BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

Drucksache 11/3529

11. Wahlperiode

08.01.85

Der Hamburgische Datenschutzbeauftragte

An den
Herrn Präsidenten der Bürgerschaft

Betr.: Dritter Tätigkeitsbericht
des Hamburgischen Datenschutzbeauftragten zum 1. Januar 1985

Gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen Dritten Tätigkeitsbericht, den ich zum 1. Januar 1985 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 Wartenberg & Söhne GmbH, Theodorstraße 41 w, 2000 Hamburg 50, Telefon 89 39 48

Dritter Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten

vorgelegt zum 1. Januar 1985
gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes
Redaktionsschluß: 20. November 1984

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

Inhaltsverzeichnis/Abkürzungsverzeichnis

Abkürzungsverzeichnis

ABM	=	Arbeitsbeschaffungsmaßnahme
AbzG	=	Gesetz betreffend die Abzahlungs-Geschäfte
ADV	=	Allgemeiner Direktwerbe- und Direktmarketing-Verband e.V.
ADV	=	Automatische Datenverarbeitung
AGB	=	Allgemeine Geschäftsbedingungen
AGB-Gesetz	=	Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen
AO	=	Abgabenordnung
AP	=	Nachschlagewerke des Bundesarbeitsgerichts
AsylVfG	=	Asylverfahrensgesetz
AuslG	=	Ausländergesetz
AuslVwV	=	Ausländerverwaltungsvorschrift
AVAD	=	Auskunftsstelle über den Versicherungsaußendienst e.V.
AVwV	=	Allgemeine Verwaltungsvorschrift zu § 15 StVZO
AZR	=	Ausländerzentralregister
BAFL	=	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAG	=	Bundesarbeitsgericht
BAJS	=	Behörde für Arbeit, Jugend und Soziales
BBNU	=	Behörde für Bezirksangelegenheiten, Naturschutz um Umweltgestaltung
BDE	=	Betriebsdatenerfassungssystem
bDSB	=	betrieblicher Datenschutzbeauftragter
BetrVG	=	Betriebsverfassungsgesetz
BDSG	=	Bundesdatenschutzgesetz
Bfl	=	Behörde für Inneres
BGB	=	Bürgerliches Gesetzbuch
BGH	=	Bundesgerichtshof
BIGFON	=	Breitbandiges integriertes Glasfaser-Ortsnetz
BIPS	=	Bremer Institut für Präventivforschung und Sozialmedizin
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtgesetz
BMI	=	Bundesminister des Inneren
BND	=	Bundesnachrichtendienst
BR	=	Betriebsrat
BPAG	=	Bundespersonalausweisgesetz
BremVerSchG	=	Bremisches Verfassungsschutzgesetz
BSB	=	Behörde für Schule und Berufsbildung
BseuchG	=	Bundesseuchengesetz

BSHG	=	Bundessozialhilfegesetz
BStatG	=	Bundesstatistikgesetz
Btx	=	Bildschirmtext
BVerfG	=	Bundesverfassungsgericht
BVerfSchG	=	Bundesverfassungsschutzgesetz
BVM	=	Bundesverband Deutscher Marktforscher e.V.
BVSt	=	Besoldungs- und Versorgungsstelle
BZR	=	Bundeszentralregister
BZRG	=	Bundeszentralregistergesetz
COM	=	Computer-output on Mikrofilm
DBP	=	Deutsche Bundespost
DEVO	=	Datenerfassungsverordnung
DÜVO	=	Datenübermittlungsverordnung
DV	=	Datenverarbeitung
DV AuslG	=	Verordnung zur Durchführung des Ausländergesetzes
DVZ	=	Datenverarbeitungszentrale
EC-Karte	=	Eurocheque-Karte
ED	=	Erkennungsdienst
EDV	=	elektronische Datenverarbeitung
EG	=	Europäische Gemeinschaft
EV	=	Eidesstattliche Versicherung
EWG	=	s. EG
FB	=	Finanzbehörde
FD	=	Fachdirektion
GG	=	Grundgesetz
GVBl	=	Gesetz- und Verordnungsblatt
GVGw	=	Gesetz über die Vereinbarung des Gesundheitswesens
GWG	=	Gesetz über das Gesundheitswesen
HASPA	=	Hamburger Sparkasse
HHA	=	Hamburger Hochbahn AG
HmbMG	=	Hamburgisches Meldegesetz
HmbHG	=	Hamburgisches Hochschulgesetz
HmbDSB	=	Hamburgischer Datenschutzbeauftragter

HmbSOG	–	Hamburgisches Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
HStatG	–	Hochschulstatistikgesetz
HmbVerfSchG	–	Hamburgisches Verfassungsschutzgesetz
HUK-Verband	–	Verband der Haftpflicht-, Unfall-, Auto- und Rechtsschutzversicherer e.V.
INPOL	–	Informationssystem der Polizei
KAN	–	Kriminalaktennachweis
KBA	–	Kraftfahrtbundesamt
KPMD	–	Allgemeiner Kriminalpolizeilicher Meldedienst
KPMD-S	–	Allgemeiner Kriminalpolizeilicher Meldedienst im Staatsschutz
KpS	–	Kriminalpolizeiliche personenbezogene Sammlung
LAG	–	Landesarbeitsgericht
LfV	–	Landesamt für Verfassungsschutz
LKA	–	Landeskriminalamt
LVV	–	Landesverkehrsverwaltung
MAD	–	Militärischer Abschirmdienst
ME	–	Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder
MeldDÜV	–	Meldedatenübermittlungsverordnung
MiStra	–	Mitteilungen in Strafsachen
MiZi	–	Mitteilungen in Zivilsachen
MSI	–	Unternehmen der Markt-, Meinungs- und Sozialforschung
NJW	–	Neue Juristische Wochenschrift
NRW	–	Nordrhein-Westfalen
NVwZ	–	Neue Zeitung für Verwaltungsrecht
OWiG	–	Ordnungswidrigkeitengesetz
PB	–	Polizeiliche Beobachtung
PC	–	Personal Computer
PIN	–	Identifizierungsnummer
PIOS	–	Inpol-Anwendungen Personen, Institutionen, Objekte und Sachen
PIS	–	Personalinformationssystem
PHW	–	personenbezogener Hinweis

POS	-	Point of Sale
PsychKG	-	Hamburgisches Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten
SCHABS	-	Schufa-Auskunfts- und Beobachtungssystem
Schufa	-	Schutzgemeinschaft für allgemeine Kreditsicherung
SGB	-	Sozialgesetzbuch
SMD	-	Sondermeldedienst
SOG	-	s. HmbSOG
SPUDOK	-	Spurendokumentation
StA	-	Staatsanwaltschaft
StaLa	-	Statistisches Landesamt
StBauFG	-	Städtebauförderungsgesetz
StGB	-	Strafgesetzbuch
StPO	-	Strafprozeßordnung
StVG	-	Straßenverkehrsgesetz
StVZO	-	Straßenverkehrszulassungsordnung
TA	-	Technische Abwicklung des Auskunfts- und Meldeverfahrens der Schufa
TAN	-	Transaktionsnummer
TB	-	Tätigkeitsbericht
TEMEX	-	Telemetry Exchange
TSG	-	Transsexuellengesetz
UKE	-	Universitätskrankenhaus Eppendorf
VO	-	Verordnung
VZ-Urteil	-	Volkszählungsurteil
WoBindG	-	Wohnungsbindungsgesetz
ZAW	-	Zentralausschuß der Werbewirtschaft e.V.
ZEVIS	-	Zentrales Verkehrsinformations-System
ZK	-	Zentralkartei
ZKI	-	Zoll-Kriminalamt
ZPO	-	Zivilprozeßordnung

Vorwort

Der 4. Abschnitt meines 2. Tätigkeitsberichts (Datenschutz im nicht-öffentlichen Bereich) hat einige Mißverständnisse ausgelöst. Ich wiederhole deshalb den 1. Absatz des Vorworts, das ich meinem 1. Tätigkeitsbericht vorangestellt habe:

> Das Hamburgische Datenschutzgesetz bestimmt in § 20 Abs. 2 S. 2, daß der Hamburgische Datenschutzbeauftragte (DSB) jährlich zum 1. Januar Senat und Bürgerschaft einen Tätigkeitsbericht zu erstatten hat. Die Berichtspflicht des DSB ist auf den Anwendungsbereich des Hamburgischen Datenschutzgesetzes beschränkt, das die Verarbeitung personenbezogener Daten durch die hamburgische Verwaltung regelt. Dem Hamburgischen Datenschutzbeauftragten sind aber auch die Aufgaben der Aufsichtsbehörde nach §§ 30/40 Bundesdatenschutzgesetz (BDSG) übertragen. Meines Erachtens liegt es im Interesse der Bürgerschaft, des Senats und auch der Öffentlichkeit, wenn ich über den gesetzlichen Auftrag hinaus in meinem Tätigkeitsbericht auch auf den Datenschutz im nicht-öffentlichen Bereich eingehe; denn erst die Zusammenfassung beider Kontrollfunktionen, der des Landesbeauftragten im öffentlichen Bereich und der der Aufsichtsbehörde im nicht-öffentlichen Bereich, ergibt ein vollständiges Bild des Datenschutzes in der Freien und Hansestadt Hamburg und der Tätigkeit des Hamburgischen Datenschutzbeauftragten.

