitlichen Zwänge im Gesetzgebungsverfahren ist der Spielraum für Veränderungen am Gesetzentwurf in diesem Stadium naturgemäß nur noch begrenzt. Meine Vorstellung, die im Bauordnungsverfahren datenschutzrechtlich bedeutsamen Sachverhalte direkt im Gesetz zu regeln, konnte ich daher auch nicht durchsetzen. Ich habe aber erreicht, daß in das Gesetz — in § 81 Abs. 2 als Nr. 4 — eine Regelung aufgenommen wurde, durch die der Senat ermächtigt wird, zum bauaufsichtlichen Verfahren durch Rechtsverordnung auch Vorschriften zu erlassen über „das Erheben und Verarbeiten personenbezogener Daten zum Zweck der Erfüllung der bauaufsichtlichen Aufgaben nach § 58, insbesondere die Übermittlung im Rahmen der notwendigen Beteiligung anderer öffentlicher Stellen, sowie die Übermittlung an sonstige Stellen, soweit diese der Daten zur Erfüllung der ihnen obliegenden öffentlichen Aufgaben bedürfen. Dabei sind Art, Umfang und Empfänger der zu übermittelnden Daten sowie die Zwecke der Verwendung und die Dauer der Speicherung zu bestimmen".

Ich gehe davon aus, daß der Senat aufgrund dieser Ermächtigung umgehend eine Rechtsverordnung zu § 81 Abs. 2 Nr. 4 HBauO erläßt, die folgendem Rechnung trägt:

(1) Im Baugenehmigungsverfahren hat der Bauherr detaillierte Angaben zu machen, die Einblick in seine Lebensverhältnisse und in seine wirtschaftlichen Verhältnisse gestatten. Der Bürger, der bauen will, ist zur Abgabe von Anträgen, Anzeigen, Mitteilungen usw. verpflichtet, um die erforderlichen Baugenehmigungen zu erhalten. Im Gesetz sind die anzugebenden Daten nicht im einzelnen aufgezählt; lediglich die Schriftform für die Anträge ist im Gesetz festgelegt (§ 59). In der Rechtsverordnung muß daher geregelt werden, welche Daten die Beteiligten angeben müssen,

um eine Sachentscheidung der Bauaufsichtsbehörde über die Baugenehmigung herbeizuführen. Falls die Bauaufsichtsbehörde die Benutzung amtlicher Vordrucke für die Anträge usw. zwingend vorschreiben will, müßte eine entsprechende Klausel in die Rechtsverordnung aufgenommen werden.

(2) Der Bauherr überläßt seine Daten der Bauaufsichtsbehörde als der für die Entscheidung über seinen Bauantrag zuständigen Stelle. Im Rahmen der Prüfung der Bauvorlagen muß die Baubehörde in aller Regel aber weitere öffentliche Stellen beteiligen, weil die Erteilung einer Baugenehmigung von der Zustimmung einer anderen Behörde abhängig sein kann oder weil das Vorhaben der Genehmigung oder Erlaubnis einer anderen Behörde bedarf. Die Übermittlung von Daten des Bauherrn an andere am Baugenehmigungsverfahren beteiligte öffentliche Stellen kann also zum Zwecke der Erteilung der Baugenehmigung erforderlich sein. Aus dem Gesetz kann der Bürger jedoch nicht erkennen, ob und an welche Stellen seine Daten weitergegeben werden, in welchem Umfang das geschieht und zu welchem Zweck. Daher ist, um das Baugenehmigungsverfahren für den Bürger durchschaubar zu machen, in der Rechtsverordnung die Übermittlung von Daten aus dem Bauantragsverfahren an andere öffentliche Stellen zu regeln.

(3) Nicht nur zum Zweck der Erteilung einer Baugenehmigung, mithin zu dem vom Antragsteller angestrebten Ziel, für das er seine Daten preisgibt, sondern auch zu anderen Zwecken kann es zur Übermittlung von Daten aus dem Bauantragsverfahren kommen, und zwar sowohl an öffentliche als auch an nichtöffentliche Stellen. So besteht z.B. die Übung, zur Planung von Versorgungsleitungen den HWW, HGW und HEW Ablichtungen der Baugenehmigungsbescheide zu übermitteln. Dies geschieht sicher auch im Interesse des Bauherrn, der sein Bauvorhaben an diese öffentlichen Versorgungsleitungen anschließen möchte. Da aus dem Gesetz aber weder die Tatsache der Übermittlungen an sich noch die Übermittlungsempfänger, der Umfang der übermittelten Daten, der Verwendungszweck und die Dauer der Aufbewahrung beim Empfänger ersichtlich sind, muß in der Rechtsverordnung geregelt werden, welche Übermittlungen zu anderen Zwecken unter welchen Bedingungen zulässig sein sollen. Bisher ist mir noch kein Entwurf der zu erlassenden Rechtsverordnung, die den Titel „Bauvorlagenverordnung" erhalten wird, zugegangen. Nach Aussage der Baubehörde kann mit dem Abstimmungsverfahren erst 1987 begonnen werden.

5.5.2 Baugesetzbuch

Das Baugesetzbuch ist am 23. Oktober 1986 vom Bundestag verabschiedet worden. Am 28. November 1986 hat es die Zustimmung des Bundesrates erhalten, und mit der Verkündung ist im Dezember zu rechnen. Das Gesetz soll am 1. Juli 1987 in Kraft treten. Da es sich bei dem Baugesetzbuch um ein Bundesgesetz handelt, sind meine Möglichkeiten der Einflußnahme sehr beschränkt. Allenfalls durch Anregungen gegenüber der Baubehörde als der fachlich zuständigen Behörde konnte ich versuchen Einfluß zu nehmen. Das habe ich — allerdings ohne Erfolg — getan. Leider sind auch die vom Bundesbeauftragten für den Datenschutz gegebenen Anregungen zu den als datenschutzrechtlich relevant erkannten Bestimmungen bzw. zu fehlenden, aus datenschutzrechtlicher Sicht aber notwendigen Regelungen nur teilweise berücksichtigt worden.

Mit dem Baugesetzbuch wird ein ganzes Bündel von Zielen — außerhalb des Datenschutzes — verfolgt: Das Bundesbaugesetz und das Städtebauförderungsgesetz werden zusammengefaßt, der Abbau der Mischfinanzierung im Bereich der Städtebauförderung wird geregelt, die Länder werden zu abweichenden landesgesetzlichen Regelungen in bestimmten Rechtsbereichen ermächtigt. Dabei werden Vorschriften umgestellt und teilweise geändert. Es ist auch versucht worden, die im Gesetz enthaltenen datenschutzrechtlich relevanten Vorschriften den inzwischen geltenden Anforderungen an Normenklarheit und Verhältnismäßigkeit anzupassen. Das Baugesetzbuch wäre auch der geeignete Ort für eine Grundsatznorm über das Liegenschaftskataster gewesen. Diese Grundsatznorm fehlt noch immer.

Datenschutzrechtlich relevant sind § 138 BauGB (Auskunftspflicht der Eigentümer, Mieter usw. im Rahmen von Sanierungsmaßnahmen) sowie § 195 BauGB (Kaufpreissammlung). § 138 Abs. 1 BauGB entspricht § 3 Abs. 4 Städtebauförderungsgesetz, der die Auskunftspflicht der Eigentümer, Mieter, Pächer, u.a. im Rahmen von Sanierungsvorhaben regelt. Mit Abs. 2 und 3 soll der Rechtsprechung des Bundesverfassungsgerichts zum Volkszählungsgesetz Rechnung getragen werden, d.h., die Verwendung der zu Sanierungszwecken erhobenen personenbezogenen Daten soll auf gesetzlich bestimmte Zwecke begrenzt bleiben und es soll ein ausreichender Schutz gegen Zweckentfremdung geschaffen werden. Einzige Ausnahme: wie bisher schon dürfen auch in Zukunft Daten für Zwecke der Besteuerung an die Finanzbehörden weitergegeben werden. § 138 Abs. 4 BauGB entspricht § 87 des Städtebauförderungsgesetzes, der die Verletzung der Auskunftspflicht nach § 3 Abs. 4 des Städtebauförderungsgesetzes zum Gegenstand hat.

Mit dem Problem der Auskunftspflicht im Rahmen von Sanierungsvorhaben habe ich mich bereits früher auseinandergesetzt (3. TB 3.4.1). Ich hatte seinerzeit festgestellt, daß die Vorschrift nicht mit hinreichender Klarheit regelt, welche Daten die Betroffenen anzugeben haben. § 138 BauGB in der vorliegenden Fassung ist nicht geeignet, diesen Mangel zu beheben. Auch die neue Fassung nennt in einer Aufzählung nur beispielhaft die zu erhebenden Daten und läßt die Erhebung weiterer, nicht näher bezeichneter Daten zu. Damit läßt auch die neue Fassung noch breiten Raum für Auseinandersetzungen, so z.B. über die seinerzeit bei der Befragung im Karolinenviertel strittige Frage nach dem Haushaltseinkommen.

Mit dem Grundsatz der Verhältnismäßigkeit läßt sich nach meiner Auffassung nicht vereinbaren, daß Fragen zur Vorbereitung und Durchführung der Sanierung auch nach der neuen Vorschrift bereits gestellt werden können, wenn noch nicht einmal über die Sanierungsbedürftigkeit eines Gebietes entschieden ist. Das bedeutet, daß die Datenspeicherung zumindest dann unzulässig ist, wenn die Sanierungsbedürftigkeit letztlich nicht festgestellt wird.

§ 195 Abs. 1 und 2 BauGB entsprechen § 143a Abs. 1 und 4 des geltenden Bundesbaugesetzes (BBauG), Absatz 3 ist neu hinzugefügt und soll es ermöglichen, Auskünfte aus der Kaufpreissammlung zu geben. Die Regelung der Einzelheiten bei der Erteilung von Auskünften ist den Ländern überlassen. Es bleibt abzuwarten, ob die landesrechtlichen Vorschriften den Kreis der Auskunftsberechtigten und die Voraussetzungen für die Auskunftserteilung sowie den Umfang der in der Auskunft enthaltenen Daten — entsprechend der in der Begründung vom Gesetzgeber ausgesprochenen Erwartung — unter Wahrung der datenschutzrechtlichen Belange der Betroffenen festlegen werden. Ein Problem könnte sich daraus ergeben, daß die Anonymisierung von Grundstücksdaten aus tatsächlichen Gründen kaum möglich ist, selbst wenn man jeden Hinweis auf die Person des Eigentümers unterläßt. Die Beschreibung des Grundstücks wird in den meisten Fällen zu seiner Identifizierbarkeit führen.

Die Baubehörde hat sich meinen Bedenken nicht anschließen mögen und mir mitgeteilt, sie beabsichtige keine weiteren Aktivitäten zur Veränderung des § 138 BauGB.

5.5.3 Wohnraumdatei

In meinem 3. TB (3.4.2) und meinem 4. TB (4.5.2) habe ich ausführlich über meine Bedenken gegen den Umfang der Datenverarbeitung im Rahmen der automatisierten Wohnraumdatei berichtet. Das Ergebnis meiner Umfrage unter den Datenschutzbeauftragten des Bundes und der Länder war eine Bestätigung meiner Auffassung. Schließlich hat mit Schreiben vom 29. Oktober 1986 auch die Baubehörde eingeräumt, daß sie ihren Standpunkt im Hinblick auf das Ergebnis ihrer eigenen Anfrage an die Mitglieder der Fachkommission Wohnungsbindungs- und Berechnungsrecht und an den Bundesminister für Raumordnung, Bauwesen und Städtebau nicht länger aufrechterhalten kann. Nach allem kann ich berichten, daß in Zukunft die umstrittenen Daten Geschlecht, Nationalität, Zahl der Familienangehörigen, Geburtstag und -monat des Woh-

nungsinhabers nicht mehr gespeichert werden sollen. Diese Daten sollen in Zukunft auch nicht mehr aus dem Veränderungsdienst im Einwohnermeldeverfahren an die für die Führung der Wohnraumdatei zuständigen Stellen übermittelt werden. Die betreffende Vorschrift in der Hamburgischen Meldedatenübermittlungsverordnung ist (im Entwurf) bereits entsprechend geändert. Meine Umfrage unter den Datenschutzbeauftragten hat im übrigen zu einem Schreiben des Bundesbeauftragten für den Datenschutz an den Bundesminister für Raumordnung, Bauwesen und Städtebau geführt, in dem auf die fehlende Normenklarheit der für die Wohraumdateien (Wohnraumkarteien) maßgeblichen Vorschrift des § 2 Abs. 1 WoBindG hingewiesen wird. Eine Antwort auf dieses Schreiben steht noch aus.

Ich habe die Baubehörde gebeten, in angemessener Zeit die Bereinigung des Verfahrens zur Führung der Wohnraumdatei sowie die Löschung der für die rechtmäßige Aufgabenerfüllung nicht erforderlichen Daten im automatisiert geführten Datenbestand durchzuführen.

5.5.4 Die Baubehörde, die Mieter und der Datenschutz

Die Baubehörde hat auch im abgelaufenen Berichtsjahr — wie in den Vorjahren — Befragungen bei Bürgern, meistens Mietern von öffentlich geförderten Wohnungen, durchgeführt. In fast allen Fällen konnte sie sich dabei nicht auf spezielle Rechtsvorschriften stützen, die die betreffenden Erhebungen vorschreiben oder auch nur erlauben. Einzige Ausnahme: Erhebungen im Rahmen der Prüfung von Sanierungsbedürftigkeit und Sanierbarkeit von Altbaugebieten, für die die Datenerhebung in § 3 Abs. 4 Städtebauförderungsgesetz geregelt ist. (Die Problematik dieser Vorschrift habe ich oben unter 5.5.2 und in meinem 3. Tätigkeitsbericht unter 3.4.1 dargestellt.) Da die Baubehörde bei den meisten Befragungen ohne bereichsspezifische Rechtsgrundlage die Daten nicht anonym, sondern personenbezogen erheben wollte, mußte das HmbDSG beachtet werden. Und damit tat sich die Baubehörde nun allerdings sehr schwer.

Zwei Problembereiche haben immer wieder zu zähen Verhandlungen geführt, wobei es auch zu ärgerlichen Mißverständnissen gekommen ist. Die beiden Problembereiche betrafen zum einen

— die Frage, welche Daten, die die Baubehörde zu erheben wünschte, noch als erforderlich zur rechtmäßigen Aufgabenerfüllung der speichernden Stelle angesehen werden konnten (§ 9 Abs. 1 HmbDSG),

und zum anderen

— die Form der Aufklärung der Betroffenen über Gegenstand, Inhalt und Umfang der beabsichtigten Datenverarbeitung sowie die Form der Einwilligungserklärung (§ 5 Abs. 2 HmbDSG).

Das zuerst genannte Problem ist bei freiwilligen Befragungen weniger gravierend als bei Befragungen, bei denen der Bürger zur Auskunftserteilung verpflichtet ist. Ist die Teilnahme an einer Befragung überhaupt freiwillig, kann der Betroffene natürlich trotz grundsätzlich bestehender Bereitschaft zur Mitwirkung die Beantwortung ihm zu weitgehend erscheinender Fragen immer noch ablehnen. Bei Erhebungen, bei denen unter Berufung auf eine Rechtsvorschrift die Beantwortung aller Fragen zur Pflicht erklärt wird, ist das Problem allerdings von Bedeutung, und zwar dann, wenn die herangezogene Rechtsvorschrift den Datenkatalog nicht klar und eindeutig festgelegt (z. B. § 3 Abs. 4 Städtebauförderungsgesetz und § 2 Abs. 1 Wohnungsbindungsgesetz, s. oben 5.5.2 und 5.5.3) oder wenn der gesetzlich vorgegebene Datenkatalog derart extensiv ist, daß der Grundsatz der Verhältnismäßigkeit verletzt sein könnte. Die Baubehörde hatte nach meinen Feststellungen die Neigung, unter Hinweis auf ihr obliegende — nicht näher spezifizierte — Aufgaben der „Planung und Steuerung im Bereich des Wohnungswesens" die vorhandenen speziellen Rechtsvorschriften über Gebühr auszudehnen. Dem habe ich entgegengewirkt.

Das zweite Problem tritt im Zusammenhang mit Befragungen auf freiwilliger Basis auf. Hierfür hat der Gesetzgeber verlangt, daß die Betroffenen vorher in die Datenverarbei-

tung einwilligen. An die Form der Einwilligung hat er aus guten Gründen bestimmte Anforderungen gestellt: Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Gegenstand, Inhalt und Umfang der erlaubten Verarbeitung, insbesondere die Art der Daten, die Adressaten der Übermittlung, der Verwendungszweck und die Dauer der Aufbewahrung sind in der Einwilligungserklärung klar und verständlich zu bezeichnen. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen.

Die Baubehörde hat durchweg versucht, bei diesen strengen Anforderungen Abstriche zu machen. Sie hat stets eingewandt, ohne die gewünschten Daten könne sie wichtige Aufgaben nicht erfüllen und sie müsse befürchten, die Beteiligung an der Befragung verringere sich um so mehr, je genauer die zu Befragenden über den Auftraggeber, den Grund der Befragung und die möglicherweise daraus folgenden Konsequenzen informiert würden. Ich habe demgegenüber betont, die klare gesetzliche Regelung lasse Einschränkungen aus Opportunitätserwägungen nicht zu. Die verantwortliche Stelle sei vielmehr herausgefordert, durch eine entsprechende Überzeugungsarbeit die Mitwirkungsbereitschaft der Betroffenen zu gewinnen.

Geradezu abschreckend auf die Bereitschaft zur Mitwirkung wirkt nach Meinung der Baubehörde die Forderung nach einer Unterschrift der Betroffenen unter die Einwilligungserklärung. Ich verkenne nicht, daß manche Bürger eine Abneigung dagegen haben könnten, bei freiwilliger Beteiligung an einer Befragung eine Unterschrift zu leisten. Diese Abneigung könnte aus der Befürchtung erwachsen, die Unterschrift diene dazu, quasi die Wahrheit und Richtigkeit der gemachten Angaben zu beurkunden. Diese Bedeutung hat die gem. § 5 Abs. 2 HmbDSG geleistete Unterschrift jedoch nicht, sondern sie dient ausschließlich der Qualifizierung und dem Nachweis der vom Gesetz zum Schutz der Bürger verlangten Einwilligungserklärung. Ich meine, es ist eine durchaus lösbare Aufgabe der verantwortlichen Stelle, die Betroffenen über diese Bedeutung der Unterschrift aufzuklären.

Während das Gesetz hinsichtlich der Schriftform der Einwilligungserklärung — wenn auch unter ganz engen Voraussetzungen — Ausnahmen zuläßt („. . ., soweit nicht wegen besonderer Umstände eine andere Form angemessen ist"), muß jeder Versuch, die Betroffenen durch fehlende, ausweichende oder gar irreführende Aufklärung über Zweck und Inhalt einer Befragung im unklaren zu lassen oder sie gar bewußt zu täuschen, als Verstoß gegen § 5 Abs. 2 HmbDSG beurteilt werden.

Dazu ein Beispiel:

Für die von der Baubehörde geplante „Mobilitäts- und Wohnwünscheuntersuchung", bei der Mieter von großen, unterbelegten Sozialwohnungen über ihre Wohnsituation, Wohnwünsche und Mobilitätsbereitschaft befragt werden sollten, um Erkenntnisse über mögliche wohnungspolitische Maßnahmen mit dem Ziel einer im Sinne der Aufgaben des sozialen Wohnungsbaus besseren Belegung zu gewinnen, war mit mir ein Hinweistext für die Betroffenen abgesprochen. Diesem Text hatte ich gerade noch zustimmen können, weil der Informationsgehalt bloß den Mindestanforderungen entsprach. Bei der Durchführung der Befragung benutzte die Baubehörde dann jedoch einen mit mir nicht abgesprochenen „überarbeiteten" Text, in dem der Hinweis auf die Baubehörde als Auftraggeber ersetzt war durch die Angabe, „die GFM/Gesellschaft für Marktforschung mbH führt . . . eine aktuelle Bestandsaufnahme . . durch". Während in der Fassung, der ich zugestimmt hatte, noch ausgesagt wurde, daß Mieter von Sozialwohnungen befragt werden sollten und daß es um die Diskrepanz zwischen Wohnungsleerständen einerseits und der unbefriedigten Nachfrage nach preiswertem Wohnraum („begehrt aber knapp") andererseits ginge, heißt es in dem „überarbeiteten Text": „Die GFM/Gesellschaft für Marktforschung mbH führt deshalb eine aktuelle Bestandsaufnahme der Wohnsituation, der Wohnwünsche und Wohnbedürfnisse von Hamburger Haushalten durch. Ihr Haushalt ist durch eine Zufallsauswahl ermittelt worden." Der Text, mit dem die Interviewer die Befragung beginnen sollten und der auf dem Fragebogen vor dem Fragenteil abgedruckt ist, lautet sogar: „. . . Ich komme von

der GFM/. . .. Ihr Haushalt ist zufällig ausgewählt worden, um einen repräsentativen Querschnitt aller Hamburger Bürger zu aktuellen Themen zu befragen." Ich brauche wohl nicht zu betonen, daß ich einem solchen — wie ich meine — irreführenden Hinweis nicht zugestimmt habe und dies auch nicht getan hätte, wenn mir der Text vorgelegt worden wäre.

Ich habe die Baubehörde mit Entschiedenheit darauf hingewiesen, daß ich ihr Vorgehen in dieser Angelegenheit mißbillige. Sie hat zwar eingewandt, sie sei sich bei der Überarbeitung der Texte nicht bewußt gewesen, daß die Veränderungen datenschutzrechtliche Auswirkungen haben könnten. Dieser Einwand zeigt, wie immer man ihn werten mag, zumindest eine nicht zu tolerierende Unkenntnis über Aufgaben und Ziele des Datenschutzes im allgemeinen sowie Sinn und Zweck des § 5 Abs. 2 HmbDSG im besonderen.

Ich habe inzwischen mit der Baubehörde Einvernehmen in der Beurteilung dieser Angelegenheit erzielt und die Zusicherung erhalten, daß die datenschutzrechtlichen Anforderungen in Zukunft eingehalten werden.

Ein dritter Problemkomplex im Zusammenhang mit den Datenerhebungen der Baubehörde betrifft die Durchführung der Befragungen, die in aller Regel im Wege der Auftragsdatenverarbeitung erfolgt. Im Rahmen meiner Berichterstattung über die Befragung im Karolinenviertel (3. TB 3.4.1, S. 34 und 4. TB 4.5.1, S. 48) hatte ich auf die Bedeutung der sorgfältigen Auswahl des Auftragnehmers und die Notwendigkeit exakter, schriftlicher Auftragserteilung sowie der Kontrolle der auftragsgetreuen Durchführung hingewiesen. Zu der im Berichtszeitraum durchgeführen Datenerhebung zum Mietenspiegel liegt mir inzwischen die Eingabe eines Betroffenen vor, der sich darüber beschwert, daß ein junger Mann, der sich nicht als Interviewer auswies, bei ihm erschien und ein wenige Tage vorher von einem anderen Interviewer begonnenes Interview doch noch zu Ende bringen wollte. Das Interview war beim ersten Treffen vom Betroffenen abgebrochen worden, weil er keine Angaben zur Höhe der Miete machen wollte. Der junge Mann war nicht nur im Besitz des Fragebogens mit den Angaben zu den bereits beantworteten Fragen, sondern in dem Fragebogen war nun auch bereits die Höhe der Miete (fast auf die Mark genau zutreffend) eingetragen.

Ich habe versucht aufzuklären, ob der junge Mann als Interviewer eingesetzt war oder ob der erfolglose erste Interviewer Daten des Betroffenen unbefugt an einen Außenstehenden weitergegeben hatte. Weiter habe ich versucht, die Herkunft der Mietangabe zu ermitteln.

Die Baubehörde hat dazu folgende Erklärung abgegeben: Der eingesetzte (erste) Interviewer habe zu einer achtköpfigen Gruppe von Interviewern gehört, die zur Verstärkung der in Hamburg rekrutierten Kräfte aus dem Bereich Köln-Bonn angereist sei. Der Interviewer habe den teilweise ausgefüllten Fragebogen bei seinem Auftraggeber (dem Markt- und Meinungsforschungsinstitut, das von der Baubehörde mit der Durchführung der Datenerhebung beauftragt war) vorgelegt und erklärt, er habe die Miete und die Mietnebenkosten in diesem Fall geschätzt. Der Interviewer sei darauf hingewiesen worden, daß das Interview so nicht verwendbar sei. Der Koordinator der zugereisten Gruppe habe daraufhin eine weitere Kraft, den jungen Mann, beauftragt, einen zweiten Versuch zu unternehmen, um doch noch die notwendigen Angaben von dem Betroffenen zu erhalten und sich belegen zu lassen.

Alle acht Mitglieder der Interviewer-Gruppe hätten sich auf Verlangen mit ihrem Interviewerausweis und dem dazugehörigen Personalausweis legitimieren können, und sie seien alle auf das Datenschutzgesetz verpflichtet gewesen. Die Daten des Betroffenen seien wegen der geschilderten Umstände nicht in die Mietenspiegeluntersuchung 1986 eingeflossen.

Abgesehen einmal von der Frage, ob diese Darstellung in allen Punkten zutreffend ist — es ist immerhin verblüffend, daß ein aus Köln-Bonn angereister Interviewer die Miete einer in Hamburg gelegenen nicht preisgebundenen Wohnung, die einem privaten Eigentümer gehört, fast exakt schätzt —, ist zu dem Vorgang aus meiner Sicht folgendes anzumerken:

Bei Auftragsdatenverarbeitung ist der Auftraggeber bei der Auswahl des Auftragnehmers und bei der Formulierung des Auftrages zu besonderer Sorgfalt verpflichtet. Handelt es sich bei dem hier beschriebenen Fall der Eintragung nicht erhobener und nachgewiesener, sondern unzulässigerweise geschätzter Daten um eine Ausnahme, um einen Einzelfall, so sind Zweifel an der nötigen Sorgfalt der Beteiligten dadurch allein sicher noch nicht angezeigt. Dies könnte sich aber ändern, wenn mir weitere ähnliche Fälle zur Kenntnis gelangen sollten.

Zweck der Mietenspiegelerhebung ist im übrigen die Aufstellung eines „Hamburger Mietenspiegels", der bei Mietstreitigkeiten vor Gericht Bestand hat. Die Gerichte erkennen den Mietenspiegel aber nur dann an, wenn er auf geprüften Daten beruht. Wenn sich erweisen sollte, daß entgegen der schriftlichen Anweisung der Baubehörde, nur nachgewiesene Daten bei der Aufstellung des Mietenspiegels zu berücksichtigen, in Wahrheit auch nicht belegte oder gar nur geschätzte Daten oder veränderte Daten verarbeitet worden sind, so müßte der Mietenspeigel insgesamt in Frage gestellt werden, und zwar weniger von mir und aus Datenschutzgründen (der Mietenspiegel enthält nur anonymisierte, aggregierte Daten), sondern vielmehr von den Gerichten, weil diese seine Tauglichkeit als Beweismittel anzweifeln müßten. Alle Beteiligten wären daher gut beraten, wenn sie die Vorgaben für die Erstellung des Mietenspiegels akribisch beachteten.

5.6 Steuerwesen

5.6.1 Steuerbereinigungsgesetz 1986

Die in früheren Tätigkeitsberichten (2. TB 3.4.1, S. 51, 3. TB 3.3.1, S. 30) bereits mehrfach angekündigten datenschutzrechtlich bedeutsamen Änderungen der Abgabenordnung (AO) wurden im Rahmen des Steuerbereinigungsgesetzes 1986 vom 19. Dezember 1985 (BGBl. I S. 2436) eingeführt. Die Änderungen berücksichtigen lange erhobene Forderungen der Datenschutzbeauftragten und tragen zur Verbesserung der Position des Bürgers bei.

In § 30 AO wurde eine Regelung aufgenommen, nach der schon der unbefugte Abruf von dem Steuergeheimnis unterliegenden Daten, die in einer automatisierten Datei gespeichert sind, als Verstoß gegen das Steuergeheimnis zu beurteilen ist, ohne daß es daneben auf eine unbefugte Offenbarung oder Verwendung der abgerufenenen Daten ankommt. Der automatisierte Abruf von dem Steuergeheimnis unterliegenden Daten aus einer Datei ist nur zulässig, soweit er der Durchführung eines Verfahrens im Sinne von § 30 Abs. 2 Nr. 1 Buchstabe a und b oder der zulässigen Weitergabe von Daten dient. Zur Wahrung des Steuergeheimnisses kann der Bundesminister der Finanzen durch Rechtsverordnung mit Zustimmung des Bundesrates bestimmen, welche technischen und organisatorischen Maßnahmen gegen den unbefugten Abruf von Daten zu treffen sind, vgl. 5.6.2.

Mit § 93a AO wurde die lange geforderte gesetzliche Grundlage für Kontrollmitteilungen geschaffen. Nach der nun geltenden Regelung (der Regelungsgehalt der Vorschrift ist den Einflüssen diverser Interessengruppen ausgesetzt gewesen) sind Kontrollmitteilungen zulässig, wenn sie aufgrund einer allgemeinen, durch Rechtsverordnung näher bestimmten Mitteilungspflicht erfolgen. In § 93a werden die Tatbestände genannt, für die in der Rechtsverordnung allgemeine Mitteilungspflichten angeordnet werden können. Weiter werden die Daten festgelegt, die den Finanzbehörden von den mitteilungspflichtigen Stellen aus Anlaß einer Kontrollmitteilung übermittelt werden dürfen. In § 93a wird auch vorgegeben, daß in der zu erlassenden Rechtsverordnung die Verpflichtung zur Unterrichtung der Betroffenen über jede abgesandte Kontrollmitteilung zu regeln ist. Schließlich wird zugelassen, daß insbesondere in Fällen von geringer steuerlicher Bedeutung auf eine Mitteilung an die Finanzbehörden verzichtet werden kann. Ebenso wie die Mitteilungen selbst im einzelnen in der Rechtsverordnung festzulegen sind, sind auch die Fälle, in denen ausnahmsweise von einer Mitteilung abgesehen werden soll, in der Rechtsverordnung zu bezeichnen, vgl. 5.6.3.

§ 309 Abs. 2 AO ist durch folgenden Satz ergänzt worden: „Die an den Drittschuldner zuzustellende Pfändungsverfügung soll den beizutreibenden Geldbetrag nur in einer Summe, ohne Angabe der Steuerarten und der Zeiträume, für die er geschuldet wird, bezeichnen." Diese Ergänzung trägt den berechtigten Beschwerden Betroffener Rechnung, die sich dagegen wandten, daß die Finanzämter in den Drittschuldnern zuzustellenden Pfändungs- und Überweisungsbeschlüssen den Schuldgrund angeben und die Steuerschulden des Vollstreckungsschuldners im einzelnen aufzählen. Die Datenschutzbeauftragten haben sich mit ihrer Auffassung durchgesetzt, daß die bisherige Verfahrensweise den Bürger unverhältnismäßig belastet, weil der Eingriff zur Erreichung des vom Gesetzgeber angestrebten Zwecks (Bekanntgabe der Pfändungsverfügung an den Drittschuldner) nicht erforderlich ist. Die jetzt vorgesehene Form, die allerdings erst am 1. Januar 1987 in Kraft tritt, ist zur Erreichung des Zwecks ebenso geeignet und belastet den Betroffenen weniger.

5.6.2 Verordnung zu § 30 Abs. 6 Satz 2 AO (Steuerdaten-Abruf-Verordnung)

Der Bundesminister der Finanzen hat inzwischen den Entwurf einer Verordnung über den Abruf von Steuerdaten im automatisierten Verfahren beim Bundesamt für Finanzen, bei Landesfinanz- und Gemeindebehörden (Steuerdaten-Abruf-Verordnung — StDAV) vorgelegt. Die Datenschutzbeauftragten untersuchen z. Z., ob noch Regelungslücken bestehen und redaktionelle Verbesserungen möglich sind.

Nach § 1 Abs. 1 ist die StDAV auf Daten anzuwenden, die dem Steuergeheimnis unterliegen. Der Schutz der Verordnung erfaßt daher nicht nur — wie nach den Datenschutzgesetzen — personenbezogene Daten im Sinne von Daten natürlicher Personen, sondern auch die Daten juristischer Personen. Nicht erfaßt werden Daten, die nicht dem Steuergeheimnis unterliegen, wie z. B. Daten der Personalverwaltung der Finanzämter. Weitere Voraussetzung für die Anwendbarkeit der StDAV ist, daß die dem Steuergeheimnis unterliegenden Daten von einer Finanzbehörde in einem Verfahren nach der AO oder in einem Verfahren der Gemeinden zur Erhebung von Realsteuern oder von einer Stelle im Auftrag der genannten Behörden in einem automatisierten Verfahren gespeichert werden.

Nach § 2 StDAV unterliegt bereits die Einrichtung eines Datenabrufverfahrens engen Voraussetzungen, die schlagwortartig wie folgt umrissen werden können:

1. Die Daten müssen zur Durchführung bestimmter Verfahren geeignet und erforderlich sein.
2. Es müssen Zugriffsberechtigte und deren Berechtigungen festgelegt werden.
3. Zugriffsberechtigungen sind an die jeweilige Aufgabe des Berechtigten gebunden.
4. Die Einrichtung eines Abrufsverfahrens bedarf der Einwilligung der obersten Finanzbehörde oder des Leiters der Gemeindeverwaltung.

Nach § 3 StDAV sind für den Betrieb von Datenabrufverfahren technische und organisatorische Maßnahmen gegen unbefugten Datenabruf zu treffen. Unbefugt sind Zugriffe durch nicht zugriffsberechtigte Personen und Zugriffe in Überschreitung einer eingeräumten Zugriffsberechtigung. § 3 StDAV nennt konkrete Maßnahmen zur Verhinderung bzw. Aufdeckung unbefugter Zugriffe. Darüber hinaus wird die klare Festlegung von Zweck und Bedingungen des Abrufverfahrens sowie eine für sachverständige Dritte verständliche Dokumentation des Verfahrens vorgeschrieben.

In Hamburg ist mit dem neuen Datenerfassungs-, Auskunfts- und Entwicklungssystem der Steuerverwaltung ein Verfahren eingeführt worden bzw. noch in der Einführungsphase, das an den Anforderungen der Steuerdaten-Abruf-Verordnung zu messen sein wird, vgl. 5.6.4.

5.6.3 Verordnung zu § 93a AO (Kontrollmitteilungsverordnung)

An einem Entwurf für eine Verordnung zu § 93a AO wird im Bundesfinanzministerium gearbeitet. Eine noch nicht mit Bundes- und Landesressorts abgestimmte Fassung, die von einer Unterkommission der Finanzbehörden des Bundes und der Länder erarbeitet wurde, wirft vor allem die Frage auf, ob die Verordnung auch auf Sozialdaten an-

wendbar sein wird. Davon ausgehend, daß § 93a AO in § 71 Abs. 1 Nr. 3 SGB X nicht genannt ist, ist zu prüfen, ob § 93a AO eine Verordnungsermächtigung zur (teilweisen) Konkretisierung der in § 93 Abs. ; AO enthaltenen Vorschrift über die Heranziehung Dritter zur Auskunft darstellt. § 71 Abs. 1 Nr. 3 SGB X erlaubt die Offenbarung von Sozialdaten, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflichten zur Sicherung des Steueraufkommens nach den §§ 93, 97, 105, 111 Abs. 1 und 5 und § 116 der AO, soweit diese Vorschriften unmittelbar anwendbar sind. § 71 Abs. 1 Nr. 3 SGB X enthält keinen Verweis auf § 93a AO, so daß ich eine Offenbarung personenbezogener Daten durch einen Sozialleistungsträger aufgrund einer Rechtsverordnung zu § 93a AO schon nach dem Wortlaut des § 71 Abs. 1 Nr. 3 SGB X für ausgeschlossen halte.

Auch im Wege der Gesetzesauslegung kommt man zu keinem anderen Ergebnis. § 93a AO stellt meines Erachtens keine Konkretisierung der Auskunftspflicht „anderer Personen" im Sinne von § 93 AO dar, sondern mit § 93a AO wird ein eigener, anderer Sachverhalt geregelt. Während dem § 93 der Gedanke zugrunde liegt, daß im allgemeinen Festsetzungsverfahren regelmäßig die Betroffenen zur Auskunft herangezogen und erst, wenn dieser Weg im Einzelfall nicht zum Erfolg führt, Dritte befragt werden sollen, regelt § 93a AO ein Mitteilungsverfahren, das unabhängig von fehlender oder vorhandener Mitwirkungsbereitschaft der Betroffenen regelmäßig durchgeführt werden soll, und zwar neben dem allgemeinen Erhebungsverfahren. Das Verfahren nach § 93a AO in Verbindung mit der noch zu erlassenden Verordnung stellt eine neue Qualität des Eingriffs in das informationelle Selbstbestimmungsrecht dar. Eventuellen Bestrebungen, durch Einbeziehung des § 93a AO in die Vorschrift des § 71 Abs. 1 Nr. 3 SGB X das Sozialgeheimnis einzuschränken, kann ich nicht zustimmen.

5.6.4 Neues Datenerfassungs-, Auskunfts- und Entwicklungssystem der Steuerverwaltung

Im Berichtszeitraum wurde im Finanzamt für Steuererhebung ein neues Datenerfassungs-, Auskunfts- und Entwicklungssystem eingeführt. Dieses Verfahren soll anschließend mit den notwendigen Modifikationen sukzessive in allen Finanzämtern eingeführt werden. Das neue System ist Teil des „Integrierten Steuerfestsetzungs- und -erhebungsverfahrens (INFES)". Mit diesem System wird der Automatisierungsgrad in der Steuerverwaltung weiter erhöht.

Die Datenerfassung im Erhebungsbereich — das ist im wesentlichen die Erfassung der Daten über Zahlungseingänge von Papierbelegen (Überweisungsgutschriften) auf automatisierte Datenträger — geschieht nicht mehr über die Schritte OCRA-Beleg-Erstellung und automatisiertes Lesen der OCRA-Belege, sondern durch Eingabe der Daten über Terminals direkt in einen automatisierten Datenbestand, der anschließend zur DVZ übertragen wird. Die Terminals sind an sogenannte „Subsysteme", dezentrale Rechner, die ausschließlich für dieses Verfahren eingesetzt sind, angeschlossen. Die in den Finanzämtern installierten Subsysteme sind ihrerseits mit einem Rechner in der DVZ, dem Host, verbunden. Die Verarbeitung der Daten erfolgt schließlich im INFES-Verfahren auf der Anlage in der DVZ.

Mitarbeiter der Steuerverwaltung mit entsprechender Befugnis haben seit 1982 (damals begann die Ausstattung mit den erforderlichen Sichtgeräten) die Möglichkeit, sich Daten aus den Speicherkonten der Steuerbürger anzeigen und ausdrucken zu lassen. Die jetzt eingeführten Geräte sind sowohl für den Abfrageverkehr als auch für die Datenerfassung ausgelegt. Die Einführung dieses Konzepts der kombinierten Gerätenutzung durch Datenerfassungskräfte und Sachbearbeiter in den Finanzämtern hat die schon vorher aus Gründen des Datenschutzes, insbesondere des Steuergeheimnisses erhobene Forderung nach stärkerer Differenzierung der Zugriffsbefugnisse der Sachbearbeiter noch mehr verstärkt und erweitert: hinzugekommen ist die Forderung nach Differenzierung der Zugriffsberechtigungen entsprechend den Funktionen Datenerfassung und Sachbearbeitung. Schließlich ist die Aufgabe, eine komplexe Regelung der Zugriffsberechtigungen zu erarbeiten und systemtechnisch umzusetzen, dadurch unabweisbar geworden, daß die Subsysteme auch der Anwendungsprogrammierung für die Entwicklung und Pflege von Programmen zur Verfügung gestellt werden sollen.

Die Sachbearbeiter in den Finanzämtern haben bisher Zugriff auf alle Speicherkonten im Zuständigkeitsbereich des Finanzamtes, dem sie angehören. Der einzelne Sachbearbeiter ist jedoch nur für einen Teil dieser Konten zuständig. Im Zuge der Einführung des neuen Systems ist eine Einschränkung der Zugriffsmöglichkeiten vorgesehen dahingehend, daß die Berechtigung jedes Sachbearbeiters auf die Konten der jeweiligen Verwaltungsstelle in seinem Finanzamt beschränkt wird. Eine solche Regelung ist erst möglich geworden durch die Neuordnung der Finanzämter, die weitgehend realisiert ist.

Ich habe im Berichtszeitraum die Regelung der Zugriffsberechtigungen im Finanzamt für Steuererhebung geprüft. Die Prüfung galt der Frage, ob durch die realisierte Regelung der Berechtigungen die Einhaltung der Datensicherheit im Sinne von § 8 HmbDSG nebst Anlage dazu gewährleistet ist. Die Steuerdaten-Abruf-Verordnung (vgl. 5.6.2) konnte noch nicht angewendet und auch noch nicht als Maßstab herangezogen werden, weil noch nicht einmal der Entwurf bekannt war. Das Auskunftssystem und eine Komponente des Erfassungssystems (Zugriff auf Namenssuchdatei) stellen aber unzweifelhaft ein Verfahren „zum Abruf von Steuerdaten im automatisierten Verfahren" dar, für das die StDAV gelten wird. Es wird daher zu gegebener Zeit zu prüfen sein, ob es den Bestimmungen der StDAV entspricht.

Der Untersuchungsgegenstand umfaßte zwei Aspekte:

(1) Ist das organisatorische Konzept für die Erteilung von Berechtigungen an Personen mit bestimmten Funktionen angemessen?

Angemessen ist das organisatorische Konzept der Berechtigungen dann, wenn der Umfang der individuell zugeschnittenen Berechtigung jeweils nur soweit reicht, wie es zur Aufgabenerfüllung des jeweiligen Mitarbeiters (in seiner Hauptfunktion und in seiner Eigenschaft als Vertreter eines Kollegen) erforderlich ist. Darüber hinaus dürfen keinem Mitarbeiter Berechtigungen eingeräumt werden.

(2) Ist die Umsetzung des organisatorischen Konzepts im System gelungen?

Die Umsetzung ist gelungen, wenn durch das System (Hard- und Software) sowie durch technisch-organisatorische Maßnahmen im Umfeld (z. B. Raumsicherung) erreicht wird, daß

- Befugte das System nur im Rahmen ihrer Befugnis benutzen können,
- kein Unbefugter Zugang zu den Datensichtgeräten und Zugriff auf die gespeicherten Daten erhält,
- nachträglich jederzeit festgestellt werden kann, wer für welche Zeit welche Berechtigungen hatte und
- nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in das Datenverarbeitungssystem eingegeben worden sind (siehe Anlage zu § 8 HmbDSG, dort Nrn. 1—5, 7 und 10).

Nach meinen Erkenntnissen ist das organisatorische Konzept angemessen, soweit es den Produktionsbetrieb nach Beendigung der Einführungsphase betrifft. Das organisatorische Konzept für die Phasen des Testbetriebes und der Einführung im echten Betrieb konnte jedoch noch nicht befriedigen. Während der Test- und Einführungsphase hatten nämlich die ADV-Organisationssachbearbeiter, die die Software für das Verfahren entwickelten, Zugriffsberechtigungen auf den echten Datenbestand. Im Bereich des INFES-Verfahrens ist der Grundsatz der Funktionstrennung ein Eckpfeiler der Organisationskontrolle, und zwar nicht nur wegen der Pflicht zur Wahrung des Steuergeheimnisses, sondern auch aus Gründen des Kassenrechts. Bei Einhaltung der Funktionstrennung dürfen die Software-Entwickler grundsätzlich keine Zugriffsberechtigung auf „echte Daten" haben. Bei auftretenden Störungen und in Fehlerfällen dürfen sie „echte Daten" nur in dem Umfang zur Kenntnis nehmen, wie er zur Behebung der Störung oder Aufklärung des Fehlers erforderlich ist.

Die Finanzbehörde hat beachtliche Gründe dafür vorgetragen, weshalb sie die Tests nicht mit einem Testdatenbestand auf einem Testsystem durchgeführt und den ADV-Organisationssachbearbeitern bis zur Stabilisierung des Verfahrens im „Produktions-

betrieb" so umfassende Befugnisse eingeräumt hat. Ich verkenne nicht, daß unter den mir geschilderten Umständen die Aufrechterhaltung der Funktionstrennung mit erheblichen Schwierigkeiten verbunden, vielleicht sogar bei aller Anstrengung nicht möglich war. Schließlich verlangt auch das Datenschutzgesetz nur im Verhältnis zum Schutzzweck angemessene Maßnahmen. Meine Bedenken wurden dadurch jedoch nicht ausgeräumt:

Bei fast allen größeren Neuentwicklungen der hamburgischen Verwaltung wird Neuland betreten, ob es sich nun um die Automatisierung des Einwohnerwesens oder um die Umstellung auf Dialogerfassung bei der BVSt oder anderen Stellen handelt. Wenn jedesmal mit Hinweis auf die Sachzwänge wesentliche Datenschutz-/Datensicherheitsgrundsätze zur Disposition gestellt werden sollten, so liefe das auf eine zeitweise Außerkraftsetzung der Datenschutzbestimmungen hinaus, die natürlich nicht hingenommen werden kann. Ich meine, es müssen noch größere Anstrengungen unternommen werden, um auch für Ausnahmesituationen datenschutzrechtlich unbedenkliche Lösungen zu finden. Ich habe dazu einige Vorschläge gemacht, von denen ich aufgrund meiner Prüferfahrung weiß, daß sie realisiert werden können.

Abgesehen von dem geschilderten konzeptionellen Risiko habe ich bei der technischen Umsetzung des Konzepts noch diskussionsfähige Aspekte gefunden. So könnte meiner Meinung nach die Sicherheit noch erhöht werden, wenn die Identitätsprüfung eines Benutzers mittels einer Magnetkarte ergänzt würde durch eine Authentizitätsprüfung des Kartenbenutzers mittels Paßwortkontrolle. Ergänzend zu den technischen Maßnahmen sind jedoch organisatorische Maßnahmen getroffen worden, bei deren konsequenter Durchsetzung ich davon ausgehe, daß das System als ganzes den Sicherheitsanforderungen genügt. Die organisatorischen Regelungen betreffen den Umgang mit den Magnetkarten, den Betrieb der Terminals, das Verhalten bei Unterbrechen der Tätigkeit am Terminal, das Verschließen nicht besetzter Räume, die Dienstaufsicht sowie die Konsequenzen bei Verstößen gegen die Regelungen für den Betrieb des Systems.

Das System wird in jeweils angepaßter Form in allen Finanzämtern eingeführt werden. Ich habe darum gebeten, mich über den Fortgang der Umstellungsarbeiten auf dem laufenden zu halten und mich zu beteiligen. Die Finanzbehörde steht meinen Forderungen nicht grundsätzlich ablehnend gegenüber, es bleibt aber abzuwarten, inwieweit in Zukunft das Problem der Zugriffsberechtigungen der ADV-Organisationssachbearbeiter bewältigt wird. Ob die Frage der zusätzlichen Paßwortkontrolle nochmals aufgegriffen wird, hängt nicht zuletzt von dem in der DVZ eingesetzten Betriebssystem und der dort installierten Sicherungssoftware ab. Auch durch das Bekanntwerden von mißbräuchlicher Verwendung der Magnetkarten könnte die Diskussion über die Paßwortkontrolle wieder aufleben.

5.7 Einwohnerwesen

5.7.1 Automation im Meldewesen

Ich habe mich in meinen bisher erschienenen Tätigkeitsberichten (zuletzt 4. TB, 4.8.1, S. 55) ausführlich mit der Automation des Meldewesens in Hamburg auseinandergesetzt. Im Oktober 1986 wurde das Einwohneramt des Bezirksamtes Harburg als erste von insgesamt 28 hamburgischen Einwohnerdienststellen in das automatisierte Verfahren übernommen.

Auch wenn durch die jetzt realisierte Lösung, an der ich von Beginn an beteiligt war, Mängel des bisherigen Verfahrens beseitigt werden, entstehen mit dem Einsatz modernster Datenbanktechnologien mit ihren zunehmenden Integrationsmöglichkeiten auch zusätzliche Gefahren für den Bürger. Waren bei der herkömmlichen Programmierung für die Verknüpfung verschiedener Dateien umfangreiche und zeitaufwendige Programmierarbeiten notwendig, so können bei Einsatz moderner Abfrage-Sprachen („Query-Systeme") im Rahmen von Datenbankverwaltungssystemen in verschiedenen Dateien gespeicherte Merkmale ohne größeren Aufwand zusammengeführt werden. Zwar gibt es bei diesen Verfahren auch sehr wirksame Zugriffssicherungen (vgl. meine

Ausführungen zur On-line-Übermittlung im 4. Tätigkeitsbericht, 3.2, S. 11 ff). Diese Sicherungen können jedoch durch die dazu Autorisierten außer Kraft gesetzt werden. Ohne daß ich den Verantwortlichen entsprechende Absichten unterstellen will, ist doch die Tatsache von Bedeutung, daß eine technische Infrastruktur entsteht, die derartige Mißbräuche ermöglicht.

Ich werde diesen Aspekt bei der anstehenden Entwicklung neuer Verfahren (z.B. bei der Kfz-Zulassungsstelle und bei der Sozialhilfe) besonders kritisch beobachten.

5.7.2 Regelmäßige Datenübermittlungen aus dem Melderegister

Die Novellierung des Hamburgischen Meldegesetzes (HmbMG), die mit der Bekanntgabe der Neufassung vom 6. Mai 1986 abgeschlossen wurde, machte auch eine Überarbeitung der bisherigen Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister erforderlich. Deshalb hat die Behörde für Inneres im August 1986 den Entwurf einer neuen Verordnung zur Festlegung der Einwohnerdatenbestände und über regelmäßige Datenübermittlungen aus dem Melderegister vorgelegt.

Die Automatisierung des Einwohnerwesens eröffnet die Möglichkeit, die Übermittlung von Daten weitestgehend aus dem maschinellen Bestand heraus abzuwickeln. Aufgrund des organisatorischen Konzepts werden die örtlichen Meldebehörden in die Lage versetzt, den größten Teil der regelmäßige Datenübermittlungen, die bisher von der zentralen Meldebehörde vorgenommen wurden, selbst durchzuführen.

Das neue Konzept ermöglicht auch eine geänderte Systematik der Datenübermittlung. Bisher wurden bei ereignisbezogenen Übermittlungen (z. B. Einzug, Auszug, Änderung des Personenstandes oder Tod) alle in der jeweiligen Vorschrift genannten Daten des Einwohners übermittelt. Nunmehr soll eine Differenzierung zwischen dem eigentlichen Übermittlungsanlaß (in der Regel der Einzug eines Einwohners) und der Mitteilung von Veränderungen (Folgemitteilungen) vorgenommen werden. Während beim Einzug die Daten des Einwohners möglichst umfassend zu übermitteln sind, kann sich die Mitteilung von Veränderungen auf das veränderte Datum sowie die für dessen Zuordnung erforderlichen Angaben (Identifizierungsdaten) beschränken. Die Übermittlung der übrigen Daten ist entbehrlich, da sie dem Empfänger bereits bekannt sind.

In der Neufassung des HmbMG sind darüber hinaus Regelungen enthalten, die sich unmittelbar auf diese Verordnung auswirken:

1. § 33 HmbMG enthält nunmehr eine abschließende Regelung über die regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Religionsgesellschaften. § 13 der Verordnung in der bisherigen Fassung wird dadurch gegenstandslos.
2. § 30 Abs. 5 HmbMG schafft — klarstellend — eine ausdrückliche Ermächtigungsgrundlage für die Regelung der Datenübermittlungen zwischen den örtlichen Meldebehörden und der zentralen Meldebehörde. Bisher wurde die Ermächtigung zur Regelung dieser Datenübermittlungen aus § 31 Abs. 5 HmbMG (in der Fassung vom 19. Mai 1982) abgeleitet.
3. Das Gesetz enthält nunmehr in § 2 Abs. 3 eine Ermächtigung zur Festlegung der bei den örtlichen und bei der zentralen Meldebehörde zu führenden Datenbestände. Aufgrund des engen Sachzusammenhangs zwischen den Datenbeständen und der Datenübermittlung soll diese Regelung in die neue VO einbezogen werden.

In meiner Stellungnahme zum VO-Entwurf habe ich zum Ausdruck gebracht, daß damit einer Reihe von Bedenken, die ich in der Vergangenheit an der Praxis der regelmäßigen Datenübermittlungen aus dem Melderegister geäußert habe (2. TB, 3.8.1.1, S. 61), Rechnung getragen wird. Insbesondere wird zukünftig die von mir kritisierte Übersendung von Meldescheinen an die Ausländerbehörde unterbleiben. Allerdings habe ich erneut die vorgesehene Abgleichsregelung zu polizeilichen Zwecken kritisiert. Die erforderliche gesetzliche Grundlage gibt es nicht. Da das HmbMG auch keine Ermächtigung enthält, den Abgleich in einer VO zu regeln, hält der VO-Entwurf insoweit einer verfassungsrechtlichen Prüfung nicht stand.

Aus Gründen der Systematik und des Sachzusammenhangs müßte eine entsprechende Ermächtigungsnorm im übrigen im Rahmen der anstehenden Novellierung des HmbSOG geschaffen werden. Davon unberührt bleiben meine materiell-rechtlichen Bedenken, die ich gegen den Meldedatenabgleich erhoben habe (3. TB, 3.8.5.6, S. 81 und 4. TB, 4.9.3.2.5, S. 72).

Demnach bleibt festzuhalten, daß es derzeit für den Meldedatenabgleich zu polizeilichen Zwecken keine gesetzliche Grundlage gibt und sie durch die VO auch nicht geschaffen werden kann. Deshalb wäre er z.Z. nur dann rechtmäßig, wenn er zur Aufrechterhaltung der Funktionsfähigkeit staatlicher Einrichtungen für eine Übergangszeit auch ohne gesetzliche Ermächtigung hinzunehmen wäre (so auch das Bundesverfassungsgericht in diversen Entscheidungen). Dann müßte er auch unter strenger Anwendung des Verhältnismäßigkeitsgrundsatzes zu den unerläßlichen Eingriffen zu rechnen sein, die ohne gravierende Nachteile für das Gemeinwohl nicht aufgegeben werden können. Diesen Anforderungen wird der Melderegisterabgleich sicher nicht gerecht. Auf ihn muß deshalb nach meiner Überzeugung bis zur Schaffung einer tragfähigen Rechtsgrundlage verzichtet werden.

Im übrigen sind im VO-Entwurf zwei weitere Datenabgleiche vorgesehen:

— Der Datenabgleich für Zwecke der Versorgungsverwaltung soll künftig an die Stelle der sog. Lebensbescheinigungen treten. Diese müssen derzeit alle zwei Jahre von den Versorgungsempfängern bei der Meldebehörde eingeholt und dem Versorgungsamt vorgelegt werden. Mir erscheint ein solches Verfahren zweckmäßig. Allerdings müßte dessen Zulässigkeit im Bundesversorgungsgesetz geregelt werden. Ich habe deshalb gefordert, daß Hamburg eine entsprechende gesetzgeberische Initiative ergreifen soll.

— Der Datenabgleich zu Vermeidung von Überzahlungen bei der Gewährung von Leistungen der Sozialhilfe und Wohngeld ist nach Auffassung des Senatsamtes für Bezirksangelegenheiten erforderlich, weil in einer Vielzahl von Fällen die zuständigen Dienststellen erst verspätet über den Tod oder den Fortzug eines Leistungsempfängers unterrichtet würden. Dadurch komme es in diesen Bereichen leicht zu Überzahlungen, die neben einem erheblichen Verwaltungsaufwand auch einen finanziellen Schaden für den öffentlichen Haushalt bedeuten würden. Die BAJS hat im Rahmen des Abstimmungsverfahrens Zweifel daran geäußert, daß die Mehrzahl der Überzahlungsfälle durch den vorgesehenen Datenabgleich vermieden werden kann und er deshalb — auch unter dem Gesichtspunkt des Datenschutzes — als erforderlich anzusehen ist. Weiter befürchtet die BAJS, daß ein solches Verfahren in einem unangemessenen Verhältnis zum Erfolg steht.

Ich teile diese Bedenken der BAJS und habe bei meinem gegenwärtigen Kenntnisstand ebenfalls Zweifel an der Erforderlichkeit eines solchen Datenabgleichs. Bis zum Redaktionsschluß dieses Tätigkeitsberichts konnte mir das Senatsamt für Bezirksangelegenheiten jedenfalls keine Gründe nennen, aus denen sich ergibt, daß auf diesen Datenabgleich nicht verzichtet werden kann.

5.7.3 Informationsverarbeitung bei der Verwarnungs- und Bußgeldstelle

In meinem 4. TB (4.8.5, S. 57) habe ich über die Prüfung der Verwarnungs- und Bußgeldstelle, die zuständig ist für die Durchführung von Bußgeld- und Verwarnungsangelegenheiten im Straßenverkehr, berichtet. Meine Gespräche mit der Behörde für Inneres sind inzwischen abgeschlossen. Ich komme zu folgender datenschutzrechtlicher Bewertung:

1. Ich habe hinsichtlich der Verfahrensvorschriften für die Ahndung von Ordnungswidrigkeiten und Straftaten (§§ 35, 46 und 53 OWiG) bezweifelt, ob diese den Grundsätzen der Normenklarheit entsprechen. Da diese Frage allerdings von grundsätzlicher Bedeutung ist, soll die Angelegenheit weiter mit der Justizbehörde vertieft werden. Materiell-rechtliche Bedenken hinsichtlich des Umfangs der erhobenen Daten bestehen nicht.

2. Die Behörde für Inneres wird die Hinweise in den Anhörbögen, aus denen die Möglichkeit der freiwilligen Beantwortung einiger Fragen ersichtlich ist, noch deutlicher machen.
3. Sowohl die Kartei der Unfallbeteiligten als auch die Kartei der Fahrverbote dienen jeweils als Such-, Hinweis- und Auskunftskartei. Sie enthalten Daten, die aus den dazugehörigen Akten stammen. Nach meinen Feststellungen erfüllen die Karteien die Begriffsmerkmale einer Datei nach § 4 Abs. 4 Ziff. 3 HmbDSG und fallen somit nicht unter die Bestimmung des § 1 Abs. 2 Satz 2 HmbDSG (interne Datei). Die Behörde für Inneres hat in den Gesprächen zwar eine andere Auffassung vertreten, wollte die beiden Karteien allerdings im Interesse eines möglichst geringen Verwaltungsaufwandes, um nämlich auch Auskünfte ohne Ziehung der jeweiligen Akte geben zu können, zum Datenschutzregister nachmelden. Das ist bisher trotz Erinnerung nicht erfolgt.
4. Sofern gegen einen Betroffenen ein Fahrverbot nach § 25 StVG festgesetzt und rechtskräftig wird, machte die Verwarnungs- und Bußgeldstelle bisher hiervon eine Mitteilung an die zuständige Führerscheinstelle. Da für diese Mitteilung eine Rechtsgrundlage nicht vorhanden ist, wird künftig darauf verzichtet.
5. Die Behörde für Inneres hat sich bereit erklärt, die von mir festgestellten Mängel hinsichtlich der äußeren Datensicherheit (z.B. keine Sicherheitsschlösser in den Zimmertüren, keine verschließbaren Aktenschränke, Zwischenlagerung erledigter Akten erfolgt in einem nicht verschließbaren Raum) abzustellen.

Da ich bis auf diese Punkte keine Unregelmäßigkeiten bei der Informationsverarbeitung durch die Verwarnungs- und Bußgeldstelle feststellen konnte, bin ich zu dem Ergebnis gekommen, daß dort im großen und ganzen die zahlreichen personenbezogenen Daten mit der gebotenen Sorgfalt behandelt werden.

5.7.4 Paß- und Personalausweiswesen

5.7.4.1 Maschinenlesbarer Personalausweis

Gegen die schwerwiegenden Bedenken, die ich in meinen letzten drei Tätigkeitsberichten (2. TB, 3.8.2, S. 66 ff; 3. TB, 3.7.2, S. 54 ff; 4. TB, 4.8.4, S. 57) im einzelnen beschrieben habe, haben die Regierungsparteien mit dem Zweiten Gesetz zur Änderung personalausweisrechtlicher Vorschriften vom 19. April 1986 (BGBl. I S. 545) den maschinenlesbaren Personalausweis durchgesetzt. Die schon im Jahre 1980 von allen Fraktionen des Bundestages für notwendig erachteten flankierenden Maßnahmen, nämlich bereichsspezifische Datenschutzregelungen für die Sicherheitsbehörden, stehen noch aus. Es ist also nach wie vor ungeklärt, unter welchen Voraussetzungen die Polizei — bei der Gefahrenabwehr wie bei der Strafverfolgung — mit Hilfe des neuen Ausweissystems Personenkontrollen durchführen und Personalien feststellen darf und unter welchen Voraussetzungen sie die so gewonnenen Informationen verwerten darf. Der neue § 163 d StPO enthält nur für einen winzigen Ausschnitt der in der StPO zu lösenden Probleme eine Regelung. Mithin hat der Bundestag, ohne sicher zu wissen welches Ausmaß an Kontrollen der Bevölkerung zugemutet wird, die mit dem computerlesbaren Ausweis verbundenen Risiken überhaupt nicht angemessen bewerten und schon gar nicht gegen den vermeintlichen — von den Experten weiterhin angezweifelten — Sicherheitsgewinn abwägen können.

Ob und wann bereichsspezifische Regelungen für die polizeiliche Informationsverarbeitung, die zudem rechtsstaatlichen Prinzipien der Normenklarheit und Verhältnismäßigkeit entsprechen, einmal vom Bundesgesetzgeber und den Parlamenten aller Länder verabschiedet sein werden, ist noch völlig ungewiß.

Meine verfassungsrechtlichen Bedenken gegen den neuen Personalausweis muß ich daher in vollem Umfang aufrechterhalten: Vor der Einführung derartiger Technologien müssen ihre Folgen absehbar und ggf. durch klare Regelungen eingegrenzt sein.

5.7.4.2 Landesrechtliche Umsetzung

Das Bundespersonalausweisgesetz in der jetzt beschlossenen Fassung bedarf noch einer landesrechtlichen Umsetzung durch Ausführungsgesetze und Verwaltungsvorschriften, die in den meisten Bundesländern begonnen hat. Immerhin soll nach der Vorstellung des Bundesgesetzgebers der neue Personalausweis schon ab. 1. April 1987 benutzt werden. Ob in Hamburg schon entsprechende Entwürfe erarbeitet worden sind, ist mir nicht bekannt.

5.7.4.3 Maschinenlesbarer Paß

Zeitgleich mit dem maschinenlesbaren Personalausweis wurde mit dem „Paßgesetz und Gesetz zur Änderung der Strafprozeßordnung" vom 19. April 1986 (BGBl. I S. 537) der maschinenlesbare Paß eingeführt. Für ihn gelten meine Ausführungen unter 5.7.4.1 entsprechend.

5.7.4.4 § 163d StPO (Schleppnetzfahndung)

Die Änderungen der personalausweis- und paßrechtlichen Vorschriften sind darüber hinaus zum Anlaß genommen worden, die sog. „Schleppnetzfahndung" durch die Einfügung eines § 163d in die Strafprozeßordnung gesetzlich zu verankern. Im Rahmen des Gesetzgebungsverfahrens habe ich mich an einer vom Innenausschuß des Deutschen Bundestages durchgeführten öffentlichen Anhörung von Sachverständigen beteiligt. Meine Bedenken gegen die ursprünglich vorgeschlagene Fassung lassen sich wie folgt zusammenfassen:

- Die Speicherungsvorschrift des § 163d ist auf die Erhebungsstatbestände der StPO und des Polizeirechts in keiner Weise abgestimmt und hängt gleichsam in der Luft. Der Entwurf läßt jede Tatsache ausreichen, die die Annahme rechtfertigt, daß durch die Verarbeitung der Daten die Straftat aufgeklärt oder der Täter ergriffen werden kann. § 163d würde damit die Speicherung sog. „Massendaten" ermöglichen.
- § 163d räumt also in sehr großzügiger Weise die Hindernisse beiseite, die einer Weiterentwicklung der polizeilichen Datenverarbeitung von der Speicherung von Daten über Verdächtige und Beschuldigte bis zur Speicherung von Daten über Begleitpersonen, Kontaktpersonen und sonstige „andere Personen" noch im Wege stehen.
- Bedenklich ist vor allem, daß der Grundsatz der Zweckbindung im Entwurf ohne Not fallengelassen wird. Die bei Kontrollstellen gewonnenen Erkenntnisse dürfen auch „zu anderen Maßnahmen der Strafverfolgung" verwendet werden. Auch Zufallsfunde und Abfallprodukte einer Maßnahme können damit neuen Zwecken zugeführt werden. Sogar für die Verfolgung von Vergehen soll die Polizei die mit Hilfe der Kontrollen und Sonderdateien erlangten Erkenntnisse gebrauchen dürfen, wenn die Strafverfolgung „aus Gründen des öffentlichen Interesses unerläßlich ist".
- Der Katalog des § 100a StPO, der ca. 80 Straftatbestände umfaßt, ist als Maßstab für die Verarbeitung von Massendaten ungeeignet. Während der von § 100a betroffene Personenkreis sich auf die Benutzer bestimmter Fernmeldeanschlüsse beschränkt, die mit einem Tatverdächtigen kommunizieren, kann jeder unbeteiligte Dritte in einer Fahndungsdatei nach § 163d aufgenommen werden, weil er rein zufällig in eine Personenkontrolle geraten ist. Es ist nicht ersichtlich, wie eine Eingrenzung des Personenkreises nach bestimmten Merkmalen und Eigenschaften erfolgen und wie eine partielle Protokollierung technisch realisiert werden soll.
- Mit seiner fast uferlosen Regelungsbreite ist § 163d unvereinbar mit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz, in dem der Gesetzgeber zu normenklaren bereichsspezifischen Regelungen bei der Eingriffsdatenverarbeitung unter Berücksichtigung des Verhältnismäßigkeitsprinzips und des Zweckbindungsgebotes aufgefordert wird.

Wesentliche Teile dieser Bedenken sind durch die endgültige Fassung des Gesetzes ausgeräumt worden. Andere müssen aufrechterhalten werden. So ist es zu begrüßen, daß der Gesetzgeber den Katalog von Straftaten, die die Anordnung von Maßnahmen nach § 163d rechtfertigen, eingeschränkt hat. Andererseits wird dieser — datenschutzrechtlichen Belangen entgegenkommenden — Entscheidung ihre Wirkung weitgehend dadurch wieder genommen, daß die so gewonnenen Daten auch zur Verfolgung beliebiger anderer Straftaten verwendet werden dürfen. Meine Zweifel, ob hier nicht gegen das Zweckbindungs- und Verhältnismäßigkeitsprinzip verstoßen wird, sind also nicht zerstreut worden. Ebensowenig ist es vertretbar, daß jede Grenzkontrolle, gleichviel, ob sie aus Gründen der Strafverfolgung oder der Gefahrenabwehr durchgeführt wurde, Anlaß für Speicherungen und Auswertungen im Rahmen des § 163d sein kann. Gleichwohl soll nicht verkannt werden, daß durch Präzisierungen und Einengungen einige Verbesserungen erreicht wurden.

5.7.5 Ausländerzentralregister

Schon in meinem zweiten (3.8.3, S. 71) und dritten Tätigkeitsbericht (3.7.3.6, S. 62) hatte ich von Überlegungen berichtet, die eine Neukonzeption des Ausländerzentralregisters (AZR) zum Gegenstand haben. Es geht darum, das AZR, das seit 1953 als bundeszentrale Datei aller im Bundesgebiet behördlich erfaßten Ausländer geführt wird und weit über 100 Mio. Daten von etwa 10 Mio. Personen im Bestand hat, auf eine tragfähige gesetzliche Grundlage zu stellen und für verschiedene politische Aufgaben besser nutzen zu können. So beabsichtigt der Bundesinnenminister, das Register stärker in das System zum Schutz der Inneren Sicherheit einzubinden und für die Gewinnung ausländerpolitischer Planungsdaten auszubauen. Die von ihm initiierte Bund-Länder-Arbeitsgruppe hat im August dieses Jahres ihre Beratungsergebnisse vorgelegt, die vor allem Vorschläge für die Datensätze und die Kommunikationsstrukturen enthalten, aber auch Regelungsbedarfe aufzeigen. Ungeklärt scheint zu sein, ob die geplanten gesetzlichen Bestimmungen die Gestalt eines Registergesetzes (ähnlich dem Bundeszentralregistergesetz) erhalten oder als bereichsspezifische Informationsverarbeitungsregeln in das Ausländergesetz aufgenommen werden sollen.

Eine Bewertung der Arbeitsergebnisse und der Gesetzesplanung hat von folgendem auszugehen: Nach der Rechtsprechung des Bundesverfassungsgerichts ist das Recht auf informationelle Selbstbestimmung Teil des in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verankerten allgemeinen Persönlichkeitsrecht. Dieser Grundrechtsschutz steht (anders als etwa das Grundrecht aus Art. 12 GG — Berufsfreiheit —) uneingeschränkt auch den in der Bundesrepublik Deutschland und Berlin lebenden Angehörigen anderer Staaten zu. Auch sie müssen Eingriffe und Einschränkungen in ihre Rechte nur im überwiegenden Allgemeininteresse hinnehmen. Vor diesem Hintergrund wird in den kommenden Gesetzesberatungen darauf hinzuwirken sein, daß die für diese Personengruppe zu erwartenden Sondervorschriften nicht zu einer allgemeinen Diskriminierung führen. So ist nicht hinreichend begründet, warum die geplante Einstellung des polizeilichen INPOL-Fahndungsbestandes in das AZR erforderlich sein soll.

Weiter von Bedeutung für die datenschutzrechtliche Bewertung des Registers sind die Funktionen, die es erfüllen soll. Außer Frage steht seine Verwendung als Indexregister zum Zweck der Feststellung, ob eine — und wenn ja, welche — Ausländerbehörde Unterlagen über einen bestimmten Ausländer besitzt. Damit soll das AZR den Zugang zu den eigentlichen Ausländer- und Meldedaten erleichtern; es kann und darf den Rückgriff auf die bei den örtlichen Behörden gesammelten Informationen nicht ersetzen. Keinesfalls darf das AZR zu einem bundesweiten zentralen Melderegister ausgebaut werden. Allenfalls bei Eilentscheidungen sollten die im Register gespeicherten Daten unmittelbar für Maßnahmen der Verwaltung herangezogen werden.

Für nichtöffentliche Stellen und Privatpersonen darf der Zugang zu den Daten des AZR nur in eng begrenzten Ausnahmefällen gewährt werden, die gesetzlich festzulegen sind. Nur wenn die Verwendung der Daten im Register sowie ihre Anlieferung und Wei-

tergabe gesetzlich klar und eindeutig vorgegeben sind, kann der Betroffene den Eingriff in sein Recht auf informationelle Selbstbestimmung einschätzen. Allein ein Registergesetz genügt diesen Anforderungen nicht. Eine zeitlich parallele Novellierung des Ausländerrechts ist deshalb unabdingbar. Gleichzeitig muß auch der Datenaustausch zu Fahndungszwecken und zur Erfüllung anderer polizeilicher Aufgaben in der Strafprozeßordnung und in Polizeigesetzen geregelt werden. Eine gesetzliche Regelung ausschließlich des Teilnehmerkreises und des Datenumfangs wäre nicht ausreichend, solange nicht präzise festgelegt wird, für welche konkreten Zwecke die Behörden Daten abrufen dürfen, bzw. das AZR an sie übermitteln darf. Nur eine verwendungsorientierte Regelung macht den potentiellen Verwendungszusammenhang transparent und würde den Anforderungen des Bundesverfassungsgerichts genügen. Deshalb würde eine Festlegung, daß den Benutzern nur solche Daten übermittelt werden, die sie zur Aufgabenerfüllung benötigen, nicht ausreichen; es bedarf gerade der Festlegung der Aufgaben, zu deren Erfüllung Datenübermittlungen vorgenommen werden sollen. Auch eine Differenzierung nach Abfragearten, die jeweils verschiedene, stufenweise gestaffelte Datenmengen umfassen, wäre ungenügend, solange nicht feststeht, für welche Aufgaben welche Behörden die festgelegten Datenmengen abrufen können.

Der On-line-Zugriff auf die im AZR gespeicherten Daten stellt eine besonders intensive Form des Zugriffs auf personenbezogene Informationen dar. Er bedarf daher der besonderen Rechtfertigung, die in der Aufgabenstellung der beteiligten Behörde begründet sein muß.

An einer solchen gesetzlichen Regelung haben sich auch die in das AZR aufzunehmenden Datensätze auszurichten, die insoweit noch der Überarbeitung bedürfen. Besonders problematisch wäre die Speicherung und Verwendung des Datums „Einreisebedenken". Unter diesem Datum sollen belastende Vorgänge im Umfeld des Ausländers erfaßt werden, die noch keine ausländerrechtlichen Maßnahmen ausgelöst haben. Damit erhält der Datensatz eine neue Qualität: Gespeichert werden nicht mehr Informationen über in einem formalisierten und rechtsstaatlichen Verfahren ergangene Maßnahmen der Ausländerbehörde, sondern auch unpräzise Angaben über ein vermutetes (Fehl-) Verhalten des Ausländers selbst. Hinzu kommt: Die Speicherung derart „weicher" Daten steht in deutlichem Widerspruch zu der Forderung des Bundesverfassungsgerichts, der Bürger müsse wissen, was wann und bei welcher Gelegenheit an Informationen über ihn gespeichert und weitergegeben wird. Demgegenüber kann sich dieses Datum auf eine ganze Palette von Vorgängen beziehen und hängt in großem Maße von der subjektiven Bewertung des einzelnen Sachbearbeiters ab.

Eine Verarbeitung dieses Datums wäre allenfalls hinnehmbar, wenn

— die unter diese Angaben fallenden Tatbestände zumindest durch Rechsverordnung präzise umschrieben werden und

— aufgrund der Registerauskunft ohne Hinzuziehen der Ausländerakte keine negativen Entscheidungen getroffen werden dürfen.

Im übrigen ist sicherzustellen, daß die Verarbeitung von Daten, die ausschließlich für statistische und Planungszwecke erhoben werden, getrennt von den anderen Daten der Betroffenen erfolgt. Außerdem müssen die Daten derart anonymisiert werden, daß eine Verbindung zu personenbezogenen Daten nicht mehr hergestellt werden kann.

5.8 Polizei

Schon in meinem ersten Tätigkeitsbericht habe ich auf die Dringlichkeit der Schaffung bereichsspezifischer gesetzlicher Grundlagen für die polizeiliche Informationsverarbeitung hingewiesen. Aus den zunächst zögerlichen, nach Bekanntwerden des Volkszählungsurteils des Bundesverfassungsgerichts intensiveren Bemühungen der Innenministerkonferenz einen Musterentwurf und Hamburgs, einen verabschiedungsreifen Entwurf zur Novellierung des SOG zu erarbeiten, habe ich mich ständig beteiligt (vgl. die Darstellungen im 3. TB, 3.8.5, S. 76 ff. und 4. TB, 4.9.1, S. 59 ff.). Im Laufe des Berichtsjahres ist die Gesetzgebungsarbeit jedoch in der Innenministerkonferenz

ebenso wie beim Bund und auch in Hamburg wieder zum Erliegen gekommen. Da einerseits inzwischen unstreitig sein dürfte, daß für die meisten Eingriffe der Polizei in das informationelle Selbstbestimmungsrecht von Bürgern verfassungsrechtlich hinreichende gesetzliche Grundlagen nicht vorhanden sind, das Bundesverfassungsgericht andererseits aber solche Eingriffe nur auf der Grundlage normenklarer, dem Gebot der Verhältnismäßigkeit entsprechender Rechtsvorschriften für zulässig hält, stellt sich die Frage, wie die Informationsgewinnung und -verarbeitung gegenwärtig zu beurteilen ist.

5.8.1 Übergangslösungen

Mit dem Sachverhalt, daß für Eingriffsmaßnahmen die erforderlichen Rechtsgrundlagen fehlen oder unzureichend sind, mußte sich das Bundesverfassungsgericht schon mehrmals auseinandersetzen (vgl. BVerfGE Bd. 41 S. 251/266 ff.; Bd. 51 S. 268/287 ff.). Zur Übergangsregelung hat es dabei in allgemeiner Form wie folgt Stellung genommen:

> „Grundsätzlich hat die Feststellung, daß eine Verwaltungsmaßnahme, die in einen grundrechtlich geschützten Bereich eingreift und der verfassungsrechtlich gebotenen gesetzlichen Grundlage entbehrt, zwar die Aufhebung dieser Maßnahme zur Folge. 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, verfassungsrechtlich bedenklich geworden ist, die Notwendigkeit von Übergangsfristen anerkannt, in welchen der Gesetzgeber die Gelegenheit einer verfassungsmäßigen (Neu-) Regelung haben sollte. Eine solche Übergangsfrist kann insbesondere dann notwendig sein, wenn eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden soll, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand. Bei der Zubilligung von Übergangsfristen ist nach der Schwere des Eingriffs zu differenzieren: Je tiefergreifender eine Verwaltungsmaßnahme Grundrechte des Betroffenen berührt, desto strengere Anforderungen sind an die Einräumung von Übergangsfristen und die innerhalb dieser Fristen unerläßlichen Maßnahmen zu stellen; ist der Eingriff weniger schwerwiegend, kann eine großzügigere Anerkennung von Übergangsfristen in Betracht kommen.
>
> Für die Dauer derartiger Übergangsfristen können keine allgemein gültigen Maßstäbe gesetzt werden. Das Bundesverfassungsgericht hat verschiedentlich darauf abgestellt, daß eine gesetzliche Regelung jedenfalls bis zum Ende der laufenden Legislaturperiode des Parlaments erfolgen müsse. Eine Übergangsfrist könnte dann nicht mehr länger anerkannt werden, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert hätte.
>
> Während dieser Übergangsfrist kann die alte verfassungsrechtlich zu beanstandende Regelung allerdings nur noch bedingt weiter angewandt werden. Bis zur Herstellung eines verfassungsgemäßigen Zustandes durch den Gesetzgeber reduziert sich die Befugnis zu Eingriffen in verfassungsrechtlich geschützte Positionen auf das, was im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Betriebs unerläßlich ist. Die Prüfung, was in der jeweiligen Situation unerläßlich ist, darf sich nicht einfach darin erschöpfen, ob die ohnehin nur als Provisorium fortbestehende bisherige Regelung als solche korrekt angewandt worden ist. In Fällen der vorliegenden Art gehört dazu auch die weitere Prüfung, ob nicht unter Berücksichtigung der gegebenen Verhältnisse eine bislang nicht vorgesehene schonendere Maßnahme ausreicht, um die Funktionsfähigkeit sicherzustellen."

Bezogen auf die polizeiliche Praxis sind aus dieser Rechtsprechung folgende Schlußfolgerungen zu ziehen:

— Der Polizei ist für die Informationsverarbeitung eine Übergangsfrist zuzubilligen, um im Interesse der verfassungsmäßigen Ordnung ihre Funktionsfähigkeit zu erhalten.

— Während der Übergangsfrist hat sie vor allem im Bereich der vorbeugenden Verbrechensbekämpfung, wo gesetzliche Regelungen praktisch völlig fehlen, Informationseingriffe auf unerläßliche Maßnahmen zu beschränken.

— Vorhandene, aber unzureichende gesetzliche Grundlagen in den Bereichen der Gefahrenabwehr und der repressiven Polizeiarbeit sind verfassungsgemäß, d.h. in den meisten Fällen restriktiv, auszulegen.

— Bei der Bestimmung der unerläßlichen Maßnahmen ist zu berücksichtigen, daß die Informationsverarbeitung der Polizei regelmäßig besonders tief in das Grundrecht auf informationelle Selbstbestimmung eingreift.

— Die Komplexität der zu regelnden Sachverhalte rechtfertigt es, den Ablauf der Übergangsfrist nicht mit der in Hamburg zu Ende gegangenen und der im Bund auslaufenden Legislaturperiode anzunehmen. Vielmehr darf sie in die kommenden Legislaturperioden hineinreichen; endet nach meiner Auffassung jedoch spätestens mit deren Ablauf.

Danach müßte es ein dringliches Anliegen der Behörde für Inneres sein, für die Sicherheitsbehörden den Umfang der unerläßlichen Maßnahmen zu bestimmen, will sie nicht Gefahr laufen, daß die Arbeit der Polizei in den Geruch der Verfassungswidrigkeit gerät. Zu diesem Zweck habe ich der Behörde für Inneres einen Katalog mit den aus meiner Sicht gebotenen Beschränkungen übersandt. Eine Verständigung auf dieser Basis war bisher jedoch nicht möglich. Die Behörde für Inneres war allenfalls bereit zu konzedieren, daß die Informationseingriffe jedenfalls nicht weiter gehen dürften, als es der letzte Entwurf zur Novellierung des hamburgischen SOG vorsah.

Dies kann nach meiner Auffassung jedoch nur bis zur Erarbeitung eines detaillierten Beschränkungskataloges gelten und muß auch bis dahin unter dem Vorbehalt weitergehender erforderlicher Einschränkungen im Einzelfall stehen. Mit der Festlegung konkreter Beschränkungen soll nach Absprache mit der Behörde für Inneres im Rahmen der Aufarbeitung der Vorgänge auf dem Heiligengeistfeld begonnen werden.

Dringend erforderlich ist nach meiner Auffassung, daß der Umfang der Einschränkungen bis zu einer gesetzlichen Regelung den auf dieser Grundlage tätig werdenden Polizeibeamten schriftlich mitgeteilt wird, da andernfalls die Beschränkungen nur unzureichend oder gar nicht greifen können. Aber auch dies hat die Behörde für Inneres unter Hinweis auf die in der neuen Legislaturperiode zu erwartende zügige Verabschiedung der Novellierung des SOG abgelehnt. Im Hinblick auf die nach der Wahl vom 9. November 1986 entstandene schwierige politische Situation sind jedoch Zweifel angebracht, daß die dringend erforderliche Gesetzesergänzung kurzfristig zu erreichen ist. Ich muß deshalb an meinen bisherigen Forderungen festhalten, zumal es Ereignisse gibt, die zeigen, daß selbst der Minimalkonsens auf der Grundlage des letzten Entwurfs für eine SOG-Novelle bei Polizeieinsätzen nicht umgesetzt worden ist (s. 5.8.2).

5.8.2 Polizeieinsatz auf dem Heiligengeistfeld vom 8. Juni 1986

Dieser Polizeieinsatz warf auch in datenschutzrechtlicher Hinsicht verschiedene Probleme auf. Diese betrafen zunächst den Umfang der erhobenen Informationen. Es wurden nämlich

— von 781 Personen Identifizierungsdaten erhoben;

— diese Daten mit dem polizeilichen Auskunftssystem POLAS abgeglichen;

— von 311 Personen (z.T. zusammen mit Polizeibeamten) Lichtbilder angefertigt;

— Fotos und Videoaufnahmen, die den Geschehensablauf auf dem Heiligengeistfeld und der Umgebung festhalten, erstellt.

Um diese Erhebungsmaßnahmen datenschutzrechtlich zu bewerten, war es erforderlich zu prüfen, auf welcher Rechtsgrundlage der Polizeieinsatz selbst erfolgte. Ich bin zu dem Ergebnis gekommen, daß auf dem Heiligengeistfeld eine — wenn auch unangemeldete — Versammlung im Sinne von § 14ff VersG stattgefunden hatte, und daß

der Polizei deshalb unter Ausschluß des allgemeinen Polizeirechts nur die Befugnisse des Versammlungsgesetzes zur Verfügung gestanden hätten. Diese Auffassung ist nach meinen Kenntnissen inzwischen von einer Kammer des Verwaltungsgerichts Hamburg bestätigt worden. (Bei zwei weiteren Kammern sind Parallelverfahren noch anhängig.)

Das Versammlungsgesetz enthält aber keine Befugnisse, die es gestatten, alle Teilnehmer einer nicht aufgelösten Versammlung in Verwahrung zu nehmen und im Zusammenhang hiermit ihre Identität festzustellen.

— Daraus folgt, daß die Erhebung von Identifizierungsdaten aller Teilnehmer einer öffentlichen Versammlung, auf die — noch — das Versammlungsrecht anzuwenden ist, nicht zulässig ist. Dies würde im übrigen auch der Bedeutung des Grundrechts aus Art. 8 GG zuwiderlaufen. Es muß an dieser Stelle genügen, nochmals an die Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil und im Brokdorf-Beschluß zum Versammlungsrecht zu erinnern.

— Vor diesem Hintergrund ist auch der Abgleich so gewonnener Daten mit den POLAS-Dateien als rechtswidrig anzusehen. Ein Abgleich von erhobenen mit bereits gespeicherten Daten kann nur zulässig sein, wenn er vom Zweck der Erhebung erfaßt ist. Wenn aber bereits die Erhebung selbst rechtswidrig ist, kann der Abgleich auch nicht rechtmäßig sein.

— Entsprechendes gilt für die zur Identitätsfeststellung erstellten Fotografien. Da die Voraussetzungen für eine Personenkontrolle nicht vorlagen, war die Aufnahme der Fotografien unzulässig.

— Videoaufnahmen und Lichtbilder zum Festhalten von Geschehensabläufen halte ich nur dann für zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß die Begehung einer Straftat unmittelbar bevorsteht. Wird eine Straftat nicht begangen, sind solche Unterlagen nach Beendigung der Versammlung unverzüglich zu vernichten (vgl. Alternativfassung der SPD-regierten Bundesländer zu § 8b Abs. 2 des Vorentwurfes zur Änderung des Musterentwurfes eines einheitlichen Polizeigesetzes des Bundes und der Länder — Stand: 12. März 1986 —).

Im übrigen muß noch geklärt werden, ob eine solche Vorschrift als bereichsspezifische Regelung für das bundesgesetzlich geregelte Versammlungsrecht überhaupt in Ländergesetze aufgenommen werden kann.

Auf der Grundlage dieser Rechtsauffassung habe ich für die weitere Behandlung der erhobenen Daten folgende Konsequenzen gefordert:

— Soweit gegen Einzelne Ermittlungsverfahren wegen Straftaten oder Ordnungswidrigkeiten eingeleitet sind, dürfen die über diese Personen gespeicherten Daten dafür verwendet werden.

— Da die Erhebung der Identifizierungsdaten bei Anwendung des Versammlungsgesetzes für Zwecke der Gefahrenabwehr nicht zulässig war, ist auch die anschließende Speicherung für diesen Zweck nicht gestattet. D.h., erhobene Daten dürfen nicht in POLAS gespeichert werden. Kriminalakten dürfen nicht angelegt werden.

— Nicht zu beanstanden ist es, wenn die Identifizierungsdaten zu Dokumentations- und Beweiszwecken aufbewahrt werden. Es muß aber sichergestellt werden, daß sie für andere polizeiliche Zwecke nicht verwendet werden. Sie sind deshalb von sonstigen polizeilichen Datensammlungen getrennt zu verwahren.

— Da bei Anwendung des Versammlungsgesetzes ein Abgleich mit POLAS nicht zulässig war, sind die hierbei ggf. gewonnenen Erkenntnisse unverzüglich zu vernichten. Auch für Dokumentations- und Beweiszwecke ist ihre Weiterspeicherung nicht erforderlich.

— Die zur Identitätsfeststellung aufgenommenen Lichtbilder sind sofort zu vernichten (es käme auch in Betracht, sie den Betroffenen auszuhändigen).

— Da die zum Festhalten der Geschehensabläufe angefertigten Lichtbilder und Videoaufnahmen offenbar nicht für die Verfolgung von Straftaten benötigt wurden,

hatte ich zunächst gefordert, daß auch diese zu vernichten seien. Im Hinblick auf die laufenden Gerichtsverfahren bin ich jedoch damit einverstanden, daß sie ebenfalls für Dokumentations- und Beweiszwecke aufbewahrt werden.

Über diese Forderungen bestand nach kurzer Zeit Einvernehmen mit der Behörde für Inneres. Sie sind inzwischen umgesetzt, so daß dieser konkrete Polizeieinsatz datenschutzrechtlich als erledigt angesehen werden kann.

Gleichwohl besteht Anlaß, auf ihn bezüglich der unter 5.8.1 erörterten Übergangsproblematik zurückzugreifen. Unabhängig von meiner Rechtsauffassung habe ich nämlich die Frage geprüft, ob die Datenerhebung dann zulässig gewesen wäre, wenn als Rechtsgrundlage des Polizeieinsatzes allgemeines Polizeirecht hätte dienen können. Dann wäre zur datenschutzrechtlichen Bewertung im Sinne des vorgenannten Minimalkonsenses der letzte Entwurf zur Novellierung des SOG (Stand: 2. Dezember 1985) — SOG-E — heranzuziehen gewesen.

Für diesen Fall bin ich zu folgenden Ergebnissen gekommen:

— Dann dürften gem. § 11 Abs. 1 SOG-E personenbezogene Daten erhoben werden, soweit dies zur Gefahrenabwehr erforderlich ist. Ich habe schon früher klargestellt, daß damit nur die Abwehr einer konkreten Gefahr gemeint sein kann. Die Datenerhebung zur Abwehr von möglicherweise später eintretenden Gefahren ist davon nicht gedeckt.

  Für den vorliegenden Fall bleibt festzustellen, daß die vorgenommene Datenerhebung — vielfach erst nachts auf einzelnen Polizeidienststellen — zur Abwehr konkreter Gefahren ungeeignet war. Es mag sein, daß die Einschließung ein geeignetes Mittel zur Gefahrenabwehr war — dies habe ich nicht zu beurteilen —, die Erhebung der Identifizierungsdaten war es nicht. Im übrigen dürfen Maßnahmen nach § 11 Abs. 1 SOG-E nur gegen Störer gerichtet werden.

  Schließlich habe ich starke Zweifel, ob die Befugnis zur Identitätsfeststellung bei Razzien (§ 16b SOG-E) als Rechtfertigung herangezogen werden kann. Razzien sind auf die vorbeugende Bekämpfung von Straftaten mit erheblicher Bedeutung zu beschränken. Für mich ist nicht ersichtlich, daß die Polizei tätig werden mußte, um der Begehung von Straftaten dieser Qualität vorzubeugen. Zu prüfen wäre ferner, ob nicht auch andere Mittel zum gleichen Erfolg geführt hätten und es nicht unverhältnismäßig war, eine so große Anzahl von Nichtstörern in Anspruch zu nehmen.

— Sofern sich die Datenerhebung nach allgemeinem Polizeirecht richtet, wäre der vorgenommene Datenabgleich nach § 16j des von der Innenbehörde vorgelegten SOG-E zulässig. Hiernach kann die Polizei im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten voraussetzungslos mit den Daten ihrer Fahndungsdateien abgleichen; mit den übrigen polizeilichen Daten, soweit dies zur Gefahrenabwehr erforderlich ist. Ich halte die Befugnisse für zu weitgehend und habe in meinen bisherigen Stellungnahmen zum SOG-E klargestellt, daß es unverhältnismäßig wäre, wenn die Polizei beliebige Personen — ohne konkreten Anlaß — mit den Fahndungsdateien abgleichen dürfte. Meines Erachtens darf auch ein Fahndungsabgleich nur durchgeführt werden, soweit die Voraussetzungen für eine Identitätsfeststellung gegeben sind. Ein Abgleich mit sonstigen Dateien muß an wesentlich engere Voraussetzungen geknüpft werden.

— Die Aufnahme von Lichtbildern hat im Polizeirecht eine eigenständige Bedeutung. Sie stellt sich als ed-Maßnahme dar (vgl. § 16c Abs. 3b SOG-E). Als solche kann sie zur Identifizierung unbekannter Personen eingesetzt werden, wenn andere Mittel nicht zur zweifelsfreien Feststellung der Identität geführt haben (§ 16c Abs. 1). Ed-Maßnahmen sind danach zur Feststellung der Identität jedoch nur soweit zulässig, wie die Polizei zu einer Identitätsfeststellung überhaupt befugt ist. Dies ist für den Polizeieinsatz auf dem Heiligengeistfeld — wie dargelegt — auch unter polizeirechtlichen Gesichtspunkten fraglich. Im übrigen wäre auch die Frage zu stellen, ob es in allen 311 Fällen kein anderes Mittel zur zweifelsfreien Feststellung der Identität gab. Die Voraussetzung für eine ed-Behandlung nach § 16c Abs. 2 zwecks vorbeugender Straftatenbekämpfung waren offensichtlich nicht gegeben.

Diese Parallelwertung zeigt, daß die konkret handelnden Polizeibeamten und selbst die Polizeieinsatzführer über polizeiliche Eingriffsbefugnisse bis zur Verabschiedung des neuen SOG nicht ausreichend informiert sind. Die Ereignisse auf dem Heiligengeistfeld haben deshalb auch deutlich gemacht, wie notwendig konkrete Anweisungen an die Polizei bezüglich der verfassungsrechtlich gebotenen Beschränkungen sind.

5.8.3 Eingaben

Ein großer Teil der bei mir eingegangenen Bürgereingaben für den öffentlich-rechtlichen Bereich betraf die polizeiliche Informationserhebung und -verarbeitung. Der Versuch einer umfassenden Darstellung der einzelnen Probleme würde den Rahmen dieses Berichts sprengen. In sehr vielen Fällen hat meine Überprüfung dieser Eingaben ergeben, daß die Arbeit der Polizei nicht zu beanstanden ist. Wenn ich mit der polizeilichen Praxis nicht einverstanden war, ließ sich mit der Behörde für Inneres meist Einvernehmen erzielen. Dafür zwei Beispiele:

5.8.3.1 Weitergabe von Kundendaten der Hamburger Wasserwerke an die Polizei

Zur Ermittlung unzulässiger Bodenversickerungen und Einleitungen in Gewässer benötigt die Ermittlungsgruppe — Umwelt — der Polizei häufig die Menge der Trinkwasserabnahme einzelner Unternehmen und Privatpersonen. Schon 1983 ist unter meiner Mitwirkung ein Verfahren entwickelt worden, das den berechtigten Interessen der Polizei Rechnung trägt, ohne schutzwürdige Belange der betroffenen Kunden der Hamburger Wasserwerke zu beeinträchtigen (vgl. 2. Tätigkeitsbericht, 4.9.2, S. 139f). Kernstück des Verfahrens ist die Regelung, daß die Polizei Kundendaten nur dann anfordert, wenn sie auf andere Weise (insbesondere durch Nachfrage beim Beschuldigten und Einsichtnahme in seine Unterlagen) nicht beschafft werden können (vgl. auch Antwort des Senats vom 13. Juni 1986 auf die Schriftliche Kleine Anfrage des Abgeordneten Hartmut Engels vom 5. Juni 1986 — Bürgerschafts-Drs. 11/6394 —). Gleichwohl ist mir im Laufe des Berichtsjahres auf Grund einer Eingabe bekannt geworden, daß die Polizei in mindestens einem Fall die Kundendaten bei den Hamburger Wasserwerken angefordert hat, ohne zuvor bei dem Betroffenen nachgefragt zu haben. In ihrer Stellungnahme hat die Polizei dargelegt, gegen eine solche Nachfrage könnten möglicherweise ermittlungstaktische Gründe sprechen. Da mir solche Gründe nicht einleuchtend erschienen, habe ich bei der Behörde für Inneres interveniert, die mir sodann bestätigte, daß es sich um ein Versehen gehandelt habe und die Polizei auch weiterhin das abgesprochene Verfahren einhalten werde.

5.8.3.2 Fluggastüberprüfungen bei EL-AL-Flügen

Ein Petent beschwerte sich über eine besonders intensive Erhebung persönlicher Daten am Flughafen Hamburg, bevor er mit einer Maschine der EL-AL ISRAEL AIRLINES nach Tel Aviv fliegen konnte. Da die Befrager Labels mit dem Stempelaufdruck „Polizei Hamburg" trugen, hielt er sie für Mitarbeiter der hamburgischen Polizei. Meine bisherigen Nachprüfungen haben jedoch ergeben, daß es sich dabei um Sicherheitsbeauftragte der Fluggesellschaft handeln soll. Die Labels wurden diesen Personen von der Flughafengesellschaft ausgehändigt. Ich kann nicht ausschließen, daß mit dem Stempelaufdruck bei den befragten Fluggästen ein falscher — aber nicht unerwünschter — Eindruck erreicht werden sollte. Jedenfalls hat die Behörde für Inneres die Polizei angewiesen, die Stempelaufdrucke „Polizei Hamburg" auf allen Labels entfernen zu lassen. Im übrigen hat sie mir versichert, an der Datenerhebung und möglicher -verarbeitung in keiner Phase beteiligt zu sein.

Mit diesen Maßnahmen und Erklärungen der Polizei bin ich zunächst einverstanden. Weiter nachgehen werde ich jedoch den für mich offenen Fragen, ob die Datenerhebung in dieser Form zulässig ist, ob die so erhobenen Daten gespeichert und übermittelt werden und auf welcher gesetzlichen Grundlage und zu welchem Zweck dies geschieht.

5.8.4 Datenspeicherung und -übermittlung

Manchmal deckten mir bekanntgewordene Einzelfälle aber auch gravierende Probleme der polizeilichen Informationsverarbeitung auf.

So berichtete die „Hamburger Rundschau" in ihrer Ausgabe vom 13. März 1986 über den Fall eines hamburgischen Pressefotografen, dem eine Antwort der Hamburger Polizei auf eine Erkenntnisanfrage des Landeskriminalamtes Niedersachsen zugespielt worden war. Darin wird mitgeteilt, daß der Betroffene kriminalpolizeilich in fünf Fällen, beim Staatsschutz in drei Fällen in Erscheinung getreten war. Die ausgesprochenen oder angedeuteten Vorwürfe reichten vom Versicherungsbetrug über verschiedene Pressedelikte bis zu Sabotagehandlungen an Verteidigungsmitteln, so daß durchaus der Eindruck erweckt werden konnte, bei dem Fotografen handele es sich um eine Person mit beachtlicher krimineller Vergangenheit. Tatsächlich wurde der Betroffene in keinem einzigen Fall strafrechtlich verurteilt. Bei den angegebenen Staatsschutzvorfällen ist es offensichtlich nicht einmal zu staatsanwaltlichen Ermittlungsverfahren gekommen. Die ansonsten eingeleiteten Ermittlungsverfahren waren bis auf einen Fall, wo es nach Angaben des Betroffenen zu einer Verwarnung gekommen war, sämtlich eingestellt worden. Von mir zu dem Artikel in der „Hamburger Rundschau" zur Stellungnahme aufgefordert, mußte die Behörde für Inneres zugeben, daß in zwei der acht Fälle falsche Sachverhalte übermittelt wurden. Die drei benannten Staatsschutzvorgänge beruhten nicht auf eigener Kenntnis. Obwohl die Behörde für Inneres die fehlerhafte Übermittlung als indivuelles Fehlverhalten qualifizieren wollte, mußte sie gleichzeitig einräumen, daß „durch die nicht abschließende Aufzählung der aufzunehmenden Unterlagen in der polizeilichen Dienstvorschrift für die aktenführende Dienststelle nicht eindeutlich ersichtlich" sei, ob Sachverhalte dieser Art aufgenommen werden dürften.

Dieser Fall zeigt für mich exemplarisch,

- daß die Polizei in bestimmten Fällen selbst nicht weiß, welche personenbezogenen Daten sie speichern darf und daß deshalb die Überarbeitung der polizeilichen Dienstvorschriften dringend geboten ist;
- daß oft verkürzte und damit verzerrte Informationen in die polizeilichen Auskunftssysteme eingestellt werden, die den Akteninhalt nicht korrekt wiedergeben;
- daß kritiklos Informationen auswärtiger Polizeidienststellen in das eigene System übernommen und bei Anfragen dann wieder übermittelt werden;
- daß Übermittlungen an andere Stellen stattfinden, ohne daß zuvor die gespeicherten Informationen anhand der eigenen Akten überprüft werden;
- daß in der Regel die polizeiliche Wertung bestimmter Vorgänge Gegenstand der Speicherung ist, ohne daß der Betroffene Gelegenheit hat, seine abweichende Darstellung zur Geltung zu bringen, weil er in der Regel nicht darüber informiert ist, daß seine Daten auch nach Abschluß des Ermittlungsverfahrens im polizeilichen Informationssystem verbleiben (häufig selbst dann, wenn das Verfahren mit Einstellung oder Freispruch geendet hat);
- wie problematisch die weitere Speicherung und Verwendung von Daten aus eingestellten Strafverfahren für andere polizeiliche Zwecke ist. Dabei ist auch zu bedenken, daß die staatsanwaltliche Einstellungspraxis durchaus nicht einheitlich ist. Möglicherweise ist es den Staatsanwaltschaften gar nicht bewußt, daß es für die polizeiliche Behandlung von personenbezogenen Daten einen erheblichen Unterschied machen kann, ob ein Verfahren gem. § 153 Abs. 2 oder nach § 170 Abs. 2 StPO eingestellt worden ist.

Nach meiner Überzeugung würden datenschutzrechtliche Überprüfungen „vor Ort" zahlreiche weitere Mängel in der polizeilichen Datenverarbeitung aufzeigen. Dafür steht meiner Dienststelle — wie unter 2.1 dargestellt — jedoch nicht ausreichend Personal zur Verfügung.