Um es noch einmal klarzustellen: Eine Rechtspflicht, über den nicht-öffentlichen Bereich zu berichten, ergibt sich also weder aus dem Hamburgischen noch aus dem Bundesdatenschutzgesetz. Die Resonanz auf die ersten beiden Berichte hat aber gezeigt, daß das Interesse der Öffentlichkeit, über Datenschutzprobleme im nicht-öffentlichen Bereich unterrichtet zu werden, unerwartet groß ist. Das liegt vielleicht auch daran, daß bislang nur wenige Aufsichtsbehörden über ihre Tätigkeit im nicht-öffentlichen Bereich informiert haben. Der Deutsche Bundestag hat bei der Beratung des 5. Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz festgestellt, daß sich die Datenschutzdiskussion in der Vergangenheit zu stark vorwiegend mit dem öffentlichen Bereich auseinandergesetzt habe und der nicht-öffentliche auch in der künftigen Entwicklung für den Bürger von wesentlich größerer Bedeutung sein werde als der öffentliche Bereich. Meine Erfahrungen bestätigen diesen Eindruck, und ich fühle mich hierdurch ermuntert, wie bisher die Unterrichtung über Grundsatzfragen des nicht-öffentlichen Bereichs zu einem Schwerpunkt meines Tätigkeitsberichts zu machen. Um aber auch den bloßen Anschein einer einseitigen Berichterstattung zu vermeiden, will ich künftig interessierten Stellen Gelegenheit geben, sich mit eigenen Stellungnahmen im Bericht zu äußern.

1. Zur Lage des Datenschutzes

Ein Jahr nach Verkündung des Volkszählungsurteils – und zugleich am Ende des Symboljahres 1984 – besteht Veranlassung, Bilanz zu ziehen. Unstreitig hat das Urteil weitreichende Auswirkungen auf die Erhebung und Verwendung personenbezogener Daten durch alle öffentlichen und auch – diese Erkenntnis braucht etwas länger, um sich durchzusetzen – alle nicht-öffentlichen Stellen.

Heute stellt niemand mehr in Abrede, daß die Datenverarbeitung auf vielen Gebieten sich nicht auf eine gesetzliche Grundlage stützen kann, die den strengen verfassungsrechtlichen Anforderungen entspricht, wie sie das Bundesverfassungsgericht im Volkszählungsurteil formuliert hat. Das bedeutet nicht, daß das Volkszählungsurteil die Verfassungswidrigkeit der die Informationsverarbeitung der amtlichen Statistik, der Gesundheitsbehörden, der Polizei, des Verfassungsschutzes etc. regelnden Vorschriften festgestellt hätte. Wohl aber hat das Bundesverfassungsgericht im Volkszählungsgesetz Mängel und Regelungslücken aufgezeigt, die sich in vielen anderen Gesetzen wiederfinden. Diese Gesetze werden vom Verdikt des Bundesverfassungsgerichts nicht unmittelbar erfaßt; es ist aber damit zu rechnen, daß das Bundesverfassungsgericht – sofern es einen Anlaß zur Überprüfung gibt – Vorschriften, die offensichtlich von dem im Volkszählungsurteil aufgestellten Grundsätzen abweichen, für verfassungswidrig erklärt. Es ist daher ein Gebot des eigenen Interesses – von verfassungspolitischen Handlungspflichten einmal ganz abgesehen –, daß der Gesetzgeber – in Bund und Ländern – sobald wie möglich einen verfassungsgemäßen Zustand herstellt.

Was haben nun die Verantwortlichen getan, um erkannte Mängel zu beseitigen und Lücken zu schließen?

1.1. Die Lage im Bund

Zum 1.11.1984 sollte ein neuer Personalausweis eingeführt werden. Sozusagen in letzter Minute wurde das 4. BPAG, das hierfür die Voraussetzungen schaffen sollte, außer Kraft gesetzt. Aber: Die Absicht, demnächst einen computerlesbaren Personalausweis auszugeben, wurde nicht aufgegeben. Vielmehr brachten die Koalitionsfraktionen einen neuen Gesetzentwurf im Bundestag ein, der zwar eine Reihe datenschutzrechtlicher Verbesserungen enthält, aber auch einen bedeutsamen Schönheitsfehler aufweist: trotz zusätzlicher Zweifel an der Notwendigkeit eines neuen Ausweises wird nicht dargetan, warum er im überwiegenden Allgemeininteresse unverzichtbar ist. Es fehlt nach wie vor an der Grundvoraussetzung für die Einführung des neuen Systems.

Auch im Jahre 1984 wurde der Mikrozensus ausgesetzt. Aber: Es bedurfte erst einer energischen Intervention des Bundestages, ehe die Bundesregierung darauf verzichtete, die Erhebung trotz offensichtlicher Gesetzesmängel unter Berufung auf einen „Übergangsbonus" durchzuführen.
Die Bundesregierung hat inzwischen den Entwurf eines neuen Volkszählungsgesetzes beschlossen, dessen einzelne Bestimmungen den verfassungsrechtlichen Anforderungen weitgehend entsprechen. Aber: Ihre Bemühungen, die Bürger von der Notwendigkeit einer neuen Volkszählung zu überzeugen, erschöpfen sich darin, daß sie sich auf das Bundesverfassungsgericht beruft, das – nach dem gegenwärtigen Erkenntnisstand – eine Totalerhebung noch für verhältnismäßig hält, und heute schon denen mit Zwangsmitteln droht, die ihre Fragebogen nicht abgeben wollen. Es ist aber nicht – jedenfalls nicht mit hinreichender Deutlichkeit – dargetan, ob alle dem Gesetzgeber zugänglichen Erkenntnisquellen zur Notwendigkeit einer Totalerhebung ausgeschöpft sind. Insbesondere fehlen auch Nachweise für eine Prüfung, ob hinsichtlich aller Erhebungsmerkmale eine Totalerhebung erforderlich ist, oder ob nicht vielmehr jedenfalls zu einzelnen Merkmalen Stichprobenerhebungen ausreichen. Schließlich ist dem Entwurf und seiner Begründung nicht – jedenfalls nicht mit hinreichender Deutlichkeit – zu entnehmen, ob zur Frage der Auskunftspflicht bei der Abwägung des Für und Wider alle Argumente einbe-

zogen und zutreffend gewichtet worden sind. Die Ergebnisqualität der Volkszählung hängt von der Vollständigkeit und Richtigkeit der erteilten Auskünfte ab. Auskunftszwang bewirkt zwar weitgehend Vollständigkeit, nicht notwendigerweise aber auch Richtigkeit. Freiwilligkeit hingegen garantiert weitgehend Richtigkeit, nicht aber Vollständigkeit.

Rechtzeitig vor der bundesweiten Einführung von Bildschirmtext haben alle Bundesländer den Staatsvertrag ratifiziert, der für die Datenschutzprobleme, die mit dem Betrieb und der Nutzung von Bildschirmtext verbunden sind, einigermaßen befriedigende Lösungen anbietet. Aber: Der Bundespostminister ist weiterhin nicht bereit, die Regelungen des Staatsvertrages, soweit sie den Betreiber Deutsche Bundespost betreffen, in Vorschriften des Bundesrechts umzusetzen. Noch immer scheint die Deutsche Bundespost nicht einzusehen, daß im Hinblick auf die Beschränkungen der informationellen Selbstbestimmung eine den verfassungsrechtlichen Anforderungen entsprechende gesetzliche Regelung der Erhebung und Verarbeitung der Daten, die beim Betrieb von Bildschirmtext anfallen, unabdingbar ist.

Der Referentenentwurf zur Novellierung des BDSG, den das Bundesinnenministerium im Juni 1983 zur Diskussion gestellt und den ich in meinem vorigen TB als zur Fortentwicklung des Datenschutzrechtes nicht geeigneten Beitrag bezeichnet hatte, ist in der Versenkung verschwunden. Aber: Einen neuen Entwurf gibt es bislang nicht. Angeblich soll nicht die Bundesregierung, sondern wollen die Koalitionsfraktionen einen neuen Versuch wagen. Ob und wann sie sich verständigen können, ist ungewiß. Es ist kaum mehr damit zu rechnen, daß die schwierigen Beratungen im Bundestag und Bundesrat noch in dieser Wahlperiode abgeschlossen werden können.

Im Juni 1984 hat die Innenministerkonferenz ihre zuständigen Arbeitskreise beauftragt, baldmöglichst abschließende Berichte mit Formulierungsvorschlägen für bereichsspezifische Regelungen der Datenerhebung und Datenverarbeitung bei der Polizei und beim Verfassungsschutz vorzulegen. Aber: Im Beschluß heißt es weiter, daß die Vorschläge für den Bereich des Verfassungsschutzes Änderungen des Bundesdatenschutzgesetzes und die für den Bereich der Polizei vorgesehenen Änderungen des Bundesdatenschutzgesetzes und der Strafprozeßordnung berücksichtigen sollten. Wir werden noch einige Zeit warten müssen.

1.2 Die Lage in Hamburg

In seiner Stellungnahme zu meinem 2. TB schreibt der Senat, daß es ihm, bevor Änderungen des Hamburgischen Datenschutzgesetzes vorgenommen würden, empfehlenswert erscheine, zunächst die beabsichtigte Novellierung des BDSG mitzugestalten. Dem stimme ich zu, weise aber darauf hin, daß dann, wenn der Bund die ihm zugedachte Schrittmacherfunktion nicht alsbald einnimmt, eine Novellierung des Hamburgischen Datenschutzgesetzes nicht länger hinausgezögert werden darf. Mögen auch – wie der Senat weiter schreibt – die Erfahrungen des Bundes und der anderen Länder in das Hamburgische Datenschutzgesetz eingeflossen sein, gemessen an den strengen Anforderungen des Volkszählungsgesetzes ist es in vielen Punkten änderungs- und ergänzungsbedürftig.