5.8.5 Neue Arbeitsdatei „PIOS-Organisierte Kriminalität (APOK)"

Zusammen mit der Aufnahme ihres Wirkbetriebes in Hamburg (!) wurde mir die vorläufige Errichtungsanordnung für eine probeweise zu errichtende Arbeitsdatei APOK, die Bund und Länder gemeinsam betreiben wollen, zur Stellungnahme übersandt. Meine wichtigsten vorläufigen Kritikpunkte an dieser Datei lassen sich wie folgt zusammenfassen:

— Die mit dieser Datei zu erfassenden Kriminalitätsbereiche sind in der Errichtungsanordnung zum Teil konturenlos und zu weit gefaßt. Dadurch wird meines Erachtens eine uferlose Datenspeicherung, vor allem auch von Nichtverdächtigen (Kontakt- und Begleitpersonen) ermöglicht.

— Die Datei ist nach ihrem Charakter auf überregionale Kriminalitätsbekämpfung angelegt. Die Errichtungsanordnung sichert jedoch nicht ausreichend, daß nur überregional bedeutsame Erkenntnisse eingestellt werden, so daß sich unmittelbar die Frage der Verhältnismäßigkeit stellt.

— Das Verhältnis der neuen Datei zu bestehenden Dateien scheint mir noch ungeklärt. Insbesondere besteht nach meiner Auffassung die Gefahr, daß bei Übernahme von Datenbeständen von einer in eine andere Datei die Aussonderungs- und Löschungsfristen unzulässig verlängert werden.

Die zu dieser Kritik von der Behörde für Inneres abgegebene Stellungnahme hat neue Fragen entstehen lassen. Meine Bedenken konnten damit nicht ausgeräumt werden. Ich halte nach wie vor eine Überarbeitung der Errichtungsanordnung für erforderlich und werde nach Abstimmung mit den Datenschutzbeauftragten in Bund und Länder demnächst eine endgültige Bewertung vorlegen.

5.8.6 Speicherung von Suizidversuchen

Seit der Aufnahme meiner Tätigkeit habe ich mich dagegen gewandt, daß die Polizei Daten von Personen, die einen Suizidversuch unternommen haben, unbefugt speichert. In jedem meiner bisher abgegebenen Tätigkeitsberichte habe ich auf die Problematik aufmerksam gemacht. Nun kann ich berichten, daß der Senat im Januar 1986 beschlossen hat, auf die Speicherung dieser Daten in Zukunft zu verzichten und die zur Zeit noch gespeicherten Hinweise zu löschen. Allerdings ist darauf hinzuweisen, daß die Daten über Suizidversuche in den polizeilichen Auskunftssystemen nicht gesondert abrufbar sind, so daß die Löschung nur bei Gelegenheit eines Zugriffs aus anderem Grund auf einen entsprechenden Datensatz, spätestens aber nach Ablauf der in den KpS-Richtlinien vorgesehenen Aufbewahrungsdauer von 5 Jahren vorgenommen werden kann. (Im Gegensatz zur Polizei bin ich allerdings der Auffassung, daß diese Daten gem. § 15 Abs. 4 HmbDSG spätestens nach 4 Jahren zu löschen sind.) Bei dieser Sachlage ist davon auszugehen, daß erst im März 1991 die Systeme endgültig entsprechend dem Senatsbeschluß bereinigt sind.

5.8.7 Speicherung von AIDS-Infektionen

Seit einiger Zeit wird darüber beraten, inwieweit bekanntgewordene AIDS-Infektionen in polizeiliche Auskunftssysteme eingestellt werden sollen.

Die Behörde für Inneres will dabei nach Abstimmung mit mir auf allgemeine Hinweise oder Vermerke in Dateien oder KpS-Beständen verzichten. Lediglich bei Fahndungsausschreibungen soll ein Hinweis auf Ansteckungsgefahren und die Warnung vor Blutkontakt erfolgen, wenn

— die gesuchte Person aufgrund eines Hinweises von amtlicher Stelle als Träger des AIDS-Erregers gilt oder

— die gesuchte Person gegenüber amtlichen Stellen glaubhaft erklärt hatte, Träger dieser Erregers oder daran erkrankt zu sein
und

— die gesuchte Person nach amtlichen Erkenntnissen zur Gewalttätigkeit neigt.

Ich habe zusätzlich vorgeschlagen, diese Hinweise nur bei Fahndungsausschreibungen zum Zweck der Festnahme aufzunehmen, da eine Fahndung, die nur eine Aufenthaltsermittlung oder die polizeiliche Beobachtung zum Gegenstand hat, einen Blutkontakt von vornherein nicht erwarten läßt. Dazu lag mir die Stellungnahme der Behörde für Inneres bei Redaktionsschluß dieses Berichts noch nicht vor.

5.8.8 Polizei in der Zentralambulanz für Betrunkene (ZAB)

Im Mai des Berichtsjahres habe ich die ZAB datenschutzrechtlich geprüft (vgl. 5.12.7.4). Dabei habe ich festgestellt, daß dort ständig ein Polizeibeamter Dienst verrichtet.

Die ZAB ist eine am 15. August 1974 eingerichtete Außenstelle des Hafenkrankenhauses. Sie dient nach der Dienstanweisung für Einrichtung und Betrieb der ZAB in der Fassung vom 10. September 1984 — KL/K 243/582 — 20.49/3 — ausschließlich der zeitlich begrenzten Unterbringung von betrunkenen Personen, verbunden mit einer ärztlichen Untersuchung und Überwachung.

Nach dieser Dienstanweisung obliegt dem in der ZAB tätigen Polizeibeamten der Schutz des Arztes, der Pflege- und Reinigungskräfte sowie der in Gewahrsam befindlichen Personen vor tätlichen Angriffen. Nach der „Dienstanweisung für den Polizeiposten der Zentralambulanz" vom 5. August 1974 — Po 42/20.01-50 — ist klargestellt, daß diese Schutz- und Ordnungsfunktionen in erster Linie im Wege der Amtshilfe für das Personal der Gesundheitsbehörde erfüllt werden. Darüber hinaus hat der Polizeibeamte bei konkretem Verdacht auf strafbare Handlungen die notwendigen polizeilichen Maßnahmen einzuleiten und in den Fällen, in denen die Polizei bei der Einlieferung nicht beteiligt war, eine Überprüfung durch Nachfrage über POLAS und INPOL durchzuführen.

Ich halte die Erhebung von Identifizierungsdaten und deren Abgleich mit polizeilichen Auskunftssystemen von allen Patienten der ZAB für rechtswidrig. Insbesondere für Patienten, die nicht von der Polizei als „hilfslose Personen" aufgegriffen und zur ZAB gebracht wurden, gibt es für derartige polizeiliche Maßnahmen keine gesetzliche Grundlage. Darüber hinaus ist eine derartige Verwendung von Patientendaten mit dem vom Bundesverfassungsgericht geforderten Zweckbindungsgebot unvereinbar. Der davon betroffene Anteil der Patienten liegt nach Auskunft des in der ZAB ständig anwesenden Oberpflegers bei etwa 50%.

Mit Schreiben vom 23. Mai 1986 habe ich die Behörde für Inneres um Stellungnahme gebeten. Obwohl mir im Laufe des Jahres ständig schriftlich und mündlich eine Stellungnahme (teilweise mit Nennung konkreter Termine) zugesagt wurde, lag sie mir bei Redaktionsschluß zu diesem Bericht immer noch nicht vor.

Ich würde dies nicht berichten, wenn es sich dabei um einen Einzelfall handelte. Ich habe jedoch feststellen müssen, daß sowohl die Behörde für Inneres als auch die Gesundheitsbehörde (vgl. 5.12.7.3 und 5.12.7.4) meine Anfragen zeitweilig so schleppend beantworten, daß ich nicht ausschließen kann, daß auf diese Weise meine Arbeit behindert werden soll. Künftig werde ich in vergleichbaren Fällen von meinem Beanstandungsrecht Gebrauch machen.

5.8.9 ZEVIS

In meinen letzten drei Tätigkeitsberichten (2. TB, 3.10.6.3, S. 89 f; 3. TB, 3.9.2, S. 85 ff; 4. TB, 4.9.6, S. 75 f) habe ich mich ausführlich mit der Einführung des zentralen Verkehrsinformationssystems (ZEVIS) beim Kraftfahrtbundesamt in Flensburg auseinandergesetzt und insbesondere auf die Gefahren hingewiesen, die mit der Anbindung von Polizei und Nachrichtendiensten entstehen können. Mit der Einstellung der Arbeiten an den Entwürfen der sog. „Sicherheitsgesetze" wurde auch die insoweit in Aussicht genommene Änderung des Straßenverkehrsgesetzes nicht weiter verfolgt.

Mit Sorge habe ich nun beobachten müssen, wie die Koalitionsparteien am Ende der Legislaturperiode im Eilverfahren auch ZEVIS — nunmehr jedoch im Mantel der „Anti-Terror-Gesetze" — gesetzlich eingeführt haben, ohne daß dies in der Öffentlichkeit auf bemerkenswerten Widerstand gestoßen ist, obwohl allen mit der Materie Vertrauten bewußt war, daß die Bekämpfung des Terrorismus noch nie durch datenschutzrechtliche Beschränkungen beim Zugang zu Kraftfahrzeugdaten erschwert wurde.

Meine Kritik, die auch nach Verabschiedung der Gesetzesänderung nicht gegenstandslos geworden ist, will ich noch einmal zusammenfassen:

— Für verfassungsrechtlich fragwürdig halte ich, daß die Anknüpfung an den Straßenverkehr aufgegeben und die Erteilung von Auskünften an alle möglichen Behörden zu inhaltlich nicht näher bestimmten Zwecken bereits zum Speicherungszweck erhoben wurde.

— Gerade weil es — aus wohlerwogenen Gründen — kein Landesadreßregister gibt und die Polizei die kommunalen Melderegister zumeist noch nicht in direktem Abruf abfragen kann, wird dem zentralen Fahrzeugregister insbesondere mit Hilfe der P-Abfrage zwangsläufig die Funktion eines Ersatz-Bundesadreßregisters für den größten Teil der erwachsenen Bundesbevölkerung zuwachsen.

— Das besondere Risiko, das mit dem On-line-Zugriff der Polizei auf die Datenbestände des KBA verbunden ist, liegt darin, daß es der Polizei in wesentlich erweitertem Umfang technisch möglich sein wird, personenbezogene Kontrollen im Straßenverkehr durchzuführen und dies, ohne daß die betroffenen Bürger es bemerken müssen. Diese technischen Möglichkeiten wird die Polizei — wie alle bisherigen Erfahrungen zeigen, die bei der Beobachtung der polizeilichen Informationsverarbeitung gesammelt wurden — nach ihrem Verständnis von Effektivität auch ausnutzen. Kontrollmaßnahmen wie die in der Praxis immer häufiger vorkommende Überprüfung aller abgestellten Kraftfahrzeuge in der Umgebung einer Demonstration bzw. eines Versammlungslokals machen deutlich, wo die Polizei die Kontrolldichte erhöhen möchte.

— Besonders bedeutsam erscheint mir, daß die Polizei vor allem die heimlichen Kontrollen — ohne daß es zu einem direkten Kontakt mit dem betroffenen Bürger kommt — erhöhen kann, wenn eine schnelle zentrale Beantwortung aller Halteranfragen sichergestellt ist („Gitternetz"). Gerade die „H-Anfrage" ist hervorragend geeignet, Bewegungsbilder herzustellen.

— Gegenüber diesen technischen Möglichkeiten sind Rechtsgrundlagen für derartige Kontrollmaßnahmen allenfalls rudimentär vorhanden. Insbesondere Befugnisse zur heimlichen Halterfeststellung gibt es nicht. Die Vorschriften der StPO zur Errichtung von Kontrollstellen (§ 111) bzw. zur Identitätsfeststellung (§ 163b) knüpfen an das Vorliegen eines Tatverdachts an und gehen von einer offenen Vorgehensweise aus. Auch im Bereich der Gefahrenabwehr ist es äußerst zweifelhaft, ob heimliche Beobachtungen gestattet sind, ganz abgesehen davon, daß häufig die Voraussetzungen der polizeilichen Generalklausel nicht vorliegen dürften.

— Deshalb halte ich es nach wie vor für äußerst bedenklich, daß der Polizei erheblich erweiterte technische Kontrollmöglichkeiten gegeben werden, ohne daß der Gesetzgeber zuvor die Voraussetzungen dafür in der Strafprozeßordnung sowie in den Polizeigesetzen des Bundes und der Länder klar, eindeutig und nachprüfbar festgelegt hat.

— Dies gilt erst recht für die jetzt in einer Übergangsregelung des Straßenverkehrsgesetzes (!) eröffneten Befugnisse für Bundesnachrichtendienst und Militärischen Abschirmdienst.

5.8.10 Video-Überwachung von Parkhäusern

Anläßlich des Versuchs, in einem Parkhaus die Zahl der Autoradiodiebstähle durch Installierung einer Videoanlage zu senken, hatte ich mich mit der Frage zu befassen, ob

und unter welchen Umständen eine Überwachung durch Videokameras unter Datenschutzgesichtspunkten hinnehmbar ist. Ich bin dabei zu folgenden Ergebnissen gekommen:

Wenn Video-Überwachungen vorgenommen werden, um Kriminalität zu bekämpfen, aufzuklären, einzudämmen oder durch Abschreckung zu verhindern, so ist dagegen im Prinzip nichts einzuwenden. Ob dies im Einzelfall datenschutzrechtlich problematisch ist, hängt von der Ausgestaltung der Anlage, dem konkreten Zweck und anderen Faktoren wie insbesondere der Art der Beteiligung der Polizei ab.

In dem Versuch, den ich zu beurteilen hatte, sind mehrere Video-Kameras zeitweilig in einem Parkhaus installiert worden, um zu prüfen, ob durch diese Maßnahmen die gestiegene Zahl der kriminellen Delikte (Aufbrüche, Diebstähle, Beschädigungen) gesenkt werden kann. Elektronische Bewegungsmelder lösen die Kameras aus. Durch einen Videorecorder werden die Bewegungen dann aufgezeichnet. Die Kamerabilder sind gleichzeitig auf einem Monitor zu sehen. Daneben kann auf einem weiteren Monitor jede beliebige Kamera von Hand eingeschaltet werden. Der Betriebsraum ist nur zeitweilig durch Mitarbeiter der Parkhausbetreibergesellschaft besetzt.

Ich habe diesen Versuch für datenschutzrechtlich vertretbar gehalten, wenn folgende Bedingungen eingehalten werden:

— Die Video-Aufzeichnungen dürfen lediglich im Betriebsraum des Parkhauses stattfinden und müssen nach drei Tagen wieder gelöscht werden. Es kann somit sowohl eine Überwachung durch Mitarbeiter der Betriebsgesellschaft an den Monitoren als auch eine Videoaufzeichnung erfolgen, wenn die Aufzeichnungen nicht länger als drei Tage aufbewahrt werden.

— Den Benutzern des Parkhauses muß in geeigneter Weise deutlich gemacht werden, daß eine derartige Videoüberwachung stattfindet, damit sie entscheiden können, ob sie unter diesen Umständen das Parkhaus benutzen wollen.

— Nicht vertretbar ist ein Anschluß der örtlichen Polizeirevierwache mit oder ohne Aufzeichnungsmöglichkeit oder eine direkte Überwachung der Monitore im Betriebsraum des Parkhauses durch Polizeibeamte, denn dies wäre mit dem geltenden Polizeirecht nicht vereinbar. Zur Gefahrenabwehr wäre ein Anschluß der Polizei auch nach ihrer eigenen Einschätzung nicht geeignet, da sie nicht rechtzeitig am Tatort sein könnte, um die Tatausführung zu verhindern. Zur Strafverfolgung ist ein direkter Anschluß der Polizei nicht erforderlich, da sie sich von der Parkhaus-Betriebsgesellschaft die Aufzeichnungen besorgen kann, die sich als Beweismittel für konkret angezeigte Straftaten ohne Beschränkung auf Autoradiodiebstähle eignen. Die Betriebsgesellschaft darf dann allerdings auch nur die Aufzeichnungen an die Polizei herausgeben, die zur Aufklärung konkreter Straftaten notwendig sind. Darüber hinaus darf die Polizei jedoch keinen Zugang zu den Monitoren oder den Video-Aufzeichnungen haben. Es wäre unzulässig, der Polizei eine flächendeckende Überwachung des gesamten Verkehrs im Parkhaus und die Nutzung der so gewonnenen Daten auch für andere Zwecke zu ermöglichen.

5.8.11 Automation des Kraftfahrzeug-Zulassungswesens

Anfang November 1986 hat eine bei der Behörde für Inneres angesiedelte Lenkungsgruppe für das Projekt „Automation Kraftfahrzeug-Zulassungswesen" ihre Arbeit aufgenommen. Ich beabsichtige, die Arbeit der Gruppe in allen Phasen zu beobachten und mit Anregungen zu begleiten. Durch die Behörde für Inneres ist eine ständige und umfassende Information zugesichert.

5.9 Verfassungsschutz

Wie schon in den vergangenen Jahren (vgl. 3. TB, 3.10.5, S. 92; 4. TB, 4.10.8, S. 88) habe ich mich auch im Berichtsjahr mit der Frage auseinandersetzen müssen, wie die

in allen Datenschutzgesetzen inhaltlich gleich geregelten Auskunftsrechte der Bürger gegenüber dem Verfassungsschutz mit geltendem Verfassungsrecht in Einklang zu bringen sind.

Anknüpfungspunkt in diesem Jahr war die mir und den anderen Datenschutzbeauftragten vom Bundesverfassungsgericht eingeräumte Gelegenheit, zu einem Vorlagebeschluß des Verwaltungsgerichts Schleswig Stellung zu nehmen. Das Verwaltungsgericht ist der Auffassung, die Vorschriften des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG) über die Auskunftsmöglichkeiten gegenüber den Verfassungsschutzbehörden verstießen gegen Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG (informationelles Selbstbestimmungsrecht) und Art. 19 Abs. 4 GG (Rechtsweggarantie), weil sie das Recht auf informationelle Selbstbestimmung beeinträchtigten, ohne daß die Rechtmäßigkeit dieser Beeinträchtigung im Einzelfall gerichtlich effektiv kontrolliert werden könnten.

Die in Frage gestellten Vorschriften des § 14 Abs. 1 bis 3 LDSG haben folgende Fassung:

§ 14 Abs. 1 S. 1:

Dem Betroffenen ist auf Antrag durch die speichernde Stelle Auskunft über die zu seiner Person gespeicherten Daten zu erteilen.

§ 14 Abs. 2 Nr. 1a:

Abs. 1 gilt nicht für die Verfassungsschutzbehörden . . .

§ 14 Abs. 3:

Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit und Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteil bereiten würde,
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen,
4. die Auskunft sich auf die Übermittlung personenbezogener Daten an die in Abs. 2 Nr. 1 genannten Behörden bezieht.

§ 14 HmbDSG und § 13 BDSG enthalten wortgleiche Bestimmungen. Gegenüber dem Bundesverfassungsgericht habe ich mich wie folgt geäußert:

Der in § 14 LDSG-SH normierte Auskunftsanspruch ist verfassungsrechtlich unmittelbar Inhalt des aus Art. 1 und 2 GG abgeleiteten Rechts auf informationelle Selbstbestimmung, denn es wäre mit diesem Recht eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Gleichzeitig stellt er — neben der Beteiligung unabhängiger Datenschutzbeauftragter — eine wesentliche verfahrensrechtliche Schutzvorkehrung gegen die unberechtigte Speicherung und Zweckentfremdung personenbezogener Daten dar.

Allerdings ist das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet. Der einzelne muß Einschränkungen seines Rechts auf informationelle Selbstbestimmung — und damit auch Einschränkungen seines Auskunftsanspruchs — im überwiegenden Allgemeininteresse hinnehmen. Diese Beschränkungen bedürfen jedoch (verfassungsmäßiger) gesetzlicher Grundlagen, aus denen sich Voraussetzungen und Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen. Ferner hat der Gesetzgeber den mit Verfassungsrang ausgestatteten Grundsatz der Verhältnismäßigkeit zu beachten. Der allgemeine Freiheitsanspruch des Bürgers gegenüber dem Staat darf von der öffentlichen Gewalt nur soweit beschränkt werden, als es zum Schutz öffentlicher Rechte unerläßlich ist.

Danach dürfte § 14 Abs. 3 LDSG-SH Ausprägung des Grundsatzes sein, daß Einschränkungen im überwiegenden Allgemeininteresse hinzunehmen sind. Gleichwohl stellt sich — insbesondere im Hinblick auf § 14 Abs. 3 Nr. 4 LDSG-SH — die Frage, ob es verfassungsrechtlich geboten und mit dem Grundsatz der Verhältnismäßigkeit vereinbar ist, in den dort genannten Fällen die Auskunftserteilung gesetzlich zu verbieten. Nach meiner Auffassung darf bei Vorliegen eines der Tatbestände des § 14 Abs. 3 LDSG-SH der Verwaltung nur das Recht eingeräumt werden, die Auskunft zu verweigern. Ein solches Auskunftsverweigerungsrecht aus Gründen des öffentlichen Geheimhaltungsinteresses hat in der Rechtsordnung Vorbilder und kann den Grundsätzen des § 99 Abs. 1 Satz 2 VwGO entnommen werden.

Erst eine Ausgestaltung des Rechts in dieser Weise würde die Prüfung ermöglichen, welches Gewicht dem rechtlich geschützten öffentlichen Geheimhaltungsinteresse zukommt und wie sich seine Schutzwürdigkeit im Einzelfall in der Abwägung mit dem Auskunftsinteresse des einzelnen darstellt. Nur so kann überzeugend geklärt und überprüft werden, welche Beschränkungen des Auskunftsrechts im Einzelfall zum Schutz öffentlicher Interessen unerläßlich sind.

Zur Gewährleistung mindestens einer verwaltungsinternen Überprüfung ist weiterhin zu fordern, daß die Pflicht zur Darlegung des öffentlichen Geheimhaltungsinteresses nicht bei der datenhaltenden Stelle, sondern bei der obersten Aufsichtsbehörde liegen muß. Eine solche Zuständigkeitsverteilung ist Ausdruck eines für das öffentliche Geheimhaltungsinteresse allgemein geltenden Rechtsgedankens. Er hat nicht nur vielfachen einfachgesetzlichen Niederschlag gefunden (§ 99 Abs. 1 S. 2 VwGO, § 96 StPO, § 62 Abs. 4 BBG), sondern auf ihn hat auch die höchstrichterliche Rechtsprechung mehrfach abgestellt (BVerfGE Bd. 57 S. 289; BVerwGE Bd. 49 S. 50). Nur so ist Gewähr geboten, daß die Sachkompetenz der obersten Aufsichtsbehörde in die Entscheidung über die Geheimhaltung einfließt und eine Überbewertung des Geheimhaltungsinteresses durch die Behörde, der die Geheimhaltung dienen soll, weitgehend ausgeschlossen wird.

Weiter müßte klargestellt werden, daß grundsätzlich über Vorgänge, die abgeschlossen sind, Auskunft zu erteilen ist. Selbst das Gesetz zur Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz — G 10 —) sieht in seinem § 5 Abs. 5 eine Mitteilungspflicht über die Beschränkungsmaßnahmen gegenüber den Betroffenen vor, sobald eine Gefährung des Zwecks der Beschränkung ausgeschlossen werden kann. Es ist unter keinem Gesichtspunkt ersichtlich, daß unmittelbare Eingriffe in die Grundrechte aus Art. 10 GG weniger schutz- und geheimhaltungsbedürftig sind als andere Tätigkeiten der Verfassungsschutzbehörden.

Neben dem derzeitigen § 14 Abs. 3 LDSG-SH hat die Vorschrift des § 14 Abs. 2 Nr. 1 LDSG-SH keine eigenständige verfassungsrechtliche Berechtigung mehr: § 14 Abs. 2 LDSG-SH wird — wie auch die entsprechenden Vorschriften der anderen Datenschutzgesetze — nach herrschender Auffassung so ausgelegt, daß die Entscheidung über ein Auskunftsersuchen im pflichtgemäßen Ermessen der ersuchten Behörde steht. Die ersuchte Behörde hat danach das Auskunftsinteresse des Betroffenen mit einem bestehenden Geheimhaltungsinteresse abzuwägen. Nur ein Geheimhaltungsinteresse von erheblichem Gewicht ist angesichts des — in das Recht auf informationelle Selbstbestimmung eingebetteten und deshalb mit Verfassungsrang ausgestatteten — Auskunftsrechts geeignet, ein überwiegendes Allgemeininteresse zu begründen, das die Beschränkung des Auskunftsrechts rechtfertigt. Gründe, die ein Geheimhaltungsinteresse von diesem Gewicht verursachen, hat der Gesetzgeber selbst schon enumerativ — und nach meiner Auffassung auch erschöpfend, wenn nicht gar abundant — in § 14 Abs. 3 LDSG-SH aufgeführt. Daneben sind nach meiner Auffassung keine Gründe erschtlich und denkbar, die eine Einschränkungen des Auskunftsrechts zulassen. Für eine zusätzliche Ermessensentscheidung bleibt deshalb kein Raum mehr.

Nach Art. 19 Abs. 4 GG steht den Bürgern der Rechtsweg gegen Maßnahmen der öffentlichen Gewalt zu. Dies beinhaltet das Recht, staatliche Informationseingriffe, wie die Erhebung, Speicherung, Weitergabe und sonstige Verwendung personenbezoge-

ner Daten gerichtlich überprüfen zu lassen. Art. 19 Abs. 4 GG soll einen lückenlosen umfassenden Rechtsschutz gewährleisten. Allerdings wird nicht nur das formelle Recht und die Möglichkeit, die Gerichte anzurufen, sondern auch die Effektivität des Rechtsschutzes gewährleistet. Der Bürger hat einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle. Insbesondere darf auch das Verfahrensrecht keine so hohen Hindernisse aufbauen, daß die Gefahr einer Entwertung der materiellen Grundrechtsposition entsteht.

Der so skizzierten Verfassungslage entspricht ganz sicher nicht die bisherige Praxis des Bundesamtes und der Landesämter für Verfassungsschutz, die die weit überwiegende Anzahl von Auskunftsersuchen ohne weitere Begründung und damit ohne die Möglichkeit effektiven Rechtsschutzes ablehnen. Von mir und anderen Datenschutzbeauftragten ist diese Praxis deshalb schon mehrfach kritisiert worden.

Auch § 14 Abs. 3 LDSG-SH würde gegen Art. 19 Abs. 4 S. 1 GG verstoßen, müßte er so ausgelegt werden, daß es der ersuchten Behörde gestattet wäre, durch einfachen Hinweis auf einen der dort geregelten Tatbestände ohne weitere Begründung ein Auskunftsersuchen abzulehnen. Möglicherweise käme aber auch eine verfassungsgemäße Auslegung von § 14 Abs. 3 LDSG-SH dergestalt in Betracht, daß der ersuchten Behörde (oder wie ich meine: der obersten Aufsichtsbehörde) eine Darlegungslast auferlegt wird, die die Entscheidungslage und den Abwägungsvorgang deutlich macht.

Zwar ist einzuräumen, daß die Gründe der Geheimhaltung hinsichtlich geheimhaltungsbedürftiger Tatsachen häufig nur allgemein benannt werden können, weil die konkrete Benennung der Gründe die Offenbarung der geheimzuhaltenden Tatsachen bedeuten könnte. Es entspricht aber der Rechtsprechung des Bundesverwaltungsgerichts, daß auch die allgemeine Benennung der Gründe — jedenfalls im Verfahren ihrer gerichtlichen Überprüfung — so einleuchtend dargelegt werden müssen, daß sie unter Berücksichtigung rechtsstaatlicher Belange noch als triftig anerkannt werden können. Danach genügt keinesfalls der Hinweis auf die Tätigkeit von Sicherheitsbehörden.

Die gerichtliche Kontrolle kann auch nicht durch die Einschaltung der Datenschutzbeauftragten ersetzt werden. Deren rechtliche Möglichkeiten sind beschränkt. Selbst wenn ein Datenschutzbeauftragter unzulässige Informationseingriffe des Verfassungsschutzes feststellte, dürfte er weder den Betroffenen davon unterrichten, worin die Verstöße im einzelnen bestehen, noch hätte er die Möglichkeit, eine Mängelbeseitigung beim Verfassungsschutz — im Konfliktfalle — durchzusetzen.

Es bleibt abzuwarten, wie das Bundesverfassungsgericht über die dringend klärungsbedürftigen Fragen an der Schnittstelle zwischen Geheimhaltungsbedürfnissen und der Wahrnehmung von Bürgerrechten entscheidet. Wie notwendig die Klärung der Verfassungslage ist, zeigt ein Blick in die geplante Zukunft des datenschutzrechtlichen Auskunftsanspruches. Der Entwurf zur Änderung des Bundesdatenschutzgesetzes, der gegenwärtig in der Diskussion ist, sieht sogar eine Verschlechterung der Rechtsposition des auskunftssuchenden Bürgers vor. Nach § 13 Abs. 4 des Entwurfs sollen die Verfassungsschutzbehörden generell die Ablehnung von Auskunftserteilungen nicht mehr zu begründen brauchen.

Daneben wird die Entscheidung voraussichtlich eine beträchtliche Wirkung auf die zu schaffenden bereichsspezifischen Grundlagen für die Informationsverarbeitung der Verfassungsschutzbehörden, die auch in Hamburg noch fehlen, entfalten. Hier erwarte ich Anfang des kommenden Jahres einen ersten Gesetzesentwurf.

Bis solche Rechtsgrundlagen jedoch geschaffen sind, muß auch für das Landesamt für Verfassungsschutz festgelegt werden, welche Informationseingriffe für die Aufrechterhaltung der verfassungsmäßigen Ordnung (ohne gesetzliche Grundlage) unabdingbar sind.

5.10 Justizwesen

Im Berichtszeitraum hat sich — wie erwartet — die Diskussion über die Schaffung bereichsspezifischer Rechtsgrundlagen für die Informationsverarbeitung im Justizbe-

reich intensiviert. Das hängt — unabhängig von der Anstoßfunktion des Volkszählungsurteils des Bundesverfassungsgerichts — vor allem damit zusammen, daß in allen Justizbereichen die Möglichkeiten der elektronischen Datenverarbeitung zukünftig stärker genutzt werden sollen als bisher.

5.10.1 Zur Novellierung der StPO

Schon in meinem 4. Tätigkeitsbericht (4.11.1, S. 88) habe ich darauf hingewiesen, daß der Schaffung präziser Rechtsgrundlagen für Informationseingriffe im Rahmen strafverfahrensrechtlicher Ermittlungstätigkeit ebenso große Bedeutung beizumessen ist wie der Novellierung des Polizeirechts. Soweit die repressive Tätigkeit der Polizei angesprochen ist, handelt es sich, genau betrachtet, nur um die andere Seite der gleichen Medaille. In diesem Zusammenhang wird es notwendig sein, die vorhandenen polizeilichen und die geplanten staatsanwaltschaftlichen Informationssysteme unter den Gesichtspunkten der Erforderlichkeit, der Datenstrukturierung und der Verantwortlichkeiten zu überprüfen. Bei Zugrundelegung der gesetzlichen Prämisse, daß die Staatsanwaltschaft Herrin des Strafermittlungsverfahrens ist, liegt es nahe, polizeiliche Datenbestände strikter als bisher voneinander zu trennen und den unterschiedlichen polizeilichen Aufgaben zuzuordnen, wobei die Verantwortung für Datenbestände, die im Rahmen von Ermittlungsverfahren angelegt wurden, den Staatsanwaltschaften zu übertragen sind.

Nach Abstimmung mit den übrigen Datenschutzbeauftragten sind — zusammengefaßt — folgende Forderungen an die Novellierung der StPO zu stellen:

5.10.1.1 Generalklausel?

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 bisher eingehaltenen Prinzip des gesetzlich präzise beschriebenen Einzeleingriffs festgehalten und die Strafprozeßordnung auch zukünftig möglichst von Generalklauseln freigehalten werden. Eine solche Vorschrift kann allenfalls als engbegrenzte Auffangregelung in Betracht kommen.

5.10.1.2 Fahndungsmaßnahmen

Zentrale Bedeutung werden den Regelungen über Fahndungsmaßnahmen zukommen, denn bei der Fahndung nach Beschuldigten und Zeugen werden in erheblichem Umfang 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.

Die Fahndung nach dem Beschuldigten zum Zwecke der Festnahme kann in der Regel nur zugelassen werden, wenn ein vollziehbarer Haft- oder Unterbringungsbefehl 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).

Art und Umfang der zulässigen Fahndungsmaßnahmen nach dem Beschuldigten sind auf der Grundlage des Verhältnismäßigkeitsprinzips gesetzlich festzulegen.

Besondere Zurückhaltung ist bei der Fahndung von Zeugen angezeigt. Sie kann nur 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.

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 Rechts-

grundlagen für die Fahndung gestützt werden, sondern bedarf einer eigenständigen gesetzlichen Regelung.

5.10.1.3 Besondere Ermittlungsformen

5.10.1.3.1 Rasterfahndung

Bei der Diskussion um besondere Ermittlungsmethoden hat vor allem die sog. „Rasterfahndung", für die eine gesetzliche Grundlage ebenfalls fehlt, starke Beachtung gefunden. Dabei geht es um den Abgleich mit öffentlichen und privaten Datenbeständen nach bestimmten festgelegten Merkmalen. Zu fordern ist, daß die verschiedenen zulässigen Möglichkeiten von Datenabgleichen zu beschreiben und unter Berücksichtigung der dabei verwendeten Verfahren getrennt zu regeln sind.

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.

Der Einsatz der Rasterfahndung ist auf die Strafverfolgung bei besonders schwerwiegenden Straftaten, die enumerativ aufzuführen sind, zu beschränken. Den Straftatenkatalog des § 100a StPO (80 Straftaten) halte ich für zu weitgehend. Die Rasterfahndung sollte wegen ihrer weitreichenden Wirkung nur durch ein Gericht angeordnet werden.

Die Herausgabe von Datenbeständen darf nur verlangt werden, wenn die 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.

Zeigt sich, daß der Zweck eines Abgleichs nicht erreicht werden kann, ist die Rasterfahndung abzubrechen und alle im Zusammenhang mit der Maßnahme angefallenen Unterlagen sind sofort zu vernichten. Nach Durchführung des Abgleiches sind angefallene Unterlagen, die für die weiteren Ermittlungen nicht mehr erforderlich sind, umgehend zu vernichten. Die Daten und Unterlagen über Betroffene, gegen die nach konventioneller Ermittlung keine weiteren Verdachtsmomente festgestellt werden können, sind ebenfalls unverzüglich zu vernichten.

Die durch die Rasterfahndung gewonnenen Daten dürfen nur für das Verfahren genutzt werden, für das die Maßnahme angeordnet wurde. 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 nur durch ein Gericht angeordnet werden.

Die nach Durchführung des Datenabgleichs von gezielten Ermittlungsmaßnahmen betroffenen Personen sind hiervon zu unterrichten, sobald dies ohne Gefährdung des Untersuchungszweckes geschehen kann.

5.10.1.3.2 SPUDOK's

Automatisierte Dateien, die zur Unterstützung strafrechtlicher Ermittlungsverfahren durch temporäre Dokumentation und Recherche von Hinweisen, Ermittlungsergebnissen oder Spuren im weitesten Sinne in beliebigere 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 Sachverhaltes 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.

5.10.1.3.3 Polizeiliche Beobachtung

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 (engerer Katalog als Rasterfahndung) begangen oder ihre Begehung in strafbarer Weise versucht 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.

5.10.1.3.4 Planmäßige Observation

Auch die Informationserhebung im Rahmen der planmäßigen Observation muß gesetzlich geregelt werden. 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.

5.10.1.3.5 Einsatz technischer Mittel

Der Einsatz technischer Mittel zu Zwecken der Strafverfolgung ist ebenfalls zu regeln, da hierin ein zusätzlicher Eingriff in das informationelle Sebstbestimmungsrecht liegt. Die Verwendung von Abhörgeräten und die heimliche Aufnahme des in der Öffentlichkeit gesprochenen Wortes auf Tonträger ist nur zulässig, wenn dies zur Aufklärung einer in § 100a StPO bezeichneten Straftat 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 noch engeren Voraussetzungen als die Anordnung der Hausdurchsuchung zulässig.

5.10.1.3.6 Verdeckte Ermittler und V-Leute

Die Erhebung von Informationen durch Informanten gegen die Zusicherung der Vertraulichkeit oder durch den Einsatz von V-Personen und verdeckten Ermittlern ist rechtspolitisch besonders umstritten. Zum Schutze des Betroffenen sind Voraussetzungen und Inhalt des verdeckten Tätigwerdens der Ermittlungsorgane gesetzlich ge-

nau zu beschreiben, und 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) vorzusehen.

Die Entscheidung über den Einsatz von V-Personen sowie verdeckten Ermittlern hat die Staatsanwaltschaft zu treffen.

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 verdeckten Ermittler gewonnenen Ersterkenntnisse (sog. „Basisermittlungen") durch eigene weitere Ermittlungen 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.

5.10.1.3.7 Überwachung von Post und Telefon, Durchsuchung von Dritten und Verwertungsverbote

Gemäß § 101 Abs. 1 StPO sind die Beteiligten von Maßnahmen, die zur Überwachung des Postverkehrs (§§ 99, 100 StPO) und des Fernmeldeverkehrs (§§ 100a, 100b 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 sind hierzu ferner Löschungsbestimmungen und Verwertungsverbote aufzunehmen. Die bei der Gelegenheit der Telefonüberwachung gewonnenen Erkenntnisse können nicht uneingeschränkt, sondern ausdrücklich nur zur Verfolgung von Katalogstraftaten nach § 100a StPO verwertet werden. Die Voraussetzungen von Zweckdurchbrechungen müssen genau beschrieben werden.

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 verwert ist, ausgeschlossen wird.

5.10.1.4 Erkennungsdienstliche Behandlung

Die Befugnis zur erkennungsdienstlichen Behandlung im § 81b 1. Alternative StPO ist zu präzisieren und im Verhältnis zu § 163b StPO normenklar abzugrenzen. § 81b 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.

5.10.1.5 Straßenkontrollen

In § 111 Abs. 3 StPO (Straßenkontrollen) ist deutlicher darauf hinzuweisen, daß für § 111 StPO die Regelung von § 163b Abs. 2 StPO gilt, wonach Nichtverdächtige nicht gegen ihren Willen erkennungsdienstlich behandelt werden dürfen.

5.10.1.6 Datenspeicherung durch die Staatsanwaltschaft

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.

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. Gesetzlich ist auch zu regeln, ob und ggf. welche der im Rahmen der Strafverfolgung angefallenen Unterlagen bei der Polizei verbleiben dürfen.

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 Staatsanwaltschaften erforderlich ist. Das Ersuchen um Datenweitergabe ist von der anfordernden Staatsanwaltschaft schriftlich zu begründen.

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 Aufgabenerfüllungen erforderlich sind.

Anders als bei umfangreichen Informationssystemen ist bei zentralen Namensdateien und vergleichbaren 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 Dateiinhalts getroffen werden.

5.10.1.7 Aufbewahrung und Löschungsfristen

Auch die Aufbewahrung und Löschung der Daten der Strafjustiz in Akten und 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 und für Daten, die in automatisierten Dateien zu Fahndungszwecken (z. B. SPUDOK) geführt werden.

5.10.1.8 Akteneinsicht

Gesetzlich neu zu beschreiben sind die Akteneinsichtsrechte. 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 Einsichtsnahme von Dritten in Prozeßakten enge Grenzen gezogen. In keinem Fall dürfen über eine Einsichtnahme in Strafakten besondere Geheimhaltungsbestimmungen unterlau-

fen werden. Die Einsichtnahme in beigezogene Akten kann in der Regel nur mit Genehmigung der Ausgangsbehörde gestattet werden.

— 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.

— 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.

  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.

— 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. Im übrigen verweise ich auf meine Ausführungen unter 5.10.2.

5.10.1.9 Terminsankündigung, Zustellung und öffentliche Verhandlung

Auch bei Terminsankündigungen, Zustellungen und in öffentlicher Verhandlung werden personenbezogene Daten offenbart. Dafür sind gesetzliche Grundlagen erforderlich.

— Die öffentliche Bekanntgabe der persönlichen Daten eines Angeklagten durch Aushang der Terminsankündigung im Gericht ist auf Vor- und Zunamen 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 gem. § 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 we-

sentliche 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 dies beantragen. Dabei ist die Möglichkeit einer teilweisen Verlesung zu prüfen.

5.10.1.10 Auskünfte an die Medien

Besonders zu regeln sind Auskünfte durch die Justiz und die Polizei an die Medien. Eine 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. 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 für andere Verfahrensbeteiligte (wie Zeugen und Sachverständige) verfahren werden. Besonderer Schutz muß den Angehörigen gelten, die mit der Straftat nichts zu tun haben. Ein Anspruch der Presse auf Bildherausgabe sollte ausgeschlossen werden. In Strafverfahren gegen Jugendliche und Heranwachsende überwiegt in der Regel das schutzwürdige private Interesse der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten.

5.10.1.11 Aussage- und Zeugnisverweigerung

Erweitert werden müssen die Aussage- und Zeugnisverweigerungsrechte und Beschlagnahmeverbote für die Träger von Berufsgeheimnissen. Zu berücksichtigen ist dabei auch der Schutz solcher Informationen, die Wissenschaftlern zu Forschungszwecken offenbart worden sind.

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 ferner 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 würde.

5.10.2 Erstes Gesetz zur Verbesserung der Stellung des Verletzten im Strafverfahren

Ein weiteres datenschutzrechtlich relevantes Gesetzesvorhaben im Bereich des Strafrechts ist das „Erste Gesetz zur Verbesserung der Stellung des Verletzten im Strafverfahren". Nach den Vorstellungen des Bundesministers der Justiz sollen damit die Informationsmöglichkeiten aller Verletzten — ungeachtet welcher Straftat sie zum Opfer gefallen sind — über den Stand des Verfahrens gegen die Täter verbessert werden. Allen Verletzten soll ein gesetzliches Recht auf Akteneinsicht und auf Mitteilung über Verlauf und Ausgang des Strafverfahrens eingeräumt werden. Besondere Bedeutung erhalten die geplanten Vorschriften im Zusammenhang mit der vorgesehenen Erleichterung der Durchführung des Adhäsions-Verfahrens (Verfolgung zivilrechtlicher Schadensersatzansprüche im Strafverfahren) sowie der Privat- und Nebenklage. Zutreffend hat der Bundesrat in seiner Stellungnahme (Anlage 2 zum Gesetzesentwurf der Bundesregierung, BT-Drs. 10/5305) darauf hingewiesen, daß die gesetzliche Regelung auch den schutzwürdigen Belangen und den informationellen Selbstbestimmungsrechten der Beschuldigten und Dritter, über die sich Erkenntnisse in den Verfahrensakten befinden, zu berücksichtigen hat.

Diesem Bedürfnis wird nach meiner Auffassung der von der Bundesregierung vorgelegte Gesetzesentwurf bisher nicht gerecht. Dies gilt vor allem für den Zeitraum des staatsanwaltlichen Ermittlungsverfahrens, in dem eine Vielzahl höchst sensibler Informationen über den Beschuldigten erhoben werden, von denen zum Teil noch nicht abzusehen ist, in welchem Umfang sie für spätere Entscheidungen (Erhebung einer An-

klage, Eröffnung des Hauptverfahrens) relevant sind. In diesem Stand des Verfahrens wäre deshalb ein generelles Einsichtsrecht nach meiner Auffassung ein unverhältnismäßiger Eingriff in die Rechte des Betroffenen und Dritter. Diesen Bedenken könnte dadurch Rechnung getragen werden, daß das Akteneinsichtsrecht des Verletzten den verschiedenen Verfahrensabschnitten angepaßt wird.

Während der Dauer des Ermittlungsverfahrens sollte die Akteneinsicht wegen der hier besonderes Gewicht beanspruchenden Unschuldsvermutung des Betroffenen und der Möglichkeit einer Einstellung des Verfahrens gem. § 170 Abs. 2 StPO generell nicht gestattet werden.

Während dieses Verfahrensabschnittes ist auch ein — die schutzwürdigen Belange des Betroffenen und Dritter überwiegendes — berechtigtes Interesse des Verletzten kaum denkbar. Deshalb sollte dem Verletzten ein Akteneinsichtsrecht erst nach der Abschlußverfügung der Staatsanwaltschaft eingeräumt werden.

Zu Recht weist aber der Bundesrat in seiner Stellungnahme darauf hin, daß es auch dann geboten ist, den Einblick in Strafakten auf das unumgänglich Notwendige zu begrenzen. Daher unterstütze ich den Vorschlag des Bundesrates, in den Fällen, in denen das Informationsinteresse des Verletzten nicht die Kenntnis der gesamten Strafakten erfordert, dieses Interesse durch Auskünfte oder kopierte Teile der Akten zu befriedigen. Eine solche Regelung würde i.ü. auch die Verantwortung der informationsgebenden Stelle für den Umgang mit den ihr zur Verfügung stehenden Daten und Informationen deutlich machen.

Noch nicht berücksichtigt scheinen mir die Besonderheiten der Strafverfahren gegen Jugendliche und Heranwachsende. Das Jugendstrafrecht ist seinem Charakter nach überwiegend Erziehungs- und Täterstrafrecht, da Art und Gewicht der strafrechtlichen Reaktion weniger durch die Tat, als vielmehr durch die Persönlichkeit des Täters bestimmt werden. Die Erforschung der Täterpersönlichkeit (vgl. § 43 JGG) spielt hier demzufolge eine sehr viel größere Rolle als beim herkömmlichen Erwachsenenstrafrecht und führt zu einer sehr viel umfangreicheren Ansammlung von personenbezogenen Daten in den Akten.

Für das formelle Jugendstrafrecht finden sich im Jugendgerichtsgesetz zwar einige besondere Verfahrensvorschriften, i.ü. gelten jedoch die Vorschriften des allgemeinen Verfahrensrechtes, soweit sie nicht ausdrücklich, etwa gem. §§ 79 ff. JGG, von der Anwendung ausgeschlossen sind (vgl. § 2 JGG). Die in Aussicht genommenen Akteneinsichtsrechte würden danach grundsätzlich auch im Jugendstrafverfahren in Anspruch genommen werden können. Nach meiner Auffassung besteht dafür in Jugendstrafverfahren jedoch kein Bedürfnis, da im Verfahren gegen Jugendliche gem. §§ 80, 81 JGG Privat- und Nebenklage sowie Adhäsions-Verfahren ausgeschlossen sind. Daher erscheint es unabdingbar, die Anwendung des neuen Rechts für die Verfahren gegen Jugendliche durch besondere Vorschrift — etwa im Rahmen des § 81 JGG — auszuschließen.

Ähnlich gestaltet sich die Rechtslage in Verfahren gegen Heranwachsende, auf die unter den Voraussetzungen des § 105 JGG materielles Jugendstrafrecht Anwendung findet. Zwar ist gem. § 109 Abs. 2 JGG i.V.m. § 81 JGG ein Adhäsions-Verfahren ausgeschlossen, Privat- und Nebenklage sind jedoch zulässig. Da sich aber auch hier das Verfahren an der Persönlichkeit des Täters orientiert (§ 109 Abs. 1 Satz 1 JGG i.V.m. § 83 JGG) und den Umfang der Ermittlungen (und damit die Sammlung spezifischer personenbezogener Daten) bestimmt, liegt im Vergleich zum normalen Erwachsenenstrafrecht hier ebenfalls eine erhöhte Schutzbedürftigkeit des Beschuldigten (sowie der Personen aus seinem sozialen Umfeld) vor. Dies müßte nach meiner Auffassung zu der Konsequenz führen, daß in diesen Verfahren das Informationsinteresse des Verletzten ausschließlich durch Auskünfte und fotokopierte Teile der Strafakten befriedigt wird.

5.10.3 Neues Informationssystem der Staatsanwaltschaften

Zurückgehend auf einen Beschluß der Generalstaatsanwälte und des Generalbundesanwaltes vom 29. November 1984 hat sich ein Ausschuß der Konferenz der Justizminister und -senatoren mit dem Aufbau eines besonderen länderübergreifenden staatsanwaltlichen Informationssystems (SISY) beschäftigt. Eine von dem Ausschluß eingesetzte Arbeitsgruppe hat vorgeschlagen, die Erfassung sämtlicher staatsanwaltlicher Verfahren in ein bundesweites Verbundsystem vorzunehmen.

Dieses Vorhaben ist kritisch und zurückhaltend zu beurteilen. Völlig unklar erscheint beim gegenwärtigen Stand der Beratungen der Bedarf für ein solches System. Die Arbeitsgruppe hat mit geschätzten ungesicherten Zahlen operiert. Von einer Bedarfsanalyse kann keine Rede sein. Vor allem wäre vor dem Aufbau eines weiteren bundesweiten Informationssystems zu prüfen, ob die vorhandenen Systeme — insbesondere die der Polizei, soweit es sich um Informationen handelt, die für Zwecke der Strafverfolgung gesammelt werden — für die Staatsanwaltschaften nutzbar gemacht werden können. Im übrigen gehe ich davon aus, daß eine Verwirklichung von SISY nicht in Betracht gezogen wird, bevor dafür verfassungsrechtlich hinreichende gesetzliche Grundlagen (z.B. in der StPO) geschaffen sind.

5.10.4 Mitteilungen in Straf- und Zivilsachen

Die Notwendigkeit der Schaffung gesetzlicher Grundlagen für die bisher in Verwaltungsanordnungen geregelten Mitteilungen in Straf- und Zivilsachen und die dabei zu beachtenden und zu regelnden Problembereiche habe ich ausführlich in meinem 4. Tätigkeitsbericht (4.11.2 und 4.11.3, S. 90/91) dargestellt.

Während der Abfassung dieses Berichts wurde mir nunmehr ein innerhalb der Bundesregierung noch nicht abgestimmter Entwurf des Bundesministers der Justiz für ein „Gesetz über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz)" zur Stellungnahme zugeleitet. Bei einer ersten Durchsicht habe ich zwar einige begrüßenswerte Ansätze und Verbesserungen, aber auch noch Defizite festgestellt. Der Entwurf ist vor allem durch eine enttäuschend geringe Regelungsdichte gekennzeichnet. Offenbar ist beabsichtigt, das neue Justizmitteilungsgesetz durch bloße Verwaltungsvorschriften auszufüllen. Dem könnte ich nicht zustimmen. Eine dezidierte Stellungnahme werde ich nach Abstimmung mit den anderen Datenschutzbeauftragten abgeben. In die weitere Gesetzesarbeit wird wohl auch die zu erwartende Entscheidung des Bundesverfassungsgerichts über eine anhängige Verfassungsbeschwerde gegen die Anordnung über Mitteilungen in Strafsachen einfließen müssen.

5.10.5 Schuldnerverzeichnis

In meinem 4. Tätigkeitsbericht (4.11.4.1, S. 91 ff.) hatte ich ausführlich über die Bemühungen berichtet, die Vorschriften über Auskünfte aus dem Schuldnerverzeichnis unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht neu zu regeln. Ich hatte auch dargestellt, welchen datenschutzrechtlichen Bedenken der vom Bundesminister der Justiz im Jahre 1985 vorgelegte Entwurf begegnet.

Der Bundesjustizminister hat sich nun im Laufe des Jahres 1986 entschlossen, in der ablaufenden Legislaturperiode keine Gesetzesnovelle mehr in den Bundestag einzubringen. Zur Begründung erklärte er, er habe zu seinem Bedauern zur Kenntnis nehmen müssen, daß für den Datenschutz zuständige Behörden seinen Vorschlag in entscheidenden Punkten ablehnen. Die von den Datenschutzbehörden kritisierten Punkte seien in den jahrelangen Diskussionen dieses Themas gründlich erörtert worden. Er habe sich davon überzeugen lassen müssen, daß Forderungen, wie sie die datenschutzrechtliche Seite jetzt wieder vorbringe, nicht zu verwirklichen seien.

Weiter erklärte der Bundesminister der Justiz, die ablehnende Haltung der für den Datenschutz zuständigen Stellen habe offensichtlich dazu geführt, daß auch die Wirtschaftskreise von den Diskussionsentwürfen wieder abrückten. Nachdem so von beiden Seiten — Datenschutz und Wirtschaft, die er durch seinen Kompromißvorschlag für eine angemessene Lösung der Problematik habe gewinnen wollen — die Entwürfe wieder in Frage gestellt worden seien, sehe er keine Chance mehr, in der auslaufenden Legislaturperiode noch eine gesetzliche Regelung durchzusetzen. Er werde seine Bemühungen gleichwohl mit Nachdruck fortsetzen und nehme in Aussicht, die Änderung des § 915 ZPO und die ergänzenden Regelungen im Rahmen einer umfassenden Novellierung des Zwangsvollstreckungsrechts zu verwirklichen, die für die nächste Legislaturperiode geplant sei.

Ich bedauere, daß der Bundesminister der Justiz sich durch die unterschiedlichen Meinungen zu seinen Entwürfen hat davon abhalten lassen, eine Änderung der rechtlich nicht mehr haltbaren alten Regelung der Schuldnerverzeichnisses in die Wege zu leiten. Ich hoffe, daß eine Anpassung an zeitgemäße Datenschutzanforderungen in der nächsten Legislaturperiode doch noch gelingen wird.

5.10.6 Einsicht in Gerichtsakten

Mehrfach während des Berichtsjahres mußte ich mich mit dem Problem beschäftigen, welchen nicht verfahrensbeteiligten Dritten Einsicht in Gerichtsakten gewährt werden kann. Dabei handelte es sich nicht um Akteneinsichtsrechte in laufenden Gerichtsverfahren, die von meiner Überwachung gem. § 20 Abs. 1 Satz 1 HmbDSG ausgenommen sind, sondern um Einsichtsbegehren nach Abschluß der Verfahren.

So wurde ich vom Verband der Scheidungsgeschädigten — VSBI e.V. — darauf aufmerksam gemacht, daß Akten der Familiengerichte bundesweit zu Forschungszwecken eingesehen wurden. Ich habe dazu die Auffassung vertreten, daß angesichts des sensiblen Datenmaterials in Familiengerichtsakten und der dazu ergangenen Rechtsprechung des Bundesverfassungsgerichts (BVerfGE Bd. 34 S. 209 ff.) einerseits und des Fehlens einer Forschungsklausel für Gerichtsakten andererseits bei der Abwägung der widerstreitenden Interessen im Rahmen von § 299 Abs. 2 ZPO oder § 34 FGG das wissenschaftliche Interesse im Regelfall zurückzutreten hat. Allerdings hätte ich gegen eine wissenschaftliche Verwertung anonymisierten Aktenmaterials bis zur Einführung einer Forschungsklausel schon heute keine Bedenken.

Eine Forschungsklausel müßte folgenden Anforderungen gerecht werden:

- 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.

Bei dem andersgelagerten Problem, wie vom Arbeitsgericht Aktenübersendungsgesuche der Arbeitsämter zu behandeln sind, habe ich mit dem Präsidenten des Arbeitsgerichts Übereinstimmung darin gefunden, daß die Übersendung vollständiger Prozeßakten im Regelfall ausscheidet, weil in ihnen eine Fülle von Daten — vor allem auch von Dritten — enthalten sind, die für evtl. Entscheidungen der Arbeitsämter im konkreten Einzelfall nicht von Bedeutung sein können. So ist es z. B. nach Abschluß eines Kündigungsschutzprozesses nicht erforderlich, daß das Arbeitsamt sämtliche Daten von Mitarbeitern eines Betriebes erhält, die im Rahmen der Kündigung in das soziale Auswahlverfahren einbezogen waren, wenn es nur erfahren muß, ob der Arbeitnehmer die ihm gegenüber ausgesprochene Kündigung veranlaßt hat, um daraus Konsequenzen für die Zahlung von Arbeitslosengeld zu ziehen. Eine solche Praxis setzt allerdings voraus, daß die Arbeitsämter bei entsprechenden Amtshilfeersuchen konkret die Daten und Schriftstücke bezeichnen, deren Kenntnis für ihre Entscheidung erforderlich ist.

Häufig richten Rechtsanwälte und Behörden an Gerichte auch die Bitte, Ausfertigungen bestimmter Urteile zu übersenden, um die darin geäußerten Rechtsansichten in anderem Zusammenhang zu verwerten. Es sollte für die Gerichte in diesen Fällen selbstverständlich sein, ausschließlich anonymisierte Ausfertigungen zu versenden. Kann wegen des Prozeßgegenstandes oder des mit der Anonymisierung verbundenen Arbeitsaufwandes eine hinreichende Anonymisierung nicht gewährleistet werden, kann nach meiner Auffassung eine Urteilsübersendung nur mit Zustimmung der Prozeßparteien in Betracht kommen.

Wie diese Beispiele zeigen, werden die Gerichte mit Akteneinsichtsbegehren aus verschiedensten Motiven konfrontiert. Ich werde deshalb im nächsten Jahr Kontakt zu den hamburgischen Gerichten aufnehmen, um eine möglichst einheitliche Praxis bis zur Verabschiedung bereichsspezifischer Rechtsgrundlagen zu erreichen.

5.10.7 Öffentliche Gerichtsverhandlungen und Datenschutz

Da Gerichtsverhandlungen und die Verkündung von Urteilen in der Regel öffentlich erfolgen, müsse man — so eine gelegentlich in Zuschriften an mich vertretene Auffassung — auch später die Daten erfahren können, die Gegenstand einer bestimmten Gerichtsverhandlung oder eines Urteils waren. Diese Ansicht ist verfehlt. Zweck des Öffentlichkeitsgrundsatzes von Gerichtsverhandlungen, der als Folge politischer Forderungen gegen die geheime Kabinettsjustiz entstanden ist, ist nämlich nicht die Publizität, sondern die Kontrolle des Verfahrens durch die Allgemeinheit. Öffentlichkeit bedeutet danach, daß im Rahmen der tatsächlichen Gegebenheiten des Verhandlungsortes die Möglichkeit des Eintritts für beliebige Zuhörer gewährleistet ist. Da sie ausschließlich der Verfahrenskontrolle dient, kann sie nicht zur Folge haben, daß nach Abschluß des Verfahrens Akteneinsicht zu gewähren oder Auskunft über die Prozeßbeteiligten zu erteilen ist.

5.10.8 Gruppengeschäftsstellen beim Amtsgericht

Eine Prüfung der Datensicherung bei den DV-Anwendungen in den Gruppengeschäftsstellen des Amtsgerichts hat gravierende Mängel ergeben, die unter 3.1.4.2 im einzelnen dargestellt sind. Eine Stellungnahme zu meinen Vorschlägen zur Beseitigung der Mängel liegt mir bisher noch nicht vor.

5.10.9 Notare und Datenschutz

Schon in meinem letzten Tätigkeitsbericht (4.11.5, S. 94) habe ich darauf hingewiesen, daß die hamburgischen Notare bislang ihrer Verpflichtung, die von ihnen geführten Dateien zu melden, nicht nachkommen. Die im letzten Tätigkeitsbericht erwähnte Bitte um Stellungnahme, die ich im September 1984 an die Notarkammer gerichtet habe, ist immer noch unbeantwortet, obwohl ich mehrfach schriftlich und fernmündlich an die Beantwortung erinnert habe. Die Justizbehörde, als Aufsichtsbehörde über die Notarkammer, befindet sich in gleicher Lage. Obwohl sie versucht hat, die Notarkammer mit

insgesamt sechs Schreiben zu einer Stellungnahme zu den datenschutzrechtlichen Problemen im Notarbereich zu bewegen, ist sie ohne Antwort geblieben.

In der Sache geht es um folgende Fragen:

— Sind die Notare als „sonstige öffentliche Stellen" im Sinne der Datenschutzgesetze anzusehen?

— Werden die Datenschutzgesetze durch das Berufsrecht der Notare verdrängt?

— Verletzen die datenschutzrechtlichen Meldepflichten die Verschwiegenheitspflicht der Notare aus § 18 BNotO?

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die Justizverwaltungen der Länder, die sich bisher geäußert haben (Baden-Württemberg, Berlin, Bremen, Niedersachsen und Nordrhein-Westfalen) und der Bundesminister der Justiz vertreten übereinstimmend die Auffassung, daß Notare als „sonstige öffentliche Stellen" anzusehen sind, die deshalb ihre Dateien zum Datenschutzregister zu melden haben, da auch die Verschwiegenheitspflicht aus § 18 BNotO der Meldepflicht nicht entgegensteht. Allenfalls besondere — von den Notaren zu beachtende — bereichsspezifische Datenschutzregelungen (wie z. B. § 51 BeurkG, § 203 Abs. 1 Nr. 3 StGB) sind danach als den Datenschutzgesetzen vorgehende Spezialnormen anzusehen.

Die Bundesnotarkammer sowie die Notarkammern der Länder, die bisher Stellung bezogen haben, vertreten in allen entscheidenden Punkten entgegenstehende Auffassungen.

Sollten die hamburgischen Notare weiterhin ihrer Meldepflicht nicht nachkommen, sähe ich mich veranlaßt, dies im nächsten Jahr gem. § 21 Abs. 1 Nr. 2 HmbDSG zu beanstanden.

5.11 Strafvollzug

5.11.1 Bereichspezifische Rechtsgrundlagen

In meinem letzten Tätigkeitsbericht (4.12) hatte ich auf erste Ansätze hingewiesen, die gesetzlichen Regelungsdefizite für die vielfachen Informationseingriffe im Bereich des Strafvollzugs zu beseitigen und das Strafvollzugsgesetz den verfassungsrechtlichen Anforderungen anzupassen.

Nach meinen Informationen sollte der im September 1985 vorgelegten „Entwurfsskizze" für datenschutzrechtliche Ergänzungen des Strafvollzugsgesetzes im April 1986 ein zweiter Entwurf folgen, auf dessen Grundlage ein erster Referentenentwurf erarbeitet werden sollte. Diese Arbeiten scheinen sich jedoch verzögert zu haben; jedenfalls bin ich über Fortschritte bisher nicht informiert worden.

5.11.2 Eingaben

Auch im Berichtsjahr 1986 habe ich viele Eingaben von Strafgefangenen erhalten, die sich von Informationseingriffen betroffen fühlten. In den abgeschlossenen Fällen war die Praxis der Vollzugsanstalten — abgesehen von den fehlenden Rechtsgrundlagen — jedoch nicht zu beanstanden. Bei der Überprüfung von Bezugspersonen im Rahmen der Gewährung von Urlaub an Strafgefangene (vgl. 5. TB, 4.12.2, S. 95) sollte das Strafvollzugsamt nach meiner Auffassung allerdings die schriftliche Einwilligung der Bezugspersonen für eine Überprüfung einholen; schon um nachweisen zu können, daß die dabei erforderlichen Informationseingriffe rechtlich abgesichert erfolgen.

5.11.3 Anforderungen von Anwaltsdaten durch den Generalbundesanwalt

Nachdem verschiedene Obergerichte die Ansicht geäußert haben, daß auf die anwaltliche Vertretung in Strafvollzugs- und Strafvollstreckungsangelegenheiten das Verbot

der Mehrfachverteidigung (§ 146 StPO) entsprechend anzuwenden sei, hat der Generalbundesanwalt die Justizverwaltungen aufgefordert, die Vollzugsanstalten zu veranlassen, ihm Namen und Anschriften derjenigen Rechtsanwälte mitzuteilen, die wegen terroristischer Gewalttaten und/oder wegen eines Vergehens nach § 129a StGB verurteilte Gefangene in Strafvollzugs- und Strafvollstreckungsangelegenheiten — auch in Untervollmacht — vertreten haben oder sich künftig als Vertreter melden. Er benötige diese Informationen zur Prüfung, ob in den von ihm geführten Verfahren die Voraussetzungen des § 146 StPO vorlägen.

Zur Stellungnahme aufgefordert, habe ich gegen dieses Begehren des Generalbundesanwalts Bedenken erhoben, da die regelmäßige Weitergabe der geforderten Daten das informationelle Selbstbestimmungsrecht der beteiligten Rechtsanwälte unzulässig verletzen würde. Im einzelnen lassen sich meine Bedenken wie folgt zusammenfassen:

— Zunächst ist in formalrechtlicher Hinsicht darauf hinzuweisen, daß für solche Datenübermittlungen eine — nach der Rechtsprechung des Bundesverfassungsgerichts erforderliche — gesetzliche Grundlage fehlt.

— Auch für eine Übergangszeit — bis zur Schaffung einer gesetzlichen Grundlage — kann die vom Generalbundesanwalt gewünschte Übermittlung nicht akzeptiert werden, da sie für die Prüfung der Voraussetzungen des § 146 StPO nicht erforderlich ist. Vielmehr besteht die Gefahr einer verfassungsrechtlich unzulässigen Datensammlung auf Vorrat. Um zu prüfen, ob im Einzelfall die Voraussetzungen des § 146 StPO für die Zurückweisung eines Verteidigers vorliegen, reicht es nach meiner Auffassung aus, den Rechtsanwalt selbst nach Tatsachen zu befragen, die eine unzulässige Mehrfachverteidigung begründen. Sollten Anhaltspunkte dafür bestehen, ob der Rechtsanwalt solche Fragen — unter Verletzung seiner allgemeinen Berufspflichten — unrichtig oder unvollständig beantwortet, so kommt eine einzelfallbezogene Nachfrage bei Vollzugsanstalten in Betracht.

Diese Auffassung, die von der Justizbehörde geteilt und in einem Schreiben der Justizsenatorin dem Generalbundesanwalt eingehend erläutert wurde, hat dieser als abwegig bezeichnet. Dies hat die Justizsenatorin in gebotener Form und Klarheit zurückgewiesen.

Der Vollständigkeit halber soll darauf hingewiesen werden, daß auch der Justizminister des Landes Nordrhein-Westfalen die Datenübermittlung mit gleicher Begründung abgelehnt hat.

5.11.4 AIDS im Strafvollzug

Angemessene Reaktionen auf HTLV-III-Infektionen sind nicht nur Gegenstand der allgemeinen gesundheitspolitischen Diskussion, sondern beschäftigen auch andere Träger der öffentlichen Verwaltung. So war insbesondere der Strafvollzug gefordert, sich darüber Gedanken zu machen, wie der Umgang mit HTLV-III-infizierten Strafgefangenen zu gestalten ist. Neben den konkreten Anforderungen an den Vollzugsablauf war dabei zu klären, unter welchen Voraussetzungen HTLV-III-Antikörper-Test durchgeführt und welche Personen/Institutionen im Falle positiver Testergebnisee informiert werden dürfen.

Sofort einig war ich mir mit dem Strafvollzugsamt darüber, daß HTLV-III-Antikörper-Tests nur auf freiwilliger Grundlage erfolgen können und daß positive Testergebnisse dann weitergegeben werden dürfen, wenn dafür das Einverständnis des Betroffenen vorliegt.

Bei der Frage der Unterrichtung von Stellen und Personen innerhalb und außerhalb des Vollzuges gegen den Willen des Betroffenen ging es für das Strafvollzugsamt um den Schutz Dritter vor Infektionen bei der Anwendung unmittelbaren Zwangs und bei der Versorgung von Sport- und Arbeitsverletzungen.

Ich habe Zweifel daran, ob die Infektionsgefahren so hoch einzuschätzen sind, daß sie die Durchbrechung der ärztlichen Schweigepflicht ohne Einverständnis der Betroffe-

nen rechtfertigen können. Der Senat selbst geht davon aus, daß Infektionen regelmäßig über Sexualkontakte und den gemeinsamen Gebrauch von Infektionsnadeln bei Drogenabhängigen stattfinden. Ihm ist kein Fall bekannt geworden, wo das Virus durch eine gewaltsame Auseinandersetzung übertragen worden ist (vgl. Antwort des Senats vom 25. Oktober 1985 auf die Schriftliche Kleine Anfrage des Abg. Herrmann — GAL —, Bürgerschafts-Drs. 11/5103). Er mag dies allerdings auch nicht gänzlich ausschließen.

Vor diesem Hintergrund fällt zweierlei auf: Das in Strafanstalten offensichtlich bestehende Infektionsrisiko bei Sexualkontakten zwischen Strafgefangenenen wird faktisch nicht diskutiert. Dagegen wird das nur theoretisch bestehende Risiko der Infektion Bediensteter und anderer Betreuungspersonen besonders herausgestellt und zur Grundlage massiver Eingriffe in das Recht auf informationelle Selbstbestimmung gemacht.

Wenn ich mich gleichwohl mit den im folgenden dargestellten Informationswegen einverstanden erklärt habe, beruht dies auf der Annahme, daß die medizinischen Erkenntnismöglichkeiten über die Infektionsgefahren möglicherweise noch nicht abgeschlossen sind, und daß im Hinblick auf die sehr hohe Infektiosität, die das Virus besitzt, wenn es in die Blutbahn eingedrungen ist, jede Gefahr der Infektion möglichst ausgeschlossen werden muß. Darüber hinaus kann ich mich nicht der Tatsache verschließen, daß die Diskussion in der Öffentlichkeit weiterhin von Vorurteilen und Angst geprägt ist und deshalb eine möglichst weitgehende Aufklärung und Information der Vollzugsbediensteten und anderer Kontaktpersonen zur Aufrechterhaltung eines geordneten Vollzuges auch mit HTLV-III-infizierten Strafgefangenen für eine Übergangszeit notwendig erscheint. Das Strafvollzugsamt bleibt jedoch aufgefordert, anhand neuer medizinischer Erkenntnisse seine Informationspraxis ständig zu überprüfen, zumal diese ohne eine hinreichende gesetzliche Grundlage erfolgt. Dazu mögen auch die Diskussionen im „Hamburger Arbeitskreis AIDS — Untergruppe Strafvollzug —" beitragen, an denen sich meine Dienststelle ebenfalls beteiligt hat.

Im einzelnen habe ich mich mit der Weitergabe positiver Testergebnisse auch gegen den Willen des Betroffenen in folgenden Fällen einverstanden erklärt:

— Unterrichtung aller Bediensteter, die sich dienstlichen Kontakten mit dem Gefangenen nicht entziehen können.

— Unterrichtung von Vergewaltigungsopfern, wenn sich im Vollzug eine HTLV-III-Infektion des Täters herausgestellt hat und zu befürchten ist, daß der Täter das Opfer angesteckt haben könnte.

— Unterrichtung der Polizei bei der Fahndnung nach infizierten Gefangenen, wenn aufgrund konkreter Vorkommnisse im Vollzug oder aus anderen Erkenntnisquellen bekannt ist, daß der Gefangene zur Gewalttätigkeit neigt.

Eine Unterrichtung von Mitgefangenen, Betreuern und Arbeitgebern der Freigänger halte ich dagegen ohne Zustimmung des Betroffenen nicht für zulässig. Ich bin mir jedoch mit dem Strafvollzugsamt darüber einig, daß auf die infizierten Gefangenen verständnisvoll dahingehend eingewirkt werden soll, daß sie zumindest Gefangene, mit denen sie näheren Kontakt haben, und ihre Gruppenbetreuer informieren. Zum Zeitpunkt der Gespräche habe ich es auch für zulässig gehalten, die Genehmigung zur Teilnahme an besonders verletzungsgeneigten Freizeitbeschäftigungen (Sport, Steinmetz- und andere Bastelgruppen) im Einzelfall davon abhängig zu machen, daß der Gefangene sich offenbart, um Infektionsgefahren bei Sport- und Arbeitsunfällen zu vermeiden.

5.12 Gesundheitswesen

5.12.1 Entwurf eines Hamburgischen Krankenhausgesetzes

In meinem letzten Tätigkeitsbericht (4.13.1, S. 97) habe ich erwähnt, daß ich den zuständigen Behörden Vorschläge für eine normative Regelung der Datenverarbeitung im

Krankenhaus unterbreitet habe, um das auch hier bestehende Defizit an bereichsspezifischen Datenschutzregelungen beseitigen zu helfen.

Ein erster Referentenentwurf der Gesundheitsbehörde für ein Hamburgisches Krankenhausgesetz, der mir im Februar des Berichtsjahres zur Stellungnahme zugeleitet worden war, berücksichtigte diese Vorschläge noch nicht. Inzwischen hat jedoch die Gesundheitsbehörde meine Anregungen aufgegriffen. Erste Gespräche mit beteiligten Institutionen haben stattgefunden, in die auch eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zum Datenschutz im Krankenhaus einbezogen war. Diese Gespräche haben mir gezeigt, daß um das Verständnis für die Notwendigkeit von Datenschutzregelungen im Krankenhausbereich noch intensiv geworben werden muß. Das hat mich zunächst überrascht, da doch in der ärztlichen Schweigepflicht der Datenschutzgedanke mit langer Tradition verankert ist. Allerdings habe ich feststellen müssen, daß das Arztgeheimnis im Krankenhaus manchmal als Krankenhausgeheimnis verstanden wird. Dabei wird von mir nicht übersehen, daß eine sinnvolle Behandlung der Patienten natürlich auch die Information von Pflegepersonal und mitbehandelnden Ärzten erforderlich macht. Gleichwohl darf dabei nicht das Schutzgut des § 203 Abs. 1. Nr. 1 StGB aus dem Auge verloren werden.

Ich gehe davon aus, daß die Arbeiten an diesem wichtigen Gesetz im kommenden Jahr intensiviert werden.

5.12.2 Dienstanweisung für die Behandlung von Krankenakten und Röntgenbildern

Einen ersten Schritt in die einzuschlagende Richtung hat der Landesbetrieb Krankenhäuser mit dem „Entwurf einer Dienstanweisung für das Anlegen, die Aufbewahrung und die Herausgabe von Krankenakten und Röntgenbildern" unternommen. Die darin vorgenommene Verarbeitung neuerer Erkenntnisse über den Patientendatenschutz und den Versuch, Datenflüsse zu beherrschen und zu kontrollieren, begrüße ich. Neben verschiedener — noch verbesserungsfähiger — Einzelregelungen ist aber auch in diesem Entwurf das Problem der Weitergabe von Patientendaten von Arzt zu Arzt noch nicht befriedigend gelöst. So halte ich es für erforderlich, daß

— sowohl die Informationsweitergabe an vor- und nachbehandelnde Ärzte

— als auch die Beiziehung früherer Krankenakten

von der ausdrücklichen Einwilligung und Schweigepflichtsentbindung durch den betroffenen Patienten abhängig gemacht wird. Der Landesbetrieb will meine Anregungen berücksichtigen.

Im übrigen kann natürlich auch eine solche Dienstanweisung nicht das bestehende Regelungsdefizit beseitigen. Ich sehe sie deshalb als Übergangslösung an und habe empfohlen, die in dem übersandten Entwurf formulierten Vorstellungen des Landesbetriebs in die Arbeiten für ein Hamburgisches Krankenhausgesetz mit einzubringen.

5.12.3 Entwurf eines Hamburgischen Maßregelvollzugsgesetzes

Kurz vor Abschluß dieses Berichts hat mir die Gesundheitsbehörde einen überarbeiteten Entwurf für ein Hamburgisches Maßregelvollzugsgesetz übersandt, der auch umfangreiche Datenverarbeitungsvorschriften enthält, die gegenüber dem ersten Entwurf völlig neu formuliert wurden. Bei einer ersten Durchsicht habe ich positive Ansätze ausgemacht; eine umfassendere Bewertung werde ich Anfang des kommenden Jahres vornehmen.

5.12.4 Erste Erfahrungen mit dem Hamburgischen Krebsregistergesetz

Am 1. Januar 1985 ist das Hamburgische Krebsregistergesetz in Kraft getreten. In meinem zweiten Tätigkeitsbericht (3.16.2.2, S. 105 f.) hatte ich auf einige datenschutzrechtlich besonders bedeutsame Problembereiche hingewiesen. Insbesondere hatte ich auf

die Form der Einwilligung und die Vorschrift des § 2 Abs. 2 hingewiesen, nach der Patientendaten ausnahmsweise auch ohne Einwilligung zum Register gemeldet werden dürfen. Gleichzeitig hatte ich empfohlen zu überprüfen, ob in der Praxis Meldungen ohne Einwilligung tatsächlich die Ausnahme bleiben.

Die Bürgerschaft, die die Ausnahmevorschrift in der vom Senat vorgeschlagenen Form in das Gesetz aufgenommen hat, hatte in ihrer Sitzung vom 20./21. Juni 1984 gleichzeitig beschlossen, den Senat zu ersuchen,

> bis zum 1. Oktober 1986 über die Erfahrungen mit den Meldungen gemäß § 2 des Gesetzes zu berichten. Insbesondere ist darzustellen, ob die Einwilligung in die Meldung des Patienten nur schriftlich erteilt werden sollte. Es ist weiter darzustellen, in welchem Umfang von den Ausnahmeregelungen des § 2 Absatz 2 Gebrauch gemacht worden ist und ob sie sich bewährt hat.

Dieser Berichtspflicht ist der Senat mit einer Mitteilung an die Bürgerschaft vom 16. September 1986 (Bürgerschafts-Drs. 11/6876) nachgekommen. Er hat u.a. ausgeführt, daß

— der Berichtszeitraum zu kurz gewesen sei, um abschließend Erfahrungen bewerten zu können,

— eine Befragung von Ärzten ergeben habe, daß die mündliche Form der Patienteneinwilligung eindeutig gegenüber der Schriftform bevorzugt werde, weil
  - der behandelnde Arzt in einem Gespräch mit dem Patienten jeweils individuell auf dessen psychische Situation eingehen und in geeigneter Weise um die Datenweitergabe an das HKR bitten könne;
  - bei Anwendung der Schriftform im Nachgang in der Regel ein klärendes Gespräch notwendig sei, um die beim Patienten aufkommenden Fragen zu beantworten, und der zeitliche Aufwand insgesamt erhöht werde;
  - die Schriftform zu bürokratisch sei und daher eine höhere Ablehnungsquote erwartet werde;
  - vom Standpunkt der medizinischen Behandlung aus die mündliche Form vorzuziehen sei;

— in etwa 19 % der Fälle von der Ausnahmeregelung (Meldungen ohne Einwilligung) Gebrauch gemacht worden sei.

Gleichzeitig hat der Senat angekündigt, zum 1. Oktober 1986 erneut zu berichten.

Das begrüße ich, denn auch aus meiner Sicht geben die bisherigen Erfahrungen keine tragfähige Beurteilungsgrundlage ab. Zu dem Bericht des Senats habe ich folgendes anzumerken:

Nach wie vor bin ich der Auffassung, daß die Patienteneinwilligung grundsätzlich in schriftlicher Form vorliegen sollte. Sie schützt das Recht des Patienten auf informationelle Selbstbestimmung deshalb umfassender, weil er sich über den Inhalt seiner Erklärung bewußter ist und auch der Arzt die Aufklärungsnotwendigkeit besser erkennt. Zusätzlich wird im Arzt-/Patientenverhältnis Rechtsklarheit und Rechtssicherheit geschaffen. Das ist angesichts der Strafandrohung des § 203 Abs. 1 Nr. 1 StGB kein zu unterschätzender Vorteil. Die dagegen aufgeführten Argumente vermögen nicht zu überzeugen. So ist nicht ersichtlich, warum der zeitliche Aufwand beim schriftlichen Verfahren durch das klärende Gespräch erhöht wird, wenn zuvor als Vorteil der mündlichen Einwilligung hervorgehoben wird, daß der behandelnde Arzt in einem Gespräch individuell auf die psychische Situation des Patienten eingehen kann. Daß die Schriftform, die im übrigen in verschiedenen Bereichen der medizinischen Behandlung und auch in vergleichbaren Situationen (vgl. Registrierung von Dialysepatienten, 5.12.6.1) selbstverständlich geworden ist, zu bürokratisch und vom Standpunkt der medizinischen Beratung zurückzustellen ist, sind aus meiner Sicht nicht belegte Feststellungen.

Hinsichtlich der Meldungen ohne Einwilligung habe ich bei einem Übermittlungsanteil von nahezu 20 %, der sich auf die übermittelnden Ärzte sehr unterschiedlich verteilt,

erhebliche Zweifel, ob alle Beteiligten den Ausnahmecharakter von § 2 Abs. 2 HmbKrebsRG wirklich erkannt haben. Meines Erachtens sollte deshalb die Zeit bis zum nächsten Erfahrungsbericht auch für die Aufklärung der übermittelnden Ärzte genutzt werden.

Um die Zahl der Meldungen zum Krebsregister zu erhöhen, hat die Gesundheitsbehörde gleichzeitig ein Verfahren zur Einholung pauschaler schriftlicher Einwilligungen erprobt. Danach wird von allen Patienten, die in eines der dem Onkologischen Schwerpunkt angeschlossenen Krankenhäuser eingeliefert worden sind, unabhängig von der Einweisungsdiagnose die schriftliche Einwilligung zur Meldung an das Krebsregister erbeten. Dieses Verfahren stößt ebenfalls auf datenschutzrechtliche Bedenken.

Da die Einwilligungserklärung ausnahmslos von allen in die Krankenhäuser des Onkologischen Schwerpunktes eingelieferten Patienten unterschrieben werden soll, sind zunächst einmal zwei Patientengruppen zu unterscheiden; einerseits die Gruppe der Patienten, die mit einer Krebsdiagnose oder einem Verdacht auf Krebs eingeliefert werden und davon wissen; andererseits die Gruppe der Patienten, die mit gänzlich anderen Diagnosen oder als Unfallopfer eingeliefert werden.

Für die erste Gruppe kann die unterschriebene Einwilligungserklärung grundsätzlich als Einwilligung im Sinne von § 2 Abs. 1 Satz 1 HmbKrebsRG angesehen werden.

Das trifft leider für die zweite Gruppe der Patienten nicht zu. Eine wirksame Erklärung im rechtlichen Sinne setzt mindestens voraus, daß der Erklärende sich über den Inhalt der Erklärung bewußt ist. Bei Patienten, die gar nicht ahnen, daß sie an Krebs erkrankt sind oder sogar subjektiv davon überzeugt sind, es nicht zu sein, ist dieses Erklärungsbewußtsein nicht anzunehmen. Hinzu kommt, daß die Erklärung auch eine Entbindung von der ärztlichen Schweigepflicht beinhaltet und der Patient den Arzt kennen muß, den er von der Schweigepflicht entbindet, denn rechtlich gesehen gibt es nur ein Arztgeheimnis und nicht etwa ein „Krankenhausgeheimnis".

Aufgrund dieser Rechtslage ist zu fordern, daß spätestens dann, wenn die Krankenhausdiagnose eine Krebserkrankung ergibt, der Patient zumindest noch einmal mündlich dazu gehört werden muß, ob er an seiner Erklärung festhalten will. Dies sollte dokumentiert werden, ein Dokumentationsfeld könnte schon auf der Einwilligungserklärung vorgesehen werden.

Die Möglichkeit des § 2 Abs. 2 HmbKrebsRG bliebe hiervon allerdings unberührt.

Für das Verfahren ist weiterhin zu fordern, daß die Einwilligungserklärungen von Patienten, bei denen die Diagnose keine Krebserkrankung ergibt, spätestens zum Zeitpunkt der Entlassung zu vernichten sind. Keinesfalls dürfte von diesen Erklärungen anläßlich späterer Krankenhausaufenthalte Gebrauch gemacht werden. Darauf sind die Patienten hinzuweisen.

Die Erklärung selbst müßte neben der Aufklärung darüber, zu welchem Zweck die Daten weitergegeben werden, noch folgenden Anforderungen gerecht werden:

— Zunächst sollten die Patienten deutlich auf die Freiwilligkeit ihrer Erklärung und darauf hingewiesen werden, daß ihnen aus der Verweigerung weder rechtliche noch therapeutische Nachteile entstehen.

— Dazu gehört auch ein Hinweis auf die Möglichkeit des Widerrufs der Erklärung.

— Weiter müßte deutlich werden, daß die Erklärung in zeitlicher Hinsicht nur für den gegenwärtigen Krankenhausaufenthalt gelten soll und nicht bei späteren Behandlungen herangezogen wird.

— In sachlicher Hinsicht sollten die Patienten darauf hingewiesen werden, daß die Erklärungen spätestens bei der Entlassung vernichtet werden, wenn bis dahin eine Krebserkrankung nicht diagnostiziert wurde.

— Außerdem fordert das Recht auf informationelle Selbstbestimmung einen Hinweis auf die Möglichkeit der weiteren Übermittlung personenbezogener Daten gem. § 9 HmbKrebsRG.

— Letztlich sollte zum Schutz der Ärzte die Einwilligung mit der ausdrücklichen Entbindung von der ärztlichen Schweigepflicht verbunden sein.

Ich werde die Praxis der Krebsregistrierung in Hamburg auch weiterhin aufmerksam beobachten und in einem der nächsten Tätigkeitsberichte darauf zurückkommen.

5.12.5 Hamburgisches Apothekergesetz

Die Bürgerschaft hat inzwischen das Hamburgische Apothekergesetz beschlossen (verkündet am 23. September 1986, GVBl. S. 282), mit dessen Informationsverarbeitungsregelungen ich einverstanden bin. Insbesondere die Aufbewahrungs- und Löschungsvorschriften (§ 14 Abs. 1) passen sich in die bestehende Rechtsordnung ein. Sie entsprechen § 10 Abs. 3 HmbMG und teilweise § 15 Abs. 2 S. 3 und Abs. 3 HmbDSG.

5.12.6 Weitere Einzelprobleme

5.12.6.1 Patientenfragebogen der European Dialysis and Transplant Association (EDTA)

Schon 1985 war den Datenschutzbeauftragten bekannt geworden, daß Nierenabteilungen staatlicher Krankenhäuser, aber auch niedergelassene Ärzte Fragebogen mit detaillierten Angaben über namentlich genannte Dialyse-Patienten an die EDTA nach London übersenden, ohne daß von diesen Patienten Einwilligungserklärungen vorliegen. In Hamburg hat sich daran neben niedergelassenen Ärzten auch das Allgemeine Krankenhaus Heidberg beteiligt.

Bei der EDTA handelt es sich um eine seit 20 Jahren bestehende Europäische Fachgesellschaft auf dem Gebiet der Dialysebehandlung und Nierentransplantation. Eine der Schwerpunktaufgaben der EDTA seit 20 Jahren ist die Erstellung einer europaweiten Statistik. Darin werden alle Patienten erfaßt, die wegen terminalem Nierenversagen entweder mit Hämodialyse oder Transplantation behandelt werden müssen. Die EDTA-Statistik dient dem Zweck der Erforschung der Erkrankungsursachen, der Hauptkomplikationen und der Todesursachen bei Dialyse-Patienten und Transplantierten, der Verbesserung von Therapie-Schemata, der Überprüfung der Verträglichkeit von Fremdmaterialien sowie der Information von Patient und Arzt über prognostische Faktoren der Erkrankung. Sie kann darüber hinaus zur Bedarfsanalyse für Dialysisbehandlungseinrichtungen eingesetzt werden. Die Datensammlung, die inzwischen auf eine Anzahl von ca. 160.000 Krankheitsverläufe angewachsen ist, erfolgt zentral im Londoner St. Thomas-Hospital.

Nachdem die anliefernden Ärzte davon überzeugt werden konnten, daß die Datenübermittlung nur mit Einwilligung der betroffenen Patienten zulässig ist, wurde das Berichtsjahr dazu genutzt, in Zusammenarbeit mit Kliniken aus dem gesamten Bundesgebiet und den Datenschutzbeauftragten, eine Einwilligungserklärung als Grundlage der Datenweitergabe zu entwickeln, die das Interesse an der Erforschung der Nierenerkrankungen und die Persönlichkeitsrechte der betroffenen Patienten angemessen aufeinander abstimmt.

5.12.6.2 Diagnose-Statistik

Nach §§ 16 Abs. 4, 24 Abs. 2 der Verordnung zur Regelung der Krankenhauspflegesätze vom 21. August 1985 — BPflVO — (BGBl. I S. 1666 ff.) haben die Krankenhausträger seit dem 1. Januar 1986 im Rahmen ihres Leistungsnachweises eine anonymisierte Diagnosestatistik zu führen und erstmalig für die Pflegesatzverhandlungen im Jahre 1987 den Krankenkassen vorzulegen. Die Patienten werden von der Verwendung ihrer Daten für diese Statistik in der Regel nicht informiert. Ausdrückliche Einwilligungen werden nicht eingeholt. Ich habe es jedoch für vertretbar gehalten, konkludente Einwilligungen der Patienten anzunehmen, da die Statistik in einem weiteren Sinne für Abrechnungszwecke eingesetzt wird und die Patienten davon ausgehen müssen, daß

auch ein Teil der medizinischen Daten für die Abrechnung den Krankenhausverwaltungen zugänglich gemacht werden. Dabei ist jedoch folgendes zu beachten:

— Eine Offenbarung weiterer, in den §§ 16 Abs. 4 Satz 2 Nr. 1, 24 Abs. 2 BPflVO und der entsprechenden Anlage nicht vorgesehener Daten an die Krankenhausverwaltung ist nicht zulässig. Dies gilt insbesondere für Nebendiagnosen.

— Die offenbarten personenbezogenen Daten dürfen nur für die Erstellung der Diagnosestatistik verwendet werden. Eine konkludente Einwilligung der Patienten umfaßt allenfalls eine Offenbarung der medizinischen Daten gegenüber der Krankenhausverwaltung zu diesem Zweck. Keinesfalls dürfen die Daten der Krankenhausverwaltung für andere Zwecke zur Verfügung gestellt werden. Die Daten sind so schnell wie möglich zu anonymisieren.

— Sofern die Daten in einer anonymisierten Datei gespeichert werden und Rückschlüsse auf einzelne Patienten nicht mehr möglich sind, dürfen sie mit anderen, bereits in der Krankenhausverwaltung vorhandenen, Daten zu statistischen Zwecken nur zusammengeführt werden, wenn sich dadurch das Reidentifikationsrisiko nicht erhöht.

5.12.6.3 Berufsaufsicht über Ärzte der hamburgischen staatlichen Krankenhäuser

Geben Beschwerden oder geltend gemachte Schadensersatzansprüche von Patienten und deren Angehörigen sowie Eingaben von nicht-ärztlichen Mitarbeitern Anlaß zu der Vermutung, ein Arzt könne gegen die ärztliche Berufsordnung verstoßen haben, beabsichtigt die Gesundheitsbehörde, die für die Überwachung der ärztlichen Berufspflicht zuständige Ärztekammer Hamburg einzuschalten. Bei der Abstimmung einer entsprechenden Dienstanweisung habe ich die Auffassung vertreten, daß bei gleichzeitig beabsichtigter Übermittlung von Patientendaten dafür ebenfalls die Zustimmung der Patienten erforderlich ist. Die Gesundheitsbehörde hat dies bei der Formulierung der endgültigen Fassung der Dienstanweisung, die am 29. September 1986 in Kraft getreten ist, berücksichtigt.

5.12.7 Überprüfungen und Ergebnisse

5.12.7.1 AIDS-Beratungs- und Informationsstelle der Gesundheitsbehörde im Allgemeinen Krankenhaus St. Georg

Mit datenschutzrechtlichen Fragestellungen bei der Verwendung und Aufbewahrung personenbezogener Daten durch die AIDS-Beratungs- und Informationsstelle habe ich mich auf Bitte der dortigen Mitarbeiter befaßt. Hintergrund für diese Bitte war die Einschätzung, daß die Beratungsstelle die potentiellen Adressaten ihrer Angebote nur dann erreicht, wenn weitgehende Anonymität zugesichert werden kann, da in den Risikogruppen die Befürchtung besteht, daß — entgegen den Äußerungen der politisch Verantwortlichen — doch noch eine Meldepflicht für HTLV-III-Infektionen eingeführt wird. Die Wahrung der Anonymität der Betroffenen ist somit zur Voraussetzung der inhaltlichen Arbeit erhoben worden. Datenschutzrechtliche Probleme können so faktisch nicht entstehen:

— Einzelfallberatungen werden streng anonym durchgeführt. Im Beratungsregister wird lediglich durch entsprechende Zeichen vermerkt, ob eine männliche oder weibliche Person beraten wurde und wann die Beratung stattfand.

— Bei der Durchführung anonymer und kostenloser HTLV-III-Antikörpertests benutzt die Beratungsstelle für die Einsendung des Blutes Codes, deren Zusammensetzung auch den Testpersonen nicht mitgeteilt wird. Telefonische Auskünfte über Testergebnisse werden nicht erteilt; für Aufzeichnungen, die zur Zuordnung der Testergebnisse erforderlich sind, werden ebenfalls nur diese Codes verwendet. Datenschutzrechtlich ist dagegen nichts einzuwenden: Um die Gefahr von Verwechslungen der Testergebnisse bei Code-Übereinstimmungen noch weiter zu verringern, habe ich eine Verfeinerung der Codes angeregt.

— Soweit für einzelne Mitarbeiter aus der Berufsordnung für Ärzte eine Dokumentationspflicht folgt, habe ich geraten, zusammen mit der Gesundheitsbehörde und

der Ärztekammer Hamburg eine Lösung anzustreben, die einerseits die Anonymität der Betroffenen gewährleistet, andererseits aber die Mitarbeiter nicht der Gefahr von Berufspflichtverletzungen aussetzt.

5.12.7.2 Gesundheitsämter

In meinem 4. Tätigkeitsbericht (4.13.2, S. 103 ff.) habe ich ausführlich über die datenschutzrechtliche Prüfung eines Gesundheitsamtes berichtet. Der Senat hatte in seiner Stellungnahme zu meinem 4. Tätigkeitsbericht (Bürgerschafts-Drs. 11/5992) darauf hingewiesen, daß sich eine Arbeitsgruppe mit den angesprochenen Problemen beschäftigen solle. Ich habe daraufhin angeboten, mich an der Diskussion von Anfang an zu beteiligen, da erfahrungsgemäß die Veränderung von Arbeitsergebnissen — vor allem wenn sie von Arbeitskreisen vorgelegt werden — nur unter unverhältnismäßigem Aufwand zu erreichen ist. Darüber hinaus gehört die Beratung des Senats zu meinen gesetzlichen Aufgaben (§§ 18 Abs. 4 S. 1, 20 Abs. 1 S. 2 HmbDSG).

Leider hat die Verwaltung von meinem Angebot keinen Gebrauch gemacht. Ich wurde lediglich darüber unterrichtet, daß der Arbeitskreis eingerichtet wurde und einzelne Themenbereiche Arbeitsgruppen aus Vertretern der Gesundheitsbehörde und einzelner Gesundheitsämter zugewiesen wurden. Welche Themen behandelt werden und wer in den Arbeitsgruppen vertreten ist, wurde mir nicht mitgeteilt, so daß mir nicht ausgeschlossen scheint, daß schon auf der Ebene der Ermittlung der datenschutzrechtlich relevanten Problemstellungen Defizite entstehen können, die nachträglich die gesamte Arbeit des Arbeitskreises in Frage stellen können. So habe ich u.a. angefragt, ob beispielsweise die Schaffung zeitgemäßer bereichsspezifischer gesetzlicher Grundlagen auch Gegenstand der Beratungen sein soll, da dies nach dem Volkszählungsurteil des Bundesverfassungsgerichts ein dringliches Anliegen ist. Diese Anfrage wurde jedoch ebenso wenig beantwortet wie meine Anregung, wegen der aufgeworfenen Rechtsfragen auch die Rechtsdezernenten der Bezirksämter zu beteiligen. Nach allem muß ich annehmen, daß ich bewußt von den Problemen ferngehalten werden soll, was mit der Pflicht der Verwaltung, den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen (§ 20 Abs. 4 HmbDSG), nur schwer in Einklang zu bringen ist.

5.12.7.3 Allgemeines Krankenhaus Altona

Ebenfalls im 4. Tätigkeitsbericht (4.13.1.1, S. 97 ff.) hatte ich von einer Überprüfung der Abrechungsabteilung des Allgemeinen Krankenhauses Altona berichtet. Im Dezember 1985 hatte ich meinen Prüfbericht der Gesundheitsbehörde mit der Bitte um Stellungnahme bis zum 31. März 1986 zugeleitet. Obwohl mir im Laufe des Jahres mehrfach telefonisch und schriftlich zu bestimmten Terminen eine Stellungnahme von der Gesundheitsbehörde zugesagt wurde, liegt sie mir bis heute nicht vor.

5.12.7.4 Zentralambulanz für Betrunkene (ZAB)

Schon an anderer Stelle dieses Berichts (vgl. 5.8.8) habe ich berichtet, daß ich die ZAB Anfang Mai 1986 datenschutzrechtlich überprüft habe. Dabei habe ich eine Reihe von Mängeln festgestellt:

— So existierte in den Räumen der ZAB eine vollständige Namenskartei für den Zeitraum 1974-1984, ohne daß diese eine erkennbare oder benennbare Funktion hat (Die vollständigen Behandlungsbögen werden gesondert verwahrt).
— Ebenfalls noch vorhanden sind die vollständigen Aufnahme- und Abrechnungsbögen, die überwiegend nicht mehr benötigt werden.
— Letztere werden darüber hinaus im Hafenkrankenhaus, teilweise in offenen Regalen auf dem Flur — und damit praktisch jedem zugänglich — aufbewahrt.
— Wegen der datenschutzrechtlichen Probleme, die die ständige Anwesenheit eines Polizeibeamten mit sich bringt, verweise ich auf die Ausführungen unter 5.8.8.

Meinen Prüfbericht habe ich der Gesundheitsbehörde mit der Bitte um Stellungnahme bis zum 28. Mai 1986 zugeleitet. Auch in diesem Fall wurde eine Stellungnahme mehrfach mündlich und schriftlich angekündigt. Sie liegt ebenfalls bis heute nicht vor.

Ich verkenne nicht, daß in Teilbereichen der Verwaltung Engpässe auftreten, die Verzögerungen in der Bearbeitung mit sich bringen können. Auch ich kann — bei der gegenwärtigen personellen Ausstattung meiner Dienststelle — nicht alle Stellungnahmen zu den vorgesehenen Terminen abgeben. Gleichwohl kann ich die geschilderte Behandlung wichtiger datenschutzrechtlicher Anliegen nicht länger akzeptieren. Wie dazu unter 5.8.8 angekündigt, werde ich diese Praxis in vergleichbaren Fällen zukünftig förmlich beanstanden (§ 21 Abs. 1 HmbDSG).

Nach meiner Auffassung müßte der Senat darüber hinaus der allgemein nachlassenden Sensibilität für datenschutzrechtliche Belange durch gezielte Maßnahmen begegnen. Dazu gehört auch, daß der Senat und die einzelnen Senatoren die Verwaltung zu vertrauensvoller Zusammenarbeit mit der Dienststelle des Datenschutzbeauftragten veranlassen.

6. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

6.1 Bildschirmtext

6.1.1 Verdeckte Datenerhebung über Bildschirmtext

Die Überprüfung von hamburgischen Anbietern führte durchweg zu dem Ergebnis, daß die Regeln des Staatsvertrages über Bildschirmtext (StV-Btx) eingehalten worden sind.

In drei Fällen mußte ich allerdings tätig werden.

Diese Anbieter (darunter eine Btx-Agentur) haben gegen Art. 9 Abs. 8 Nr. 2 des StV-Btx verstoßen, indem sie sich auf mehreren Antwortseiten verdeckt mehr Daten übermitteln ließen, als der Absender auf seinem Bildschirm sehen konnte. Das konnte dadurch geschehen, daß für den Hintergrund dieselbe Farbe gewählt worden war wie für die Schrift. Auf diese Weise wurden das Datum, die sekundengenaue Absendezeit und die Teilnehmer-Nummer vom Absender unbemerkt und auch unbeabsichtigt übermittelt.

Nach Art. 9 Abs. 8 Nr. 2 StV-Btx hat der Anbieter die technischen und organisatorischen Maßnahmen zu treffen, die über die Vorschriften der Datenschutzgesetze hinaus erforderlich sind, um sicherzustellen, daß der Btx-Teilnehmer personenbezogene Daten nur durch eine eindeutige und bewußte Handlung übermitteln kann. Das bedeutet, daß zunächst die Vorschriften der Datenschutzgesetze einzuhalten sind. Darüber hinaus stellt der StV-Btx zusätzliche Anforderungen. Nach § 3 BDSG ist die Datenverarbeitung u.a. erlaubt, wenn der Betroffene eingewilligt hat, und zwar regelmäßig in schriftlicher Form. Wegen der Besonderheiten der Btx-Kommunikation verlangt Art. 9 Abs. 6 letzter Satz StV-Btx statt einer schriftlichen Einwilligung die Bestätigung durch den Betroffenen. Praktisch bedeutet das, daß der Betroffene bei der Datenerhebung durch Absenden einer Antwortseite die Ziffern 1 und 9 einzugeben hat. Daß für Btx eine andere Form der Einwilligungserklärung als angemessen angesehen wird, ändert nichts daran, daß die Einwilligung inhaltlich denselben Anforderungen genügen muß wie die Einwilligung nach § 3 Satz 2 BDSG. Unstreitig liegt eine wirksame Einwilligung nur vor, wenn der Betroffene nicht nur weiß, daß er personenbezogene Daten mitteilt, sondern auch, welche Daten er im einzelnen preisgibt.

Die hier verdeckt übertragenen Daten sind unstreitig personenbezogene Daten des Betroffenen. Sie sagen aus, welchen Btx-Anschluß der Betroffene zu welcher genauen Zeit für die Absendung der Antwortseite benutzt hat. Darüber hinaus können auch personenbezogene Daten eines weiteren Betroffenen, nämlich des Anschluß-Inhabers, übermittelt werden.