An anderer Stelle heißt es in der Stellungnahme des Senats, daß die geforderten gesetzlichen Grundlagen für die staatlichen Informationserhebungen und Übermittlungen dort zu schaffen seien, wo bislang nichts geschehen sei; ein Schwerpunkt im landesrechtlichen Bereich werde die Novelle des SOG sein. Leider ist die Innenbehörde mit ihren Bemühungen, einen Entwurf zur Änderung des SOG fertigzustellen, im Jahre 1984 aber nicht einen Schritt vorangekommen; sie hat sich – ganz im Gegenteil – mehrere Schritte zurückbewegt. Über andere Initiativen des Senats ist mir folgendes bekannt: der Senat wird demnächst den Entwurf eines Landesmediengesetzes vorlegen, der auch Datenschutzvorschriften enthalten wird; ausgelöst durch die geplante Automation des Meldewesens wird es eine Novellierung des Meldegesetzes geben; über den Stand der Vorar-

beiten am Archivgesetz, die der Senat in seiner Stellungnahme erwähnt, bin ich nicht unterrichtet. Aus meiner Sicht sind – neben dem Archivgesetz sowie dem SOG und der Melderechtsnovelle – folgende Regelungen vordringlich: Novellierungen des Verfassungsschutzgesetzes, des Gesetzes über das Gesundheitswesen und des Personalvertretungsgesetzes sowie ein Katastergesetz.

Ab 1.5.1984 ist § 6 Abs. 1 Nr. 4 Hamburgisches Datenschutzgesetz in Kraft getreten. Nach dieser Vorschrift hat jeder das Recht, die Übermittlung der zu seiner Person gespeicherten Daten an andere öffentliche Stellen zu sperren, soweit die Übermittlung nicht durch Gesetz zugelassen ist. Obwohl die Verwaltung 3 Jahre Zeit gehabt hatte, sich auf das Inkrafttreten des § 6 Abs. 1 Nr. 4 vorzubereiten, war die Verwirrung groß, als die ersten Anträge auf Sperrung eingingen. Besondere Schwierigkeiten bereiteten diejenigen Anträge, die sich nicht gezielt auf die Sperrung bestimmter Daten richteten, sondern sich pauschal auf alle zur Person des Antragstellers von den Hamburger Behörden gespeicherten Daten erstrecken. Nach mühsamer Abstimmung gelang es schließlich aufgrund einer Staatsrätebesprechung vom 4.9.1984, die Hinweise zur Durchführung des Hamburgischen Datenschutzgesetzes um eine Regelung zu ergänzen, die die organisatorische Bewältigung der Sperranträge sicherstellen soll.
Mit der Dreijahresfrist, die der Gesetzgeber der Verwaltung einräumte, wollte er ihr allerdings nicht die Gelegenheit geben, sich in aller Ruhe auf die Bearbeitung der Sperranträge einzurichten. Vielmehr wollte er sie veranlassen, ihre Datenflüsse zu überprüfen, sie auf das unerläßliche Minimum zu beschränken und für die verbleibenden notwendigen Übermittlungen bereichsspezifische Rechtsgrundlagen – zugleich als Ausschluß des Rechts auf Sperrung nach § 6 Abs. 1 Nr. 4 – zu schaffen. Hierauf hatte die Justizbehörde bereits mit Schreiben vom 19.5.1981 aufmerksam gemacht. Doch hat dieser Hinweis – ebenso wie meine Erinnerungen in beiden Tätigkeitsberichten – nur wenig Resonanz gefunden, wobei die Bfl allerdings ausgenommen werden muß, die sich – wenngleich bislang erfolglos – bemüht hat, die polizeilichen Informationsbeziehungen rechtlich abzusichern. Deshalb wurde in der schon erwähnten Staatsrätebesprechung weiter beschlossen, „daß parallel zur Durchführung des § 6 Abs. 1 Nr. 4 in den Behörden die erforderlichen rechtlichen Prüfungen vorzunehmen sind, inwieweit bereichsspezifische gesetzliche Regelungen zur Datenübermittlung vorhanden sind oder welche entsprechenden einschlägigen Gesetzgebungsvorhaben ggf. vorzubereiten oder einzuleiten sind." Es ist bedauerlich, daß die Staatsräte sich darauf beschränkt haben, die Tragfähigkeit der Rechtsgrundlagen für die Datenübermittlung überprüfen zu lassen, obwohl das Bundesverfassungsgericht inzwischen über die Anforderungen der Hamburger Bürgerschaft noch weit hinausgegangen ist. Aufgrund des VZ-Urteils ist es unabdingbar, daß für sämtliche Informationsakte der Verwaltung geprüft wird, ob sie erforderlich sind und ob sie sich zudem auf ausreichende Rechtsvorschriften stützen können.

1.3 Konsequenzen

Viel Positives gibt es also nicht zu berichten. Zwar haben die Bundesregierung und auch die meisten Landesregierungen Stellungnahmen zum VZ-Urteil abgegeben. Aber Versuche, die gewonnenen Erkenntnisse in konkrete Regelungsvorschläge umzusetzen, sind kaum zu verzeichnen. Zur Entschuldigung wird vorgebracht: das Urteil habe mehr Fragen offengelassen als Antworten gegeben. Die Aussagen des Bundesverfassungsgerichts bedürften eingehender Erörterungen zwischen Politik, Verwaltungspraxis und Wissenschaft. Auch sei eine intensivere Abstimmung zwischen dem Bund und allen Ländern erforderlich.

Gern wird dabei übersehen, daß die Aussage, Beschränkungen des Rechts auf informationelle Selbstbestimmung seien nur zulässig im überwiegenden Allgemeininteresse und auf einer rechtlichen Grundlage, die den rechtstaatlichen Geboten der Normenklarheit und Verhältnismäßigkeit entspreche, nicht neu ist, sondern an Entscheidungen geknüpft, die z. T. Jahrzehnte alt sind. Auch sei daran erinnert, daß die Datenschutzdiskussion schon in den Jahren vor dem VZ-Urteil von der Forderung nach bereichsspezifischen und präzisen gesetzlichen Regelungen der Datenverarbeitung beherrscht war.

Als ein Beispiel sei die Entschließung des Bundestages vom 17.1.1980 erwähnt, in der die Bundesregierung aufgefordert wird, die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen.

Nicht nur, daß der „Umsetzungsbonus" in nicht hinnehmbarer Weise strapaziert wird; viel beunruhigender ist, daß kaum eine der bisherigen Äußerungen zum VZ-Urteil so zu verstehen ist, als wollten die Verantwortlichen nunmehr für eine konsequente und umfassende Verwirklichung des Datenschutzes sorgen. Die Anstrengungen scheinen sich eher darauf zu richten, die Überlegungen des Bundesverfassungsgerichts als beiläufige und folgenlose Bemerkungen auszugeben. Aus vielen Stellungnahmen läßt sich die zufriedene Feststellung herauslesen, daß das geltende Datenschutzrecht die Anforderungen des Gerichts im großen und ganzen bereits berücksichtige. Weiter wird vor einer maximalistischen Interpretation des Urteils gewarnt, die zum Stillstand weiter Teile der Verwaltung und einem erheblichen Bürokratiezuwachs führen würde. Schließlich wird beklagt, daß die Forderung nach bereichsspezifischen datenschutzrechtlichen Regelungen mit den Bemühungen zur Eindämmung der Normenflut kollidiere.

Die Konferenz der Datenschutzbeauftragten ist in ihrer Entschließung zu den Auswirkungen des Volkszählungsurteils entschieden der Tendenz entgegengetreten, bereichsspezifische Regelungen allenfalls dort zu erwägen, wo es zu einer zwangsweisen Erhebung kommt. Auf der anderen Seite wird niemand den Datenschutzbeauftragten vorwerfen können, daß sie das Urteil in einer Weise interpretierten, die die Funktionsfähigkeit der Verwaltung gefährden könnte. Die Feststellung des Bundesverfassungsgerichts, daß es von Art, Umfang und denkbaren Verwendungen der personenbezogenen Daten sowie von der Gefahr ihres Mißbrauchs abhänge, in wieweit das Recht auf informationelle Selbstbestimmung und im Zusammenhang damit der Grundsatz der Verhältnismäßigkeit zu gesetzlichen Regelungen der Datenverarbeitung zwingen, ermöglicht m. E. Lösungen, die sich zwar in erster Linie an der Situation der Betroffenen zu orientieren haben, die Bedürfnisse der Behördenpraxis aber nicht außer acht lassen. Auf keinen Fall ist es ausreichend, die Generalklauseln in den allgemeinen Datenschutzgesetzen durch ebenso unbestimmte Formulierungen in Spezialgesetzen zu ersetzen und den speichernden Stellen hiermit einen Verarbeitungsrahmen zur Verfügung zu stellen, der es ihnen freistellt, ihre bisherigen Verfahren auch unter geänderten gesetzlichen Bedingungen beizubehalten.

Die Datenschutzbeauftragten müssen sich fragen, welche Konsequenzen daraus abzuleiten sind, daß es für die Informationstätigkeit der Verwaltung vielfach keine oder nur sehr unzulängliche Rechtsgrundlagen gibt und daß nicht abzusehen ist, wann dieser – inzwischen von allen Beteiligten als nicht mehr verfassungskonform bewertete – Zustand beendet wird. Ganz neu ist die Situation für sie nicht, denn schon in der Vergangenheit hatten sie auf den verschiedensten Aufgabengebieten das Fehlen gesetzlicher Erlaubnistatbestände für die von der Verwaltung getätigten Informationseingriffe gerügt. Neu ist nur, daß das Bundesverfassungsgericht ihre – früher nicht unbestrittene – Auffassung so eindeutig bestätigt hat.