Im übrigen bin ich der Meinung, daß das Erheben des Datums, der genauen Uhrzeit und der Teilnehmer-Nummer für das Zusenden von abgefordertem Prospektmaterial überhaupt nicht erforderlich ist. Da der Benutzer eine konkrete postalische Anschrift angibt, die auch tatsächlich verwendet wird, kann man auf diese zusätzlichen Daten verzichten. Es werden also über den Rahmen des Art. 9 Abs. 6 S. 1 StV-Btx — nämlich über die Erforderlichkeit im konkreten Falle — hinaus Daten erhoben.

Die Btx-Agentur nannte verschiedene Gründe für die verdeckte Datenerhebung:

- Der Teilnehmer würde sich in der Menge der angezeigten Daten nicht mehr zurechtfinden.
- Die erhobenen Daten würden auch ohne die Übermittlung auf dieser Antwortseite dem Empfänger bekannt werden, da die Bundespost diese Angaben (allerdings mit Ausnahme der Teilnehmer-Nummer) im Rahmen des Mitteilungsdienstes ohnehin in der Übersicht der eingegangenen Mitteilungen an den Empfänger weitermeldet.
- Die erhobenen Daten seien nicht brisant.
- Die Ästhetik der Grafik leide unter überflüssigen Texten.

Sie war aber bereit, die beanstandeten Antwortseiten in einem angemessenen Zeitraum umzugestalten.

Einem anderen Anbieter war überhaupt nicht bewußt, daß er in verdeckter Form zusätzliche Daten erhob, weil er schon vor Inkrafttreten des Btx-Staatsvertrages eine Agentur mit der Erstellung des Btx-Programmes, aber nicht mit der ständigen Pflege beauftragt hatte. Da ihm nicht eine für das Erkennen der verdeckten Daten notwendige Buchstabentastatur, sondern nur eine Zifferntastatur zur Verfügung stand, konnte er die zusätzlich empfangenen Daten gar nicht auswerten.

Die beanstandeten Antwortseiten sind inzwischen in allen drei Fällen so geändert worden, daß die zusätzlichen Daten sichtbar sind und der Teilnehmer nun genau weiß, welche personenbezogenen Daten er absendet.

6.1.2 Home-banking mit Btx

Das Angebot der Kreditinstitute, Bankgeschäfte über Btx zu erledigen (home-banking), ist eine Angebotsart aus der breiten Btx-Angebotspalette, die ich im Berichtszeitraum näher untersucht habe. In die Untersuchung wurden die Angebote aller Kreditinstitute einbezogen, die in Hamburg als Btx-Anbieter auftreten. Zweck der Untersuchung war es, ein möglichst geschlossenes Bild über die technischen und organisatorischen Bedingungen des home-banking zu gewinnen, durch Analyse der ermittelten Fakten festzustellen, ob und ggf. welche Risiken sich daraus für den Datenschutz und das Vermögen der Kontoinhaber ergeben könnten, diese Risiken zu bewerten und schließlich aufzuzeigen, welche Fragestellungen sich im Hinblick auf die Geschäftsbedingungen der Banken (Beweislast und Verteilung des Risikos bei Mißbrauch, fehlerhafter Verarbeitung und Störungen im Ablauf) ergeben. Das Ergebnis der Untersuchung habe ich in einer umfangreichen und detaillierten Ausarbeitung dargestellt.

Es war meine Absicht, den Teil der Ausarbeitung, der im engeren Sinne das Angebot der Kreditinstitute zur Btx-Kontoführung betrifft, in meinem Tätigkeitsbericht darzustellen. Ich hatte dem Zentralen Kreditausschuß (ZKA) einen Entwurf des entsprechenden Kapitels zur Stellungnahme übersandt. Leider ist die Stellungnahme des Zentralen Kreditausschusses hier so spät eingetroffen, daß die darin aufgeworfenen Fragen — insbesondere nach der Gewichtung von Bedienungskomfort auf der einen und Sicherheit auf der anderen Seite — zwischen uns nicht mehr rechtzeitig geklärt werden konnten. Der ZKA hat im übrigen die Befürchtung geäußert, daß die Darstellung möglicher Angriffe auf das Sicherheitssystem potientielle Täter erst animieren könnte. Ein Gespräch hierüber wird erst im Januar 1987 möglich sein. Vom Ausgang wird es abhängen, wann und in welcher Form das Untersuchungsergebnis veröffentlicht wird.

6.2 Versandhandel

6.2.1 Ehegatten-Anfrage bei der SCHUFA

Die bereits in mehreren Tätigkeitsberichten (zuletzt 4. TB, 5.1, S. 117) dargestellte Problematik der SCHUFA-Anfragen des Versandhandels über die Ehegatten von Erstbestellern konnte nach langen Bemühungen im Berichtsjahr endlich gelöst werden.

Im letzten Jahr war bereits erkennbar geworden, daß der Versandhandel bereit war, meinen Bedenken zumindest zum Teil Rechnung zu tragen. Die von den Vertretern des Versandhandels vorgeschlagene Lösungsmöglichkeit (vgl. 4. TB, 5.1, S. 117) wäre bereits eine wesentliche Verbesserung gewesen, hätte jedoch auch einige datenschutzrechtliche Probleme ungelöst gelassen. Ich habe deswegen auf eine Lösung gedrängt, die auch die verbleibenden Restrisiken beseitigt.

Eine solche Lösung konnte nunmehr gefunden werden. Der Versandhandel hat nach Bewertung der umfangreichen Verbesserungen seiner internen Bonitätsprüfungssysteme die Entscheidung getroffen, auf die generelle SCHUFA-Anfrage über die Ehegatten von Erstbestellern zu verzichten. Künftig wird nur noch in Einzelfällen und entweder mit Einwilligung oder nach sorgfältiger Abwägung der berechtigten Interessen des Ver-

sandhandels mit den schutzwürdigen Belangen der Ehegatten von Erstbestellern über diese bei der SCHUFA angefragt. Außerdem wird durch geeignete organisatorische Maßnahmen sichergestellt, daß die Zulässigkeit der Anfrage und der SCHUFA-Auskunft jederzeit nachgewiesen werden kann.

Diese Änderung begrüße ich sehr. Ich bin froh, daß hier durch meine jahrelangen Bemühungen ein datenschutzrechtlich einwandfreies Ergebnis erzielt werden konnte.

Der Versandhandel benötigt für die Umstellung auf das neue Anfragesystem und die Schulung insbesondere von Kundenbetreuung und Außendienst eine gewisse Zeit und wird deswegen erst zum Ende Februar 1987 endgültig auf die generelle SCHUFA-Anfrage über die Ehegatten von Erstbestellern verzichten können. Diese Zeitspanne für die Umstellung halte ich für hinnehmbar.

6.2.2 Einzelfälle

6.2.2.1 SCHUFA-Anfrage über Mitbesteller

Ein Bürger hat sich bei mir darüber beschwert, daß der Versandhandel eine angeblich negative SCHUFA-Auskunft über ihn an den Sammelbesteller weitergegeben habe, über den er als Mitbesteller regelmäßig Waren des Versandhandels bezog. Der Sammelbesteller habe ihm erklärt, er dürfe von ihm keine Bestellungen mehr annehmen, da er — der Mitbesteller — negative Eintragungen bei der SCHUFA habe. Darüber sei er von dem örtlichen Vertreter des Versandhandelsunternehmens unterrichtet worden.

Nach Klärung der Angelegenheit mit dem betroffenen Versandhandelsunternehmen hat sich folgender Sachverhalt ergeben:

SCHUFA-Anfragen über Mitbesteller dürfen nur die Agenturen des Unternehmens einholen und nicht die Sammelbesteller, und dies auch nur mit ausdrücklicher Einwilligung der Betroffenen. Bestellscheine von Sammelbestellern mit Bestellungen für verschiedene Mitbesteller werden vor einer Belieferung gegen Rechnung jedoch darauf überprüft, ob für die angegebenen Besteller in einem Teil des Unternehmens offene Schulden, Betrugsanschriften, Anschriften abgelehnter Interessenten oder gesperrte Kundenkonten verzeichnet sind. Trifft eines dieser Merkmale zu, lehnt das Versandhandelsunternehmen für den betroffenen Mitbesteller eine Belieferung gegen Rechnung ab. Die bestellte Ware kann dann nur gegen Nachnahme oder Barzahlung beim Sammelbesteller bezogen werden.

Im Beschwerdefall stellte sich heraus, daß die Ehefrau des Beschwerdeführers ein gesperrtes Kundenkonto bei dem Versandhandelsunternehmen gehabt hatte, was zu dem Hinweis an den Sammelbesteller führte, künftig keine Bestellungen mehr an diese Familie auszuliefern.

In Fällen wie diesem wird der Sammelbesteller ohne ausdrückliche Begründung über die Nichtbelieferung des Mitbestellers informiert. Weil nun im Beschwerdefall der Sammelbesteller gegenüber dem Mitbesteller erwähnt hatte, daß der Grund der Ablehnung eine negative SCHUFA-Auskunft sein könnte, war der — unzutreffende — Eindruck entstanden, das Versandhandelsunternehmen habe SCHUFA-Informationen eingeholt und weitergegeben.

Gegen die dargestellte Praxis der Bonitätsprüfung innerhalb des Unternehmens ist datenschutzrechtlich nichts einzuwenden. Dieser Fall ist jedoch auf der anderen Seite ein Beispiel dafür, wie durch die leichtfertige Verwendung von Behauptungen über mögliche SCHUFA-Informationen bei Betroffenen unbegründete Ängste über unzulässige Datenübermittlungen heraufbeschworen werden können. Ich kann aus diesem Anlaß nur dazu aufrufen, mit derartigen Behauptungen vorsichtiger zu sein. Natürlich hat auch das Versandhandelsunternehmen die Pflicht, darauf hinzuwirken, daß seine Mitarbeiter und Vertragspartner (hier: Sammelbesteller) nicht leichtfertig mit derartigen Behauptungen operieren.

In einem anderen Beschwerdefall war ein Mitbesteller darüber unterrichtet worden, daß wegen eines noch offenen Kreditkontos keine Lieferung gegen Rechnung möglich sei. Es stellte sich heraus, daß noch eine offene Forderung gegen den Betroffenen aus dem Jahr 1974 bestand, was der Sammelbestellerin aber nicht mitgeteilt worden war. Diese war ohne nähere Angaben lediglich darüber unterrichtet worden, daß eine Lieferung gegen Rechnung an diesen Mitbesteller nicht möglich sei. Dagegen ist aus Datenschutzgesichtspunkten nichts zu sagen. Der Eindruck, es seien nähere Angaben über die mangelnde Bonität herausgegeben worden, erwies sich als falsch.

6.2.2.2 Zweifelhafte Datenerhebung durch Außendienstmitarbeiter

Ein sicher nicht typischer Beschwerdefall warf ein Schlaglicht darauf, mit welch zweifelhaften Methoden mancher auf Steigerung seiner Provision bedachte Außendienstmitarbeiter von Versandhandelsunternehmen Datenerhebung betreibt.

Ein Ehepaar erlebte folgendes: Nachdem es unverbindlich den Katalog eines Versandhandelsunternehmens angefordert hatte, erschien unangemeldet ein Außendienstmitarbeiter dieses Unternehmens. Da das Ehepaar nicht anwesend war, klingelte er bei einem Nachbarn und erfragte persönliche Daten der Beschwerdeführer. Zum Schluß forderte der Außendienstmitarbeiter den Nachbarn auf, einen Bestellschein mit dem Namen der Beschwerdeführer zu unterschreiben. Bestellt wurde auf diese Weise ein Artikel, der dann nicht lieferbar war, was der Außendienstmitarbeiter möglicherweise wußte. Ihm ging es wahrscheinlich nur darum, den Beschwerdeführern zu einem Kundenkonto bei dem Versandhandelsunternehmen zu verhelfen, um es auf diese Weise zu Bestellungen zu veranlassen.

Das Versandhandelsunternehmen mußte bestätigen, daß der Vorgang sich so zugetragen hatte. Der Außendienstmitarbeiter, der sich noch in der Probezeit befand, wurde entlassen. Die in dieser zweifelhaften Weise erhobenen Daten der Betroffenen wurden gelöscht. Das Unternehmen hat sich bei den Beschwerdeführern entschuldigt. Es hat angekündigt, durch Schulungsmaßnahmen seiner Außendienstmitarbeiter zu verhindern, daß sich ein solcher Fall wiederholt.

6.2.2.3 SCHUFA-Eintragung nach Katalogbestellung?

Ein Bürger beschwerte sich bei mir darüber, daß seine Bestellung eines Versandhauskatalogs dazu geführt habe, daß das Versandhandelsunternehmen ihn mit dem Merkmal „Versandhauskonto" an die SCHUFA gemeldet habe.

Eine Klärung der Angelegenheit erbrachte folgendes: Die Ehefrau des Beschwerdeführers hatte nicht nur einen Katalog, sondern auch drei Artikel bestellt. Vor der Lieferung gegen Rechnung hatte das Versandhandelsunternehmen bei der SCHUFA unter Angabe des Merkmals „Versandhauskonto" über den Ehemann der Bestellerin angefragt, was dazu führte, daß dieses Merkmal für ihn bei der SCHUFA gespeichert wurde. Dieses Vorgehen entspricht der bislang praktizierten Anfrage des Versandhandels über die Ehegatten von Bestellern (vgl. oben 6.2.1). Das Unternehmen hat auf die Beschwerde hin angeboten, die SCHUFA-Eintragung über den Ehemann zu löschen und die Bestellerin eintragen zu lassen. Dies entspricht dem neuen Verfahren, in Zukunft nicht mehr generell über die Ehegatten von Bestellern anzufragen.

Dieser Fall zeigt, wie notwendig die Lösung der Problematik der SCHUFA-Anfragen über die Ehegatten von Bestellern war. Es bestand keine Veranlassung, hier über den Ehegatten anzufragen und dadurch dafür zu sorgen, daß für ihn jahrelang das Merkmal „Versandhauskonto" bei der SCHUFA gespeichert ist.

Gleichzeitig macht dieser Fall aber auch deutlich, daß — entgegen der Annahme des Beschwerdeführers — nicht bereits eine Katalogbestellung zu einer SCHUFA-Anfrage führt, sondern erst eine Warenbestellung. Etwas anderes wäre datenschutzrechtlich auch nicht zu rechtfertigen.

6.3 Werbung

6.3.1 Keine Fortschritte bei der Adressenvermietung

Die bereits seit Jahren andauernden Gespräche mit der Werbewirtschaft über Probleme der Direktwerbung (vgl. zuletzt 4. TB, 5.2, S. 117 ff.) konnten im Berichtsjahr zwar fortgesetzt werden, sind aber jetzt in ein schwieriges Stadium gekommen, in dem nur wenige konkrete Ansätze für eine Verbesserung des Datenschutzes bei der Direktwerbung erkennbar sind.

In einem Gespräch zwischen den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich und Vertretern der Werbewirtschaft wurden folgende Lösungsvorschläge skizziert:

- Vergleichbar dem Verfahren bei der Bundespost (bei Telefonanträgen) und dem Kraftfahrtbundesamt (bei Kfz-Anmeldungen) wird bei dem ersten Kontakt mit einem werbenden Unternehmen (z. B. auf dem Erstbestellschein) durch ein entsprechendes Ankreuzfeld dem Betroffenen die Möglichkeit eröffnet, der Weitergabe seiner Anschrift zu Werbezwecken an Dritte zu widersprechen. Das werbende Unternehmen stellt dies durch einen Sperrvermerk in seiner Kundendatei sicher.
- Widersprüche der Betroffenen gegen die Weitergabe ihrer Daten zu Werbezwecken an Dritte sammelt das werbende Unternehmen zunächst, um sie bei der nächsten turnusmäßigen Kundenstammbehandlung (ca. alle 3 bis 6 Monate) abzugleichen und dann mit einem Sperrvermerk zu versehen. Die dadurch eintretende Verzögerung bei der Sperrung muß von dem Betroffenen hingenommen werden, weil ein sofortiger Abgleichlauf in aller Regel einen unverhältnismäßigen wirtschaftlichen Aufwand darstellen würde.
- Widerspricht ein Betroffener im Fall der Adressenmittlung bei dem werbenden Unternehmen der Verwendung seiner Anschrift, bittet dieses den Betroffenen ggf. um weitere Aufklärung über den Zweck des Widerspruchs. Erklärt der Betroffene seinen Widerspruch generell für alle Werbesendungen, meldet ihn das werbende Unternehmen an die „Robinson-Liste". Soll durch den Widerspruch nur die Sperrung der Anschrift bei dem Adresseneigentümer erreicht werden, wird dies über den Adressenmittler beim Adresseneigentümer veranlaßt.
- In die Werbeschreiben werden Hinweise auf die Selektionskriterien und die Herkunft der Anschriften aufgenommen. Soweit im Einzelfall die Interessen der Werbewirtschaft am Schutz ihrer Geschäftsgeheimnisse einer genauen Bezeichnung im Werbeschreiben entgegenstehen, könnte dem Betroffenen die Möglichkeit eingeräumt werden, auf Nachfrage nähere Angaben zu den Selektionskriterien zu erfahren.

In dem Gespräch wurde deutlich, daß eine Umsetzung der Lösungsvorschläge in die Praxis wesentlich davon abhängig ist, ob sie auch vom Versandhandel akzeptiert werden. Es wurde vereinbart, mit dem Versandhandel ein gesondertes Gespräch zu führen, an dem Vertreter der Werbewirtschaft teilnehmen.

Der Bundesverband des Versandhandels zeigte jedoch zunächst keine Gesprächsbereitschaft und verwies auf die seit langem ausstehende Novellierung des BDSG, die eine erleichterte Weitergabe von Anschriften zu Werbezwecken möglich machen werde. Es sei nicht sinnvoll, noch vor der Neufassung des Gesetzes Gespräche zu führen.

In letzter Zeit hat der Versandhandel jedoch Verhandlungsbereitschaft erkennen lassen, so daß ich die Hoffnung habe, daß die Gespräche in Kürze weitergeführt werden können.

6.3.2 Probleme bei der Ermittlung der Herkunft von Werbeadressen

Ich hatte bereits in meinem 3. TB (4.1.2, S. 101 ff.) über die Probleme berichtet, die Empfänger von Werbesendungen bei der Ermittlung der Herkunft ihrer zu Werbezwecken verwendeten Daten (neben der Adresse die Zuordnung zu einer bestimmten

Personengruppe) haben. Ich hatte auch dargestellt, daß der Umworbene meiner Meinung nach einen Anspruch darauf hat, die Quelle zu erfahren.

Verschiedene Eingaben haben auch in diesem Berichtsjahr wieder gezeigt, daß Bürger nicht in der Lage sind, die Herkunft der Werbeadressen ausfindig zu machen, um selbst dort dafür sorgen zu können, daß ihre Anschrift nicht mehr für Werbezwecke verwendet wird. Wenn sie allerdings — ausnahmsweise — herausgefunden hatten, welcher Adressenhändler ihre Anschrift an das werbende Unternehmen vermietet hatte, konnten sie unter Umständen die Löschung beim Adressenhändler erreichen. Nur in wenigen mir bekannten Fällen war dieser dann aber zu der Mitteilung bereit, wo er seinerseits die Anschrift erhalten hatte, so daß die Betroffenen den Weg ihrer Daten weiter zurückverfolgen konnten, um sie schließlich auch bei der Quelle löschen zu lassen oder ihrer Weitergabe zu widersprechen.

In einem Fall war noch nicht einmal aufklärbar, woher der Werbende (in diesem Fall ein politisch orientierter Verein) die Adressen hatte, die er für Werbeaussendungen benutzte. Dies war besonders unerfreulich, weil viele Empfänger der Werbeschreiben diese wegen ihrer einseitigen politischen Orientierung als Zumutung empfanden. Sie wollten deswegen nicht nur eine Löschung ihrer Anschrift bei dem Verein erreichen, sondern auch wissen, wie ihr Name und ihre Anschrift in die Datei dieses von ihnen politisch abgelehnten Vereins geraten war. Der Verein war zwar zur Löschung sofort bereit, konnte aber die jeweilige Quelle der Anschriften nicht nennen, weil er sie nicht dokumentiert hatte. Angesichts der sich häufenden Beschwerden habe ich mit dem Verein vereinbart, daß die Herkunft der Adressen für einen Zeitraum von mehreren Monaten dokumentiert werden sollte, um dem Verein bei Beschwerden den Nachweis zu ermöglichen, daß er sie — wie er behauptete — nur durch Nennung von Bekannten erhalten hat. Mein Verdacht ging aufgrund mehrerer Beschwerden dahin, daß Adressen auch aus anderen Quellen, z. B. der Abonnentenverwaltung einer Tageszeitung stammten. Die Weitergabe an den politisch einseitigen Verein durch diese Stellen hätte ich für problematisch gehalten. Zu einer Umsetzung dieser Verabredung kam es dann jedoch nicht mehr, weil der Adressenbestand des Vereins wegen eines Rechtsstreits nicht mehr genutzt werden konnte und keine Werbeaussendungen mehr stattfanden.

Dieser Fall zeigt jedoch, welche Probleme entstehen können, wenn die Quelle von Werbeanschriften herausgefunden werden soll, diese aber mangels einer Dokumentation nicht feststellbar ist. In einem problematischen Fall wie dem dargestellten kann ich, wenn die Herkunft der Werbeanschrift nicht festzustellen ist, jedenfalls nicht die datenschutzrechtliche Unbedenklichkeit der Übermittlung an den Werbenden und der Speicherung bei ihm bestätigen. Wenn der Werbende — wie der erwähnte Verein — hierauf Wert legt, muß er schon im eigenen Interesse die Herkunft der Anschriften dokumentieren, denn nur dann kann ich die Zulässigkeit der Übermittlungen und der Speicherung wirklich überprüfen und beurteilen.

6.3.3. Werbung mit Adressen von Blindenwarenkäufern

Ein erstaunlicher Fall von Adressenhandel hat sich zu Beginn des Berichtsjahres ereignet. Mehrere gemeinnützige Organisationen wiesen mich darauf hin, daß ein in Hamburg ansässiges Unternehmen Adressenmaterial anbot, das „für die Spendenwerbung interessant sein dürfte". Es handelte sich dabei um die Anschriften von Kunden, die über dieses Unternehmen Blindenwaren gekauft hatten oder Gelder gespendet hatten. Sie wurden als Firmen oder Privatpersonen angepriesen, „die mit ihren Spenden helfen wollen bzw. ihr Herz an der richtigen Stelle haben".

Ich habe das Unternehmen darauf hingewiesen, daß die Weitergabe derartiger Anschriften rechtswidrig ist. Wenn Adressen von Personen zu Werbezwecken an Dritte übermittelt werden, die entweder als Käufer von Blindenartikeln oder aber als „sozial engagiert", „spendenfreudig" oder „mit dem Herzen an der richtigen Stelle" beschrieben werden, ohne daß die Betroffenen dies beeinflussen können, dann werden ihre schutzwürdigen Belange erheblich beeinträchtigt. Als Dank für eine gute Tat werden die Betroffenen anschließend mit Werbe- oder Bettelbriefen überhäuft. Aus daten-

schutzrechtlichen Gründen halte ich es mithin nicht für zulässig, daß diese Adressen an andere Interessenten weitergegeben werden, wenn nicht sicher ist, daß kein einziger der Betroffenen Einwendungen dagegen hätte.

Das Unternehmen hat auf meinen Hinweis von dem Verkauf der so angebotenen Adressen Abstand genommen.

6.3.4 Beispiel für Adressenhandel

Eine Bürgerin beschwerte sich über die Werbezusendung eines Finanzmaklers aus dem Raum Bremen, der ihr einen „Kredit ohne SCHUFA-Auskunft" anbot mit dem Hinweis, sie habe sich bereits einmal vergeblich um einen Kredit bemüht. Die Petentin, die gerade zu dieser Zeit ihren Überziehungskredit bei einem Hamburger Kreditinstitut voll ausgeschöpft hatte, wollte wissen, ob der Finanzmakler von dem Kreditinstitut oder einer anderen Stelle über ihre Liquiditätsschwierigkeiten unterrichtet worden war. Es stellte sich heraus, daß weder das Kreditinstitut noch die SCHUFA Informationen herausgegeben hatte. Der Finanzmakler hatte ihre Anschrift vielmehr zusammen mit 2000 anderen Andressen als Anschrift eines angeblich Kreditsuchenden von einem Adressenhändler im Saarland gekauft. Da unter diesen Umständen der Verdacht bestand, daß die Anschrift unter Verletzung schutzwürdiger Belange der Betroffenen gespeichert und weitergegeben worden sein könnte, wurde die Spur der Anschrift zurückverfolgt. Dabei ergab sich, daß der Adressenhändler im Saarland, der seinen nebenberuflichen Adressenhandel inzwischen aufgegeben hatte, die Anschrift der Betroffenen wiederum von einem Adressenhändler in Nürnberg bezogen hatte. Dieser ließ sich jedoch nicht unter der angegebenen Anschrift ermitteln, so daß die Angelegenheit zur weiteren Aufklärung der Polizei übergeben werden mußte. Deren Nachforschungen sind noch nicht abgeschlossen.

An diesem Fall zeigt sich, auf welch obskuren Wegen Adressen für Werbezwecke weitergegeben werden können und wie wenig dabei die Belange der Betroffenen zur Geltung kommen. Die Verbände der Werbewirtschaft werden darauf zu achten haben, daß ihr guter Ruf nicht von Praktiken wie den hier geschilderten beeinträchtigt wird.

6.3.5 Werbung mit Adressen von Bürgern der DDR

Ein Fall von eindeutig unzulässiger Speicherung und Übermittlung einer Werbeanschrift wurde bundesweit unter den Datenschutz-Aufsichtsbehörden diskutiert. Eine Bürgerin der DDR, die noch nie in der Bundesrepublik Deutschland war und hier auch kein Konto besaß, erhielt Werbung von einem Lotteriebetreiber. Sie fühlte sich dadurch erheblich beeinträchtigt und verlangte Löschung ihrer Anschrift bei dem werbenden Unternehmen.

Die Angelegenheit wurde auch mit der Werbewirtschaft erörtert. Es bestand Einigkeit, daß das Empfangen westdeutscher Werbesendungen für DDR-Bürger sehr unangenehme Folgen haben kann. Durch die Aufforderung zum Lotteriespiel kann der DDR-Bürger etwa dem Verdacht ausgesetzt werden, nicht angemeldete Devisen, z. B. ein Konto in der Bundesrepublik, zu besitzen, was DDR-Behörden dazu veranlassen könnte, den Vorwurf eines Vergehens gegen Devisenbestimmungen zu erheben.

Die Werbewirtschaft hat zu dem Vorgang erklärt, sie wolle weiterhin — wie bisher — vermeiden, daß DDR-Bürger Werbesendungen aus der Bundesrepublik erhalten. Als Massendrucksachen könnten solche Sendungen die Grenze zur DDR nicht überschreiten; allerdings sei dies möglich, wenn sie frankiert seien. Die Werbewirtschaft wolle weiterhin darauf achten, daß Adressen von DDR-Bürgern nicht in Dateien mit Werbeanschriften gelangen.

Im konkreten Fall war die Adresse der DDR-Bürgerin auf folgende Weise an einen Adressenhändler geraten: Ein Freund hatte für sie als Geschenk Adressenaufkleber bei einem westdeutschen Unternehmen anfertigen lassen, welches die durch derartige Aufträge gewonnenen Adressen zu Werbezwecken verkauft. Bei dem Adressenhändler, der so die Anschrift der DDR-Bürgerin erworben hatte, war diese nicht — wie sonst bei DDR-Anschriften üblich — ausgesondert worden.

Dieser Fall zeigt, wie leicht auch bei dem auf den ersten Blick harmlosen Handel mit Anschriften zu Werbezwecken die schutzwürdigen Belange der Betroffenen beeinträchtigt werden können.

6.3.6 Robinsonliste schützt nicht vor vollen Briefkästen

Ich habe bereits mehrfach in meinen Tätigkeitsberichten darauf hingewiesen, daß man die Zusendung von Direktwerbung z.T. vermeiden kann, wenn man sich in die beim Deutschen Direktmarketing Verband e.V., Schiersteiner Straße 29, 6200 Wiesbaden, geführte sog. Robinsonliste eintragen läßt. Abgesehen von den schon in früheren Tätigkeitsberichten erwähnten Mängeln dieser Liste (nur etwa 40% der Adressenhändler sind angeschlossen, die Liste wird nur zweimal im Jahr aktualisiert) ist darauf hinzuweisen, daß ein Eintrag in die Robinsonliste überfüllte Briefkästen nicht verhindert. Denn die Briefkästen werden in erster Linie durch nicht adressierte Hauswurfsendungen verstopft, die entweder direkt vom Werbenden oder vom Postboten in alle Briefkästen verteilt werden. Die Flut dieser Werbematerialien läßt sich auch durch einen Eintrag in die Robinsonliste nicht eindämmen, denn diese erfaßt nur die adressierte Direktwerbung.

6.4 Kreditwirtschaft/SCHUFA

6.4.1 Neues SCHUFA-Verfahren

In meinem letzten Tätigkeitsbericht hatte ich bereits ausführlich dargestellt, welche Folgen das SCHUFA-Urteil des Bundesgerichtshofs vom 19. September 1985 für die Neufassung einer verbesserten SCHUFA-Klausel und für die Neugestaltung des gesamten SCHUFA-Auskunftssystems haben würde (4. TB, 5.5.3.1, S. 134 ff.). In der ersten Hälfte des Berichtsjahres konnten nun die Verhandlungen zwischen Kreditwirtschaft, SCHUFA und Datenschutz-Aufsichtsbehörden über diesen Themenkomplex abgeschlossen werden. Das Ergebnis entspricht den im letztjährigen Tätigkeitsbericht niedergelegten Grundzügen.

Im folgenden wird noch einmal kurz dargestellt, welche rechtlichen Mängel das alte SCHUFA-Verfahren hatte und wie versucht worden ist, diese im neugestalteten, im wesentlichen seit dem 1. Juli 1986 in Kraft befindlichen Verfahren zu beheben.

6.4.1.1 Die Mängel des alten SCHUFA-Verfahrens

Nach dem BGH-Urteil bestand ein Mangel der alten SCHUFA-Klausel zum einen darin, daß sie eine pauschale Ermächtigung zur Übermittlung nicht näher spezifizierter Merkmale enthielt. Zum zweiten ergibt sich aus dem Urteil des BGH, daß bestimmte problematische Negativmerkmale auch nicht mit einer differenzierteren Einwilligung, sondern nur nach einer Einzelfallabwägung der Interessen der übermittelnden Stelle, eines Dritten oder der Allgemeinheit mit den schutzwürdigen Belangen des Betroffenen an die SCHUFA übermittelt werden dürfen (§ 24 Abs. 1 Satz 1 BDSG).

Daraus ergibt sich, daß auch eine verbesserte SCHUFA-Klausel eine Einwilligung und damit Rechtsgrundlage im Sinne des § 3 BDSG nur für Übermittlungen von Positivdaten an die SCHUFA sein kann. Negativdaten können auch nach Verbesserung der Klausel nicht ohne Abwägung der berechtigten Interessen der übermittelnden Stelle, der SCHUFA oder der Allgemeinheit mit den schutzwürdigen Belangen des Betroffenen an die SCHUFA übermittelt werden. Rechtsgrundlage dafür kann also keine — verbesserte — Klausel, sondern nur § 24 Abs. 1 Satz 1 letzte Alt. BDSG sein.

Bei dieser somit notwendigen Einzelfallabwägung sind die einzelnen Negativmerkmale unterschiedlich zu behandeln. Der BGH hat in zwei Urteilen aus dem Jahr 1983 Anhaltspunkte für diese Differenzierung gegeben. In seinem Urteil vom 7. Juli 1983 (NJW 1984, 436) hat er nach Betonung der Verpflichtung zur Einzelfallabwägung der zu beachtenden Interessen vor einer Datenübermittlung ausgeführt, dieses Abwägungsge-

bot schließe allerdings nicht aus, „daß in bestimmten Fällen eine Datenübermittlung regelmäßig zulässig sein wird, weil dem für eine Datenübermittlung sprechenden berechtigten Interesse ein solches Gewicht zukommt, daß die Belange des Betroffenen demgegenüber zurücktreten müssen. So werden die berechtigten Interessen der Allgemeinheit an einem Schutz vor der Vergabe von Krediten an Zahlungsunfähige oder -unwillige eine Weitergabe von Daten über die Eröffnung des Konkursverfahrens, die Abgabe der eidesstattlichen Versicherung nach § 807 ZPO durch den Schuldner oder die Zwangsvollstreckung in sein Vermögen in aller Regel rechtfertigen" (NJW 1984, 437).

Die Übermittlung dieser auch „harte" Negativmerkmale genannten Daten kann also nach einer verhältnismäßig pauschalen Abwägung der involvierten Interessen mit den schutzwürdigen Belangen des Betroffenen erfolgen. Die Kreditinstitute brauchen in diesen Fällen keine sehr differenzierte Einzelfallabwägung vorzunehmen.

Anders ist dies bei Negativmerkmalen, deren Aussagekraft über die Bonität des Kunden zweifelhaft ist. Diese auch „weiche" Negativmerkmale genannten Daten, bei denen viel eher eine Beeinträchtigung der schutzwürdigen Belange der Kunden denkbar ist, können nur nach einer sehr sorgfältigen Abwägung der berechtigten Interessen mit den schutzwürdigen Belangen des Betroffenen an die SCHUFA übermittelt werden. Dazu hat der BGH in seinem Urteil vom 15. Dezember 1983 (NJW 1984, 1889) nähere Ausführungen gemacht. Er betonte erneut — diesmal bezogen auf die Zulässigkeit der Speicherung der Daten —, daß die datenverarbeitende Stelle gehalten ist, „zwischen den im Einzelfall miteinander kollidierenden berechtigten Interessen der Datei oder Dritter an der Datenverarbeitung und den entgegenstehenden schutzwürdigen Belangen des Betroffenen abzuwägen" (NJW 1984, 1890). Bei der Speicherung des Merkmals „Mahnbescheid" sah der BGH erhebliche Gefahren für den Betroffenen, wenn dieser „zu Unrecht mit einer solchen gerichtlichen Zahlungsaufforderung überzogen worden ist und durch die Speicherung dieser Maßnahme bei der Beklagten eine unzutreffende Beurteilung seiner Kreditwürdigkeit zu gewärtigen hat" (NJW 1984, 1890). Nur wenn der von dem Betroffenen gegen den Mahnbescheid eingelegte Widerspruch ebenfalls im Datenbestand vermerkt wurde, und zwar ebenso deutlich und ebenso schnell, wie das bei den gegen den Schuldner gerichteten Vorgängen geschieht, sei die Gefahr einer unberechtigten Beeinträchtigung seiner Belange deutlich herabgesetzt.

Aus dieser Rechtsprechung wird somit deutlich, daß nach Auffassung des BGH die Abwägung der beteiligten Belange und Interessen vor einer Übermittlung oder Speicherung von Daten insbesondere dann unabdingbar ist, wenn es sich um Negativmerkmale handelt, deren Aussagekraft über die Bonität des Kunden zweifelhaft ist.

6.4.1.2 Die Neugestaltung des SCHUFA-Verfahrens

Ausgehend von dem Leitgedanken, den Betroffenen Gelegenheit zu geben, ihre Belange in die nach dem BDSG notwendigen Abwägungen einzubringen, sind nach Erlaß des BGH-Urteils vom 19. September 1985 zwischen Kreditwirtschaft, SCHUFA und Datenschutz-Aufsichtsbehörden Neufassungen der SCHUFA-Klauseln und verschiedene Änderungen des SCHUFA-Verfahrens erarbeitet worden, die im wesentlichen zum 1. Juli 1986 in Kraft getreten sind. Durch diese Veränderungen wird mehr Transparenz für den Betroffenen hergestellt, er erhält Gelegenheit zum Einbringen seiner Belange, und durch Reduzierung von SCHUFA-Merkmalen und -Vertragspartnern sind wesentliche Probleme ausgeräumt worden. Diese Neuregelungen hatten den Zweck, das informationelle Selbstbestimmungsrecht der Betroffenen im SCHUFA-Verfahren zur Geltung zu bringen.

Die Neugestaltungen umfassen im einzelnen folgende Punkte:

6.4.1.2.1 Neue SCHUFA-Klauseln

Die neuen SCHUFA-Klauseln für die Eröffnung von Girokonten, Abschlüsse von Kreditverträgen und Ausfertigung von Bürgschaftübernahmeerklärungen, die lediglich die Rechtsgrundlage für die Übermittlung von Positivdaten an die SCHUFA (und darüber

hinaus auch die Befreiung vom Bankgeheimnis für alle Datenübermittlungen an die SCHUFA) bilden, sind sehr viel ausführlicher als die alten Klauseln. Sie geben dem Kunden damit erstmals genauere Kenntnisse, in welche Datenübermittlungen er einwilligt. Dies ist nicht nur Voraussetzung dafür, daß diese Klauseln wirksame Einwilligungen im Sinne des § 3 BDSG sind, es führt daneben auch zu einer größeren Transparenz des gesamten Verfahrens. Darüber hinaus wird jeder Kunde, der eine SCHUFA-Klausel unterschreibt, darin darauf aufmerksam gemacht, daß er sich ein erläuterndes SCHUFA-Merkblatt aushändigen lassen kann, welches im übrigen bei den meisten Kreditinstituten auch auf der Rückseite jeder SCHUFA-Klausel abgedruckt ist.

Für die Übermittlung von Positivdaten bedarf es also in jedem Fall der Unterschrift des Kunden unter die SCHUFA-Klausel. Diese Einwilligung darf das Kreditinstitut allerdings nicht „erzwingen". Entgegen der verbreiteten Praxis vieler Kreditinstitute darf die Bank oder Sparkasse eine Unterschrift unter die Klausel nur verlangen, wenn die einzugehende Geschäftsverbindung mit einem Kreditrisiko verbunden ist. Wenn der Kunde deutlich macht, daß er das Girokonto nur auf Guthabenbasis führen und keine Schecks mit Scheckkarte haben will, oder wenn das Kreditinstitut von sich aus diese Einschränkung macht (z. B. bei Minderjährigen, Strafgefangenen und anderen „Kundengruppen mit beschränkter Bonität"), darf keine Unterschrift unter die SCHUFA-Klausel verlangt werden. Denn in diesen Fällen geht die Bank oder Sparkasse keinerlei Kreditrisiko ein, sie hat demzufolge auch kein berechtigtes Interesse im Sinne des § 32 Abs. 2 Satz 1 BDSG am Erhalt von SCHUFA-Nachmeldungen, die sie aufgrund ihrer Meldung des Girokontos automatisch von der SCHUFA erhält. Sie verleitet auf diese Weise die SCHUFA zu Datenübermittlungen, die nicht von § 32 Abs. 2 Satz 1 BDSG gedeckt und somit unzulässig sind.

6.4.1.2.2 Neuorganisation des SCHUFA-Auskunftsverfahrens

Der BGH hat in seinem Urteil vom 19. September 1985 u.a. ausgeführt, daß das Kreditinformationssystem so organisiert sein muß, daß die gespeicherten Daten insgesamt ein möglichst vollständiges, aktuelles Bild der Kreditwürdigkeit bieten und daß die Weitergabe sich auf Anschlußnehmer beschränkt, die ein berechtigtes Interesse haben, über die Kreditwürdigkeit eines Betroffenen unterrichtet zu werden. Daraus ist zunächst zu folgern gewesen, daß insgesamt die Aussagekraft der von den Kreditinstituten übermittelten Merkmale überdacht werden mußte.

Aus dem Katalog der von den Kreditinstituten an die SCHUFA zu meldenden Merkmale sind insbesondere solche gestrichen worden, die einseitige Maßnahmen der Banken und Sparkassen gegen ihre Kunden betreffen. So werden jetzt etwa die Merkmale „Klageerhebung" und „letzte außergerichtliche Mahnung" nicht mehr an die SCHUFA gemeldet, weil sie eine zu geringe Aussagekraft über das tatsächliche Bestehen einer Forderung haben und weil in diesen Fällen zu leicht eine Beeinträchtigung der schutzwürdigen Belange des Betroffenen möglich ist. Das Merkmal „Mahnbescheid" wird nur noch dann an die SCHUFA gemeldet, wenn die Forderung selbst unbestritten ist und der Kunde nur im Moment nicht zahlen kann oder will. Wenn schon vor Beantragung eines Mahnbescheids deutlich wird, daß der Kunde sich gegen die Forderung an sich wendet, wird das Merkmal „Mahnbescheid" nicht mehr gemeldet.

Wie bereits angesprochen, ist durch verschiedene Maßnahmen eine Steigerung der Transparenz des gesamten SCHUFA-Meldeverfahrens für den Kunden erreicht worden, um diesem die Kenntnisse zu geben, die er benötigt, um seine Belange in die im Rahmen dieses Verfahrens notwendigen Abwägungen einbringen zu können und auf diese Weise sein informationelles Selbstbestimmungsrecht geltend zu machen. Dies kann er nur, wenn er das gesamte Meldeverfahren durchschaut.

Das SCHUFA-Verfahren ist durch folgende Maßnahmen transparenter gestaltet worden:

- Die Änderungen der SCHUFA-Klausel führen zu einer Verbesserung der Information der Kunden.
- Das SCHUFA-Merkblatt, das den Kunden auf Wunsch ausgehändigt wird und das z. T. auch auf der Rückseite der SCHUFA-Klausel abgedruckt ist, enthält umfangreiche Erläuterungen des gesamten Auskunftsverfahrens.

— Vor der Übermittlung „weicher" Negativmerkmale an die SCHUFA wird der Kunde jetzt über die Absicht der Übermittlung unterrichtet, damit er Gelegenheit hat, notfalls dagegen vorzugehen. So wird etwa dem Schuldner vor Beantragung eines Mahnbescheids nicht nur diese Absicht, sondern darüber hinaus auch mitgeteilt, daß dies der SCHUFA gemeldet werden wird. Er erhält damit die Möglichkeit, seine Belange noch vor der Meldung an die SCHUFA geltend zu machen, so daß sie in die von dem Kreditinstitut vorzunehmende Abwägung nach § 24 Abs. 1 Satz 1 BDSG einfließen kann.

— Weiter ist es selbstverständlich dabei geblieben, daß sofort eine Nachmeldung an die SCHUFA erfolgt, wenn der Betroffene Widerspruch gegen einen Mahnbescheid eingelegt hat.

— Der Betroffene erhält von der SCHUFA eine Auskunft, die neben den zu seiner Person gespeicherten Daten und der — bislang schon von der SCHUFA mitgeteilten — Angabe, wer diese Daten zur Speicherung übermittelt hat, jetzt auch den Hinweis umfaßt, wer in den letzten Monaten eine Anfrage an die SCHUFA gerichtet und eine Auskunft erhalten hat.

6.4.1.2.3 Verringerung der SCHUFA-Vertragspartner

Im Rahmen der Neuorganisation des SCHUFA-Auskunftsverfahrens ist weiter eine Einschränkung des Kreises der SCHUFA-Vertragspartner vorgenommen worden. Die Datenschutz-Aufsichtsbehörden hatten schon länger gefordert, daß die SCHUFA sich von Vertragspartnern trennen sollte, die selbst keine Kredite gewähren. Die einzelnen SCHUFA-Gesellschaften haben demzufolge zum 30. Juni 1986 einer Reihe von Vertragspartnern gekündigt. Diese Kündigungen sind zwar zunächst wegen eines Verfahrens vor dem Bundeskartellamt (siehe unten 6.4.2) ausgesetzt worden. Es ist aber davon auszugehen, daß dieses in Kürze abgeschlossen sein wird und daß dann die meisten Kündigungen wirksam werden. Auf diese Weise wird der Kreis der Anschlußnehmer auf solche begrenzt werden, die selbst Kredite gewähren.

Durch diese Maßnahme ist erreicht worden, daß jetzt nicht mehr Stellen über SCHUFA-Informationen verfügen können, die kein Kreditschutzinteresse, sondern nur ein ganz anders geartetes wirtschaftliches oder sonstiges Interesse haben. Die SCHUFA wird somit auf ihre eigentliche Aufgabe zurückgeführt, Kreditschutzinteressen zu dienen.

6.4.1.2.4 Fazit

Durch alle dargestellten Neuregelungen im SCHUFA-Auskunftsverfahren ist versucht worden, die nach § 24 BDSG vorzunehmenden Abwägungen der berechtigten Interessen mit den schutzwürdigen Belangen in einer Weise für den Betroffenen durchschaubar und beeinflußbar zu machen, die ihn in die Lage versetzt, sein informationelles Selbstbestimmungsrecht im SCHUFA-Verfahren zu wahren. Bei dieser mit den Datenschutz-Aufsichtsbehörden abgesprochenen Neuregelung handelt es sich allerdings nur um einen Kompromiß zwischen den beteiligten Interessen. Sie stellt somit nichts anderes als einen Versuch dar, die dargestellten Mängel des alten SCHUFA-Verfahrens zu beseitigen und sowohl die Interessen der Kreditwirtschaft als auch die des Datenschutzes zu berücksichtigen.

Eine tragfähige Grundlage für ein datenschutzrechtlich einwandfreies Verfahren kann diese Neugestaltung jedoch nur für eine Übergangszeit sein. Diese Kompromißregelung ist nur so lange hinnehmbar, wie noch keine bereichsspezifischen Datenschutzregelungen für die Kreditwirtschaft geschaffen worden sind. Es muß jedoch das Ziel sein, derartige auf die besonderen Probleme dieses Wirtschaftsbereiches abgestimmten Datenschutznormen zu schaffen, ähnlich wie im öffentlichen Bereich bereichsspezifische Datenschutzregelungen zu normieren sind.

6.4.2 Kartellrechtliche Entwicklung

Die Kündigung einer Reihe von Vertragspartnern durch die SCHUFA, die keine Kreditrisiken eingehen, hat — wie eben bereits erwähnt — zu kartellrechtlichen Problemen geführt.

In den Verhandlungen zwischen Kreditwirtschaft, SCHUFA und Datenschutz-Aufsichtsbehörden im Gefolge des BGH-Urteils zur SCHUFA-Klausel vom 19. September 1985 war u.a. vereinbart worden, daß die SCHUFA die Verträge mit einigen Vertragspartnern kündigen sollte, die keine Kreditrisiken eingehen. Dabei handelte es sich insbesondere um Wohnungsvermieter, Versicherungen und Auto- und Gerätevermieter. Die SCHUFA hat daraufhin zum 30. Juni 1986 eine Reihe von Kündigungen ausgesprochen, nachdem sie bereits im Vorgriff darauf zum Ende des Jahres 1985 die Vertragsverhältnisse mit einigen Vertragspartnern (Wohnungsvermieter, Makler, Bauträgergesellschaften) beendet hatte (vgl. 4. TB, 5.5.3.1.2, S. 137). Die Beschwerde eines Gerätevermietungsunternehmens und einer Bausparkasse (die sich gegen die Umstellung ihres A-Vertrages auf einen B-Vertrag sträubte) veranlaßten das Bundeskartellamt Mitte des Jahres zu der Einleitung einer Untersuchung, ob das Diskriminierungsverbot des § 26 des Gesetzes gegen Wettbewerbsbeschränkungen durch die Kündigungen verletzt sein könnte. Die Frage war, ob die SCHUFA die gekündigten Vertragspartner diskriminierte, indem sie nur diese von ihren Informationen ausschloß, während die anderen Vertragspartner nach wie vor daran partizipieren können. Auf Bitte des Bundeskartellamtes wurden die zum 30. Juni 1986 ausgesprochenen Kündigungen dann zunächst für die Zeit der Untersuchungen des Amtes ausgesetzt, so daß die gekündigten Vertragspartner vorerst an die SCHUFA angeschlossen blieben. Die gekündigten Unternehmen, die nicht Kredite gewähren, sondern nur Risiken aus wirtschaftlichen Vorleistungen eingehen, erhalten deswegen vorerst weiter Daten von der SCHUFA. Sie bekommen allerdings keine Daten, die Kreditinstitute übermittelt haben. SCHUFA und Kreditwirtschaft haben diese Regelung getroffen, da die von Kreditinstituten übermittelten Daten entsprechend ihrer SCHUFA-Klausel einer Zweckbindung unterliegen und die Datenweitergabe auf solche Unternehmen beschränkt ist, die Kredite in Geld- oder Warenform gewähren.

Die Problematik wurde verschiedentlich und in unterschiedlicher Zusammensetzung zwischen Bundeskartellamt, Kreditwirtschaft, Datenschutz-Aufsichtsbehörden und Vertretern der gekündigten Wirtschaftszweige erörtert. Ziel ist es, eine Lösung zu finden, die sowohl den Anforderungen des Kartellrechts als auch des Datenschutzes genügt:

— Ein noch ungelöstes Problem stellt die Frage dar, inwieweit Unternehmen an die SCHUFA angeschlossen sein sollen, die grundpfandrechtlich gesicherte Kredite für Wohnungsbaufinanzierungen vergeben (öffentliche und private Bausparkassen, Hypothekenbanken und Versicherungen ebenso wie Universalkreditinstitute). Einige dieser Unternehmen hatten zunächst Wert darauf gelegt, uneingeschränkt Zugang zu SCHUFA-A-Daten zu erhalten. Sie meinten, auch bei grundpfandrechtlich gesicherten Krediten sei wegen der derzeit schlechten Verwertbarkeit von Grundstücken das Ausfallrisiko so groß, daß sie ohne Zugang zu den SCHUFA-A-Daten ein unvertretbar hohes wirtschaftliches Risiko bei der Kreditvergabe eingehen würden. Die Datenschutz-Aufsichtsbehörden haben demgegenüber zu bedenken gegeben, daß dies zu einer unangemessenen Ausweitung des Kreises der A-Vertragspartner führen würde. Dadurch würden Mitteilungen auch über höhere Verbindlichkeiten und über das Vermögen der Betroffenen in das SCHUFA-System gelangen, die jedenfalls nach bisheriger Auffassung für die Gewährung von Konsumentenkrediten keine Relevanz haben. Sie haben sich aber davon überzeugen lassen, daß die Eintragung von Grundpfandrechten keine ausreichende Sicherung für die Kreditgeber ist und daß für die Wohnungsbaufinanzierung deswegen der Zugang zu SCHUFA-Daten eröffnet sein muß. Die Lage bei der Wohnungsbaufinanzierung ist wegen der dinglichen Sicherung oder, wenn Bausparkassen bei Krediten bis zu DM 15 000,— auf die Eintragung eines Grundpfandrechts verzichten, der sog. Negativerklärung, mit der der Kreditnehmer versichert, daß er das Grundstück nicht anderweitig belasten wird, nicht mit der von Kreditinstituten zu vergleichen, die Konsumentenkredite ohne derartige Sicherungen vergeben. Es wird deswegen eine Lösung gefunden werden müssen, die den Besonderheiten der Wohnungsbaufinanzierung Rechnung trägt und weder ein reiner A-Vertrag noch B-Vertrag sein kann.

— Die Kündigungen der Autovermieter müssen nach Meinung der Datenschutz-Aufsichtsbehörden bestehen bleiben, weil diese eindeutig keine Kreditrisiken eingehen und deswegen vom Geschäftszweck der SCHUFA nicht erfaßt werden. Darüber hinaus haben die SCHUFA-Auskünfte nur eine sehr begrenzte Aussagekraft, um das Vermögensrisiko der Autovermieter zu vermindern. Für die Beurteilung des Risikos, ob ein gemietetes Fahrzeug unterschlagen wird, haben die SCHUFA-Auskünfte keinerlei Relevanz. Das Risiko, daß der Mietzins vom Mieter nicht gezahlt wird, kann durch Hinterlegung einer höheren Sicherheit aufgefangen werden. Lediglich für das Risiko, daß ein vom Mieter verursachter Schaden von diesem nicht beglichen wird, könnten SCHUFA-Daten relevant sein. Ob allein dafür ein SCHUFA-Anschluß der Kfz-Vermieter zuzulassen ist, muß noch diskutiert werden. Wie gering die praktische Verwertbarkeit der SCHUFA-Auskünfte für die Autovermieter ist, zeigt sich daran, daß sie hieraus zuweilen Schlußfolgerungen ziehen, die mit einer Aussage über die Kreditwürdigkeit der Betroffenenen nichts zu tun haben. So habe ich in meinem 4. TB (5.5.3.3, S. 139 f.) berichtet, daß ein Autovermieter aus dem SCHUFA-Merkmal KI (= keine Information) den Schluß gezogen hat, der Betroffene habe möglicherweise falsche Papiere vorgelegt, und daß er deshalb an ihn kein Auto vermietet hat. KI bedeutet jedoch lediglich, daß zu dem Betroffenen weder ein Girokonto noch ein Kredit von einem SCHUFA-Vertragspartner gemeldet worden ist. Er kann z. B. deshalb der SCHUFA unbekannt sein, weil er ein Postgirokonto hat (das nicht an die SCHUFA gemeldet wird).
— Auch Gerätevermieter gehen keine Kreditrisiken ein. Sie könnten nur dann weiter Zugang zu SCHUFA-Daten haben, wenn ihre Verträge als Leasinggeschäfte angesehen werden können. Leasingunternehmen sind nicht von der SCHUFA gekündigt worden. Der Unterschied zu gewerbsmäßigen Vermietern besteht darin, daß die Risiken von Leasinggeschäften denen von Krediten gleichzusetzen sind. Die geschäftlichen Risiken, die Leasingunternehmen eingehen, fallen damit in den Geschäftszweck der SCHUFA.

Den Datenschutz-Aufsichtsbehörden sind Fälle bekanntgeworden, in denen von der SCHUFA gekündigte Unternehmen ihre Geschäftspartner auffordern, eine Selbstauskunft beizubringen. Dagegen bestehen erhebliche Bedenken, denn auf diese Weise würde zum einen die Kündigung umgangen und ein früherer Vertragspartner nicht nur die Informationen von der SCHUFA erhalten, von denen er gerade abgeschnitten werden sollte, er würde künftig sogar noch mehr erfahren. In einem derartigen Vorgehen könnte zudem ein Verstoß gegen Treu und Glauben liegen, denn es wäre praktisch dem „Erzwingen" einer Unterzeichnung der SCHUFA-Klausel gleichzusetzen. Darüber hinaus erscheint es mir zumindest zweifelhaft, ob es mit § 9 des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen vereinbar ist, wenn die Aufforderung zur Vorlage der Selbstauskunft formularmäßig erfolgen würde. Ein solches Verlangen wäre als unangemessene Benachteiligung anzusehen, weil es von wesentlichen Grundgedanken des BDSG abwiche.

6.4.3 Guthaben-Konten — Verhalten der Kreditinstitute gegenüber ihren Alt-Kunden

Nachdem das neue, mit den Datenschutz-Aufsichtsbehörden abgestimmte SCHUFA-Verfahren am 1. Juli 1986 in Kraft getreten war, benachrichtigten alle Kreditinstitute ihre sogenannten Alt-Kunden, die mit ihnen schon eine Geschäftsbeziehung unterhielten, mit einem Schreiben oder in Mitteilungsblättern über die neuen SCHUFA-Klauseln und das neue Auskunftsverfahren. Durch dieses sogenannten Altkundenschreiben, das ebenfalls mit den Datenschutz-Aufsichtsbehörden abgestimmt war, wurde den Kunden Gelegenheit zum Widerspruch gegen die Datenübermittlung an die SCHUFA und ihre Speicherung durch die SCHUFA gegeben. Den Kunden wurde mitgeteilt, das Kreditinstitut werde von ihrem Einverständnis mit dem neuen Verfahren ausgehen, wenn sie es nicht in den nächsten Wochen ansprächen. Diese Widerspruchslösung wurde gewählt, weil es für zu aufwendig gehalten wurde, jedem einzelnen Kunden die neue SCHUFA-Klausel zur Unterschrift vorzulegen. Aus der Sicht des Datenschutzes erschien diese Lösung vertretbar, weil die Betroffenenen auf diese Weise Gelegenheit erhielten, ihre Belange geltend zu machen, um unter Umständen Übermittlungen an die

SCHUFA zu verhindern oder die Löschung bei der SCHUFA zu erreichen. Viele Kunden waren unsicher, wie sie auf dieses Schreiben reagieren sollten. Einige Bürger wandten sich nach Erhalt dieses Schreibens schriftlich oder telefonisch an die Datenschutz-Aufsichtsbehörden, baten um Auskunft über das neue Verfahren und erbaten Ratschläge für das Verhalten gegenüber dem jeweiligen Kreditinstitut.

Zunächst war die Situation von der Weigerung einiger Kreditinstitute gekennzeichnet, die Geschäftsverbindung mit Kunden weiterzuführen, die der Datenübermittlung an die SCHUFA widersprachen. Andere Kreditinstitute haben derartige Fälle von Anfang an flexibler gehandhabt und im Falle des Widerspruchs das Konto auf Guthabenbasis weitergeführt und lediglich den Dispositionskredit gestrichen und vielleicht auch Scheckformulare und die Scheckkarte eingezogen. Nach meinem Eindruck haben sich inzwischen auch die Kreditinstitute, die ursprünglich eine harte Haltung eingenommen hatten, zu einer kulanteren Handhabung der Widersprüche bereitgefunden.

Die Einräumung eines Dispositionskredits und die Ausgabe von Scheckvordrucken mit Scheckkarte stellen nach Auffassung der Kreditwirtschaft in der Regel ein Kreditrisiko dar, auch wenn der Kunde von dem Überziehungskredit keinen Gebrauch macht und auch wenn nicht schon durch die Ausgabe von Schecks das Konto überzogen wird. Da der Kunde ohne weitere Prüfung durch das Kreditinstitut von diesen Möglichkeiten Gebrauch machen könne, habe er die Option der Kreditinanspruchnahme. Ich halte es deswegen für vertretbar, einen Dispositionskredit grundsätzlich nur einzuräumen, wenn eine SCHUFA-Anfrage keine negativen Informationen über den Kunden ergeben hat. In den Fällen allerdings, in denen durch eine langjährige Geschäftsbeziehung deutlich ist, daß kein Risiko für das Kreditinstitut besteht, ist meiner Meinung nach eine Überwachung durch die SCHUFA nicht zu rechtfertigen.

Darüber hinaus ist in allen Fällen, in denen der Kunde entweder selbst deutlich macht, daß er an Dispositionskredit und Schecks nicht interessiert ist und sein Konto nur im Guthabenbereich führen will, oder wenn das Kreditinstitut von sich aus nur zu einer Guthabenkontoführung bereit ist (z. B. bei Minderjährigen, Strafgefangenen oder anderen Gruppen mit nach Ansicht der Kreditwirtschaft „beschränkter Bonität"), mit der Einrichtung des Girokontos keinerlei Kreditrisiko verbunden, so daß eine SCHUFA-Anfrage datenschutzrechtlich nicht gerechtfertigt werden kann. Das Kreditinstitut hat in diesen Fällen kein berechtigtes Interesse im Sinne des § 32 Abs. 2 Satz 1 BDSG am Erhalt von SCHUFA-Nachmeldungen, die es aufgrund seiner Meldung des Girokontos automatisch von der SCHUFA erhält. Es verleitet auf diese Weise die SCHUFA zu Datenübermittlungen, die nicht von § 32 Abs. 2 Satz 1 BDSG gedeckt und somit unzulässig sind.

Wie bei den Datenschutzaufsichtsbehörden sind auch beim Bundesaufsichtsamt für das Kreditwesen (BAKred) Anfragen und Beschwerden darüber eingegangen, daß viele Kreditinstitute die Eröffnung von Girokonten ohne Einwilligung in die SCHUFA-Klausel ablehnten. Das BAKred hat den Zentralen Kreditausschuß um Stellungnahme dazu gebeten und dabei den Standpunkt vertreten, daß die Einwilligung des Kunden in die SCHUFA-Klausel nicht Voraussetzung für die Führung eines Girokontos ist, eine einheitliche Ablehnung also nicht erfolgen darf, sondern eine Einzelfallprüfung stattfinden muß. Dies sei besonders dann angebracht, wenn das Girokonto auf reiner Guthabenbasis geführt werde. Für die Teilnahme am SCHUFA-Verfahren dürfte nach Ansicht des BAKred ein Bedürfnis nur im Hinblick auf Geschäfte mit Kreditrisiken bestehen. Wenn negative SCHUFA-Auskünfte über einen Kunden vorlägen, könne es zwar manchmal gerechtfertigt sein, die Kontoführung abzulehnen. Aber dabei seien jeweils die besonderen Umstände des Einzelfalls zu berücksichtigen und die Führung des Girokontos sollte nicht schlechthin abgelehnt werden.

Die Kreditwirtschaft hat dem BAKred daraufhin mitgeteilt, daß Bürger, die beim Antrag auf Eröffnung eines Girokontos die Unterzeichnung der SCHUFA-Klausel verweigern, nicht grundsätzlich befürchten müßten, daß die Kontoführung von den Kreditinstituten abgelehnt wird. Es sei in diesen Fällen üblich, nach Prüfung des Einzelfalls abzuwägen, ob eine Kontoeröffnung möglich sei. Dies werde in aller Regel dann zu bejahen sein, wenn das Konto auf Guthabenbasis unter Verzicht auf die Ausgabe einer Scheck-

karte geführt werden solle. Betont werden müsse allerdings, daß letztlich die Entscheidung des jeweiligen Kreditinstituts maßgeblich sei und auch die Zurückweisung eines Eröffnungsantrages nicht generell ausgeschlossen werden könne. Das gleiche gilt nach Darstellung der Kreditwirtschaft, wenn sich im Zusammenhang mit dem Antrag auf Eröffnung eines Girokontos herausstellt, daß Negativmerkmale bei der SCHUFA gespeichert sind. Hier komme es letztlich entscheidend auf das Gewicht des jeweiligen Merkmals an. Ein Mahnbescheid werde allgemein nicht ohne weiteres zur Ablehnung der Kontoführung führen. Gravierender erscheine dagegen beispielsweise die Abgabe einer eidesstattlichen Versicherung.

In der Diskussion hat auch eine Rolle gespielt, ob Kreditinstitute sich weigern können, für Arbeitslose und Sozialhilfeempfänger Girokonten einzurichten. Hierzu hat die Kreditwirtschaft erklärt, daß Arbeitslosigkeit oder der Bezug von Sozialhilfe für sich genommen kein Grund sei, der der Einrichtung einer Kontoverbindung entgegenstehe. Auch hier würden die Kreditinstitute den Kontoeröffnungsantrag im jeweiligen Einzelfall prüfen. Die Kreditwirtschaft sei sich dabei des sozialen Aspekts durchaus bewußt.

Auch die Bundesregierung sah sich auf eine parlamentarische Anfrage hin genötigt, sich in diese Diskussion einzuschalten. Sie erklärte, es sei jedem Bankkunden freigestellt, ob er die am 1. Juli 1986 in Kraft getretene SCHUFA-Klausel annehmen will. Tue er dies nicht, so sei es möglich, daß ein Kreditinstitut das Girokonto nur noch auf der Grundlage von Guthaben zu führen bereit sei. Das bedeute, daß der Kunde dann von der ihm bisher eingeräumten Möglichkeit der Inanspruchnahme eines Überziehungskredits keinen Gebrauch mehr machen könne. Allerdings könne es auch vorkommen, daß einzelne Kreditinstitute eine Weiterführung des Kontos ganz ablehnten. Aufnahme, Aufrechterhaltung und Ausgestaltung von Geschäftsbeziehungen lägen jedoch in der alleinigen geschäftspolitischen Verantwortung jedes einzelnen Kreditinstituts. Die Bundesregierung habe die Spitzenverbände des Kreditgewerbes gebeten darauf hinzuwirken, daß die Nichtanerkennung der SCHUFA-Klausel allein nicht zur Kündigung eines Girokontos führe. Ebenso sollte nach Auffassung der Bundesregierung sichergestellt sein, daß die Eröffnung eines Girokontos auf der Grundlage von Guthaben auch bei Nichteinwilligung in die SCHUFA-Klausel möglich sei.

Ich sehe mich durch diese Ansichten bestätigt und ich begrüße es, daß auch die Kreditwirtschaft selbst eingeräumt hat, daß bei der Girokontenführung auf Guthabenbasis keine Grundlage für das Verlangen der Unterzeichnung der SCHUFA-Klausel besteht.

6.4.4 Verhältnis der SCHUFA zu den B-Vertragspartnern

Die B-Vertragspartner, die selbst keine Kredite geben und die nur Negativdaten erhalten und an die SCHUFA liefern, lassen sich von ihren Kunden keine Einwilligung für diese Datenübermittlungen geben. Sie brauchen dies auch nicht, da sie nicht wie die Kreditinstitute auch Positivdaten melden und im übrigen auch keine ausdrückliche Erlaubnis zur Durchbrechung des Bankgeheimnisses benötigen. Bei ihnen reicht es aus, wenn die nach § 24 Abs. 1 Satz 1 BDSG nötige Abwägung im Einzelfall vorgenommen wird.

Die Datenschutz-Aufsichtsbehörden fordern allerdings von den B-Vertragspartnern, dem Kunden transparent zu machen, welche Datenübermittlungen und -speicherungen im Zusammenhang z. B. mit Bestellungen der Kunden vorgenommen werden, damit die Betroffenen ihre Belange wenn nötig in einer Weise geltend machen können, die deren Berücksichtigung bei den für Speicherungen und Übermittlungen notwendigen Abwägungen nach §§ 23, 24 und 32 BDSG ermöglicht.

Wenn jemand z. B. bei einem Handelsunternehmen eine Ware bestellt, schließt das Unternehmen in vielen Fällen den Vertrag erst ab, wenn eine SCHUFA-Anfrage über den Besteller dessen Kreditwürdigkeit erwiesen hat. Zum Zweck dieser SCHUFA-Anfrage werden die Daten zunächst beim Handelsunternehmen gespeichert und mit der Anfrage an die SCHUFA übermittelt. Dies ist zulässig nach §§ 23, 24 Abs. 1 BDSG im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses, das durch die Bestellung des prospektiven Kunden entstanden ist.

Dabei ist aber zu beachten, daß die Datenspeicherung und -übermittlung nur zulässig ist, soweit dies die Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses zuläßt. Wenn der Kunde nicht weiß, daß der Vertrag mit dem Handelsunternehmen nur nach einer SCHUFA-Anfrage über ihn zustandekommen kann, und er somit vor Abgabe der Bestellung nicht die Möglichkeit der Entscheidung hatte, ob er den Vertrag unter dieser Voraussetzung überhaupt eingehen will, kann nicht gesagt werden, daß die SCHUFA-Anfrage und die dafür notwendigen Datenspeicherungen und -übermittlungen noch im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses liegen.

Der Betroffene weiß bei der Abgabe seiner Bestellung z. B. nicht, daß das Handelsunternehmen ihm nach seiner geschäftlichen Auffassung schon durch die Einräumung einer Zahlungsfrist einen Kredit gewährt, zu dem es ggf. erst nach einer SCHUFA-Anfrage über den Betroffenen bereit ist. Der Betroffene weiß auch nicht, daß das Handelsunternehmen, bei dem er eine Ware geringen Wertes bestellt, unter Umständen aufgrund dieser Bestellung nicht nur die Waren liefern, sondern auch ein Kundenkonto für den Besteller eröffnen will, das ihm einen Kreditrahmen bei dem Handelsunternehmen verschafft, das Kreditkonto aber nur nach erfolgter SCHUFA-Anfrage eingerichtet wird. Die Datenspeicherungen und -übermittlungen, die aus diesem Grund vorgenommen werden, liegen ebenfalls nicht „im Rahmen der Zweckbestimmung" des vertragsähnlichen Vertrauensverhältnisses, das durch die schlichte Bestellung einer Ware entstanden ist, wenn der Betroffene über diese Folgen seiner Bestellung nichts weiß.

Wenn diese Datenspeicherungen und -übermittlungen im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses vorgenommen werden sollen, muß der prospektive Kunde über die Zusammenhänge aufgeklärt werden, damit er die Möglichkeit hat, von einer Bestellung abzusehen oder — wenn dies möglich ist — die Lieferung der Ware per Nachnahme zu bestellen, sofern er diese Folgen eines Kaufs gegen Rechnung nicht hinnehmen will. Die Verpflichtung zu einer entsprechenden Aufklärung des Kunden (Bestellers) ergibt sich aus der zwischen diesem und dem Handelsunternehmen entstandenen vertragsähnlichen Rechtsbeziehung, die im Geiste des durch das Bundesverfassungsgericht im Urteil zum Volkszählungsgesetz 1983 aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG abgeleiteten Rechts auf informationelle Selbstbestimmung auszulegen ist. Wenn auch die unmittelbare Drittwirkung von Grundrechten in der Rechtslehre umstritten ist, so ist doch heute allgemein anerkannt, daß die Interpretation des Privatrechts nicht im Widerspruch zu der in den Grundrechten zum Ausdruck kommenden Wertordnung erfolgen darf, vielmehr in einer Weise vorzunehmen ist, die dieser verfassungsrechtlich vorgegebenen Wertordnung in angemessener Weise Rechnung trägt. Die hiernach notwendige Unterrichtung des Kunden wäre durch entsprechende Hinweise auf den Bestellformularen sicherzustellen. Denkbar wäre dabei, einen solchen Hinweis nicht pauschal in alle Bestellformulare aufzunehmen, sondern dies nur für bestimmte Arten von Bestellungen vorzusehen, bei denen tatsächlich eine SCHUFA-Anfrage in Betracht kommt.

Die Speicherung der Merkmale AV oder VK bei der SCHUFA aufgrund der Anfrage eines Versandhandelsunternehmens ist nach § 32 Abs. 1 BDSG zulässig, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Wenn die SCHUFA aufgrund der Anfrage eine Auskunft an das Handelsunternehmen gibt, stellt diese eine Datenübermittlung dar, die nach § 32 Abs. 2 BDSG zulässig ist, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat. Dazu ist nach ganz überwiegender Ansicht der Literatur auch eine Interessenabwägung erforderlich, auch wenn im Gesetzeswortlaut nicht ausdrücklich auf die schutzwürdigen Belange des Betroffenen abgestellt ist. Denn ein Interesse des Empfängers an bestimmten Daten kann nicht „berechtigt" sein, wenn durch die Übermittlung das Persönlichkeitsrecht des Betroffenen verletzt würde.

Bei der Speicherung der Anfragemerkmale bei der SCHUFA ist die Schwelle etwas niedriger: Die Abwägung mit den schutzwürdigen Belangen des Betroffenen muß nur er-

folgen, wenn Grund zu der Annahme besteht, daß durch die Speicherung schutzwürdige Belange beeinträchtigt werden. Dann müssen diese allerdings in die Abwägung mit einbezogen werden.

Die Abwägung zwischen den berechtigten Interessen des Handels und der SCHUFA auf der einen Seite und den schutzwürdigen Belangen des Betroffenen auf der anderen Seite ist wiederum nur möglich, wenn der Betroffene über die beabsichtigte Anfrage bei der SCHUFA vorher unterrichtet wird, damit er seine Interessen in diese Abwägung mit einbringen kann. Dies ergibt sich ebenso aus dem Volkszählungsurteil des Bundesverfassungsgerichts, welches jedenfalls in dem bereits dargelegten Sinne einer mittelbaren Drittwirkung der Grundrechte auch für die Auslegung der Rechtsbeziehungen des Privatrechts maßgeblich ist, wie aus dem Urteil des Bundesgerichtshofes zur SCHUFA-Klausel, in dem das SCHUFA-Kreditinformationssystem nur unter der Voraussetzung für zulässig gehalten wird, es sei so zu organisieren, daß die gespeicherten Daten insgesamt ein möglichst vollständiges, aktuelles Bild der Kreditwürdigkeit bieten. Dies ist nur gewährleistet, wenn der Betroffene seine Interessen in die oben genannte Abwägung mit einbringen kann, weil ansonsten die Gefahr besteht, daß kein korrektes Bild von der Kreditwürdigkeit des Betroffenen bei der SCHUFA entsteht.

Die Datenschutz-Aufsichtsbehörden fordern somit, den Betroffenen deutlich und ausführlich über die beabsichtigten Datenübermittlungen und -speicherungen zu informieren, damit er in die Lage versetzt wird, seine Belange geltend zu machen.

Über diese Forderung ist noch keine Einigung mit dem Versand- und Einzelhandel herbeigeführt worden; die Gespräche darüber dauern noch an.

6.4.5 Einzelfälle

6.4.5.1 Vorlage des Personalausweises zur Auskunft an den Betroffenen

Durch eine Beschwerde wurde ich darauf aufmerksam, daß die SCHUFA Hamburg auf die Bitte von Bürgern um Auskunft über die zu ihrer Person bei der SCHUFA gespeicherten Daten (sog. Selbstauskunft) von diesen auf einem Forlumar die Angabe der zwei letzten Voranschriften sowie durch einen maschinenschriftlichen Zusatz auf dem Formular eine Fotokopie aller Seiten des Personalausweises des Betroffenen erbittet. Die SCHUFA hat mir dazu erklärt, sie bitte die Betroffenen grundsätzlich um eine Fotokopie des Personalausweises. Dies sei erforderlich für die Einsichtnahme aller aufgeführten Anschriften. Insbesondere bei Negativdaten ohne Geburtsdatum sei eine eindeutige Zuordnung nur über die Anschrift möglich. Da die Vergangenheit gezeigt habe, daß die Betroffenen nur sehr selten die Voranschriften in dem Formular angeben, erbitte die SCHUFA die Kopie des Ausweises. Die Auskunft an den Betroffenen könne andernfalls ausschließlich die unter der von ihm angegebenen Anschrift gespeicherten Daten enthalten. Beantrage er einen Kredit und gebe er dabei seine bisherigen Anschriften an — wie es nach Kenntnis der SCHUFA in den Kreditanträgen vorgesehen sei —, würden dem Kreditinstitut gegenüber auch die unter den Voranschriften gespeicherten Daten beauskunftet werden. Für den Betroffenen entstehe dadurch der Eindruck, daß die SCHUFA ihm eine unvollständige Auskunft erteilt hat. Gemäß § 34 BDSG habe der Betroffene aber Anspruch auf Beauskunftung aller zu seiner Person gespeicherten Daten.

Dies hat mich nicht überzeugt. Wenn die SCHUFA dem Betroffenen ermöglichen will, auch Auskunft über die Negativdaten zu erhalten, die ohne Geburtsdatum gespeichert sind, muß sie ihn darauf hinweisen, daß er eine vollständige Auskunft nur erhält, wenn er auch seine Voranschriften für einen bestimmten Zeitraum angibt. Der Betroffene kann dann selbst entscheiden, ob er dies will (und ob er der SCHUFA damit dann auch ermöglichen will, die bisher ohne Geburtsdatum gespeicherten Negativdaten für die Zukunft eindeutig zuzuordnen). Diese Entscheidungsmöglichkeit muß ihm gelassen werden.

Es ist nicht akzeptabel, daß die SCHUFA durch ihr Formular und die maschinenschriftlich hinzugefügte Bitte den Eindruck erweckt, eine Auskunft nach § 34 Abs. 2 BDSG

könne nur erteilt werden, wenn die Voranschriften angegeben und Ausweiskopien übersandt werden. Ich habe die SCHUFA gebeten, ihr Formularschreiben entsprechend zu ändern.

Die Praxis der SCHUFA muß ohnehin geändert werden, da ab 1. April 1987 neue Personalausweise ausgegeben werden, die keine Voranschriften mehr enthalten.

6.4.5.2 Namensverwechslung bei Daten aus dem Schuldnerverzeichnis

Es kommt immer wieder vor, daß die Daten, die die SCHUFA wie auch andere Stellen aus dem beim Amtsgericht geführten Schuldnerverzeichnis erhält, nicht eindeutig zugeordnet werden können, weil das Geburtsdatum fehlt. Wenn die SCHUFA derartige Daten in ihrem Bestand hat, gleichzeitig aber auch Daten über eine Person gleichen Namens mit Geburtsdatum vorhanden sind, so wird bei Auskunftsersuchen auch der wegen fehlenden Geburtsdatums nicht eindeutig zuzuordnende Datenbestand mit ausgedruckt. Es wird jedoch ein Hinweis hinzugefügt, daß bei den Daten ohne Geburtsdatum die Identität ungeklärt ist. Der diese Auskunft empfangende SCHUFA-Vertragspartner ist dann aufgrund seines SCHUFA-Anschlußvertrages verpflichtet, vor Verwendung der ungeklärten Daten zu prüfen, ob Identität mit der Person besteht, zu der er eine Auskunft haben wollte. Wenn diese Überprüfung in der Praxis nicht vorgenommen wird, kann dies für diese Person bei zufälliger Namensgleichheit sehr unangenehme Folgen haben.

Wenn die SCHUFA festgestellt hat, daß zwischen zwei namensgleichen Personen keine Identität besteht, vermerkt sie dies in ihrem Datensatz, so daß Verwechslungen nicht entstehen können.

6.5 Versicherungswirtschaft

6.5.1 Zentrale Dateien der Versicherungsverbände

Die bereits mehrfach dargestellte datenschutzrechtliche Problematik der Datenübermittlungen zwischen Versicherungsunternehmen und einigen Versicherungsverbänden (zuletzt 4. TB 5.4.1, S. 128 f.) wurde im Berichtsjahr weiter mit der Versicherungswirtschaft erörtert. Die Versuche zweier Verbände (Lebens- und HUK-Verband), die Meldeverfahren auf die Übermittlung anonymisierter Match-Codes umzustellen, sind fortgeschritten und werden voraussichtlich in absehbarer Zeit zu datenschutzgerechten Lösungen führen. Der Sachstand ist im einzelnen folgender:

6.5.1.1 Sonderwagnisdatei der Lebensversicherer

In meinem letzten Tätigkeitsbericht hatte ich bereits über das Match-Code-Verfahren berichtet, das der Verband der Lebensversicherungs-Unternehmen erprobt, um die datenschutzrechtlichen Probleme der Meldungen an und durch die Sonderwagnisdatei der Lebensversicherer zu beseitigen (4. TB, 5.4.1, S. 129).

Im Lebensverband wurde ein Vergleich von Neuzugangsmeldungen für Berufsunfähigkeits-Versicherungen mit dem 5-Jahres-Bestand an BV-Meldungen durchgeführt, um die Eindeutigkeit des Match-Codes zu prüfen. Das Match-Code-Verfahren führt danach nur zu einer unwesentlichen Verschlechterung der eindeutigen Identifizierbarkeit der Meldungen bei Vorliegen konkreter Anträge, führt aber andererseis zu einer Unkenntlichkeit der gespeicherten personenbezogenen Daten.

Die Versicherungswirtschaft hat erklärt, daß aufgrund der im Herbst 1986 im Lebensverband neu installierten EDV-Anlage eine Einführung des neuen Meldeverfahrens bis zum Ende des Jahres 1986 technisch möglich sein werde.

Die Datenschutz-Aufsichtsbehörden haben ihre Zustimmung zu dem neuen Meldeverfahren erklärt und erwarten, daß es in nächster Zeit von allen beteiligten Versicherungsunternehmen und dem Lebensverband umgesetzt wird.

6.5.1.2 Zentrale Registrierstelle Rechtsschutz

Wie bereits im letzten Tätigkeitsbericht (5.4.1, S. 129) dargestellt, soll möglicherweise ein dem Verfahren bei der Sonderwagnisdatei der Lebensversicherer entsprechendes Meldeverfahren auch für die Zentrale Registrierstelle Rechtsschutz des HUK-Verbandes eingeführt werden. Das Match-Code-Verfahren, das dafür seit Mitte 1986 erprobt wird, weist allerdings wegen der Andersartigkeit der Rechtsschutzversicherung mehrere Abweichungen auf (kein Geburtsdatum, statt dessen Adresse; Anfragen nur beim Unternehmen). Es ist noch keine Voraussage möglich, ob der Match-Code engmaschig genug und wie hoch die Fehlerquote ist. In die Meldungen an den HUK-Verband, bei dem erst der Match-Code gebildet wird, wird vorläufig die Postleitzahl mit aufgenommen, nicht jedoch in den Match-Code. Dies ist eine vorsorgliche Maßnahme für den Fall, daß sich im Laufe der Erprobung herausstellt, daß die Postleitzahl in den Match-Code mit aufgenommen werden muß.

In einem Gespräch mit der Versicherungswirtschaft haben die Datenschutz-Aufsichtsbehörden darauf hingewiesen, daß sie den jetzt in der Erprobungsphase vom HUK-Verband verwendeten Match-Code noch für verbesserungsbedürftig halten, da er aus ihrer Sicht noch keine genügende Anonymisierung darstellt, denn insbesondere bei kurzen Namen und Wohnorten kann zu leicht etwa mit Hilfe des Telefonbuchs festgestellt werden, um welche Person es sich handelt. Dies wäre zu vermeiden, wenn etwa der erste Buchstabe des Nachnamens und des Wohnortes weggelassen würde, denn dann wäre ein Auffinden im Telefonbuch nicht mehr möglich. Die Datenschutz-Aufsichtsbehörden würden es begrüßen, wenn hier der gleiche Match-Code wie bei den Lebensversicherern angewandt werden würde. Insbesondere halten sie es für wünschenswert, daß zur eindeutigen Identifizierung das Geburtsdatum mit aufgenommen wird. Die Versicherungswirtschaft hat darauf hingewiesen, daß es schwierig sei, im Bereich der Rechtsschutzversicherungen das Geburtsdatum zu erheben; die Versicherungsnehmer würden dafür kein Verständnis haben.

Zunächst soll die derzeit laufende Testphase beim HUK-Verband abgewartet werden. Dann sollen die Datenschutz-Aufsichtsbehörden über die Erfahrungen unterrichtet werden. Der HUK-Verband wird sich aber auch während dieser Testphase bei auftretenden größeren Schwierigkeiten bereits um eine Verbesserung des Match-Codes bemühen und ist für Änderungsvorschläge offen. Ich gehe daher davon aus, daß bei Auswertung der Ergebnisse der Erprobung die Bedenken der Datenschutz-Aufsichtsbehörden noch berücksichtigt werden können.

6.5.1.3 Meldeverfahren des Deutschen Transportversicherungsverbandes (DTV)

Über das Meldeverfahren der Reisegepäckversicherer, das vom DTV in Hamburg betrieben wird, habe ich in meinem 2. Tätigkeitsbericht (4.3.1.3, S. 116) Ausführungen gemacht. Meinen datenschutzrechtlichen Bedenken wird jetzt durch eine Neugestaltung dieses Meldeverfahrens Rechnung getragen, die ich mit dem DTV verabredet habe.

Der DTV will für die Meldungen ein neues Formular verwenden, in dem die zu übermittelnden Angaben auf Name und Adresse des Versicherungsnehmers, Schadenstag, Schadensort und Schadensart begrenzt wird. Mit diesem Formular kann das Verfahren in der bisherigen Form zum Zwecke der Regulierung konkreter Schadensfälle weitergeführt werden, d.h. die Meldungen der einzelnen Mitgliedsgesellschaften werden im DTV-Büro vervielfältigt und an die Mitgliedsgesellschaften verteilt. Hier sind die Meldungen notwendig, um für die Regulierung bestimmter Schadensfälle Doppelversicherungen und parallele Meldungen bei mehreren Versicherungsunternehmen festzustellen. Nach einer Frist, in der erfahrungsgemäß Schäden reguliert worden sind, müssen die Karteikarten dann bei den einzelnen Versicherungsunternehmen vernichtet werden.

Nach dem Abschluß der Regulierung der konkreten Schadensfälle ist es nicht vertretbar, die Karteikarten weiter bei den einzelnen Versicherungsunternehmen aufzubewahren. Für die evtl. spätere Feststellung von verschwiegenen Vorschäden kann nicht bei

allen Versicherungsunternehmen fünf Jahre lang die gesamte Karteikartensammlung weiterhin aufbewahrt werden. Dieser Zweck läßt sich auch erreichen, wenn die einzelnen Versicherungsunternehmen bei der Regulierung ihrer Schäden zur Feststellung von verschwiegenen Vorschäden bei der zentral beim DTV geführten Datei anfragen. Die Meldungen, die in der zentralen Datei des DTV geführt werden, können dort für diesen Zweck jeweils fünf Jahre aufbewahrt werden.

Die Datenschutz-Aufsichtsbehörden haben dieses Verfahren akzeptiert, sie haben aber gleichzeitig darauf hingewiesen, daß hier wie in allen anderen Fällen von Meldungen an zentrale Dateien die Datenschutzermächtigungsklausel verbessert werden muß, um mehr Transparenz für die betroffenen Versicherungsnehmer herzustellen und einige Zweifelsfragen zu beseitigen (siehe dazu im einzelnen unter 6.5.2).

6.5.2 Datenschutzermächtigungsklausel

Ich hatte bereits in meinem 2. Tätigkeitsbericht (4.3.1, S. 113 f.) darauf hingewiesen, daß die sog. Datenschutzermächtigungsklausel, die Versicherungsnehmer mit ihrem Antrag auf Abschluß einer Versicherung unterschreiben, datenschutzrechtlich problematisch ist. Die Versicherungswirtschaft weist hingegen darauf hin, daß die Klausel zusammen mit den Datenschutz-Aufsichtsbehörden in Kenntnis des gesamten Meldeverfahrens erarbeitet worden ist. Es könne deshalb davon ausgegangen werden, daß die Klausel auch nach Meinung der Datenschutz-Aufsichtsbehörden alle Datenübermittlungen im Rahmen des Meldeverfahrens abdecke. Die Aufsichtsbehörden halten es indessen für notwendig, die mittlerweile 8 Jahre alte Klausel im Lichte des Volkszählungsurteils des Bundesverfassungsgerichts und insbesondere auch des Urteils des Bundesgerichtshofes zur SCHUFA-Klausel neu zu überdenken.

Die Datenschutzermächtigungsklausel bildet nach ihrem Wortlaut keine den Anforderungen des § 3 BDSG genügende Einwilligung zur Übermittlung von Versicherungsunternehmen an zentrale Dateien, wenn der Zweck der Übermittlung darin besteht, andere Versicherungen auf Sonderwagnisse (Lebensversicherer) oder Vertragskündigungen (Rechtsschutzversicherer) hinzuweisen, die bei Abschluß neuer Verträge möglicherweise verschwiegen werden. Der Zweck „zur Beurteilung des Risikos und der Ansprüche" deckt nur Übermittlungen ab, die Risiko und Ansprüche im Rahmen des beantragten Versicherungsvertrages betreffen, nicht aber Übermittlungen zur Beurteilung des Risikos bei später zu beantragenden Versicherungsverträgen. Wenn auch Übermittlungen zu diesem Zweck von der Klausel umfaßt sein sollen, müßte die Klausel entsprechend umformuliert werden.

Weiter bildet die Datenschutzermächtigungsklausel keine Grundlage für Datenübermittlungen an zentrale Dateien nach Ablehnung oder Rücknahme des Antrages auf Abschluß eines Versicherungsvertrages. Denn die Einwilligung zu Datenübermittlungen ist ihrem Wesen nach streng akzessorisch; d.h. sie wird nur im Zusammenhang mit einem bestimmten den Betroffenen interessierenden Rechtsgeschäft abgegeben. Die Klausel ist regelmäßig Bestandteil des Antragsformulars. Es entspräche nicht dem Willen oder den Vorstellungen des Antragstellers, einen Fortbestand der Einwilligung über den Antrag hinaus anzunehmen.

Wenn die Datenschutzermächtigungsklausel auch Datenübermittlungen im Falle des Nichtzustandekommens von Versicherungsverträgen abdecken soll, müßte ihr Wortlaut entsprechend geändert werden. Dies wäre notwendig, da sich nicht sagen läßt, daß die Datenübermittlungen an die zentralen Dateien jedenfalls nach § 24 Abs. 1 Satz 1 BDSG zulässig sind. Die Datenübermittlungen finden ohne Einzelfallprüfung statt. Sie wären ohne Einzelfallprüfung nach § 24 Abs. 1 Satz 1 BDSG jedoch nur zulässig, wenn schlechthin kein Fall vorstellbar wäre, in dem eine Beeinträchtigung schutzwürdiger Belange Betroffener denkbar ist. Eine derartige Beeinträchtigung kann jedoch durchaus in Betracht kommen, z. B. wenn es Streit zwischen Versicherung und Betroffenem über die Beurteilung seines Gesundheitszustandes oder über die Rechtswirksamkeit der Kündigung einer Rechtsschutzversicherung gibt. Wenn die Versicherungs-

wirtschaft wegen der großen Anzahl der Fälle auf eine Einzelfallprüfung verzichten will, muß sie sich jeweils eine Klausel unterschreiben lassen, die die beabsichtigten Datenübermittlungen deckt.

Die Versicherungswirtschaft weist demgegenüber darauf hin, daß sich die früher geäußerte Kritik an der pauschalen Weitergabe von Daten durch die Verbände mit der Einführung des Match-Code-Verfahrens erledigt habe. Im Hinblick auf die positive Würdigung der bisher verwendeten Klausel in der Öffentlichkeit und auf die in der Praxis gewonnene Erkenntnis, daß das Bedürfnis nach zusätzlicher Information sehr gering sei, sind die Vertreter der Versicherungswirtschaft der Meinung, daß sich an dieser Einschätzung auch durch die Rechtsprechung der letzten Jahre nichts geändert habe und insofern kein Bedarf für eine Änderung der Klausel gesehen werde; wenn es nur um die Transparenz gehe, sei eine Verbesserung der zusätzlichen Information des Betroffenen ausreichend. Hierzu sei die Versicherungswirtschaft bereit.

Eine Konkretisierung der Klausel hält die Versicherungswirtschaft nicht für sinnvoll. Je konkreter eine Klausel werde, desto umfangreicher und desto schwerer lesbar und evtl. auch unverständlicher werde sie für den Betroffenen; dies könne sogar dazu führen, daß falsche Vorstellungen hervorgerufen werden. Ziel einer jeden Änderung der Klausel müsse aber eine Verbesserung der Lesbarkeit und der Verständlichkeit sein. Aus der Formulierung „. . . an den Verband und andere Versicherer zur Beurteilung des Risikos und der Ansprüche . . ." ergebe sich, daß hiermit nicht die Beschränkung auf das konkrete Risiko, dessen Deckung der Antragsteller begehre, gemeint sei. Die Formulierung sei vielmehr lediglich der Kürze wegen gewählt worden, da sich die Beurteilung auch auf die Ansprüche beziehe und eine Wiederholung vermieden werden solle. Eine Konkretisierung in diesem Punkt könnte in jedem Fall irreführend sein, da dann der Eindruck erweckt werde, daß immer übermittelt werde, was gerade nicht der Fall sei. Insofern beständen gute Gründe für eine Beibehaltung der Klausel in der jetzigen Form. Man sei aber bereit, das Merkblatt zu verbessern. Auch wurde auf die Frage der Rechtssicherheit und ihre Bedeutung für die Unternehmen hingewiesen.

Zu dem Argument, die Datenschutzermächtigungsklausel bilde keine Grundlage für eine Datenübermittlung an zentrale Dateien nach Ablehnung oder Rücknahme des Antrags auf Abschluß eines Versicherungsvertrages, erklärte die Versicherungswirtschaft:

Die Datenübermittlung an zentrale Dateien werde von der Datenschutzermächtigungsklausel auch nach Ablehnung oder Rücknahme des Antrages auf Abschluß eines Versicherungsvertrages gedeckt, solange die Einwilligung nicht zurückgenommen worden ist. Sinn und Zweck der Klausel sei es gerade, auch über den konkreten Vertrag hinaus eine sichere Rechtsgrundlage zu bieten, d.h. insbesondere in dem vorvertraglichen Stadium, bei Rücknahme oder Ablehnung eines Antrags, bei Nichtigkeit des Vertrages, bei Kündigung des Vertrages bei anderweitiger Antragstellung. Deshalb sei auch nur von „dem Risiko" und nicht von dem zu versichernden Risiko o.ä. die Rede. Insofern beziehe die Einwilligung sich notwendigerweise auch auf Datenübermittlungen, die über den konkreten Vertrag hinausgehen. Sie werde zwar anläßlich eines Antrags auf Abschluß eines bestimmten Rechtsgeschäfts abgeschlossen, sie sei in ihrem Bestand aber nicht davon abhängig. Sie verliere mit dem Nichtzustandekommen des Vertrages auch nicht ihren Sinn, da gerade die Tatsache des Nichtzustandekommens von Interesse sein kann. Allerdings könne der Betroffene für die Zukunft sein Einverständnis zurücknehmen; die im Vertrauen auf die Einwilligung bis dahin erfolgte Datenverarbeitung bleibe rechtmäßig.

Die Problematik der Datenschutzermächtigungsklausel wurde in verschiedenen Gesprächen mit der Versicherungswirtschaft erörtert. Der letzte Stand ist folgender:

Die Datenschutz-Aufsichtsbehörden wollen keine völlige Neufassung der Klausel erreichen, sondern meinen, daß die erforderlichen Verbesserungen auch durch Umformulierungen der bestehenden Klausel erreicht werden können.

Die Frage, ob Datenübermittlungen der Absicherung durch eine Klausel bedürfen, wenn die Daten in Match-Codes umgewandelt worden sind, läßt sich noch nicht ab

schließend beantworten, da noch unklar ist, ob alle von der Versicherungswirtschaft derzeit erprobten Match-Codes eine faktische Anonymisierung der Daten darstellen. In jedem Fall bedarf die Datenübermittlung von den Versicherungsunternehmen an die zentralen Dateien, die in nicht anonymisierter Form geschieht, der Absicherung durch eine Klausel.

Es soll weiter geprüft werden, ob eine klarere Formulierung für den Fall nötig ist, daß der Versicherungsvertrag (entweder wegen Rücknahme des Antrags durch den Interessenten oder wegen Nichtannahme durch das Versicherungsunternehmen) nicht zustandekommt, und daß aus der Klausel deutlicher hervorgehen muß, welche Übermittlungen stattfinden.

Die Datenschutz-Aufsichtsbehörden sind — wie dargestellt — der Ansicht, daß bei Nichtzustandekommen des Versicherungsvertrages nicht die Einwilligung des Kunden, sondern nur § 24 Abs. 1 Satz 1 BDSG als Rechtsgrundlage für eine Datenübermittlung in Betracht kommt. Sie halten einen Hinweis darauf in der Klausel für nötig. Der Betroffene muß dies wissen, um die Möglichkeit zu haben, seine Belange in die nach § 24 Abs. 1 Satz 1 BDSG von dem Versicherungsunternehmen vor der Übermittlung vorzunehmende Abwägung einbringen zu können.

Es sollen nun unter Berücksichtigung der erörterten Gesichtspunkte Vorschläge für eine Neuformulierung der Datenschutzermächtigungsklausel erarbeitet werden.

6.5.3 Schweigepflichtentbindungsklausel

Wie bereits mehrfach berichtet (zuletzt 4. TB, 5.4.2, S. 129 f.) unterliegt auch die bei Anträgen auf private Kranken-, Unfall- und Lebensversicherungen verwandte Schweigepflichtentbindungsklausel datenschutzrechtlichen Bedenken. Meine Position dazu soll im folgenden noch einmal kurz dargestellt werden.

6.5.3.1 Schweigepflichtentbindungsklausel in Fällen, auf die das Sozialgesetzbuch (SGB) anwendbar ist

§ 67 SGB X verlangt eine Einwilligung im Einzelfall, d.h. die Einwilligung muß aus einem konkreten Anlaß erfolgen und sich auf konkret erkennbare Datenflüsse beziehen. Bei der Einwilligung ist die von § 67 Satz 2 SGB X vorgeschriebene Form zu beachten.

Wegen des Erfordernisses der Einwilligung im Einzelfall kann die Befreiung von der Schweigepflicht grundsätzlich nur auf den Zeitpunkt der Antragstellung beschränkt sein. Den Betroffenen darf keine Einwilligung in Datenübermittlungen abverlangt werden, die in der Zukunft liegen und bei denen im Zeitpunkt der Abgabe der Erklärung noch nicht erkennbar ist, welche datenverarbeitende Stelle für die Zukunft von der Schweigepflicht entbunden wird. Wenn in der Zukunft eine Schweigepflichtentbindung nötig wird, ist es dem Versicherungsunternehmen zuzumuten, dann eine Schweigepflichtentbindungserklärung einzuholen. Es ist allenfalls vertretbar, daß für den Fall des Todes oder der Bewußtlosigkeit eine Schweigepflichtentbindung bereits zum Zeitpunkt der Antragstellung erklärt wird.

Es ist zu berücksichtigen, daß die Einwilligungserklärung gegenüber dem von der Schweigepflicht zu entbindenden Sozialleistungsträger abzugeben ist. Das Versicherungsunternehmen ist insoweit nur Bote. Daraus folgt, daß die von der Schweigepflicht zu entbindenden Sozialleistungsträger in der Erklärung einzeln aufgeführt werden müssen.

6.5.3.2 Schweigepflichtentbindungsklausel in Fällen, auf die das SGB nicht anwendbar ist

Eine umfassende Klausel, die alle Datenverarbeitungsvorgänge abdeckt, ist nicht zwingend notwendig. Der Betroffene muß im Einzelfall entscheiden können, ob und ggf. wann und in welchem Rahmen er von der Schweigepflicht entbinden will. Dabei muß er in dem Wissen handeln, daß eine Verweigerung der Schweigepflichtentbindung unter Umständen eine Versagung der Versicherungsleistung zur Folge haben kann.

Es besteht die Gefahr, daß eine umfassende Klausel in der bisher üblichen Form gegen den Bestimmtheitsgrundsatz verstößt und deshalb möglicherweise in gerichtlichen Verfahren für unwirksam erklärt wird.

Es ist erforderlich, daß mehr Transparenz für den Betroffenen hergestellt wird.

In Anbetracht der Sensibilität der hier angesprochenen personenbezogenen Daten dürfen die Versicherungsunternehmen Betroffenen die Schweigepflichtentbindung nur in den Fällen abverlangen, in denen dies unverzichtbar ist.

6.5.3.3 Bereichsspezifische Schweigepflichtentbindungsklauseln

6.5.3.3.1 Für Lebensversicherungen

Bei der von den Lebensversicherern verwendeten Schweigepflichtentbindungsklausel ist der Präzisierungsbedarf nicht so groß wie bei den anderen Klauseln. Gleichwohl ist hier klarzustellen, daß es sich um die Überprüfung des Gesundheitszustandes bei Vertragsabschluß handelt. Die Ermächtigung, bei Behörden anzufragen, muß aus der Klausel entfernt werden. Wenn sich herausstellen sollte, daß eine Notwendigkeit dafür besteht, wäre das Erfordernis der Einzelfallermächtigung für bestimmte Behörden zu berücksichtigen.

Die Klausel für Lebensversicherungen soll inhaltlich so begrenzt werden, daß nur Anfragen möglich sind, die für den konkreten Fall notwendig sind. Anfragen bei anderen Personenversicherern sollen auf die Unternehmen eingegrenzt werden, bei denen der Antragsteller versichert war oder ist.

6.5.3.3.2 Für Unfallversicherungen

Eine Schweigepflichtentbindungsklausel im Antrag auf Abschluß einer Versicherung ist lediglich für den Zweck der Risikoprüfung vor Vertragsabschluß zulässig.

Eine Schweigepflichtentbindung für den Zweck der Überprüfung der Leistungspflicht im Schadensfall darf dagegen nicht schon im Antrag auf Abschluß eines Versicherungsvertrages enthalten sein, da den Versicherern zuzumuten ist, sie einzuholen, wenn der Versicherungsnehmer einen Versicherungsfall meldet. Lediglich für den Fall, daß ein Unfall zum Tod oder zum Koma des Versicherungsnehmers führt, wäre eine vorherige Entbindung von der Schweigepflicht im Antrag auf Abschluß der Versicherung zulässig. Dem Versicherungsnehmer muß bei Vertragsabschluß deutlich gemacht werden, daß die Ermächtigung zur Schweigepflichtentbindung im Versicherungsfall eine Obliegenheit darstellt, deren Verletzung einen Verlust des Versicherungsschutzes zur Folge haben würde.

Hinsichtlich der Schweigepflichtentbindung von Sozialleistungsträgern muß der Versicherungsnehmer im Antrag darauf hingewiesen werden, daß ihn die Obliegenheit trifft, im Versicherungsfall anzugeben, wo im einzelnen angefragt werden darf.

6.5.3.4 Verhandlungen mit der Versicherungswirtschaft

Über die datenschutzrechtliche Problematik der Schweigepflichtentbindungsklausel haben die Datenschutz-Aufsichtsbehörden inzwischen einige Gespräche mit der Versicherungswirtschaft und dem Bundesaufsichtsamt für das Versicherungswesen (BAV) geführt. Zu der Frage der Schweigepflichtentbindung gegenüber Sozialversicherungsträgern erklärten die Vertreter der Versicherungswirtschaft, daß sich die Bedeutung von Anfragen bei diesen in den vergangenen Jahren sehr reduziert habe, so daß grundsätzlich ein weiterer Regelungsbedarf nicht vorhanden sei und die Schweigepflichtentbindung für Sozialversicherungsträger aus den Klauseln herausgenommen werden könne. Eine abschließende Äußerung durch die zuständigen Gremien der Fachverbände müsse allerdings noch abgewartet werden.

Die Vertreter der Versicherungswirtschaft erklärten weiter, daß auf die Schweigepflichtentbindung für Behörden in der Klausel nicht verzichtet werden könne. Für die Lebensversicherung sei zu berücksichtigen, daß Tote keine Einwilligung mehr geben können. Hier würden die Behörden aber auch nicht über die Gesundheitsverhältnisse der Betroffenen befragt, sondern über die Todesursache und die Gründe für den Tod.