Ich fordere nicht, daß alle Aktivitäten der Verwaltung, die sich – häufig nach gemeinsamer Einschätzung – nicht auf eine tragfähige Rechtsgrundlage stützen können, sofort eingestellt werden. Doch kann solche Feststellung auch nicht ohne praktische Folgen bleiben. Bestimmte, besonders schwerwiegende Informationseingriffe, die nicht nur formalen Bedenken begegnen, bei denen vielmehr Zweifel auch an der materiellen Erforderlichkeit bestehen, können nicht fortgeführt werden (als Beispiele erwähne ich die in Nr. 3.8.4 abgehandelten Staatsschutzberichte und einige – in Nr. 3.7.3 geschilderte – Ausländer betreffende Datenflüsse). Ganz allgemein gilt, daß die Verwaltung sich auf das zu ihrer Aufgabenerfüllung unerläßliche Minimum zu beschränken hat. Diesem Grundsatz kommt – auch nach der Rechtsprechung des Bundesverfassungsgerichts – besondere Bedeutung zu, solange einwandfreie gesetzliche Grundlagen für eine Verwaltungstätigkeit noch nicht vorhanden sind. Die Erschließung neuer DV-Anwendungen aufgrund fortentwickelter Technik ist nur zulässig, sofern die rechtlichen

Voraussetzungen hierfür geschaffen sind, also auch der Datenschutz weiter entwickelt ist.

2. Überblick über die Tätigkeit meiner Dienststelle

2.1 Entwicklung der Dienststelle

2.1.1 Aufgabenerfüllung

Der jetzige Personalbestand meiner Dienststelle, nämlich

- 3 Stellen des höheren Dienstes,
- 3 Stellen des gehobenen Dienstes,
- 2 Bürokräfte,

wird von der Bewältigung der dringendsten Tagesgeschäfte in Anspruch genommen. Ich hatte schon in meinem 2. TB (Nr. 2.2, S. 6) darauf hingewiesen, daß dieser Personalbestand bei weitem nicht ausreichen würde, um die wünschenswerte Kontrolldichte zu erreichen. Dieser Hinweis hat nichts von seiner Aktualität verloren. Ganz im Gegenteil: Der Hamburgische Datenschutzbeauftragte ist inzwischen zusätzlich dafür zuständig, die Einhaltung der Datenschutzvorschriften des Bildschirmtext-Staatsvertrages bei den Anbietern im öffentlichen und nicht-öffentlichen Bereich Hamburgs zu überwachen (vgl. Nr. 2.5.2.1), ohne dafür die von mir beantragte personelle Verstärkung erhalten zu haben.

Mit den Tätigkeiten

- Beratung, Bearbeitung von Anfragen öffentlicher und nicht-öffentlicher Stellen zu Einzelproblemen,
- Bearbeitung von Eingaben,
- Beratung von Senat und Bürgerschaft bei Normensetzungsverfahren

ist die Dienststelle heute nahezu ausgelastet. Die wenigen eigenen Initiativen, die im Laufe dieses Jahres ergriffen werden konnten, waren nur möglich durch Überstunden, überobligatorischen Einsatz von Referendaren sowie verzögerliche Bearbeitung von Eingaben und Beratungsersuchen.

Nach meinen Vorstellungen reicht es für eine effektive Datenschutzkontrolle nicht aus, wenn der Datenschutzbeauftragte fast ausschließlich nur auf Anstöße von außen hin tätig werden kann. Eine angemessene Erfüllung der Überwachungsaufgabe nach § 20 Abs. 1 Satz 1 setzt vielmehr voraus, daß der Datenschutzbeauftragte und seine Mitarbeiter in erheblich größerem Umfang auf eigene Initiative und – gelegentlich mit einem gewissen Überraschungsmoment – ganze Dienststellen systematisch überprüfen können. Nur wenn die Behörden damit rechnen müssen, daß der Datenschutzbeauftragte – ähnlich wie der Rechnungshof – auch von sich aus regelmäßig umfassende Prüfungen vornimmt, werden sie die eigenen Aktivitäten für den gebotenen Datenschutz verstärken.

Besondere eigene Initiativen des Datenschutzbeauftragten sind – neben einer verstärkten Prüftätigkeit – auch auf dem Gebiet der Rechtspolitik geboten. Die bisherigen Erfahrungen z. B. mit dem Krebsregistergesetz, der SOG-Novelle sowie der Meldegesetznovelle zeigen, daß vom Datenschutzbeauftragten maßgebliche inhaltliche Impulse ausgehen müssen, um datenschutzrechtliche Regelungen zu schaffen, die den Anforderungen des Volkszählungsurteils entsprechen. Allein die erforderlichen, z. T. weitreichenden Stellungnahmen im Rahmen des Behördenabstimmungsverfahrens erfordern bereits einen hohen Arbeitsaufwand. Die Arbeitssituation in den einzelnen Referaten meiner Dienststelle – siehe die Übersicht über die Organisation meiner Dienststelle, die dem 2. TB beigefügt ist – läßt sich wie folgt beschreiben:

2.1.1.1

Dem Referat D 2 obliegt u. a. die Beratung und Kontrolle in organisatorisch-technischen Fragen (insbesondere Mitwirkung an Automationsvorhaben und technische Prüfungen). Z. Z. sind 13 kleinere, 13 mittlere und 4 große Rechenzentren der hamburgischen Verwaltung zu überprüfen.

Nach der Jahresplanung für 1984 sollten
- 2 Rechenzentren, 1 autonome dezentrale DV-Anlage, der Stand der Datensicherung bei dezentralen DV-Anlagen, 1 automatisiertes Verfahren im Bereich der sozialen Sicherung und das Gesamtkonzept der Datensicherung in der Datenverarbeitungszentrale (DVZ) geprüft werden.

Tatsächlich geprüft worden sind
- 1 Rechenzentrum,
- 1 Anwendung im Rahmen von Bildschirmtext (die Notwendigkeit für diese Prüfung hat sich nachträglich aus überregionalen Absprachen ergeben).

Die Überprüfung des Gesamtkonzepts der Datensicherung in der DVZ ist begonnen worden.
Nach den Erfahrungen, die ich bei der Prüfung des Rechenzentrums gesammelt habe, würde es bei den Kapazitäten, die für Prüfungen zur Verfügung stehen, 12-13 Jahre dauern, bis ich alle Rechenzentren der Hamburger Verwaltung einmal überprüft hätte.
Zu den technischen Prüfungen kommt die inhaltliche Prüfung von automatisierten Verfahren (Anwendungssystemen) hinzu, d. h. die Prüfung, ob personenbezogene Daten im zulässigen Rahmen verarbeitet werden. Erfahrungen über den Zeitbedarf solcher Prüfungen liegen noch nicht vor. Nach vorsichtigen Schätzungen ist für die inhaltliche Prüfung von automatisierten Verfahren mindestens derselbe Zeitaufwand erforderlich wie für die Prüfung von Rechenzentren.
Bei unveränderter Personalausstattung werden alle jetzt vorhandenen Rechenzentren und alle jetzt eingesetzten Anwendungssysteme erst nach 25 Jahren von mir überprüft sein können. Eine solche „Prüfdichte" ist unvertretbar.

2.1.1.2 Das Referat D 3 unterliegt in besonderem Maße einer Außensteuerung, weil
die vom Referat betreuten Dienststellen des öffentlichen Bereichs Bürgern besonders häufig Anlaß zu Beschwerden geben,
der Beratungs- und Informationsbedarf insbesondere in den Bereichen Gesundheits- und Sozialwesen (vor allem aufgrund der dort geltenden speziellen Vorschriften zum Patienten- und Sozialgeheimnis) besonders groß ist. Die Belastung durch einzelne Auskunftsersuchen wird häufig noch dadurch verstärkt, daß die Ersuchen spezielle Bereiche betreffen, mit denen wir noch nicht befaßt waren, die wir aber – wegen des Gefährdungspotentials – längst kennen sollten und in die wir uns jeweils erst einarbeiten müssen.

Die wenigen systematischen Prüfungen, die das Referat in diesem Jahr durchführen konnte (Gesundheitsamt Hamburg-Nord, Landesverkehrsverwaltung, Ausländerbehörde), haben unter Beweis gestellt, daß hierbei viele Unregelmäßigkeiten festgestellt und neue Erkenntnisse gewonnen wurden.
Im Zusammenhang mit der Bearbeitung von Einzelfällen, Einschätzungen von Gefährdungspotientialen und bevorstehenden Automationsentwicklungen habe ich eine Liste mit etwa 15 Dienststellen (aus den Funktionsbereichen Polizei, Verfassungsschutz, Einwohnerwesen, Sozialwesen und Gesundheitswesen) aufgestellt, deren systematische Überprüfung mir vordringlich erscheint. Allein diese Prüfungen mit besonderer Priorität könnten bei unveränderter Personalausstattung erst nach ca. 5 Jahren abgeschlossen werden. Auch ein solcher Prüfturnus ist nicht akzeptabel.

2.1.1.3 Die wesentliche Kontrollaufgabe des Referats D 4 ist die regelmäßige Überprüfung der datenverarbeitenden Stellen, die dem 4. Abschnitt des BDSG zuzuordnen sind – in der Hauptsache Auskunfteien, Markt- und Meinungsforschungsinstitute, Auftrags- Datenverarbeiter wie Rechenzentren und Erfassungsbetriebe.
Diese Stellen haben sich zu einem bei der Aufsichtsbehörde geführten öffentlichen Register zu melden, in dem heute 216 datenverarbeitende Stellen verzeichnet sind.
Da dieses Referat auch viele Eingaben (ca. 150 Eingaben jährlich) zu bearbeiten und zahlreiche Unternehmen, Betriebsräte und betriebliche Datenschutzbeauftragte zu beraten hat, könnte nach meinen Berechnungen die Überprüfung aller zu überwachenden Stellen bei gleichbleibender personeller Stärke erst in ca. 22 Jahren abgeschlossen sein. Demgegenüber haben sich die Aufsichtsbehörden der Länder im „Düsseldorfer Kreis" auf einen Prüfturnus von 3 Jahren verständigt.

2.1.2 Konsequenzen

Eine Aufgabenerfüllung, die den Anforderungen einer effektiven Datenschutzkontrolle einigermaßen gerecht wird, ist mir mit dem derzeitigen Personalbestand nicht möglich. Um die jetzigen Mitarbeiter zumindest in einigen Bereichen von einer ständigen Überlastung befreien zu können, sind umgehend folgende Maßnahmen erforderlich:

1. Bewilligung der von mir beantragten Stelle des höheren Dienstes für die Überwachung der Anbieter im Bildschirmtext.
2. Bewilligung einer Stelle des höheren Dienstes für die Überwachung der speichernden Stellen des 4. Abschnitts des BDSG. Dadurch könnte erreicht werden, daß die Prüfung aller zu überwachenden Stellen statt in 22 Jahren in ca. 7 Jahren abgeschlossen sein könnten.
3. Bewilligung einer Stelle des gehobenen Dienstes für die Kontrolle der öffentlichen Verwaltung. Dadurch wäre es möglich, zumindest die Bereiche „Einwohnerwesen und Justiz", „Sozialstaatliche Leistungsverwaltung und Gesundheitswesen" sowie die „Innere Sicherheit" von jeweils einem spezialisierten Mitarbeiter betreuen zu lassen.

Ich muß aber darauf hinweisen, daß auch nach der Erfüllung dieser Forderungen eigene Initiativen des Hamburgischen Datenschutzbeauftragten nur selten ergriffen werden könnten und die Kontrolldichte noch verhältnismäßig gering bleiben würde.

2.2 Konferenz der Datenschutzbeauftragten

Der Hamburgische Datenschutzbeauftragte führte 1984 den Vorsitz in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die in dieser Zeit zu folgenden Themen Beschlüsse faßte:

- Errichtung des bundesweiten Kriminalaktennachweises (KAN)
- Erteilung von Bankauskünften nach der Neufassung der Allgemeinen Geschäftsbedingungen der Banken und Sparkassen,
- Auswirkungen des Volkszählungsurteils,
- Mikrozensus 1984,
- Kabelkommunikation,
- Einführung von Bildschirmtext,
- 2. Meldedatenübermittlungsverordnung des Bundes,
- Mitteilungen in Zivilsachen (MiZi),
- Einführung des Telefon-Fernwirksystems „TEMEX",
- Referentenentwurf für ein Hochschulstatistikgesetz.

Daneben wurden vor allem folgende Themen intensiv erörtert:

- die geplante Änderung des Straßenverkehrsgesetzes und die damit verbundene Einführung eines „Zentralen Verkehrs-Informations-Systems (ZEVIS) und
- das Volkszählungsgesetz 1985.

2.3 Eingaben

Bis zum 30.11.1984 gingen 298 Eingaben ein. Die bislang erledigten Eingaben betrafen folgende Bereiche:

Bereiche	Anzahl	gesamt
A Öffentlicher Bereich		
– Sicherheitsbereich	28	
– Gesundheits- und Sozialbereich	35	
– übrige Bereiche	60	123

Bereiche	Anzahl	gesamt
B Nicht-öffentlicher Bereich		
– Versandhandel	7	
– Versicherungen	17	
– Kreditinstitute	19	
– Sonstige des 3. Abschnitts	40	
– Creditreform	9	
– AVAD	13	
– Schimmelpfeng	8	
– Schufa	8	
– Sonstige des 4. Abschnitts	22	143
	266	266

2.4 Verhältnis zur Verwaltung

In meinem 2. TB hatte ich einige Anmerkungen darüber gemacht, wie die Verwaltung den Belangen des Datenschutzes und der Tätigkeit des Datenschutzbeauftragten gegenüber eingestellt ist.
Im Jahr 1984 habe ich praktisch die gleichen positiven und negativen Erfahrungen gemacht: Ich kann wiederholen, daß in aller Regel die Verwaltung meinen Bedenken und Forderungen aufgeschlossen gegenüber stand, mein Beratungsangebot sinnvoll in Anspruch nahm und mich auch rechtzeitig über datenschutzrelevante Entwicklungen der Informationsverarbeitung unterrichtete. Aber keine Regel ohne Ausnahme: es besteht auch Anlaß zur Kritik. Vor allem muß ich feststellen, daß das Bewußtsein der Behörden für ihre eigene Verantwortlichkeit zur Sicherstellung des Datenschutzes (§ 16) nicht so ausgeprägt ist, wie es zu verlangen ist. Dieses mangelnde Verantwortungsbewußtsein tritt einmal in der Weise auf, daß – auch nach den Diskussionen über das Volkszählungsurteil – manche Behörden sich über die Relevanz des Datenschutzes für ein Vorhaben überhaupt nicht im klaren sind. Hierfür 2 Beispiele, die belegen, daß die Möglichkeit, sich auch den Rat des Datenschutzbeauftragten einzuholen, bedauerlicherweise gerade dann nicht genutzt worden ist, wenn von der richtigen Einschätzung der einem Vorhaben innewohnenden Datenschutzaspekte der Erfolg oder Mißerfolg dieses Vorhabens ganz wesentlich abhing:
Von der „Hundebestandsaufnahme" des Finanzamtes Hamburg-Nord, auf die ich unter Nr. 3.3.2.2 näher eingehe, erfuhr ich erst durch Presseartikel und Eingaben Betroffener. Die Finanzbehörde hatte mich an den Vorbereitungen nicht beteiligt. Auch von den „Vorbereitenden Untersuchungen nach § 4 Städtebauförderungsgesetz im Karolinenviertel" erfuhr ich erst, als die Aktion bereits lief. Ebenso wie bei der „Hundebestandsaufnahme" machte mich die Presse auf das Thema aufmerksam, und einen Fragebogen erhielt ich von einem Petenten. Finanzbehörde und Baubehörde beriefen sich für ihre Datenerhebungen auf eine gesetzliche Bestimmung als Rechtsgrundlage, die nach meiner Auffassung die Erhebungen nicht in vollem Umfang deckt, jedenfalls nicht, wenn man die strengen Anforderungen des Bundesverfassungsgerichts an Normenklarheit und Verhältnismäßigkeit zum Maßstab macht.
Bei beiden Vorhaben ging es darum, daß ein Fragebogen ausgefüllt werden sollte. In beiden Fällen war in der Aufforderung hierzu ein Verwaltungsakt zu sehen, der auch zwangsweise durchgesetzt werden konnte. In beiden Fällen scheute die zuständige Behörde aber vor klaren Aussagen zurück, verzichtete auf eine Rechtsmittelbelehrung sowie auf eine Information darüber, ob im Falle der Nichtbefolgung beabsichtigt war, von möglichen Zwangsmitteln Gebrauch zu machen. Zwar wurde jeweils in dem Aufforderungstext – eher beiläufig – auf die Beantwortungspflicht hingewiesen, doch nahmen die Appelle an Mitwirkungsbereitschaft einen viel breiteren Raum ein, so daß der unbefangene Leser auch annehmen konnte, die Beantwortung sei freiwillig. Offenbar hofften die

Behörden, wenn sie „das Kind nicht beim Namen nannten", die Akzeptanz der Befragung und damit die Rücklaufquote zu erhöhen. Genau das Gegenteil trat ein: Weil das Verwaltungshandeln inkonsequent, widersprüchlich, nicht „transparent" war, erwuchsen Mißtrauen und Widerstand.
Ich hoffe, daß die Verwaltung aus diesen Erfahrungen lernt und für die Zukunft die notwendigen Konsequenzen zieht. Ich bin der Überzeugung, daß ich in beiden Fällen nützliche Beiträge zur Verminderung des Konfliktpotentials hätte leisten können (siehe meine ausführlichen Anmerkungen a. a. O.).
Eine andere Form mangelnden Verantwortungsbewußtseins äußert sich darin, daß die Verwaltung versucht, die Verantwortung auf den Datenschutzbeauftragten abzuschieben: so ist es mehrfach vorgekommen, daß mir Unterlagen (meist Datenübermittlungsgesuche dritter Stellen an die betroffene Behörde) einfach „mit der Bitte um Prüfung in datenschutzrechtlicher Hinsicht" übersandt wurden, ohne daß die absendende Behörde irgendwelche eigenen Überlegungen angestellt hatte.
So geht es nicht: ich kann hier nur unterstreichen, was ich in meinem 2. TB (Nr. 2.4.1.1, S. 9) ausgeführt habe: ich bin jederzeit bereit, bei der Lösung datenschutzrechtlicher Probleme den Sachverstand meiner Dienststelle zur Verfügung zu stellen und beratend tätig zu werden. Die Verantwortung für die Ausführung des Datenschutzes (§ 16) kann ich jedoch niemanden abnehmen.