Zu der Frage, ob bei Unfallversicherungen nicht eine Schweigepflichtentbindung im Schadensfall reiche und die Zukunftswirkung auf Unfälle mit Todesfolge beschränkt werden könne, erklären die Vertreter der Versicherungswirtschaft, zum einen werde die Schweigepflichtentbindung bereits bei Vertragsabschluß zur Überprüfung benötigt, zum anderen sei es für Unfallopfer unzumutbar, insbesondere nach einem schweren Unfall, zunächst noch eine Schweigepflichtentbindungsklausel unterschreiben zu müssen, bevor die Versicherung in eine Prüfung des Anspruchs eintritt. Die Datenschutz-Aufsichtsbehörden halten bei einer Schweigepflichtentbindung bereits im Antrag als Korrektiv eine verbesserte Aufklärung über die auf dieser Grundlage vorzunehmenden und vorgenommenen Datenübermittlungen für notwendig. Dies halten die Vertreter der Versicherungswirtschaft für überflüssig, weil der Betroffene durch eine Mitteilung seiner Versicherung ohnehin davon erfahre, wenn sich aus dem Leistungsantrag Anhaltspunkte für eine Leistungsminderung ergeben, die überprüft werden sollen; dabei hat der Betroffene durch die Angabe des Arztes in seinem Leistungsantrag die Schweigepflichtentbindung insoweit bereits konkretisiert. Falls vor einer endgültigen Entscheidung auch noch ein anderer als der im Leistungsantrag angegebene Arzt befragt werden soll, so wird der Betroffene auch darüber unterrichtet, denn nur er kennt die Namen dieser Ärzte. Damit wisse der Betroffene im konkreten Fall genau, für wen seine Schweigepflichtentbindungserklärung gelte. Dieses Verfahren einer Unterrichtung bei Nachfragen lasse sich aus § 11 VVG ableiten. Die Unterrichtung des Betroffenen liege aber auch im Interesse der Versicherungswirtschaft, um weitere Korrespondenz u.ä. bis hin zu einem evtl. Rechtsstreit zu vermeiden. Die Vertreter der Datenschutz-Aufsichtsbehörden haben sich eine abschließende Äußerung vorbehalten.

Die Probleme der Schweigepflichtentbindungsklausel und mögliche Neuformulierungen werden weiter zwischen Versicherungswirtschaft, BAV und Datenschutz-Aufsichtsbehörden diskutiert. Ich bin zuversichtlich, daß bald ein Ergebnis wird erzielt werden können.

6.5.4 Teilungsabkommen in der Versicherungswirtschaft

In meinem 4. TB (5.4.3, S. 130 f.) hatte ich darüber berichtet, daß aufgrund von Teilungsabkommen zwischen Versicherungsunternehmen manchmal mehr an Informationen an andere Unternehmen weitergegeben wird, als nach dem Teilungsabkommen nötig ist. Dies kann die Belange der Betroffenen verletzen, wenn das empfangende Unternehmen auf diese Weise an sensible Daten kommt, die es sonst nicht erhalten hätte.

Da diese Teilungsabkommen nach Mustern geschlossen werden, die vom HUK-Verband entwickelt worden sind, habe ich die Problematik mit diesem Verband erörtert. Er hat sich in seinen Gremien damit befaßt und ist bedauerlicherweise zu dem Ergebnis gekommen, daß eine Änderung der Teilungsabkommen nicht erforderlich sei.

Der HUK-Verband hat zur Begründung erklärt, Teilungsabkommen dienten grundsätzlich zur Regelung von Standardproblemen. Bei dem Beschwerdefall habe es sich jedoch um einen Einzelfall gehandelt, der in der Praxis nur selten vorkomme. Eine Beteiligung habe in diesem Fall nur durch Übersendung der Schadenanzeige nachgewiesen werden können. In der neuesten Fassung des Standard-Teilungsabkommens sei nunmehr vorgesehen, daß auf die Vorlage von Unterlagen zum Nachweis der Höhe der erstattungsfähigen Aufwendungen grundsätzlich verzichtet wird. Sowohl der Versicherungsnehmer als auch der Geschädigte seien verpflichtet, wahrheitsgemäße Angaben zu machen. Werde also eine Schadenanzeige wahrheitgemäß ausgefüllt, so dürften Probleme der von mir genannten Art überhaupt nicht entstehen.

Ich habe dazu gegenüber dem HUK-Verband folgendermaßen Stellung genommen:

Es ist richtig, daß nach dem neuen Standard-Teilungsabkommen „grundsätzlich auf die Vorlage von Unterlagen zum Nachweis der Höhe der zu erstattenden Aufwendungen verzichtet" wird. Auf die Vorlage von Unterlagen zum Nachweis des Grundes wird somit nicht verzichtet. Außerdem wird „nicht ausgeschlossen, daß der in Anspruch genommene Abkommenspartner die Übersendung derartiger Unterlagen im Einzelfall verlan-

gen kann". Auch nach diesem neuen Standard-Teilungsabkommen kann es also zur Übersendung von Unterlagen kommen. In diesen Fällen darf, wie ich bereits im vorigen Jahr ausgeführt habe, nicht mehr an Daten übermittelt werden, als für die Geltendmachung des Anspruchs nach dem Teilungsabkommen nötig ist. Es geht keinesfalls an, sämtliche von dem Versicherungsnehmer gegenüber seiner Versicherung gemachten Angaben komplett bei der Darlegung eines Anspruchs aus dem Teilungsabkommen an eine andere Versicherung zu übermitteln. Dies sollte in dem Standard-Teilungsabkommen ausdrücklich gesagt werden.

Weiter sollte klargestellt werden, daß Versicherungsunternehmen, die im Rahmen von Teilungsabkommen Daten übermittelt bekommen, diese nur für Zwecke verwenden dürfen, für die sie die Daten erhalten haben.

Die Ansicht des HUK-Verbandes, die von mir angesprochenen Probleme dürften nicht entstehen, wenn Geschädigte entsprechend ihrer Verpflichtung nur wahrheitsgemäße Angaben machen, kann ich nicht teilen. In dem Fall, der dieser Erörterung zugrunde liegt, hatte der Geschädigte eine — wie sich später herausstellte — falsche medizinische Einschätzung seiner Verletzungen in der Schadenanzeige niedergelegt. Ihm kann also nicht vorgeworfen werden, daß er gegen seine Verpflichtung zu wahrheitsgemäßen Angaben verstoßen habe. Indem eine falsche medizinische Beurteilung ohne Notwendigkeit nach dem Teilungsabkommen weitergegeben wurde, ist der anderen Versicherung erst ermöglicht worden, sie im Prozeß gegen den Geschädigten zu verwenden. Hier kann also nicht gesagt werden, daß diese Situation nicht eingetreten wäre, wenn der Geschädigte wahrheitsgemäße Angaben gemacht hätte, denn andere Angaben waren ihm nicht möglich.

Der HUK-Verband war leider nicht bereit, seinen Standpunkt noch einmal zu überprüfen.

6.5.5 Datenübermittlungen im Rahmen von fakultativen Gruppenversicherungsverträgen

Bereits mehrfach hatte ich über das Problem berichtet, daß Vereine oder Verbände im Rahmen fakultativer Gruppenversicherungsverträge personenbezogene Daten ihrer Mitglieder an Versicherungsgesellschaften übermitteln, ohne daß die Einwilligung der Betroffenen vorliegt (zuletzt 4. TB, 5.4.4, S. 131 f.)

Durch fakultative Gruppenversicherungsverträge erhalten die Vereinsmitglieder die Möglichkeit zum Abschluß von Einzelverträgen zu günstigeren Konditionen. Nach den Auflagen des BAV werden die Einzelverträge nur wirksam, wenn mindestens 50% der Mitglieder des jeweiligen Vereins derartige Verträge abgeschlossen haben.

Es konnte eine Einigung mit dem beteiligten Versicherungsunternehmen herbeigeführt werden, daß die Daten neu eintretender Mitglieder der Vereine grundsätzlich nur mit schriftlicher Einwilligung an die Versicherung übermittelt werden dürfen. Es wird sichergestellt, daß Beitrittswillige den Vereinen auch bei Streichung dieser Einwilligungsklausel im Aufnahmeantrag beitreten können. Für die „Altmitglieder" wurde eine Widerspruchslösung vereinbart. Ihnen soll vor Beginn von Werbeaktionen des Versicherungsunternehmens, zu dessen Vorbereitung eine Liste mit den Adressen der zu umwerbenden Mitglieder an die Versicherung übermittelt werden soll, Gelegenheit gegeben werden, dieser Übermittlung zu widersprechen.

Für die Fälle, in denen einzelne Vereine nicht bereit sind, die Widerspruchs- und Einwilligungslösung zu übernehmen, erwägt das Versicherungsunternehmen eine Lösung über Satzungsänderungen. Ich hatte in meinem 4. TB bereits auf die damit verbundenen rechtlichen Probleme hingewiesen (5.4.4, S. 132). Das Versicherungsunternehmen will in diesen Fällen durch zusätzliche Informationen sicherstellen, daß die Vereinsmitglieder umfassend über die Datenübermittlungen im Zusammenhang mit der Werbung für fakultative Gruppenversicherungsverträge unterrichtet werden, so daß sie in die Lage versetzt werden, diesen Übermittlungen ggf. zu widersprechen.

Das beteiligte Versicherungsunternehmen hat mir mitgeteilt, daß der mit mir vereinbarte Text für die Widerspruchsschreiben durch völlige Neuauflage aller Informationsschreiben bei allen Vereinen (mit einer, regional begrenzten Ausnahme) eingeführt worden ist. Für die sogenannten Altmitglieder ist das abgesprochene Verfahren also in die Wirklichkeit umgesetzt. Neumitglieder sollen mit ihren Aufnahmeunterlagen ebenfalls dieses Informationsschreiben erhalten.

Die Einwilligungslösung für Neumitglieder konnte dagegen noch nicht realisiert werden: Der größte Teil der Vereine wäre zwar im Prinzip bereit, von neu eintretenden Mitgliedern eine Einwilligung zur Datenübermittlung im Rahmen der fakultativen Gruppenversicherungsverträge einzuholen. In der Praxis zeigen sich jedoch die folgenden Schwierigkeiten:

— Die Beitrittsformulare werden — anders als die oben genannten Informationsschreiben — in eigener Zuständigkeit von den Vereinen gestaltet und hergestellt. Eine Änderung ist daher nicht kurzfristig zu realisieren.
— Manche Vereine möchten individuelle Vorstellungen oder Gegebenheiten berücksichtigen.
— Auf erhebliche Widerstände stößt es, die namentliche Bezeichnung des Versicherungsunternehmens in die vereinseigenen Beitrittserklärungen aufzunehmen.

Ob Vereine eine Einwilligung in Neuaufnahmeanträgen ganz ablehnen werden und statt dessen eine Satzungsänderung durchführen, ist somit noch offen.

6.5.6 Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD)

Die Versicherungswirtschaft sowie die öffentlich-rechtlichen und die privaten Bausparkassen unterhalten in Hamburg die Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD). Wie bereits in meinem 1. Tätigkeitsbericht (7.1.2 S. 52) erläutert, ist es ihre Aufgabe, zum Schutz der Verbraucher zu erreichen, daß nur vertrauenswürdige Personen im Versicherungsaußendienst tätig sind. Die AVAD vermittelt Auskünfte über Bewerber im Außendienst nur an ihre Mitgliedsunternehmen.

6.5.6.1 Das 1985 neu eingeführte Verfahren

Das mit Wirkung vom 1. August 1985 eingeführte neue Meldeverfahren der AVAD (vgl. 4. TB, 5.5.2, S. 133 f.), durch das meine früher geäußerten datenschutzrechtlichen Bedenken dieser Meldestelle gegenüber weitgehend ausgeräumt worden sind, hat sich nach meinem Eindruck eingespielt. Anfangsschwierigkeiten nach der Umstellung konnten in Gesprächen mit der AVAD und der Versicherungswirtschaft beseitigt werden.

6.5.6.2 „Vorab-Informationen" an die AVAD

Ich hatte in meinem 4. TB (5.5.2, S. 134) über einen Fall berichtet, in dem ein Versicherungsunternehmen vor dem Ausscheiden zweier Außendienstmitarbeiter „anstelle einer Auskunft" ein formloses Schreiben an die AVAD gerichtet hatte, in dem es darüber informierte, daß es kein Neugeschäft mehr von diesen Mitarbeitern annehmen wolle und daß es die Geschäftsbeziehungen mit diesen beiden Mitarbeitern auf die unumgänglich notwendigen Beziehungen aus den vorhandenen Versicherungsbeständen beschränke. Zur Beantwortung schriftlicher Anfragen anderer Gesellschaften sei das Unternehmen bereit. Die AVAD hat dieses Schreiben als Auskunft gewertet und anderen Gesellschaften vermittelt. Die Betroffenen haben keine Kopie dieses Schreibens erhalten.

Ich habe mit der AVAD Einigkeit darüber erzielt, daß Betroffene über derartige „Vorab-Informationen" in der gleichen Weise unterrichtet werden müssen wie über eine normale AVAD-Auskunft. Andernfalls könnte die Verpflichtung zur Information der Betroffenen dadurch umgangen werden, daß statt einer regulären AVAD-Auskunft eine „Vorab-Information" an die AVAD gegeben wird, durch die der Informationsfluß zwar auch sichergestellt wird, von der der Betroffene aber nichts erfährt. Damit wären die Verbesserungen, die mit dem 1. August 1985 in Kraft getreten sind, wieder rückgängig gemacht.

In zwei ähnlich gelagerten Eingabefällen hatte ein Versicherungsunternehmen Schreiben des Inhalts an die AVAD gerichtet, daß eine endgültige Auskunft noch nicht erstellt werden könne. Interessierte Anfrager sollten von der AVAD an ein bestimmtes Vorstandsmitglied der Versicherungsgesellschaft verwiesen werden. Die AVAD hatte diese Schreiben zu den Akten der Betroffenen genommen, ohne daß diese von dem Unternehmen oder der AVAD darüber informiert worden waren.

Meine Erörterung dieser Angelegenheit mit der AVAD hat zu folgendem Ergebnis geführt: Da ein derartiges Schreiben wie eine reguläre AVAD-Auskunft wirkt, ist der Betroffene in der gleichen Weise wie bei der Erstellung einer Auskunft zu unterrichten. Aus der Sicht des Datenschutzes sind derartige Schreiben jedoch unerwünscht, weil sie unkontrollierbare telefonische Informationsflüsse geradezu herausfordern. Da sie zudem auch von der AVAD wegen der dort geplanten Umstellung des Auskunftsverfahrens auf EDV in Zukunft nicht mehr verarbeitet werden können, ist jetzt folgende Lösung gefunden worden: Wenn derartige Schreiben bei der AVAD eingehen, werden sofort alle notwendigen Informationen daraus auf ein AVAD-Auskunftsformular übertragen, das dann der meldenden Versicherungsgesellschaft zur Unterschrift vorgelegt und anschließend im regulären Auskunftsverfahren verwendet wird. Dies bedeutet, daß der Betroffene von dieser Auskunft eine Kopie erhält und somit etwaige Unrichtigkeiten berichtigen oder sperren lassen kann.

Dadurch dürfte sichergestellt sein, daß das neue AVAD-Auskunftsverfahren nicht durch formlose Schreiben umgangen wird, von denen der Betroffene nichts erfährt.

6.5.6.3 AVAD-Auskünfte über Versicherungsmakler

Ein noch ungelöstes Problem ist die Behandlung selbständinger Versicherungsmakler im AVAD-Meldeverfahren.

In der Vergangenheit hat die AVAD in Einzelfällen Auskünfte auch über Maklerverhalten auf Anfrage übermittelt. Durch den kürzlich erfolgten Beitritt eines Makler-Verbandes hält die AVAD die Notwendigkeit der Auskunftserteilung über Makler für bestätigt. Die AVAD vertritt darüber hinaus die Auffassung, daß der Versicherungskunde, der sensible personenbezogene Daten offenbaren muß, vor unlauteren Personen zu schützen ist, egal ob sie als festangestellte oder als freie Mitarbeiter oder als Makler mit einer Versicherungsgesellschaft zusammenarbeiten.

Die Frage der Behandlung der Makler scheint mir bisher nicht genügend geprüft zu sein.

Zunächst ist festzustellen, daß ein Makler nicht zum Außendienst einer Versicherungsgesellschaft zu zählen ist. Er ist anders als der selbständige oder unselbständige Versicherungsvertreter nicht für ein oder mehrere Versicherungsunternehmen tätig, sondern ist selbständiger Vermittler zwischen Kunden und Unternehmen. Die Auskunftserteilung über Makler läßt sich also nicht mit der Auflage des BAV gegenüber den Versicherungsgesellschaften rechtfertigen, sie sollten nur zuverlässige Personen im Außendienst beschäftigen.

Wenn dennoch auch über Makler Auskünfte erteilt werden sollen, muß sichergestellt sein, daß alle bisher für die Außendienstmitarbeiter erreichten datenschutzrechtlichen Regeln auch den Maklern zugute kommen:

- Jeder einzelne Makler muß bei Beginn seiner Tätigkeit ausführlich über das AVAD-Auskunftsverfahren unterrichtet werden.
- Er muß in Ermangelung eines Anstellungs- oder Handelsvertreter-Vertrages gesondert in die Datenübermittlung an die AVAD einwilligen.
- Er muß bei Beendigung der Geschäftsbeziehung und in jedem Fall der Auskunftserteilung an die AVAD die Kopie der erteilten Auskunft von der Versicherungsgesellschaft erhalten.

Eine Unterrichtung der Makler über das AVAD-Auskunftsverfahren läßt sich am besten dadurch erreichen, daß diese bei der Benachrichtigung gem. § 34 Abs. 1 BDSG gleichzeitig eine Information über die Einzelheiten des AVAD-Verfahrens erhalten. Dies kann durch Übersendung des normalen Rundschreibens oder eines für Makler modifizierten Rundschreibens geschehen.

Die AVAD hat zugesagt, meine Anregung aufzugreifen und den Verband der Versicherungsmakler (VDVM), der Mitglied der AVAD ist, zu veranlassen, seine Mitglieder zu informieren. Zwischen AVAD und VDVM wurde folgende Absprache getroffen:

Der VDVM wird nach Abstimmung mit der AVAD ein Rundschreiben an seine Mitglieder herausgeben, in dem darauf hingewiesen wird, daß — nachdem der VDVM Mitglied der AVAD geworden ist — Unternehmen, die eine Courtagevereinbarung treffen, sich bei der AVAD erkundigen können und nach Aufhebung der Courtagevereinbarung dies der AVAD melden dürfen. Mit anderen Maklerverbänden ist bisher eine derartige Vereinbarung noch nicht zustande gekommen. Deshalb werden Makler, die nicht dem VDVM angeschlossen sind, gemäß § 34 Abs. 1 BDSG im Falle einer Weitergabe der Auskunft an Dritte von der Speicherung bei der AVAD direkt unterrichtet. Die AVAD hat weiter zugesagt, nach einem Gespräch mit dem VDVM zu prüfen, ob das jetzige AVAD-Auskunftsformular für Makler geeignet ist oder ob für diese Personengruppe ein eigenes Formular erforderlich ist.

6.6 Auskunfteien

6.6.1 Angebot von bonitätsgeprüften Adressen durch Handels- und Wirtschaftsauskunfteien

Wie bereits mehrfach berichtet (zuletzt 4. TB, 5.5.1.1, S. 132), beschäftige ich mich seit einiger Zeit mit der Frage, ob die Weitergabe bonitätsgeprüfter Adressen durch Handels- und Wirtschaftsauskunfteien an ihre Kunden datenschutzrechtlich unbedenklich ist. Ich habe bei einer Auskunftei, die die bonitätsgeprüften Adressen anbietet, eine Prüfung nach § 40 BDSG vorgenommen, die folgendes ergeben hat:

Wenn ein Interessent bonitätsgeprüfte Adressen von Unternehmen zur Werbung einsetzen will, gibt er folgende Kriterien zur Zielgruppenbeschreibung an:

- Kategorien von Unternehmen, definiert nach dem Schlüssel des Statistischen Bundesamtes;
- bestimmte Kriterien, die bei der Adressenselektion berücksichtigt werden sollen (z.B. kein Unternehmen mit einem Umsatz unter DM . . .);
- eine bestimmte Bonitätseinstufung.
  Die Auskunftei ordnet, soweit ihr dafür Informationsgrundlagen vorliegen, die Unternehmen in bestimmte Bonitätsklassen ein. Die dafür verwendeten zweistelligen Zahlen entsprechen in ihrer ersten Ziffer den Schulnoten 1-6. Z.B. steht 30 für „befriedigendes Zahlungsverhalten". Innerhalb der „Noten" gibt es feinere Untergliederungen, z.B. 35, 36 etc. Diese Zahlen haben gruppenweise unterschiedliche Bedeutungen. Die zweite Ziffer gibt etwa die unterschiedliche Länge der Zahlungsziele oder ähnliches an.

Wenn ein Interessent Adressen von Unternehmen kaufen will, die in eine bestimmte Bonitätsstufe eingeordnet sind, erhält er die Adressen aller Unternehmen, für die diese Bonitätsstufe vermerkt ist. Unternehmen, für die ein anderer Bonitätscode oder wegen nicht vorliegender Informationen gar keiner gespeichert ist, fallen bei der Auswahl heraus.

Die selektierten Adressen werden in einer Liste ausgedruckt oder auf ein Band übertragen. Die Adressen werden dann zusammen mit der Rechnung an der Auftraggeber gegeben. Vertraglich ist die Nutzung konkret (in der Regel auf eine Werbeaktion) beschränkt.

Für die Selektion werden ausschließlich Adressen verwandt, die bereits im Bestand vorhanden sind. Die Betroffenen sind somit über die Speicherung schon benachrichtigt worden.

Die Übermittlung der bonitätsgeprüften Adressen von der Auskunftei an die Kunden stößt auf erhebliche rechtliche Bedenken: Wie bereits im 3. TB (4.4.1, S. 107 f.) ausgeführt, stellt die Nichtaufnahme bestimmter Unternehmen in die Marketing-Adressenverzeichnisse inzident auch eine negativ zu wertende Kreditauskunft über diese dar, denn die unter bestimmten Merkmalen selektierten Adressen werden an einen Interessentenkreis weitergegeben, der in der Mehrzahl der Fälle dem von ihm anvisierten Markt nicht völlig ohne Kenntnisse gegenüberstehen wird. Insoweit wird also auch eine (negative) Auskunft über diejenigen erteilt, die in der Liste der selektierten Adressen nicht enthalten sind. Der Interessent wird jedoch nicht in der Lage sein, ein berechtigtes Interesse an dem Erhalt dieser (negativen) Auskünfte darzulegen.

Die Auskunftei ist demgegenüber der Auffassung, daß einzelne Unternehmen aus zu vielen Gründen (Nichtvorliegen von Informationen, Zufälligkeiten bei der Auswahl der zu selektierenden Branche nach dem Schlüssel des Statistischen Bundesamtes, Robinson-Liste) in der Adressenliste fehlen können, als daß das Nichtaufnehmen in eine bonitätsgeprüfte Liste als Negativauskunft zu werten wäre. Die Auskunftei weise ihre Kunden in den Vorgesprächen vor Auftragserteilung ausführlich gerade auf diese Einzelheiten hin, damit sie sich überhaupt eine Vorstellung von dem Umfang der von der Auskunftei verfügbar gehaltenen Daten und Möglichkeiten machen könnten. Gerade aufgrund dieser eingehenden Erläuterungen würden vom Kunden die eingrenzenden Maßnahmen festgelegt, unter Berücksichtigung weiterer Eingrenzungen wie z. B. der Robinson-Liste. Es könne also nicht der Eindruck entstehen, daß eine nicht aufgeführte Firma fehle, da ihre Bonität für die Anforderung nicht ausreichend sei. Im übrigen gebe es nach Wissen der Auskunftei überhaupt keine Selektionsläufe, in denen die Anzahl der für Werbezwecke übermittelten Adressen so gering sei, daß der Kunde vorhandene oder nicht vorhandene Firmen bei der Menge der erhaltenen Unterlagen unterscheiden könne.

Gleichwohl habe ich Zweifel, ob die Kunden der Auskunftei im allgemeinen so genau über diese Zusammenhänge informiert sind, daß sie wissen, aus wie vielen Gründen ein Unternehmen in der Liste fehlen kann. Es kann doch leicht der Eindruck entstehen, das Fehlen in der Liste deute auf eine schlechte Bonität hin.

Darüber hinaus bestehen Bedenken gegen die Übermittlung der selektierten Adressen, weil die Kunden der Auskunftei nicht in der Lage sind, ein berechtigtes Interesse am Erhalt aller einzelnen Anschriften darzulegen.

Es handelt sich nicht um eine listenmäßige Übermittlung nach § 32 Abs. 3 BDSG, weil mehr als ein Merkmal über die Zugehörigkeit zu einer bestimmten Personengruppe übermittelt wird (Bonitätsklasse, Postleitzahlbezirke, Mindestumsatz etc.). Die Übermittlung ist also an § 32 Abs. 2 Satz 1 BDSG zu messen. Für die Darlegung des berechtigten Interesses im Sinne dieser Vorschrift reicht es nicht, global ein berechtigtes Interesse an einer Gruppe von Daten darzulegen. Der Interessent hat vielmehr ein spezifisches Interesse an ganz bestimmten Daten für im einzelnen zu benennende Ziele oder Geschäftszwecke glaubhaft darzulegen. Dies ist dem Kunden jedoch nicht möglich. Die Übermittlung der bonitätsgeprüften Adressen an die Kunden ist somit unzulässig, weil kein berechtigtes Interesse dargelegt ist.

Die Übermittlung wäre somit nur mit Einwilligung des Betroffenen möglich. Diese liegt jedoch nicht vor.

Die Auskunftei vertritt dagegen die Auffassung, daß eine pauschale Darlegung des berechtigten Interesses in bezug auf eine nach vorgegebenen Kriterien zusammengesetzte Gruppe von Personen den Anforderungen des § 32 Abs. 2 BDSG genüge.

Bei der Beurteilung der datenschutzrechtlichen Zulässigkeit der Speicherung der Adressen ist zu berücksichtigen, daß die Auskunftei die personenbezogenen Daten zunächst zu dem Zweck gespeichert hat, bei Kreditentscheidungen Auskünfte über die

Bonität des Betroffenen erteilen zu können. Dazu war gemäß § 32 Abs. 1 BDSG im Einzelfall zu prüfen, ob die schutzwürdigen Belange des Betroffenen hinter dem Interesse an der Speicherung der personenbezogenen Daten zum Zwecke der Auskunfterteilung bei Kreditentscheidungen zurücktreten müssen. Durch die Erweiterung des Geschäftszweckes — nämlich Weitergabe von bonitätsgeprüften Marketingadressen — wird eine zusätzliche Interessenabwägung erforderlich. Sie dürfte in der Regel dazu führen, daß die schutzwürdigen Belange des Betroffenen höher zu bewerten sind als das Interesse der Auskunftei, mit qualifiziertem Adreßmaterial zu werben. Die Speicherung wäre dann zu diesem Zweck nicht zulässig.

Die Auskunftei hat dazu erklärt, an die Beurteilung von bonitätsgeprüften Adressen seien keine anderen Maßstäbe anzulegen als die des berechtigten Interesses für eine Auskunft. Da die Auskunftei darüber hinaus über die Beachtung der Robinson-Liste diejenigen herausselektiere, die werbemäßig nicht angesprochen werden wollten, unterlägen die der Auskunftei zugänglichen Daten von seiten der Betroffenen auch keiner zusätzlichen Abwägung.

Ich teile diesen Standpunkt nicht und halte an meiner oben dargestellten Auffassung fest. Der Hinweis auf die Beachtung der Robinson-Liste geht insoweit fehl, als keineswegs jeder Bundesbürger, der die Zusendung von Werbung nicht wünscht, in der Robinson-Liste verzeichnet ist.

6.6.2 „Waschabgleich"

Die geprüfte Auskunftei bietet neben den bonitätsgeprüften Adressen einen sogenannten „Waschabgleich" an. Dabei wird ein für eine konkrete Werbeaktion von einem Unternehmen angemieteter Adressenbestand vor der Aussendung durch einen Lettershop mit dem Bestand der Auskunftei auf Eintragungen im Schuldnerverzeichnis hin abgeglichen. Die Auskunftei stellt eine Negativliste zusammen. Der Lettershop selektiert zunächst mögliche Doubletten, ggf. eigene Kunden des Werbenden, Einträge in der Robinson-Liste und schließlich die „Negativen" aus den Beständen der Auskunftei. Der Lettershop gibt die Werbung direkt zur Post auf, so daß der Werbende erst von einem Umworbenen Kenntnis erhält, wenn dieser auf die Zusendung reagiert. Die herausselektierten Adressen werden dem werbenden Kunden nicht bekannt, er erhält lediglich ein Protokoll, aus dem sich ergibt, welche Anzahl von Adressen beim einzelnen Selektionsschritt herausgefallen sind.

Bei diesem „Waschabgleich" findet eine Datenübermittlung von der Auskunftei an den Lettershop statt. Die Zulässigkeit der Datenübermittlung muß nach § 32 Abs. 2 bzw. Abs. 3 BDSG beurteilt werden. Soweit sich die Übermittlung auf die in § 32 Abs. 3 BDSG genannten personenbezogenen Daten beschränkt, habe ich keine Bedenken gegen sie. Dagegen halte ich die Übermittlung von personenbezogenen Daten über diesen Rahmen hinaus für unzulässig, da die gemäß § 32 Abs. 2 BDSG in bezug auf jeden einzelnen Betroffenen erforderliche glaubhafte Darlegung eines berechtigten Interesses nicht möglich ist. Die Auskunftei hat mir dazu mitgeteilt, daß sie bei derartigen „Waschabgleichen" nie mehr als ein Merkmal übermittele, so daß bei ihr dieses Verfahren in jedem Falle zulässig sei.

6.6.3 Anforderungen an die Glaubhaftmachung des berechtigten Interesses nach § 32 Abs. 2 BDSG

Die Datenschutz-Aufsichtsbehörden haben gelegentlich zu beanstanden, daß Auskunfteien manchmal ihren Kunden auch dann Daten übermitteln, wenn diese ein berechtigtes Interesse nicht ausdrücklich dargelegt haben, weil auf dem Anfragezettel keines der aufgeführten Merkmale angekreuzt ist.

In einem Gespräch mit Vertretern von Handelsauskunfteien erklärten diese, daß es sich hierbei um ein mehr organisatorisches als datenschutzrechtliches Problem handele. Den Sachbearbeitern der Handelsauskunfteien seien die meisten ihrer Kunden bekannt. Dementsprechend wüßten sie im allgemeinen, welche Kunden aus welchem

Grunde anfragen. Da etwa 90 % aller Anfragen wegen einer Kreditentscheidung erfolgten, hielten sie es für vertretbar, das berechtigte Interesse auch dann als glaubhaft dargelegt anzusehen, wenn der Kunde im Einzelfall versäumt haben sollte, den Anfragegrund besonders anzukreuzen. Im Falle einer „ungewöhnlichen" Anfrage werde die Auskunft erst erteilt, nachdem der Sachbearbeiter sich wegen des berechtigten Interesses des Kunden vergewissert habe. Aufgrund dieses Verfahrens komme es nur relativ selten vor, daß Auskünfte aufgrund eines vorgetäuschten berechtigten Interesses erteilt werden.

Die Vertreter der Handelsauskunfteien sagten gleichwohl zu, die ihnen angeschlossenen Auskunfteien nochmals darauf hinzuweisen, daß das berechtigte Interesse durch ausdrückliche Angabe der Gründe darzulegen ist. Dies ist inzwischen geschehen.

6.6.4 Benachrichtigung nach § 34 Abs. 1 BDSG in Verbindung mit der Aufforderung zur Selbstbeauskunftung

Ich hatte in meinem 4. TB (5.5.1.2, S. 133) darauf hingewiesen, daß Handelsauskunfteien im Zusammenhang mit der Benachrichtigung nach § 34 Abs. 1 BDSG oft um ergänzende Angaben zur Person des Betroffenen bitten. Bei einigen Betroffenen hat dieses Verfahren den Eindruck erweckt, als seien sie zur Angabe weiterer Daten verpflichtet. Verstärkt wurde dieser Eindruck auch dadurch, daß diese Anschreiben vom „betrieblichen Datenschutzbeauftragten" unterschrieben waren. Ich rege an, in Zukunft durch eine auch optisch klare Trennung der Benachrichtigung von der Bitte, weitere Angaben zur Person zu machen, derartige Mißverständnisse möglichst auszuschließen.

Eine Auskunftei hat mir dazu erklärt, die Aufteilung in zwei Briefe sei aus Kostengründen wohl kaum vertretbar. Ich meine, daß eine deutlichere Trennung auch erreichbar sein müßte, wenn die Benachrichtigung nach § 34 Abs. 1 BDSG und die Bitte um weitere Daten in einem Briefumschlag versandt werden.

Darüber hinaus würde ich es begrüßen, wenn dem Betroffenen gleichzeitig mit der Benachrichtigung die zu seiner Person gespeicherten Daten mitgeteilt würden. Die Handelsauskunfteien sehen hierzu keine Veranlassung, da zu Privatpersonen zum Zeitpunkt der die Benachrichtigung auslösenden erstmaligen Übermittlung im Regelfall nur die Daten gespeichert seien, die der Auskunftei durch die Anfrage des Kunden und ggf. aufgrund einer Auskunft der Meldebehörde bekanntgeworden sind.

Die Erfahrung zeige im übrigen, daß nur ein Bruchteil der benachrichtigten Personen Interesse an den eigenen Daten zeige. Diesem Interesse kämen die Auskunfteien dann kostenlos durch Übermittlung aller gespeicherten Daten nach.

6.6.5 Beweislast bei Unstimmigkeiten über die Richtigkeit von Auskünften

Es kommt immer wieder vor, daß Betroffene die Richtigkeit einzelner Angaben in den Auskünften von Handelsauskunfteien oder Branchenauskunftsdiensten bestreiten. Wenn diese Daten unrichtig sind, haben die Betroffenen nach § 35 Abs. 1 BDSG einen Berichtigungsanspruch. Wenn sich weder die Richtigkeit noch die Unrichtigkeit der Daten feststellen läßt, sind sie nach § 35 Abs. 2 BDSG zu sperren. Da die Auskunfteien selbst daran interessiert sind, daß nur Auskünfte mit richtigen Daten verwendet werden, ist es zum Teil Praxis, auf bloßes Bestreiten hin die bestrittenen Teile der Auskünfte bis zur Klärung vorläufig zu sperren. Die übrigen Teile der Auskünfte bleiben davon unberührt und werden dann weiter übermittelt. Erweisen sich die Einwände des Betroffenen als zutreffend, erfolgt insoweit eine Löschung. Diese Praxis begrüße ich.

In einem Fall traten jedoch Unstimmigkeiten über die Frage auf, wie konkret ein Betroffener einzelne Teile von Auskünften bestreiten muß und wie dann die Beweislast für die Richtigkeit oder Unrichtigkeit der Angaben verteilt ist. Ich bin der Ansicht, daß es zwar nicht genügt, eine Auskunft pauschal zu bestreiten, ohne die bestrittene Information

näher zu bezeichnen; der Betroffene muß vielmehr genau angeben, welchen Teil der Auskunft er bestreitet. Mehr braucht er allerdings nicht zu tun. Er braucht insbesondere nicht mitzuteilen, welche richtigen Daten an die Stelle der bestrittenen Daten gesetzt werden sollen.

Sofern ihm dies aufgrund seines Informationsstandes möglich ist, sollte der Betroffene auch mitteilen, warum seiner Meinung nach die bestrittenen Angaben falsch sind. In dem Beschwerdefall hatte ein Betroffener die Richtigkeit der Angabe in einer Auskunft bestritten, seine Mitarbeit in einem Unternehmen sei wegen „Manipulationen im Schadensbereich" beendet worden. Er wisse aber nicht, welche Manipulationen ihm vorgeworfen würden, so daß er auch nicht begründen könne, weswegen diese Angabe falsch sei. In einem Fall wie diesem muß das bloße Bestreiten ausreichen. Die Auskunftei muß dann nachweisen, daß die bestrittenen Angaben richtig sind. Nach den Regeln der Beweislastverteilung im Zivilrecht müßte eigentlich der Betroffene den Beweis dafür führen, daß die bestrittenen Angaben falsch sind, wenn er bestimmte Angaben bestreitet. Hier muß jedoch etwas anderes gelten. Der Gesetzgeber hat bereits durch seine Formulierung „wenn sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt" deutlich gemacht, daß hier die Beweislast nicht auf der Seite des Bestreitenden liegen soll. Er hat berücksichtigt, daß der Betroffene in den seltensten Fällen faktisch in der Lage sein wird, den Nachweis der Unrichtigkeit bestimmter Angaben zu führen. Dies muß zu einer Umkehrung der Beweislast zu Lasten der speichernden Stelle führen.

Der Beschwerdefall, der zur Erörterung dieser Frage geführt hat, ist inzwischen dadurch erledigt worden, daß das Unternehmen, von dem die Information stammte, seine Auskunft in dem bestrittenen Teil berichtigt hat.

6.6.6 Einzelfälle

6.6.6.1 Erschleichen einer Wirtschaftsauskunft

Gelegentlich äußern Betroffene die Vermutung, daß über sie eine Wirtschaftsauskunft an jemand erteilt wurde, der kein berechtigtes (wirtschaftliches) Interesse hieran haben kann. Ein krasses Beispiel war die Anfrage eines jungen Unternehmers, der nacheinander über drei junge Frauen, mit denen er rein private Beziehungen unterhielt, Auskünfte einholte.

In einem anderen Beschwerdefall hatte der Rechercheur einer Handels- und Wirtschaftauskunftei zwei Telefonnummern verwechselt, und dadurch kam heraus, daß der Auftraggeber sich eine Auskunft erschleichen wollte. Der Rechercheur hatte zunächst beim Betroffenen angerufen und ihn um Angaben über seine wirtschaftlichen Verhältnisse gebeten. Eine Weile später rief er noch einmal an und fragte nun nach dem früheren Arbeitgeber — offenbar um diesem das Ergebnis seiner Recherche mitzuteilen. Der Betroffene hatte sich kurz vorher in derselben Branche selbständig gemacht, und er vermutete, daß die Wirtschaftsauskunft eingesetzt werden sollte, um ihn als Mitbewerber zu beobachten.

Die Prüfung bei der Auskunftei ergab, daß der ehemalige Arbeitgeber tatsächlich mit der Begründung „Bonitätsprüfung" angefragt und eine Auskunft erhalten hatte. Für die Auskunftei war nicht erkennbar, daß die Angabe über den Anfragegrund nicht der Wahrheit entsprach und der Anfragende kein berechtigtes Interesse geltend machen konnte.

Ich habe in beiden Fällen die Betroffenen darauf hingewiesen, daß sie durch die Staatsanwaltschaft prüfen lassen könnten, ob eine strafbare Handlung vorliege.

Nicht in Betracht kommt der Tatbestand des § 41 Abs. 1 Nr. 2 BDSG. Hiernach macht sich strafbar, wer vom BDSG geschützte personenbezogene Daten unbefugt abruft. Abrufen ist jedoch lediglich die Kenntnisnahme automatisch gespeicherter Daten durch technische Hilfsmittel. Darunter fällt u.a. die Kenntnisnahme über einen Bild

schirm oder die Operator-Konsole. Da die Auskunftei die personenbezogenen Daten zwar automatisiert verarbeitet, die Auskunft aber in Form eines Briefes erteilt hat, ist diese Variante nicht erfüllt.

Nach § 41 Abs. 1 Nr. 1 BDSG ist aber auch das unbefugte Übermitteln der vom BDSG geschützten Daten strafbar. Da nach meinen Feststellungen ein berechtigtes Interesse an der Wirtschaftsauskunft nicht vorlag, ist der objektive Tatbestand der unbefugten Übermittlung des § 41 Abs. 1 Nr. 1 BDSG erfüllt.

Zweifel bestehen indessen, ob auch das subjektive Element gegeben ist. Die Auskunftei ist zu der Datenübermittlung durch Täuschung veranlaßt worden. Ihr war also nicht bekannt, daß ihr die Befugnis zum Übermitteln fehlte. Wohl aber könnte der Kunde, der unter Vortäuschung eines nicht vorhandenen berechtigten Interesses die Auskunft „erschlichen" hat, den Straftatbestand der unbefugten Datenübermittlung in mittelbarer Täterschaft verwirklicht haben, während die Auskunftei lediglich als „schuldloses, getäuschtes Werkzeug" anzusehen wäre.

Ob mit dieser Begründung eine Bestrafung möglich ist, ist bisher noch nicht gerichtlich geprüft worden.

6.7 Arbeitnehmer-Datenschutz

6.7.1 Telefondatenerfassung

In meinem 3. Tätigkeitsbericht (4.7.5, S. 125 ff.) hatte ich ausführlich über die datenschutzrechtliche Problematik der Telefondatenerfassung berichtet. Meines Erachtens hat der Arbeitgeber zwar ein berechtigtes Interesse im Sinne des § 23 Satz 1 BDSG an der Speicherung von Datum und Uhrzeit, Nebenstellennummer und Anzahl der Gebühreneinheiten, das die schutzwürdigen Belange der Arbeitnehmer überwiegt. Das Speichern der vollständigen Telefonnummer der Angerufenen, der sogenannten Zielnummer, ist jedoch nicht rechtmäßig, weil es die schutzwürdigen Belange sowohl der Angerufenen als auch der Arbeitnehmer verletzen würde.

Ich hatte bereits darauf hingewiesen, daß die Rechtsprechung divergierende Ansichten zu dieser Problematik vertritt. Meine Auffassung ist vom Arbeitsgericht Hamburg (Beschlüsse vom 3. Oktober 1984, 23 Bv 6/84, und vom 19. Dezember 1984, 6 Bv 14/83 — nicht rechtskräftig) und vom Landesarbeitsgericht Hamburg (Beschluß vom 31. Januar 1986, 8 Ta Bv 1/85 — nicht rechtskräftig —, BB 1986, S. 529, DB 1986, S. 702) bestätigt worden. Das Landesarbeitsgericht Düsseldorf hat dagegen gemeint, die Speicherung der Zielnummern sei datenschutzrechlich nicht zu beanstanden (Beschlüsse vom 30. April 1984, 10 (12) Ta Bv 10/84, und vom 17. Mai 1984, 13 Ta Bv 115/83).

Das Bundesarbeitsgericht (BAG) hat die Auffassung des Landesarbeitsgerichts Düsseldorf in seinem Beschluß vom 27. Mai 1986 (1 ABR 48/84, CR 1986, S. 571) im Ergebnis bestätigt und den angegriffenen Einigungsstellenspruch für rechtmäßig erklärt, in dem für dienstliche externe Telefongespräche u.a. die Speicherung der angewählten Teilnehmernummer vorgesehen ist. Das BAG hat darin keinen Verstoß gegen das BDSG gesehen. Zwar handele es sich bei den gespeicherten Daten der Arbeitnehmer und auch der Angerufenen um personenbezogene Daten im Sinne des § 2 Abs. 1 BDSG. Die Verarbeitung der Daten der Arbeitnehmer in Form der Erfassung der Telefondaten durch die Telefonanlage des Arbeitgebers sei aber datenschutzrechtlich zulässig, weil sie durch die Betriebsvereinbarung und den diese ergänzenden Spruch der Einigungsstelle „erlaubt" im Sinne des § 3 Satz 1 Nr. 1 BDSG werde. Eine „andere Rechtsvorschrift" im Sinne des § 3 Satz 1 Nr. 1 BDSG könnten auch die normativen Bestimmungen eines Tarifvertrages oder einer Betriebsvereinbarung sein. Daraus folge, daß sie hinsichtlich ihres zulässigen Inhalts nicht an den Vorschriften des BDSG zu messen seien. Datenschutzrechtliche Regelungen in Tarifverträgen oder Betriebsvereinbarungen müßten sich lediglich im Rahmen der Regelungsautonomie der Tarifvertragsparteien bzw. der Betriebspartner halten und die für diese Autonomie geltenden,

sich aus grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen beachten. In diesem Rahmen halte sich der angegriffene Einigungsstellenspruch. Die darin vorgesehene Erfassung von Telefondaten berücksichtige die Grundsätze für den Persönlichkeitsschutz des Arbeitnehmers im Arbeitsverhältnis und die grundgesetzliche Wertentscheidung für einen freien und ungehinderten Fernsprechverkehr.

Ob die in der Telefondatenerfassung ebenfalls enthaltene Verarbeitung personenbezogener Daten der Angerufenen als Anschlußinhaber oder gar als Gesprächsteilnehmer datenschutzrechtlich zulässig sei, habe das BAG nicht zu entscheiden gehabt. Durch den Spruch der Einigungsstelle würden Rechte auf Datenschutz dieser Dritten nicht verletzt. Betriebsvereinbarungen und diese ersetzende Sprüche der Einigungsstelle könnten nur das Verhältnis zwischen Arbeitnehmer und Arbeitgeber regeln. Für das Verhältnis des Arbeitgebers zu Dritten seien sie ohne rechtliche Bedeutung. Der Spruch der Einigungsstelle, über den allein das BAG zu entscheiden hatte, sei jedenfalls nicht deswegen unwirksam, weil durch die Telefondatenerfassung möglicherweise Datenschutzrechte der angerufenen Dritten verletzt würden.

Ich halte diese Rechtsprechung für unbefriedigend. Die rechtliche Überprüfung einer Betriebsvereinbarung oder eines diese ersetzenden Einigungsstellenspruchs über die Zulässigkeit einer Telefondatenerfassungsanlage in einem Betrieb darf nicht unberücksichtigt lassen, ob Persönlichkeitsrechte Dritter verletzt werden. Eine Betriebsvereinbarung, die die rechtswidrige Speicherung von angerufenen Telefonnummern beinhaltet, ist meines Erachtens nach § 134 oder § 138 Abs. 1 BGB nichtig.

Auch das Landesarbeitsgericht Hamburg hat in seinem Beschluß vom 31. Januar 1986 darauf hingewiesen, daß durch eine Betriebsvereinbarung oder einen Einigungsstellenspruch die Rechte der Angerufenen nicht eingeschränkt werden dürfen. „Im Verhältnis zum Dritten (Angerufenen) ist . . . das Gebot der Rangfolge der Rechtsquellen zu beachten, so daß das BDSG durch das autonome objektive Satzungsrecht einer Betriebsvereinbarung nicht verdrängt werden kann. Das verbietet sich schon deshalb, weil die Autonomieermächtigung der Betriebspartner naturgemäß auf den konkreten Sachbereich bzw. Mitgliederstand beschränkt ist" (DB, 1986, S. 703).

Ich hoffe, daß die Revision gegen den Beschluß des Landesarbeitsgerichts Hamburg dem Bundesarbeitsgericht Gelegenheit geben wird, erneut über die Speicherung von Zielnummern zu befinden, um angesichts unterschiedlicher Rechtsansichten in Rechtsprechung und Literatur eine für die Praxis wünschenswerte Klarstellung herbeizuführen.

6.7.2 Personalfragebogen

Ich habe mich bereits mehrfach (2. TB, 4.8.3, S. 133 f., 3. TB, 4.7.2.2, S. 122 f.) mit der datenschutzrechtlichen Problematik der Erhebung von Personaldaten in Bewerberfragebögen befaßt.

Das BDSG unterwirft nicht die Erhebung, sondern erst die Speicherung personenbezogener Daten einer gesetzlichen Grenze (§ 1 Abs. 1 BDSG). Da die Speicherung personenbezogener Daten in einer Datei gem. § 23 BDSG nur dann zulässig ist, wenn auch der vorausgegangene Vorgang der Erhebung rechtmäßig war, ist die datenschutzrechtliche Regelungslücke durch die in der arbeitsrechtlichen Literatur und Rechtsprechung entwickelten Grundsätze zur Begrenzung des Fragerechts des Arbeitgebers zu schließen. Bei der Frage nach der Zulässigkeit von Fragen sind das Interesse des Arbeitnehmers und das Interesse des Arbeitgebers, sich Aufklärung über den Arbeitnehmer zu verschaffen, gegeneinander abzuwägen. Daraus folgt, daß der Arbeitgeber nur Fragen stellen darf, die mit dem Arbeitplatz oder der zu leistenden Arbeit in Zusammenhang stehen. Er kann auch nach Gegebenheiten fragen, die geeignet sind, das in einem Arbeitsvertrag liegende Risiko zu erhöhen.

Mir wurde ein Bewerberfragebogen zur Überprüfung vorgelegt. Ich habe einzelne darin enthaltene Fragen auf ihre Rechtmäßigkeit hin überprüft. Da diese Fragen immer wieder in derartigen Personalfragebogen auftauchen, stelle ich die wichtigsten Ergebnisse im folgenden dar.

Zur Frage: „Sind Ihre wirtschaftlichen Verhältnisse geordnet?"

Ob diese Frage gestellt werden darf, ist bisher vom Bundesarbeitsgericht nicht entschieden worden. Zum Teil wird die Auffassung vertreten, daß bei Angestellten des unteren und mittleren Verantwortungsbereichs die Frage nach Vermögensverhältnissen unzulässig sei; lediglich bei leitenden Angestellten und solchen, denen vom Arbeitgeber besonderes Vertrauen entgegenzubringen ist (z. B. Bankkassierer), könne danach gefragt werden. Zum Teil wird die Ansicht vertreten, diese Frage sei zulässig und vom Bewerber korrekt zu beantworten, wenn er erhebliche Schulden habe. Meines Erachtens ist entscheidend, ob der Arbeitnehmer die Möglichkeit haben wird, im Rahmen seiner Tätigkeit über das Vermögen des Arbeitgebers oder Dritter zu disponieren.

Zur Frage: „Welche Rente beziehen Sie — Bezogen Sie eine Rente?"

Diese Frage steht meines Erachtens nicht im Zusammenhang mit dem Arbeitsverhältnis, sie ist daher unzulässig. Außerdem kann mit dieser Frage mittelbar nach Krankheiten gefragt werden (z. B. bei Frührentnern), dazu unten: Fragen nach Krankheiten.

Fragen nach Krankheiten: „Sind Sie aus gesundheitlichen Gründen aus dem letzten Arbeitsverhältnis ausgeschieden?", „Jetziger Gesundheitszustand", „Schwere Krankheiten der letzten 5 Jahre (Operationen)", „Haben Sie eine Kur beantragt?", „Kriegsbeschädigungen, %-Angaben"

Fragen zum gegenwärtigen Gesundheitszustand sind zulässig, soweit sie sich auf Krankheiten beziehen, die in irgendeiner Weise die Einsetzbarkeit auf dem vorgesehenen Arbeitsplatz zu beeinträchtigen vermögen. Ob der Bewerber eine Kur beantragt hat, muß er sogar ohne besondere Frage mitteilen.