2.5 Beobachtung der automatischen Datenverarbeitung (ADV)

2.5.1 Automatisierte Datenverarbeitung in der hamburgischen Verwaltung

In meinem 2. TB hatte ich Stand und Entwicklung der automatisierten Datenverarbeitung ausführlich dargestellt. Ich hatte angekündigt, daß ich das Datensicherungssystem der Datenverarbeitungszentrale (DVZ) bei der Finanzbehörde umfassend prüfen und mir einen Überblick über den Stand der Datensicherungsmaßnahmen bei dezentralen, autonomen DV-Anlagen verschaffen werde. Die Prüfung des Datensicherungssystems der DVZ hat begonnen, konnte aber noch nicht abgeschlossen werden. Die Prüfung der Datensicherungsmaßnahmen bei dezentralen, autonomen DV-Anlagen ist zugunsten anderer vordringlicher Themen zurückgestellt worden.

2.5.1.1 Das „Hacker"-Problem

In der Presse wird seit längerer Zeit über „Hacker" berichtet, in der Regel unter Verwendung von Nachrichten aus den USA. Als „Hacker" werden diejenigen bezeichnet, die sich durch die moderne Technik herausgefordert fühlen und einen sehr großen Teil ihrer freien Zeit an einem Computer verbringen. Meist sind es Jugendliche, gelegentlich sogar Kinder. Ein wichtiges Requisit ihres Treibens sind die heute weit verbreiteten Hobby- oder Tischcomputer, deren Leistungsfähigkeit beachtlich ist. Hacker fühlen sich herausgefordert, den Computer so beherrschen zu lernen, daß sie jedes Vorhaben mit ihm ausführen können. Hierzu gehört auch, daß sie unberechtigt in fremde Datenverarbeitungssysteme eindringen und dort Rechenleistung in Anspruch nehmen oder Daten oder Programme verändern.
Das Eindringen geschieht weniger aus kriminellen Motiven als aus – salopp ausgedrückt – sportlichem Ehrgeiz. Im allgemeinen werden als Beweis des Eindringens Veränderungen von Daten und Programmen hinterlassen (sozusagen als Duftmarken).
In der Bundesrepublik sind bisher kaum Fälle bekannt geworden, in denen es Hackern gelungen ist, in fremde Datenverarbeitungssysteme einzudringen. Es gibt keine fundierten Untersuchungen darüber, auf welche Ursachen es zurückzuführen ist, daß das Hacking in den USA weiter verbreitet ist. In der Diskussion verfestigt sich der Eindruck, daß die Ursachen eine andere Infrastruktur für die Datenfernverarbeitung (öffentliches Fernsprechnetz als Datenübertragungsnetz) und ein niedrigerer Standard in der Datensicherung sind. Diese Vermutung wird dadurch gestützt, daß einige Fälle von Eindringen in der Bundesrepublik eine über das öffentliche Fernsprechnetz zugängliche Einrichtung (die sog. TELEBOX) betrafen und durch einen sorglosen Umgang mit den Zugangssicherungen (den Paß- oder Kennworten) ermöglicht wurden.

Es ist für meine Dienststelle unmöglich, die Hacker-Problematik grundsätzlich und vollständig aufzuarbeiten. Ich habe mich aber mit der Frage auseinanderzusetzen, ob die Rechenzentren der hamburgischen Verwaltung ausreichend gegen das Eindringen durch unbefugte Fremde gesichert sind. Mit den in der Dienststelle verfügbaren Kapazitäten war eine nähere Prüfung nur möglich für die DVZ und das Rechenzentrum des Universitätskrankenhauses Eppendorf (UKE). Nach den bisherigen Erkenntnissen ist eine wichtige Voraussetzung für das Eindringen, daß die Datenverarbeitungssysteme über Wählvorgänge im öffentlichen Fernsprechnetz erreichbar sind. Das ist aber weder bei der DVZ noch beim Rechenzentrum des UKE möglich. Die Datenfernverarbeitungsanwendungen in der DVZ benutzen als Datenübertragungswege Standleitungen, d. h. festgeschaltete Leitungen zwischen den Benutzerstationen und dem Rechenzentum. Die an das Rechenzentrum des UKE angeschlossenen Benutzerstationen sind lokal oder über Standleitung mit den Datenverarbeitungssystemen verbunden. Die Verbindungen werden durch das Anschalten der Benutzerstationen und die Anmeldeprozeduren (zu denen u. a. auch das Eingeben von Paß- oder Kennworten gehört) aufgebaut. Ich halte daher beide Rechenzentren für ausreichend sicher gegen das unbefugte Eindringen von außen; das „Anzapfen" der Standleitungen ist technisch aufwendig und dürfte in der Regel nicht unbemerkt bleiben.
In der fachlichen Diskussion wird überwiegend die Meinung vertreten, daß das größere Risiko in dem unbefugten Eindringen durch eigene Bedienstete (Insider) liegt. Es gehört zu den Fragestellungen meiner Prüfung des Datensicherungssystems der DVZ, wie und in welchem Ausmaß dieses Risiko abgedeckt ist. Auch die entsprechende Prüfung des Datensicherungssystems im Rechenzentrum des UKE hat für mich hohe Priorität. Im Rechenzentrum der Universität Hamburg sollen nach den Richtlinien der Universität keine personenbezogenen Daten verarbeitet werden; es besteht also – wenn überhaupt – nur ein geringes Risiko, daß unbefugt eindringende Fremde personenbezogene Daten mißbräuchlich nutzen. Das hat für mich im Hinblick auf die personelle Kapazität meiner Dienststelle die erfreuliche Folge, daß eine Prüfung der Datensicherheit unter Datenschutzaspekten nicht dringlich ist.

2.5.1.2 Veränderungen in der Datenfernverarbeitung

Bei den Datenfernverarbeitungsanwendungen in der DVZ hängt es von der eingesetzten Datenfernverarbeitungssoftware ab, ob eine Benutzerstation nur für ein oder mehrere DV-Verfahren genutzt werden kann. Wenn von einer Benutzerstation aus mehrere DV-Verfahren benutzt werden können, wird das Risiko des Mißbrauchs erhöht. Der dadurch eintretende Verlust an Datensicherung muß durch andere Maßnahmen kompensiert werden. Inwieweit dies bei den in letzter Zeit in Betrieb genommenen Verfahren geschehen ist, wird Bestandteil meiner Prüfung des Datensicherungssystems der DVZ sein.

2.5.2 Neue Medien

Die Beschäftigung mit den neuen Medien nahm im vergangenen Jahr einen wesentlich breiteren Raum ein als vorher. Dabei stand der Bildschirmtext (Btx) im Vordergrund.

2.5.2.1 Bildschirmtext

Der neue Dienst „Bildschirmtext" der Deutschen Bundespost ist im Juni 1984 auf die neue Vermittlungs-Technik umgestellt worden; die in den Feldversuchen eingesetzte Technik wird voraussichtlich im Dezember völlig abgelöst sein. Damit ist Btx tatsächlich ein Informations- und Kommunikationsdienst für jedermann geworden; allerdings scheinen sich die Teilnehmer bisher in erster Linie aus dem kommerziellen Bereich zu rekrutieren.
Z. Z. ist eine erste Stufe des von der Deutschen Bundespost insgesamt vorgesehenen Systems realisiert. Eine 2. Stufe soll heute noch fehlende, wesentliche Teile des Systemkonzepts realisieren, z. B. das Mitbenutzerkonzept (d. h. die isolierte Benutzung eines Btx-Anschlusses durch mehrere Personen). Die 2. Stufe wird voraussichtlich Ende 1985 eingeführt werden.

Die Datenschutzbeauftragten haben sich seit dem vergangenen Jahr bemüht, von der Deutschen Bundespost Informationen über das technische System Btx zu erhalten. Leider bedurfte es zeitraubender Auseinandersetzungen mit der Deutschen Bundespost, um auch nur ein Mindestmaß an Informationen zu erlangen. Die Kenntnis der Datenschutzbeauftragten der Länder und damit meine eigene Kenntnis des technischen Systems Btx beruhen auf mündlichen Informationsveranstaltungen und dabei verteilten schriftlichen Unterlagen; insbesondere hat sich die Deutsche Bundespost bis heute nicht bereitgefunden, den Datenschutzbeauftragten der Länder eine vollständige Beschreibung der Dateien im technischen System Btx zur Verfügung zu stellen, die der Bundesbeauftragte für den Datenschutz – als die nach Meinung der Deutschen Bundespost für sie als Bundesbehörde allein zuständige Kontrollinstanz – in Händen hat. Allerdings muß ich einräumen, daß die mündlichen Informationen bereitwillig und von sachkundigen Referenten vorgetragen worden sind; sie vermögen jedoch nicht eine Verfahrensdokumentation zu ersetzen, die bei so umfangreichen und komplexen technischen Systemen unerläßlich ist.

2.5.2.1.1 Analyse des technischen Systems

Mangels vollständiger schriftlicher Unterlagen mußten die Datenschutzbeauftragten zu einem ungewöhnlichen Verfahren greifen, um eine verhältnismäßig vollständige und auch zutreffende Beschreibung des technischen Systems zu erhalten und zu einer Würdigung zu gelangen.

- Eine kleine Gruppe technischer Sachverständiger der Datenschutzbeauftragten stellte auf Grund der bei ihnen vorhandenen Informationen
  - eine eigene Beschreibung des technischen Systems sowie
  - Fragen, Hinweise und Risiken zusammen.
- Beschreibung und Würdigung wurden von den übrigen Datenschutzbeauftragten vervollständigt.
- Die vollständige Beschreibung und Würdigung wurde der Deutschen Bundespost zugeleitet. Sie soll mit der Deutschen Bundespost gründlich erörtert werden.