Inwieweit Fragen nach früheren Erkrankungen erlaubt sind, wird unterschiedlich beurteilt: zum Teil werden sie in beschränktem Maß für zulässig gehalten, soweit an ihrer Beantwortung für den Betrieb, die übrigen Arbeitnehmer und die Arbeit ein Interesse besteht. Für zulässig wird die Frage gehalten, ob der Arbeitnehmer in den letzten zwei Jahren wegen einer schweren Krankheit arbeitsunfähig krank gewesen sei. Andere halten dagegen nur eine Frage über den gegenwärtigen Gesundheitszustand für zulässig. Der Arbeitnehmer müsse nur Fragen im Hinblick auf seine derzeitige Einsetzbarkeit am vorgesehenen Arbeitsplatz beantworten. Angeben müsse der Arbeitnehmer eine etwaige Infektionsgefährdung von Mitarbeitern, ferner müsse der Arbeitnehmer darauf hinweisen, inwieweit er aus gesundheitlichen Gründen möglicherweise bei der vollen Ausübung der ihm vermutlich übertragenen Arbeiten Ausfälle oder Einschränkungen erwarten lasse. Einige Gerichte haben entschieden, daß Fragen nach ausgeheilten Krankheiten nicht beantwortet zu werden brauchen. An der Frage nach der Kriegsbeschädigung wird dem Arbeitgeber ein berechtigtes Interesse zugebilligt.

Zur Frage: „Fallen Sie zur Zeit unter das Mutterschutzgesetz?"

Diese Frage ist zulässig, da sich aus dem Mutterschutzgesetz für den Arbeitgeber besondere Pflichten ergeben, so daß der Arbeitgeber ein berechtigtes Interesse daran hat zu erfahren, ob die Bewerberin unter das Mutterschutzgesetz fällt. Das Mutterschutzgesetz dient dazu, einen bereits erworbenen Arbeitsplatz zu erhalten, nicht dagegen, den Erwerb eines Arbeitsplatzes zu sichern.

Zur Frage: „Welcher Krankenkasse gehören Sie an?"

An der Kenntnis der Krankenkasse hat der Arbeitgeber erst dann ein berechtigtes Interesse, wenn der Bewerber eingestellt worden ist. Die Krankenkasse kann auch im Zusammenhang mit dem Arbeitsvertrag erfragt werden. Im Bewerbungsbogen ist sie meines Erachtens nicht zulässig.

Fragen nach persönlichen Verhältnissen: Staatsangehörigkeit, Konfession, Familienstand, Kindern

Der Arbeitgeber hat ein berechtigtes Interesse an der Kenntnis der Staatsangehörigkeit des Bewerbers, da er zu prüfen hat, ob der Bewerber Ausländer ist und eine Arbeitserlaubnis gem. § 19 AFG besitzt.

Da gem. Art. 140 GG, 136 III WRV niemand verpflichtet ist, seine religiöse Überzeugung zu offenbaren, ist die Frage nach der Konfession unzulässig.

An der Kenntnis des Familienstandes und der Anzahl der Kinder hat der Arbeitgeber ebenfalls kein berechtigtes Interesse; diese Fragen sind daher unzulässig.

Zur Frage: „Sind Verwandte bei uns beschäftigt?"

Ein berechtigtes Interesse hat der Arbeitgeber an dieser Frage meines Erachtens nur, wenn die Gefahr besteht, daß Kontrollen umgangen werden können durch kollusives Zusammenarbeiten von verwandten Angestellten, z. B. indem das sogenannte Vieraugenprinzip ausgehöhlt wird.

Hinweis auf Führungszeugnis

Ein Führungszeugnis kann der Arbeitgeber meines Erachtens nicht verlangen, da aus dem Führungszeugnis mehr Vorstrafen ersichtlich sein können, als der Arbeitnehmer anzugeben verpflichtet ist. Das BAG hat entschieden, daß nicht sämtliche Vorstrafen anzugeben sind, sondern nur einschlägige Strafen, d.h. Strafen wegen Taten, die im Zusammenhang mit der beabsichtigten Tätigkeit stehen, z. B. Trunkenheitsdelikte bei Kraftfahrern, Vermögensdelikte bei Kassierern.

Das Unternehmen, das den von mir überprüften Personalfragebogen verwendet, hat bisher lediglich angekündigt, sein seit mehr als zehn Jahren verwendetes Formular auf seine rechtliche Zulässigkeit zu überprüfen. Ein Ergebnis ist mir noch nicht mitgeteilt worden.

6.7.3 Datenübermittlungen von Krankenkassen an Arbeitgeber

Durch mehrere Beschwerden erfuhr ich, daß Unternehmen von Bewerbern um einen Arbeitsplatz verlangten, ihre jeweilige Krankenkasse zu der Ausstellung von Bescheinigungen über die Krankzeiten des Bewerbers in den letzten 12 Monaten zu veranlassen. Diese zum Teil auf einem vom Unternehmen vorbereiteten Formular auszustellende Bescheinigung sollte die Krankenkasse dann direkt an den Arbeitgeber schicken.

Ich halte diese Praxis nicht für zulässig. Denn indem der Arbeitgeber den Bewerber auf diesem Wege zu Auskünften über seine Krankzeiten in den letzten 12 Monaten veranlaßt, überschreitet er die von der Rechtsprechung entwickelten Grenzen zum Fragerecht des Arbeitgebers bei Einstellungen. Nach dieser Rechtsprechung darf der Arbeitgeber lediglich Fragen stellen, die zu der Beurteilung nötig sind, ob der betreffende Arbeitnehmer den gesundheitlichen Anforderungen des konkreten Arbeitsplatzes gerecht wird. Unzulässig ist dagegen die Ermittlung von Daten, die allein der Erforschung des allgemeinen Gesundheitszustandes des Arbeitnehmers dienen und die keine Bedeutung im Hinblick auf den konkreten Arbeitsplatz haben. Die Ermittlung derartiger Daten verstößt gegen das allgemeine Persönlichkeitsrecht und das informationelle Selbstbestimmungsrecht (Art. 1 und 2 Grundgesetz) des Arbeitnehmers. Die Übermittlung durch die Krankenkasse kann sich damit nicht auf eine wirksame Einwilligung des Betroffenen stützen. Auch liegt eine gesetzliche Offenbarungsbefugnis nach dem Sozialgesetzbuch X nicht vor. Das Bundesdatenschutzgesetz ist hier nicht anwendbar, würde im übrigen aber eine Übermittlung auch nicht gestatten.

Die obersten Aufsichtsbehörden der Länder, mit denen ich dieses Thema erörtert habe, teilen meinen Standpunkt.

Einzelne Krankenkassen haben mich darauf aufmerksam gemacht, daß sie keine derartigen Auskünfte direkt an Arbeitgeber leiten, sondern sie ihrem Mitglied auf Anforderung aushändigen, so daß dieses dann selbst entscheiden kann, ob es die Auskunft der Krankenkasse dem Arbeitgeber zugänglich machen will. Dieses Verfahren verstößt nicht gegen geltende Datenschutzbestimmungen, wenngleich es auch nicht unbedenklich ist, denn der Bewerber um einen Arbeitsplatz befindet sich in einer faktischen Zwangslage, die ihm — wenn er den Arbeitsplatz haben will — praktisch keine andere Möglichkeit läßt, als die Krankenkassenauskunft dem Arbeitgeber vorzulegen. Dennoch ist dies eine datenschutzrechtlich eher vertretbare Lösung als die direkte Zulei-

tung der Auskunft von der Krankenkasse an den Arbeitgeber; denn der Bewerber hat immerhin die Möglichkeit der Entscheidung und er weiß, welche Auskunft der Arbeitgeber erhält.

6.7.4 Datensammlung durch Betriebsräte

Ein Bürger beschwerte sich bei mir darüber, daß der Betriebsrat des Unternehmens, bei dem er sich (erfolgreich) beworben hatte, die im Rahmen der Beteiligung des Betriebsrates am Einstellungsverfahren diesem übergebenen Kopien der Bewerbungsunterlagen behalten hatte und weiter aufbewahrte. Der Bürger wollte nicht, daß neben der Personalakte ein besonderer Personalvorgang beim Betriebsrat geführt wird.

Der Betriebsrat war der Meinung, daß er zu dieser Sammlung von Personalunterlagen berechtigt sei, weil er diese Informationen für die sachgerechte Durchführung seiner Arbeit benötige. Der Betriebsrat könne sein Mitbestimmungsrecht nach § 99 Abs. 2 BetrVG nur dann wahrnehmen, wenn er über eine Fülle von personenbezogenen Daten verfüge. Wenn der Betriebsrat sein Mitbestimmungsrecht bei Kündigungen gemäß § 102 BetrVG wirksam wahrnehmen wolle, müsse er eine Reihe vorsorgender Überlegungen treffen. Wolle er etwa einer Kündigung aus sozialen Gesichtspunkten widersprechen, müßten ihm alle wichtigen Sozialdaten bekannt sein. Diese müßten angesichts der Kürze der dem Betriebsrat eingeräumten Anhörungsfrist von einer Woche vor der Einleitung des Anhörungsverfahrens präsent sein. Auch die Widerspruchsrechte nach § 102 Abs. 3 Nrn. 3, 4 und 5 BetrVG könnten vom Betriebsrat nur wahrgenommen werden, wenn ihm Daten über den Qualifikationsstand, frühere Qualifikationen und Einsatzmöglichkeiten bekannt seien. Um diese Widerspruchsrechte wirksam wahrnehmen zu können, müsse und dürfe der Betriebsrat vorsorgend die dafür notwendigen Daten sammeln und präsent halten. Dies sei auch unproblematisch, denn der Betriebsrat unterliege der besonderen Verschwiegenheitspflicht des § 79 BetrVG.

Ich teile diese Ansicht nicht und meine, daß der Betriebsrat zu derartigen Datensammlungen auf Vorrat nicht berechtigt ist.

Es besteht zwar kein Zweifel daran, daß der Betriebsrat nach § 99 Abs. 1 BetrVG Anspruch auf Vorlage der erforderlichen Bewerbungsunterlagen hat. Der Betriebsrat dürfte somit auch das Recht haben, sich aus den Unterlagen schriftliche Aufzeichnungen zu machen. Zweifelhaft ist aber, ob er sich auch Kopien der Unterlagen anfertigen darf. Bei den Unterlagen, die nach § 80 Abs. 2 Satz 2 BetrVG „zur Verfügung zu stellen" sind, besteht kein Zweifel, daß der Betriebsrat sich von ihnen auch Kopien anfertigen darf, wenn sie ihm lediglich zur Einsicht vorgelegt werden. Da nach § 99 Abs. 1 BetrVG die erforderlichen Unterlagen jedoch nur „vorzulegen" sind, spricht danach manches dafür, daß der Betriebsrat hier nicht berechtigt ist, sich Kopien der Unterlagen zu fertigen, denn dies liefe praktisch auf ein „Zur-Verfügung-Stellen" der Unterlagen hinaus, was der Gesetzgeber dem Betriebsrat in § 99 BetrVG aber gerade nicht zugestehen wollte.

Das Bundesarbeitsgericht hat in seinem Beschluß vom 3. Dezember 1985 (1 ABR 72/83, NJW 1986, S. 1709, BB 1986, S. 876) den Standpunkt vertreten, der Arbeitgeber sei verpflichtet, bei Einstellungen von Arbeitnehmern dem Betriebsrat die Bewerbungsunterlagen aller Bewerber auszuhändigen und bis zur Beschlußfassung über den Antrag auf Zustimmung, längstens für eine Woche, zu überlassen.

Das BAG hat aber keine Ausführungen dazu gemacht, daß der Betriebsrat etwa ein Recht zum Archivieren der ausgehändigten Bewerbungsunterlagen habe. Es ist vielmehr offensichtlich davon ausgegangen, daß die Original-Bewerbungsunterlagen zu übergeben sind, die natürlich nicht beim Betriebsrat verbleiben können.

Meines Erachtens läßt sich aus den angeführten Normen des BetrVG 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.

Die Argumentation, die der Betriebsrat in dem Beschwerdefall vorgebracht hat, läuft im wesentlichen darauf hinaus, daß der Betriebsrat das Recht zur Sammlung von Informationen über die Mitarbeiter haben müsse, um seinen Mitwirkungs- und Mitbestimmungsrechten und -pflichten ordnungsgemäß nachkommen zu können. Dieser Argumentation kann ich nicht folgen. Sie verkennt, daß dem Betriebsrat durch verschiedene Normen des BetrVG umfangreiche Informationsrechte gegeben worden sind, die ihn in die Lage versetzen sollen, seinen Aufgaben nachzukommen. Wenn ihm einzelne Rechte und Pflichten zugewiesen worden sind, korrespondieren damit jeweils Informations- und Auskunftspflichten des Arbeitgebers. Damit der Betriebsrat sein Mitbestimmungsrecht aus § 99 BetrVG ausüben kann, hat ihm das Gesetz z. B. in § 99 Abs. 1 BetrVG das Recht auf Vorlage von Unterlagen und auf Auskunft über die Auswirkungen der geplanten Maßnahme und über den in Aussicht genommenen Arbeitsplatz und die vorgesehene Eingruppierung gegeben.

Anders als der Betriebsrat bin ich nicht der Meinung, daß eine Frist von einer Woche nicht ausreicht, um vom Arbeitgeber hinreichend unterrichtet zu werden.

Er ist somit nicht darauf angewiesen, eine Datensammlung auf Vorrat einzurichten, um im Ernstfall nicht erst die notwendigen Informationen einholen zu müssen. Es wäre mit den Pflichten des Betriebsrats sicher auch nicht zu vereinbaren, wenn er bei Entscheidungen auf möglicherweise völlig veraltete und unvollständige Informationen aus der Zeit der Einstellung der Mitarbeiter zurückgreifen würde.

Insbesondere um die nötigen Informationen für die Ausübung der Rechte nach § 80 Abs. 1 Nrn. 4, 5, 6 und 7 BetrVG zu erhalten, bedarf es keiner Datensammlung auf Vorrat. Arbeitnehmer, die besonderen Schutzgesetzen unterliegen, sind dem Betriebsrat unaufgefordert mitzuteilen. Im übrigen kann der Betriebsrat sich nach § 80 Abs. 2 BetrVG regelmäßig die Unterlagen vorlegen lassen, die er zur Durchführung seiner Aufgaben benötigt.

Nach allem läßt sich sagen, daß der Betriebsrat keine Datensammlung auf Vorrat benötigt und eine Rechtsgrundlage dafür aus dem BetrVG auch nicht abzuleiten ist.

Die Datenschutz-Aufsichtsbehörden der anderen Länder teilen meine Ansicht im wesentlichen.

6.7.5 Mitbestimmung bei technischer Überwachung — Krankheitsdaten sind Verhaltensdaten —

Das Bundesarbeitsgericht hat seine Rechtsprechung zu der Frage der Mitbestimmung des Betriebsrates bei Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer in einem Betrieb zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG), erweitert. In seinem Beschluß vom 11. März 1986 (1 ABR 12/84, NJW 1986, S. 2724) hat das BAG ausgeführt, daß Fehl- und Krankheitsdaten „Verhaltensdaten" im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sind. Sowohl Aussagen über unentschuldigte als auch über krankheitsbedingte Fehlzeiten der Arbeitnehmer seien Aussagen über ihr Verhalten. Krankheit sei zwar ein objektiver, vom Willen des Arbeitnehmers unabhängiger Zustand. Gleichwohl sei damit nicht notwendigerweise gesagt, daß der Arbeitnehmer unabhängig von seiner eigenen Willensentscheidung gehindert war, seiner Arbeitspflicht nachzukommen. Auch bei ärztlich bescheinigter und tatsächlich bestehender Arbeitsunfähigkeit bleibe dem Arbeitnehmer noch die Möglichkeit, sich zu entscheiden ob er arbeiten wolle oder nicht. Auch der tatsächlich arbeitsunfähige Arbeitnehmer entscheide sich aus den vielfältigsten Gründen immer wieder, doch zu arbeiten, obwohl er dazu nicht verpflichtet sei. Hinzu komme, daß Aussagen über krankheitsbedingte Fehlzeiten, also Aussagen über Arbeitsunfähigkeit, gleichzeitig besagen könnten, daß der Arbeitnehmer eine bestehende Krankheit zum Anlaß genommen hat, einen Arzt aufzusuchen, um gegebenenfalls arbeitsunfähig geschrieben zu werden. Damit könnten Aussagen über krankheitsbedingte Fehlzeiten gleichzeitig als Aussagen über ein zumindest denkbares Verhalten des Arbeit-

nehmers angesehen werden, nämlich darüber, in wie vielen Fällen er sich bei bestehender Arbeitsunfähigkeit entschieden hat, nicht zu arbeiten, obwohl ihm dies vielleicht möglich gewesen wäre.

Damit seien durch eine technische Einrichtung erhobene Aussagen über Krankheitshäufigkeiten, attestfreie Arbeitsunfähigkeitszeiten und unentschuldigte Fehlzeiten auch Aussagen über ein mögliches Verhalten des Arbeitnehmers. Das reiche aus, um in der Erarbeitung solcher Aussagen durch eine technische Einrichtung ein mitbestimmungspflichtiges Überwachen von Verhalten der Arbeitnehmer zu sehen.

Durch diese begrüßenswerte Rechtsprechung wird der Begriff des „Verhaltensdatums" und damit auch der Anwendungsbereich des Mitbestimmungsrechts des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG deutlich ausgeweitet. Im Ergebnis hat das BAG zwar den in dem Verfahren angegriffenen Einigungsstellenspruch für wirksam erklärt, weil die darin vorgesehenen Krankenläufe mit den Datenschutzbestimmungen vereinbar seien und weil der Einigungsstellenspruch einen angemessenen Ausgleich der Interessen der Arbeitnehmer und des Betriebs dadurch darstelle, daß er neben den Datenläufen auch regele, in welcher Weise der Arbeitgeber auf so gewonnene Erkenntnisse reagieren dürfe. Die Bedeutung der BAG-Entscheidung liegt jedoch darin, daß damit das Mitbestimmungsrecht des Betriebsrats bei der Verarbeitung von Daten über Erkrankungen und unentschuldigte Fehlzeiten mit Hilfe computergestützter Informationssysteme festgestellt worden ist.

Das BAG hat in dieser Entscheidung zwar noch an dem von mir in meinem 3. TB (4.7.2.1, S. 121) kritisierten Begriff des „Verhaltensdatums" festgehalten. Es hat aber durch die faktische Ausdehnung des Sinngehalts dieses Begriffes implizit eingeräumt, daß die selbstauferlegten Grenzen dieser unnötigen Begriffsbildung überschritten werden müssen.

6.7.6 Gesetzliche Regelung des Arbeitnehmerdatenschutzes

Die Bundesregierung hatte bereits in ihrem Bericht vom 30. April 1985 an den Innenausschuß des Deutschen Bundestages erklärt, daß sie eine gesetzliche Regelung des Datenschutzes im Arbeitsrecht für geboten hält. Ihre Überlegungen zur inhaltlichen Ausgestaltung hat sie in der Beantwortung einer Großen Anfrage der SPD-Fraktion zu Personalinformationssystemen und Datenschutz vom 19. Dezember 1985 (BT-Drucksache 10/4594) dargelegt. Sie führt darin u.a. aus, daß das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 auch für den Schutz der informationellen Selbstbestimmung im nicht-öffentlichen Bereich Bedeutung habe. Das Urteil werde bei der Vorbereitung dieser gesetzlichen Regelung auch im Hinblick auf die Einführung von Personalinformationssystemen berücksichtigt werden. In ihrer Stellungnahme zum Achten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz vom 27. August 1986 hat die Bundesregierung angekündigt, sie werde den Entwurf einer bereichsspezifischen Regelung des Arbeitnehmerdatenschutzes sobald wie möglich in der nächsten Legislaturperiode dem Deutschen Bundestag vorlegen.

Ich begrüße diese Absicht. Angesichts der bereits seit Jahren immer wieder vorgelegten Entwürfe zu diesem Bereich ist die Zeit reif für eine gesetzliche Regelung. Zu den inhaltlichen Anforderungen, denen sie nach meiner Vorstellung genügen muß, hatte ich bereits im 4. TB (6.2.2.7, S. 162 f.) Stellung genommen.

6.7.7 Vereinbarkeit von Auskünften über Arbeitnehmer mit der arbeitsgerichtlichen Rechtsprechung zum Auskunftsrecht des Arbeitgebers

Wie ich bereits in meinem 4. TB (5.5.2, S. 134) berichtet habe, hatte ich mich mit der Frage zu befassen, ob das Auskunftsverfahren eines Branchenauskunftsdienstes dazu führt, daß die restriktive Rechtsprechung der Arbeitsgerichte zum zulässigen Inhalt von Zeugnissen und zum Fragerecht des Arbeitgebers umgangen wird, indem potentielle neue Arbeitgeber durch die Auskünfte Details erfahren, die in Zeugnisse nicht

aufgenommen werden dürfen und die der Arbeitgeber bei der Einstellung auch nicht erfragen darf. Ich habe diese Problematik überprüft, was zu folgenden Zwischenergebnissen geführt hat:

Die arbeitsrechtlichen Grenzen für die Abfassung von Zeugnissen werden in der Tat bei den Meldungen von Branchenauskunftsdiensten nicht eingehalten, so daß Arbeitgeber, bei denen sich Mitarbeiter bewerben, durch diese Meldungen Tatsachen erfahren, die sie aus den vom Bewerber vorgelegten Zeugnissen nicht entnehmen können, wenn bei deren Abfassung die arbeitsgerichtlichen Beschränkungen für den Zeugnisinhalt beachtet worden sind.

Gleichzeitig ist zu beachten, daß das Frage- und Ermittlungsrecht des Arbeitgebers bei Neueinstellungen im Interesse des Persönlichkeitsschutzes des Arbeitnehmers eingeschränkt ist. Das Bundesarbeitsgericht hat in ständiger Rechtsprechung eine Beschränkung des Fragerechts aus dem in Artikel 1 Abs. 1 und Artikel 2 Abs. 1 des Grundgesetzes geschützten allgemeinen Persönlichkeitsrecht abgeleitet. Bei der Beurteilung der Zulässigkeit der Erhebung von Arbeitnehmerdaten müsse das Interesse des Arbeitnehmers an der ungestörten Privatsphäre mit dem Interesse des Arbeitgebers, sich Aufklärung über den Arbeitnehmer zu verschaffen, abgewogen werden. Hieraus folge, daß nur solche Fragen gestellt werden dürften, die mit dem Arbeitsplatz oder der zu leistenden Arbeit im Zusammenhang stehen.

Als Ausgleich dafür ist der Arbeitgeber berechtigt, bei früheren Arbeitgebern Auskünfte über Bewerber einzuholen. Nach der Rechtsprechung und der herrschenden Lehre sind frühere Arbeitgeber berechtigt, über das Zeugnis hinaus Auskünfte über den ausgeschiedenen Arbeitnehmer auch ohne dessen Einverständnis an Dritte zu erteilen, die ein berechtigtes Interesse an der Erlangung solcher Auskünfte haben. Erteilt der Arbeitgeber Auskunft, ist er aber verpflichtet, den Arbeitnehmer auf Verlangen über den Inhalt der Auskunft zu unterrichten und den Durchschlag einer schriftlichen Auskunft zur Einsicht vorzulegen.

Nach der Rechtsprechung ist der Arbeitgeber also auch ohne Zustimmung und selbst gegen den Wunsch des Arbeitnehmers grundsätzlich berechtigt, wahrheitsgemäße Auskünfte über die Person und das während des Arbeitsverhältnisses gezeigte Verhalten des Arbeitnehmers zu erteilen. Ein solches Recht zur Auskunftserteilung ergebe sich aus der Stellung von Arbeitgeber und Arbeitnehmer im Rahmen des Arbeitsverhältnisses und aus den Grundsätzen der sozialen Partnerschaft, die den Angehörigen sowohl der Arbeitgeberschaft wie der Arbeitnehmerschaft das Recht geben, andere Angehörige der gleichen Gruppe bei der Wahrung ihrer Belange zu unterstützen.

Diese Rechtsprechung ist kritisiert worden. Auch der Bundesminister für Arbeit und Sozialordnung hat in seiner Stellungnahme gegenüber dem Innenauschuß des Bundestages vom 30. April 1985 zur Frage der Notwendigkeit einer bereichsspezifischen Regelung des Datenschutzes für Arbeitnehmer erklärt, er halte es für zweifelhaft, ob das Bundesarbeitsgericht nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz noch an dieser Rechtsprechung festhalten werde. Mehrere Gerichte haben bereits entschieden, daß Auskünfte des Arbeitgebers über Arbeitnehmer nur mit deren ausdrücklicher Einwilligung zulässig sind.

Das Bundesarbeitsgericht hat allerdings mit Urteil vom 18. Dezember 1984 (3 AZR 389/83) — also nach dem Volkszählungsurteil des Bundesverfassungsgerichts — seine Rechtsprechung zum Auskunftsrecht des früheren Arbeitgebers bekräftigt. Es hat darin u.a. ausgeführt:

> „Der Beklagten ist zuzugeben, daß der Arbeitgeber aus dem Gesichtspunkt der nachwirkenden Fürsorgepflicht gehalten ist, über die Erteilung des Zeugnisses hinaus im Interesse des ausgeschiedenen Arbeitnehmers Auskünfte über diesen an solche Personen zu erteilen, mit denen der Arbeitnehmer in Verhandlungen über den Abschluß eines Arbeitsvertrages steht. Der Arbeitgeber darf solche Aus-

künfte auch gegen den Willen des ausgeschiedenen Arbeitnehmers erteilen. Er kann grundsätzlich nicht gehindert werden, andere Arbeitgeber bei der Wahrung ihrer Belange zu unterstützen."

Eine wichtige Einschränkung hat das Bundesarbeitsgericht aber gemacht, indem es erklärt hat:

„Die Auskünfte, zu denen der Arbeitgeber berechtigt ist, betreffen nur Leistung und Verhalten des Arbeitnehmers während des Arbeitsverhältnisses."

Diese Einschränkung ist zu beachten, wenn die derzeit noch gültige Rechtsprechung zum Maßstab gemacht wird, an dem die Auskunftspraxis von Branchenauskunftsdiensten gemessen wird.

Ich habe die Frage, inwieweit diese Auskunftspraxis mit der Rechtsprechung der Arbeitsgerichte zu Zeugnisinhalt, Fragerecht und Auskunftsrecht der Arbeitgeber vereinbar ist, unter den Obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich zur Diskussion gestellt. Dabei sind Bedenken an der Zulässigkeit von Auskünften über folgende Punkte geäußert worden:

— Form der Vertragsbeendigung
— Kündigung erfolgte durch Mitarbeiter oder Unternehmen
— Grund des Ausscheidens
— Einspruch oder Klage erhoben?
— Erkenntnisse über ungünstige Einkommensverhältnisse
— Bestand beim Ausscheiden ein rückforderbarer Saldo aus nicht verdienter Provision (bei Handelsvertretern)?

Bei allen diesen Punkten ist zweifelhaft, ob sie sich auf Leistung und Verhalten des Mitarbeiters während seiner Tätigkeit für das Unternehmen beziehen oder eher andere Umstände betreffen.

Ich beurteile die Problematik wie folgt: Bei Vorliegen einer Einwilligung, die den Anforderungen des § 3 BDSG und dem BGH-Urteil zur SCHUFA-Klausel genügt, wird die Datenübermittlung unbedenklich sein. Wenn keine Einwilligung vorliegt, kann die Übermittlung nicht nach §§ 24 und 32 BDSG zulässig sein, wenn die arbeitsgerichtliche Rechtsprechung derartige Übermittlungen für unzulässig hält. Das Datenschutzrecht kann nicht das Arbeitsrecht außer Kraft setzen, wenn letzteres restriktivere Regeln enthält als ersteres. In diesem Falle geht vielmehr die restriktive Rechtsprechung zum Auskunftsrecht des Arbeitgebers vor und verbietet Datenübermittlungen, die sich nicht auf Leistung und Verhalten des Arbeitnehmers während des Arbeitsverhältnisses beziehen.

Fraglich ist, ob die Übermittlung nach § 24 bzw. § 32 BDSG gerechtfertigt sein kann, wenn es sich um selbständige Handelsvertreter oder Makler handelt und keine Einwilligung vorliegt. Die Zulässigkeit ist in jedem Einzelfall unter Abwägung der involvierten berechtigten Interessen mit den schutzwürdigen Belangen des Betroffenen zu prüfen. Es läßt sich nicht sagen, daß die Übermittlung bestimmter Daten generell zulässig ist, weil sie so schwerwiegend sind, daß die schutzwürdigen Belange der Betroffenen in jedem Falle zurücktreten müßten. Fraglich ist vielmehr, ob in diesen Fällen wegen der Vergleichbarkeit der wirtschaftlichen Abhängigkeit selbständiger wie unselbständiger Handelsvertreter vom Unternehmen auch eine rechtliche Gleichstellung mit Arbeitnehmern geboten ist. Dies würde bedeuten, daß die für Arbeitnehmer entwickelten Grundsätze auch für selbständige Vertreter zu gelten hätten, über die dann ebenfalls nur unter Beachtung der restriktiven Rechtsprechung zum Auskunftsrecht des Arbeitgebers Informationen weitergegeben werden dürften.

6.8 Sonstige Probleme

6.8.1 Auskünfte von Fluggesellschaften an Dritte

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, daß die von Fluggesellschaften geübte Praxis der Auskunftserteilung datenschutzrechtliche Probleme aufwerfen kann. Eine Frau, die angab, kurz vor der Trennung von ihrem Ehemann zu stehen, flog von Hamburg in eine andere Stadt, in der ihr Freund wohnte. Der Ehemann der Frau ließ sie durch die Fluggesellschaft bei ihrer Ankunft zu ihrer großen Überraschung noch in der Maschine namentlich auffordern, sich am Ausgang zu melden, um eine Nachricht entgegenzunehmen.

Die Erörterung dieser Eingabe mit der beteiligten Fluggesellschaft hat zu folgenden Ergebnissen geführt:

Die Dienstanweisung der Fluggesellschaft zu Auskünften über Fluggäste erlaubt Auskünfte über Buchung und Beförderung außer an den Fluggast selbst auch an Dritte, wenn

- der Fluggast seine Einwilligung hierzu gegeben hat oder
- die Durchführung des Beförderungsvertrages dies erforderlich macht oder
- schutzwürdige Belange durch eine Auskunft nicht verletzt werden und der Auskunftssuchende ein berechtigtes Interesse daran hat.

In der Dienstanweisung der Fluggesellschaft wird erläutert, daß „schutzwürdige Belange" in der Regel dann nicht verletzt werden, wenn ein Anfragender wesentliche Einzelheiten der Reise kennt (mindestens Name des Fluggastes, Informationen über den Flug, Reisedatum), die er entweder nur vom Fluggast selber erfahren haben kann oder dadurch, daß er diese Reise bezahlt oder in irgendeiner Weise vorbereitet hat. Ein „berechtigtes Interesse" könne z.B. angenommen werden, wenn der Auskunftsersuchende auf Befragen mitteile, Verwandter, Mitarbeiter, Vorgesetzer oder eine Person in ähnlichem Beziehungsverhältnis zum Fluggast zu sein. Schließlich ist in der Dienstanweisung vorgesehen, daß in Zweifelsfällen möglichst die Identifikationsmerkmale (Name, Anschrift und z.B. Nummer des Identifikationspapiers und ausstellende Behörde) desjenigen, der die Auskunft verlangt, festgehalten werden sollen. Dies entspricht einer Regelung, die in den Jahren 1981 und 1982 mit den für die Fluggesellschaft zuständigen Datenschutz-Aufsichtsbehörden abgestimmt worden ist. Ich meine jedoch, daß dieses Problem jetzt nach etwa zehnjährigen Erfahrungen mit dem BDSG neu überdacht werden muß.

Ich habe die Fluggesellschaft bei der Erörterung der Eingabe darauf hingewiesen, daß ich diese Regelung für ungenügend halte, da durch sie — wie im Fall der Eingabe — nicht verhindert wird, daß Personen Auskünfte erhalten, die nach dem Willen des Fluggastes nichts über den Flug erfahren sollen. Gerade dieser Fall zeigt, daß auch Auskünfte an Personen, an die nach der Dienstanweisung vermeintlich ohne Verletzung „schutzwürdiger Belange" des betroffenen Fluggastes Auskunft gegeben werden kann, sehr wohl dessen schutzwürdige Belange verletzen können.

Ich habe deswegen angeregt, die Dienstanweisung und das Auskunftsverfahren so zu ändern, daß derartige Fälle auszuschließen sind. Dies könnte dadurch geschehen, daß den Fluggästen die Möglichkeit eingeräumt wird, Auskünfte an Dritte generell zu untersagen. Dieses Verbot der Auskunftserteilung müßte — was sicher ohne großen Aufwand möglich ist — in der EDV-Anlage der Fluggesellschaft vermerkt werden, so daß jeder Mitarbeiter im Falle einer Anfrage Kenntnis davon erhält. Die Fluggäste müßten durch Aushänge oder Hinweise in den mit der Flugkarte ausgehändigten Unterlagen auf die Möglichkeit eines Auskunftsverbots hingewiesen werden. Gleichzeitig müßte die Dienstanweisung für die Fälle klarere Anweisungen für die Mitarbeiter enthalten, in denen der Fluggast keine Auskunftssperre verlangt hat.

Ich bin sicher, daß nur sehr wenige Fluggäste von der Möglichkeit des (generellen) Auskunftsverbots Gebrauch machen würden, so daß das Anbringen eines Vermerks dar-

über in der EDV-Anlage der Fluggesellschaft in diesen wenigen Fällen nicht mit einem großen Aufwand verbunden sein dürfte. Als zu aufwendig und nicht praktikabel erscheint mir die Möglichkeit, den Fluggästen ein Auskunftsverbot nur für bestimmte potentielle Anfrager zu eröffnen; ebenfalls als der Fluggesellschaft vielleicht nicht zumutbar sehe ich es an, jeden Fluggast etwa beim Einchecken zu fragen, ob er ein Auskunftsverbot wünscht (obwohl dies etwa zusammen mit der Frage Raucher oder Nichtraucher ohne sehr großen Aufwand möglich wäre).

Von diesen Einschränkungen abgesehen halte ich die dargestellte Möglichkeit des Auskunftsverbots für einen wirksamen Weg, um Auskünfte zu vermeiden, die die schutzwürdigen Belange der betroffenen Fluggäste verletzen können. Denn den Mitarbeitern der Fluggesellschaft sind genaue Abwägungen zwischen den berechtigten Interessen des Anfragenden und den schutzwürdigen Belangen des Fluggastes praktisch nicht möglich, weil sie die Implikationen des einzelnen Falles weder kennen noch erforschen können. Außerdem haben sie keinerlei Überprüfungsmöglichkeit, ob der Anfragende tatsächlich ein Verwandter o.ä. ist.

Die Fluggesellschaft hat meine Überlegungen jetzt aufgegriffen und entwirft eine Neufassung der Dienstanweisung. Die Möglichkeit zur Auskunftssperre soll den Fluggästen in der Weise bekanntgemacht werden, daß in die zur Verteilung kommenden Taschenflugpläne ein Hinweis aufgenommen wird, wonach die Möglichkeit besteht, die Reservierungsdaten gegen eine Weitergabe an Dritte zu Auskunftszwecken sperren zu lassen. In der neuen Dienstanweisung soll auch ein Hinweis darauf enthalten sein, daß in bestimmten Fällen, in denen eine Auskunftspflicht besteht (z.B. polizeiliche Ermittlungen), trotz des Auskunftsverbots des Fluggastes Daten an Dritte gegeben werden können. Auch soll deutlich werden, daß die Fluggesellschaft keine Garantie dafür übernehmen kann, daß sich andere Fluglinien, mit denen der Passagier weiterfliegt, an dieses Auskunftsverbot halten.

6.8.2 Speicherung der Bankverbindung bei Anzeigenaufgabe per Telefon

Eine Eingabe erreichte mich, die sich auf das Bankabbuchungsverfahren eines Hamburger Verlages bezog.

Das Aufgeben einer Anzeige ist bei diesem Zeitungsverlag telefonisch möglich. Der Verlag läßt sich neben den Anzeigendaten Name, Anschrift und die Telefonnummer des Anrufers geben, um evtl. mit Hilfe des Telefonbuches die Identität prüfen zu können. Außerdem wird dem Anrufer nach Darstellung des Verlags die Möglichkeit der Abbuchung von seinem Konto angeboten. Bei Einverständnis gibt der Betroffene dem Verlag seine Bankverbindung (Kontonummer, Institut und Bankleitzahl) bekannt und erhält im Datensatz ein Kennzeichen, damit nach dem Erscheinen der Anzeige die Rechnung erstellt und die Abbuchung vom Konto vorgenommen werden kann.

Im Beschwerdefall hatte der Verlag den Anzeigenkunden auch nach seiner Bankverbindung gefragt, ohne allerdings — wie der Betroffene erklärte — den Sinn dieser Frage zu erläutern. Der Kunde gab seine Kontoverbindung an und einige Wochen später wurde der Rechnungsbetrag von seinem Konto abgebucht. Er war sich sicher, eine Ermächtigung zum Bankeinzug nicht erteilt zu haben. Der Verlag behauptete dagegen, der Betroffene sei bei der Frage nach der Bankverbindung ausdrücklich auf den Einzug des Rechnungsbetrages hingewiesen worden. Es war ihm aber nicht möglich, dieses zu beweisen.

Der Betroffene machte von der Rückrufmöglichkeit beim Bankeinzugsverfahren Gebrauch und hat die Rechnung dann durch Überweisung beglichen.

Ich habe den Verlag darauf hingewiesen, daß bei fehlender Einzugsermächtigung das Speichern der Kontonummer nicht erforderlich und damit nicht von § 23 BDSG gedeckt ist.

Um eine rechtswidrige Speicherung zu vermeiden, muß sichergestellt werden, daß Kontonummern nur gespeichert werden, wenn eine Einzugsermächtigung gegeben

worden ist. D.h., die Sachbearbeiter des Verlages müssen ausdrücklich fragen, ob der Betroffene mit der Abbuchung des Betrages einverstanden ist. Wenn er diese Frage bejaht, sollte der Sachbearbeiter dies dokumentieren, um im Zweifelsfall eine Nachprüfung zu ermöglichen.

6.8.3 HVV-Umfrage bei der Ausgabe von ermäßigten Wertmarken für den Ausbildungsverkehr

Der Hamburger Verkehrsverbund (HVV) führt bei Kunden, die ermäßigte Monats- oder Abonnementskarten im Ausbildungsverkehr erwerben wollen, in festgelegten Abständen eine Befragung durch. Er tut dies, um für den Ausbildungsverkehr höhere Zuschüsse vom Bund und den Ländern Hamburg, Schleswig-Holstein und Niedersachsen zu erhalten.

Nach § 45a des Personenbeförderungsgesetzes und § 6a des Allgemeinen Eisenbahngesetzes haben die Unternehmen des öffentlichen Personennahverkehrs einen Anspruch auf Ausgleich von 50% der ungedeckten Kosten für die Beförderung von Personen mit Zeitfahrausweisen des Ausbildungsverkehrs. Bei der Ermittlung der Kosten werden die in den Kostensatzverordnungen der Länder festgelegten Durchschnittssätze je Personenkilometer zugrunde gelegt. Für die Errechnung der Personenkilometer sind u.a. Angaben über die durchschnittliche Reisehäufigkeit (Ausnutzung der Zeitkarte) erforderlich. Ein Verzicht auf den Nachweis hätte zur Folge, daß nur die merklich niedrigeren, im Gesetz selbst festgelegten Durchschnittssätze für die Ausgleichszahlung angewendet werden dürften.

Um die Umfrage rechtlich abzusichern, wurde eine entsprechende Regelung in den Gemeinschaftstarif der im HVV zusammengeschlossenen Unternehmen aufgenommen. Dort heißt es im Teil B unter Nr. 4.51a wie folgt:

„Die Ausgabe ermäßigter Wertmarken kann darüber hinaus von der fristgerechten und ordnungsmäßigen Abgabe besonderer Erhebungsunterlagen im Zusammenhang mit § 45a Personenbeförderungsgesetz und § 6a des Allgemeinen Eisenbahngesetzes abhängig gemacht werden."

In dem Fragebogen werden folgende Angaben verlangt:

a) Name und Anschrift der Schule/Ausbildungsstätte sowie die auf dem Wege dorthin benutzte erste Einstiegs- und letzte Ausstiegshaltestelle (Anmerkung: Diese Angaben dienen lediglich zur Vornahme von Plausibilitätsprüfungen bei der Aufbereitung der Fragebogen. Sie werden weder datentechnisch erfaßt noch gespeichert.)

b) auf dem Weg zur regelmäßig besuchten Schule/Ausbildungsstätte benutzte Linien und Zahl der Benutzungstage in der Woche

c) Zahl der Benutzungstage in der Woche für mehrmalige Fahrten zur Schule/Ausbildungsstätte

d) Bei Fahrten zu sonstigen Zielen zu schulischen oder Ausbildungszwecken:
   — benutzte Linien
   — Zielhaltestelle (nur für Plausibilitätsprüfungen; s. Anmerkung zu a)
   — Zahl der Benutzungstage in der Woche

e) Zahl der Benutzungstage in der Woche mit Fahrten zu sonstigen Zwecken

f) Ausbildungsverhältnis — Schüler(in), Student(in), Auszubildende(r).

In früheren Versionen dieses Fragebogens wurde auch nach der Anschrift des HVV-Kunden gefragt, um die korrekte Angabe der Einstiegshaltestelle prüfen zu können. Hierauf wird aber schon seit einiger Zeit verzichtet.

Wer ein Zeitkarten-Abonnement hat, erhält diesen Fragebogen mit der Post etwa ein Vierteljahr vor Ablauf des Jahres-Abonnements. Er soll ihn innerhalb einer festgelegten Frist ausgefüllt beim HHA-Kundenzentrum einreichen. Wenn diese Frist nicht eingehalten wird, erlischt das Abonnement automatisch.

Ein Petent hatte bemerkt, daß auf dem Fragebogen die Kunden-Nummer seines Abonnements bei der HHA ausgedruckt ist. Sie befindet sich auf der letzten Seite auf einem kleinen Abschnitt, der mit einer Perforation abtrennbar ist. Er hatte den Verdacht, daß die Aussagen im Fragebogen später noch dem jeweiligen Kunden zugeordnet werden könnten.

Die Prüfung beim HVV ergab, daß die Kunden-Nummer verwendet wird, um die Rückgabe der Fragebogen kontrollieren zu können. Im Normalfall wird der Fragebogen zusammen mit dem Berechtigungsnachweis, der die Kunden-Nummer enthält, vorgelegt, so daß dadurch eine Rückgabekontrolle gegeben ist. Diesen Berechtigungsnachweis verlangt der HVV aber nicht, wenn der Abonnent jünger als 15 Jahre alt ist. In diesen Fällen wird unterstellt, daß es sich um Schulpflichtige handelt. Um die Rückgabe der Fragebogen dennoch anhand der Kunden-Nummer kontrollieren zu können, wird sie auf dem Fragebogen ausgedruckt und sofort nach Abgabe des Fragebogens abgetrennt. Die Zuordnung zu einer Person ist praktisch nicht mehr möglich, wenn die Fragebogen beim HVV eingegangen sind.

Gegen diese Ausgestaltung des Verfahrens habe ich keine Bedenken.

Da regelmäßig bei jeder Umfrage zahlreiche Anfragen und Beschwerden bei mir eingehen, empfehle ich dem HVV, in seinem Anschreiben an die Abonnenten und in den Aushängen noch deutlicher herauszustellen, daß die erfragten Daten nur anonymisiert und nur zur Bestimmung von Ausgleichszahlungen der öffentlichen Hand genutzt werden.

6.8.4 Daten von Vereinsmitgliedern

Mehrere Zuschriften und Anrufe haben mir gezeigt, daß große Unsicherheit über den Umgang mit Daten von Vereinsmitgliedern herrscht. Die häufigsten Zweifelsfragen beziehen sich auf die Bekanntmachung von neuen Mitgliedern oder die — oft praktizierte — monatliche Auflistung der Geburtstage in Rundschreiben oder anderen Publikationen.

Der Verein geht kein Risiko ein, wenn er sich von seinen Mitgliedern eine schriftliche Einwilligung geben läßt, die allerdings voraussetzt, daß das Mitglied genau über alle Verwendungen seiner Daten informiert wird. Wäre es sich über die Tragweite seiner Erklärung nicht im klaren, wäre die Einwilligung unwirksam.

Aus praktischen Gründen wird oftmals eine andere Lösung gesucht.

Eine Datenübermittlung — um eine solche handelt es sich auch bei der Bekanntgabe in einem Rundschreiben oder einer Vereins-Zeitschrift — ist nach § 24 Abs. 1 BDSG auch zulässig, wenn sie zur Wahrung berechtigter Interessen (des Vereins oder auch eines Außenstehenden) erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Liegt eine schriftliche Einwilligung des Betroffenen nicht vor, muß der Verein in jedem Einzelfall die Interessenlage sorgfältig prüfen. Wenn der Abstand zu den Mitgliedern relativ groß ist, werden der Vereins-Geschäftsstelle in der Regel keine Anhaltspunkte dafür bekannt sein, ob im konkreten Einzelfall schutzwürdige Belange des Betroffenen beeinträchtigt sein könnten. Deshalb halte ich es für vertretbar, wenn alle Mitglieder die Gelegenheit erhalten, der Bekanntgabe ihrer Daten zu widersprechen. Auch hierfür ist jedoch Voraussetzung, daß neuen Mitgliedern genau beschrieben wird, was mit ihren personenbezogenen Daten geschieht.

Wenn die Mitglieder Bescheid wissen und trotzdem der Bekanntgabe nicht widersprechen, kann der Verein mit hoher Wahrscheinlichkeit davon ausgehen, daß schutzwürdige Belange nicht verletzt werden. Es verbleibt allerdings ein Restrisiko, wenn ein Mitglied — durch welche Umstände auch immer — tatsächlich von einer beabsichtigten Datenübermittlung nicht wußte und seine Bedenken dagegen nicht vortragen konnte.

6.8.5 Kennzeichnung von Kfz-Stellplätzen

Ein Bürger beschwerte sich bei mir darüber, daß der von ihm gemietete Kfz-Stellplatz mit einem Namensschild gekennzeichnet werden sollte. Er wollte nicht, daß Außenste-

hende seinen Namen an dem Stellplatz lesen könnten. Ich habe den Vermieter der Kfz-Stellplätze darauf hingewiesen, daß die öffentliche Anbringung von Namen nicht nur die Persönlichkeitsrechte der Betroffenen verletzen kann, wenn sie damit nicht einverstanden sind, sondern auch Gefährdungen mit sich bringen kann, wenn etwa durch längeres Leerstehen des Kfz-Stellplatzes deutlich wird, daß der betreffende namentlich erkennbare Wohnungsinhaber verreist ist. Der Vermieter erklärte dazu, die Kennzeichnung der Stellplätze mit Namen sei auf Wunsch vieler Mieter erfolgt. Diese meinten, daß die Namenskennzeichnung länger Gültigkeit haben könne als eine Kennzeichnung mit öfter wechselnden Kennzeichen der Kraftfahrzeuge. Der Vermieter fand sich nach Erörterung der Angelegenheit jedoch bereit, den Mietern freizustellen, ob ihre Stellplätze durch Namensschilder, Kfz-Kennzeichen oder gar nicht gekennzeichnet werden sollen.

Der Beschwerdeführer konnte das von ihm beanstandete Namensschild also wieder von seinem Kfz-Stellplatz entfernen.

6.8.6 Vertragsgestaltung bei Auftrags-Datenverarbeitung

In meinem letzten Bericht (4. TB, Nr. 5.6) erwähnte ich, daß bei Verträgen zur Datenerfassung regelmäßig nicht die Schriftform gewählt wird.

Daß dies auch im Verkehr mit Auftrags-Rechenzentren vorkommt und zu großen Schwierigkeiten führen kann, wurde mir in dem nachstehend geschilderten Fall deutlich.

Ein Rechenzentrum verarbeitete Adressenbestände eines eingetragenen Vereins, die dieser regelmäßig für Werbezwecke verwendete. Der Auftrag wurde mündlich von dem verantwortlichen Mitarbeiter des Vereins erteilt. Dieser hatte für die Werbemaßnahmen eine eigens hierfür geschaffene GmbH zwischengeschaltet, die im gehörte und deren Geschäftsführer er war. Nach internen Meinungsverschiedenheiten wurde er aus dem Verein ausgeschlossen und sein Beschäftigungsvertrag fristlos gekündigt. Nach seinem Ausscheiden aus dem Verein forderte er in seiner Eigenschaft als Inhaber und Geschäftsführer der GmbH von dem Rechenzentrum die Herausgabe des Adressenbestandes mit der Begründung, die Adressen seien Eigentum der GmbH. Der Verein war der Meinung, daß die gespeicherten Werbeadressen allein ihm gehörten. Die Zwischenschaltung der GmbH sei eine Eigenmächtigkeit des ehemaligen Mitarbeiters gewesen; ein Recht an den Adressen sei nie auf die GmbH übergegangen.

Das Rechenzentrum konnte sich wegen des Fehlens schriftlicher Verträge keine Klarheit darüber verschaffen, wer der Auftraggeber und damit der Herr der Daten war. Von den getroffenen Vereinbarungen waren nur noch die praktischen Verarbeitungsdetails nachweisbar. Das Rechenzentrum wollte die Adressen an keine der beiden Seiten herausgeben, um sich nicht möglichen Schadensersatzansprüchen auszusetzen. Es appellierte an die Beteiligten, sich gütlich zu einigen. Dies war aber offensichtlich nicht möglich. Daraufhin wollte das Rechenzentrum die Magnetbänder mit den Adressen beim Amtsgericht hinterlegen, erhielt aber zunächst den Bescheid, daß dies nicht möglich sei, weil sie nicht zu den in § 372 BGB genannten Gegenständen zählen, die man hinterlegen kann.

Nun suchte das Rechenzentrum eine andere Lösung des Problems und dachte daran, die Magnetbänder zu versteigern, um dann den Erlös hinterlegen zu können. Eine derartige Verwertung wäre selbstverständlich unzulässig, weil dadurch in jedem Falle die schutzwürdigen Belange der Betroffenen, also derjenigen, deren Adressen — häufig auf einem ihnen unbekannten Wege — in diese Werbedatei gelangten, beeinträchtigt würden.

Schließlich konnte das Rechenzentrum die Magnetbänder doch beim Amtsgericht hinterlegen.

Gleichwohl wiederhole ich meine dringende Aufforderung an alle Stellen, die Datenverarbeitung im Auftrage betreiben, aber auch an alle Auftraggeber, sich durch schriftliche Verträge abzusichern.