Auf dieser Grundlage werden die Datenschutzbeauftragten in der Lage sein, zu dem technischen System Btx Stellung zu nehmen.

2.5.2.1.2 Teilergebnisse

Ich kann und will die Ergebnisse der gemeinsamen Würdigung nicht vorwegnehmen. Es ist aber sicher heute schon berechtigt festzustellen, daß die Deutsche Bundespost in der Gestaltung des technischen Systems Btx

- die Anforderungen des Staatsvertrags im wesentlichen erfüllt hat,
  aber noch einiges tun muß, um sie voll zu erfüllen. (Auf die rechtliche Problematik wird in Nr. 3.1.1 eingegangen.)

Die Bedenken richten sich weniger gegen den Umfang der Datenverarbeitung. Die Defizite betreffen vielmehr die Sicherheit in dem technischen System Btx, wie die folgenden – willkürlich herausgegriffenen – Beispiele zeigen:

1) In den Abrechnungssätzen werden die Teilnehmernummer und die Leitseite, die am Anfang des vergütungspflichtigen und in Anspruch genommenen Angebots steht, gespeichert, ohne daß es für Zwecke der Abrechnung in allen Fällen erforderlich ist.
2) Die Paßworte, die den Zugang zum Btx-System schützen sollen, werden unverschlüsselt gespeichert.
3) Durch geschickte Gestaltung können Absender Einzelmitteilungen, die der Empfänger nach erstmaliger Kenntnisnahme „zurückgelegt" (gespeichert) hat, nachträglich ändern.
4) Die Sicherheit empfindlicher Anwendungen auf externen Rechnern, z. B. das Führen eines Bankkontos (sog. home-banking), ist u. a. davon abhängig, daß der Benutzer die Information geheimhält, die den Zugang zur Anwendung auf dem externen Rechner erschließen (z. B. Geheimzahl, sog. Transaktionsnummern). Die Geheimhaltung ist aber erschwert, weil Möglichkeiten der Ausforschung durch „Anzapfen" der Fernsprechleitung bestehen; dies erfordert keinen hohen technischen Aufwand, zumal

der Dialog unverschlüsselt über die Fernsprechleitung läuft. Den Risiken hieraus kann zwar durch verstärkte Sicherheitsbemühungen in den Anwendungen und durch diszipliniertes Verhalten der Benutzer begegnet werden (in diesem Zusammenhang ist die allgemeine Bemerkung angebracht, daß jedes Sicherheitssystem nur so gut ist, wie die Benutzer es durch die Handhabung zulassen); Voraussetzung dafür ist aber, daß die Risiken bekannt sind. Daher ist eine wichtige Forderung der Datenschutzbeauftragten, daß die Deutsche Bundespost die Anbieter und Benutzer über die Risiken aufklärt.

5) Systemfehler, die insbesondere kurz nach Einführung des Systems nicht auszuschließen sind, können dazu führen, daß zufällig oder gewollt geschützte personenbezogene Daten anderen Teilnehmern offenkundig werden. Einer breiten Öffentlichkeit ist der folgende Fall bekanntgeworden. Nach eigenen Angaben sind dem Chaos-Computer-Club (eine Vereinigung, die sich u. a. intensiv mit Sicherheitsfragen im Btx befaßt) durch einen Systemfehler im Editiersystem (das ist das System für den Entwurf von Angebotsseiten) die Informationen bekanntgeworden, die ein Kreditinstitut als Teilnehmer im Btx-System identifizieren und als berechtigt ausweisen (die Deutsche Bundespost bestreitet neuerdings, daß die Zugangsinformationen auf diese Weise bekanntgeworden sein können). Der Chaos-Computer-Club hat daraufhin eine Verbindung unter dem Namen des Kreditinstituts zum Btx-System aufgebaut und wiederholt eine vergütungspflichtige Seite (9,97 DM) des Chaos-Computer-Clubs abgerufen. Mit Hilfe eines Mikrocomputers, der mehrere Stunden angeschlossen war und ca. alle 3 Sekunden diese Seite abrief, wurde das Kreditinstitut mit rd. 135.000 DM Vergütungen belastet, die dem Chaos-Computer-Club gutgeschrieben wurden. Dieser legte keinen Wert auf das Geld, sondern wollte die Öffentlichkeit auf den Fehler und seine möglichen wirtschaftlichen Konsequenzen aufmerksam machen.
   In den Presseberichten über diesen Fall ist sehr häufig – nicht zuletzt aufgrund der Überschrift in einer Presseerklärung des Chaos-Computer-Clubs – der Ausdruck „Bankraub" verwendet worden. Das könnte den Eindruck erwecken, der Chaos-Computer-Club hätte über Btx Zugang zu den bei dem Kreditinstitut geführten Konten gehabt, und das Vertrauen der Kunden zu dem Kreditinstitut beeinträchtigen. Tatsächlich handelte es sich um Vergütungen, die das Kreditinstitut – wenn die Vergütungen nicht vorher storniert würden – als Geschäftskosten zu zahlen hätte. Das Kreditinstitut nimmt mit seinen kundenbezogenen Anwendungen (home-banking) am Btx nicht teil, so daß die Konten der Kunden zu keiner Zeit gefährdet waren.

2.5.2.1.3 Btx und Hacker

Verschiedentlich wird die Ansicht vertreten, Btx und darin insbesondere der Rechnerverbund biete den Hackern für ihr Tun, vor allem also das Eindringen in fremde DV-Systeme, Voraussetzungen, wie sie in den USA wegen der anderen Struktur der Datenfernverarbeitung vorhanden sind. Da Btx über das öffentliche Fernsprechnetz zugänglich ist, ist diese Vermutung nicht unberechtigt. Eine fundierte Analyse hat bisher – soweit mir bekannt ist – noch niemand, auch die Deutsche Bundespost nicht, vorgelegt. Auch ich kann nur erste Ansätze für eine solche Analyse vortragen:

1) Die unbefugte Nutzung insbesondere vergütungspflichtiger Angebote zu Lasten eines anderen Benutzers.
   Dies ist auf zwei Wegen möglich:
   - Simulation eines anderen Teilnehmeranschlusses; hierfür sind die Kenntnis der Teilnehmernummer (in der ersten Stufe die jedermann zugängliche Telefonnummer), einer Hardware-Kennung und des Paßworts sowie die Simulation der Hardware-Kennung erforderlich. Hardware-Kennung und Paßwort können durch Anzapfen des Fernsprechanschlusses ausgeforscht werden; nach Informationen der Deutschen Bundespost erfordert es einigen technischen Aufwand, die Hardware-Kennung in derselben Weise an die Btx-Vermittlungsstelle zu senden, wie die bei einem Btx-Anschluß normalerweise benutzte Anschlußbox mit automatischer Anwahl (sog. D-BT03). (Der besondere Fall, daß anstelle der Anschlußbox D-BT03 ein anderes Modem benutzt wird, soll hier außer Betracht bleiben.) Besonders gefähr-

det sind hierbei „freizügig" geschaltete Anschlüsse (von einem solchen Anschluß aus können auch andere Teilnehmer Btx benutzen), weil hier als Zugangsinformation nur das Paßwort erforderlich ist.
- Unbemerktes Absetzen von Befehlen, die bewirken, daß vergütungspflichtige Angebote dem manipulierenden Benutzer zur Verfügung gestellt werden, ohne daß der manipulierte Benutzer dies bemerkt.

2) Verbindungsaufbau und Abruf von vergütungspflichtigen Seiten unter dem Namen eines anderen Teinehmers
3) Unberechtigtes Ändern von Angebotsseiten im Speicher der Btx-Zentrale und Vermittlungsstellen
   Die Anbieter können ihre Angebotsseiten jederzeit ändern. Die geänderten Angebotsseiten können ebenfalls über das Fernsprechnetz an die Btx-Zentrale gesandt werden. Da der Zugang für Anbieter nicht durch besondere Kennworte geschützt ist, kann ein Unberechtigter, der in der oben beschriebenen Weise den Anschluß eines Anbieters simuliert, zunächst unbemerkt Angebotsseiten ändern.
4) Zugang zu externen Rechnern
   Wenn ein Anbieter den Zugang zu einem bei ihm installierten DV-System über Btx eröffnet, dann will er damit erreichen, daß möglichst viele Benutzer davon Gebrauch machen und z. B. Waren bestellen oder Dienstleistungen in Anspruch nehmen. Gleichzeitig eröffnet er damit aber Möglichkeiten, die installierte und über Btx zugängliche Anwendung mißbräuchlich zu benutzen. So kann z. B. bei einem Versandhandelsunternehmen so lange versucht werden, die Kundennummer eines beliebigen anderen Teilnehmers einzugeben, bis der Versuch erfolgreich ist. Da das System Fehlversuche bei der Eingabe von Kundennummern nicht begrenzen, sondern nur abweisen und für jeden Versuch einen neuen Verbindungsaufbau erzwingen kann, kostet der Eindringversuch lediglich die Telefongebühren für die Dauer der Verbindung. Die Mißbrauchsmöglichkeiten eines unberechtigt eindringenden Teilnehmers sind allerdings begrenzt. Er kann sich nur innerhalb der über Btx zugänglichen Anwendungen bewegen; insbesondere kann er nur dann die Grenzen der Anwendungen überschreiten und sich frei und nach Belieben im externen Rechner des Anbieters bewegen, wenn die Anwendungsprogramme im externen Rechner nicht gegen alle Fehlerkonstellationen abgesichert sind.

Bis auf die „Produktion von Vergütungen" (siehe oben Nr. 2) ist die Möglichkeit, sich zu bereichern, gering. Der Fall des Kreditinstituts hat gezeigt, daß bei Einsatz entsprechender Mittel (programmierter Abruf von vergütungspflichtigen Seiten) beachtliche Erträge zu erzielen sind, wenn auch die Realisierung des Gewinns einige Schwierigkeiten macht (entweder „Produktion" von Vergütungen, die sich im Rahmen des üblichen halten und nicht auffallen, bei vielen Teilnehmern oder Abheben einer hohen Vergütung, bevor eine streitige Auseinandersetzung beginnt) und auch Spuren hinterlassen werden.

2.5.2.2 Andere Medien

Neben Btx gibt es andere Informations- und Kommunikationstechniken. Btx steht nur deswegen im Vordergrund der Diskussion, weil dieser Dienst über das Versuchsstadium hinaus ist. Dies kann man zumindest für Hamburg von anderen, dem Btx vergleichbaren Diensten nicht sagen. Im folgenden soll über den Stand der von der Deutschen Bundespost in Hamburg angebotenen Rundfunkverteildienste und über die Absichten zur Einführung des Fernwirkdienstes berichtet werden.

2.5.2.2.1 Rundfunkverteildienste

Rundfunkprogramme (Fernsehen und Hörfunk) werden gegenwärtig über erdgebundene Sender in der Weise verteilt, daß die in einem bestimmten Sendebereich empfangbaren Programme durch entsprechende Einrichtungen im Empfangsgerät ausgewählt werden können. Bei dieser Verteiltechnik entstehen keine Datenschutzprobleme, weil an keiner Stelle personenbezogene Daten über die Benutzung der Programme entstehen. Das Angebot, insbesondere an Fernsehprogrammen, ist aber stark begrenzt.
Andere Techniken der Verteilung können diese Begrenztheit aufheben:

- Verteilung über direkt empfangbare Satelliten;
- Verteilung über Kabel.

Die hiermit verbundenen medienpolitischen Fragen können und sollen hier nicht erörtert werden.

Da bei der Verteilung über direkt empfangbare Satelliten unter Datenschutzaspekten gegenüber dem jetzigen Zustand keine Änderung eintritt, weil auch dann das gewünschte Programm im Empfangsgerät ausgewählt wird, und daher an keiner Stelle personenbezogene Daten über die Benutzung der Programme entstehen, beschränkt sich die Darstellung auf die Verteilung über Kabel. Dabei wird nach der für das Kabelnetz verwendeten Technik unterschieden.

1) Kabelnetze für Breitband-Kommunikation mit Kupfer-Koaxial-Kabeln.
   Breitband-Kabel (im Gegensatz zu schmalbandigen Kabeln wie z. B. im Fernsprechnetz) ermöglichen auch die Übertragung von Bewegtbildern (z. B. Fernsehen). Nach dem Stand von Ende 1983 bestehen in Hamburg rund 40 „Kabelinseln", d. h. größere oder kleinere Gebiete, in denen der Rundfunkempfang über Kabel möglich ist. Es handelt sich im wesentlichen um Gebiete, in denen der Rundfunkempfang wegen Abschattung oder anderer Ursachen eine schlechte Qualität hat. Es gibt aber zunehmend auch Kabelinseln, die eingerichtet worden sind, ohne daß der schlechte Rundfunkempfang die Ursache gewesen ist. Die Erweiterung bestehender und die Anlage neuer Kabelinseln wird nach den Plänen der Post in den nächsten Jahren zügig vorangehen.
   Die Größe der Kabelinseln ist durch die Zahl der hintereinander geschalteten Verstärker begenzt. Die übertragenen Signale müssen während des Transports in relativ kurzen Abständen verstärkt werden. Mit jedem Verstärker nimmt das „Rauschen" im Nutzsignal zu. Die Deutsche Bundespost hat durch geeignete Vorschriften verhindert, daß durch die Netzgestaltung der Rauschanteil zu Beeinträchtigungen führen kann. Die Kabelinseln bestehen technisch aus der Rundfunkempfangsstation, den Verstärkerstellen in den Vermittlungsstellen, den Verstärkern und den Endgeräten.
   Die Rundfunkstation setzt sich zusammen aus
   - dem Antennenträger,dessen Antenne die ausgestrahlten Rundfunksignale auffängt und in das Netz leitet;
   - dem Verstärker, der die Signale verstärkt;
   - dem Umsetzer, der die empfangenen und verstärkten Signale auf andere Kanäle umsetzt, weil sonst die vom Gerät direkt empfangenen Signale zeitlich versetzt zu dem aus dem Kabel gelieferten Signal ankommen. Diese geringen Laufzeitunterschiede führen aber zu erheblichen Störungen; deshalb kann nur durch Frequenzversatz die gegenseitige Beeinflussung aufgehoben werden.
     Mit ihr werden die ortsüblich empfangbaren Rundfunkprogramme empfangen; es wird aber auch Satelliten-Empfang möglich sein. Die Signale werden dann verteilt an Verstärkerstellen in den Fernsprechvermittlungsstellen und von dort über die Kabelwege – über Verstärker – an die Endgeräte geleitet. Die normalen Endgeräte sind in ihrer Technik auf den Empfang von Signalen aus der Luft ausgerichtet. Damit sie, insbesondere die Fernsehgeräte, die Vorteile des Empfangs über Kabel nutzen können, müssen sie eine andere Technik haben:
   - höhere Störfestigkeit
   - größere Trennschärfe
   - Möglichkeit der Nutzung von Sonderkanälen (auf dem Markt befinden sich schon heute Endgeräte, die diesen Forderungen entsprechen).

   In den Endgeräten „liegen alle Rundfunkprogramme an" (außer Lang-, Mittel- und Kurzwelle); die Programme werden also im Endgerät ausgewählt. Diese Vermittlungstechnik wird so lange nicht geändert, wie die Übertragungswege die Übertragung aller Angebote bis zum Endgerät erlauben.
   Bei dieser Vermittlungstechnik gibt es keine Datenschutzprobleme, weil keine personenbezogenen Daten über die Benutzung von Programmen entstehen. Eine andere in den Kabelinseln in Hamburg heute noch nicht eingesetzte Vermittlungstechnik wäre folgende:
   Es werden fernsteuerbare adressierbare Teilnehmereinrichtungen (jeweils eine für

mehrere Teilnehmer) installiert, an die die Teilnehmer ihre Programmwünsche richten, die die Programme zuschalten und abrechnungsrelevante Daten speichern. Bei dieser Vermittlungstechnik müßten Erhebung, Speicherung und Übermittlung der personenbezogenen Daten geregelt werden.
Wenn in Hamburg neue, besonders entgeltpflichtige Programme zugelassen werden, müssen technische Einrichtungen vorgesehen werden, die den unberechtigten Zugang verhindern. Dies könnte durch den Einbau von Filtern am Übergabepunkt der Deutschen Bundespost erfolgen.
Z. Z. besteht auch kein Rückkanal; zwar ermöglicht das Breitbandkabel technisch den Rückkanal, doch ist die entsprechende Vermittlungstechnik nicht installiert. Der Rückkanal würde den Dialog möglich machen und damit ähnliche Datenschutzprobleme aufwerfen wie beim Bildschirmtext.

2) BIGFON-Versuch

Die Abkürzung BIGFON steht für Breitbandiges integriertes Glasfaser-Ortsnetz. Im Vergleich zu der eben beschriebenen Technik werden Glasfasern statt Kupfer als Material für die Kabel verwendet; außerdem wird von Anfang an die Zusammenfassung mehrerer Dienste angstrebt. Im BIGFON-Versuch werden daher nicht nur Rundfunkprogramme (Hörfunk und Fernsehen) verteilt, sondern zusätzlich folgende Dienste abgewickelt:
- Öffentliches Fernsprechen,
- Text- und Datenübertragung,
- Bildfernsprechen.

In einem begrenzten örtlichen Bereich (Winterhude unter Einschluß von Teilnehmern in Bramfeld und in der Innenstadt) sind z. Z. 30 Teilnehmer angeschlossen. Für diese Teilnehmer werden die eben beschriebenen Dienste nicht wie bisher über separate Netze, sondern gemeinsam über ein Glasfasernetz zur Verfügung gestellt. Ziel des Versuchs ist die Erprobung der optischen Übertragungsstrecke, d. h. der Übertragung von Signalen mit Glasfaserkabeln.
Der öffentliche Fernsprechdienst und die Text- und Datendienste werden über Einrichtungen, die die Signale umsetzen, direkt über das Glasfasernetz an die Teilnehmer herangeführt. Für die anderen Dienste steht eine zentrale Steuereinrichtung zur Verfügung, die mit einem Rechner arbeitet.
Die Hörfunkprogramme werden nicht in der zentralen Steuereinrichtung an den Teilnehmer vermittelt, sondern liegen im Empfangsgerät vollständig an; die Auswahl wird im Empfangsgerät des Teilnehmers getroffen. Da keine personenbezogenen Daten über die Benutzung von Programmen gespeichert werden, treten keine Datenschutzprobleme auf.
Dagegen werden die Fernsehprogramme in der zentralen Steuereinrichtung an den Teilnehmer vermittelt. Der Teilnehmer wählt an seinem Empfangsgerät mit einer Funktionstaste ein bestimmtes Fernsehprogramm aus; in der zentralen Steuereinrichtung sucht der Rechner einen freien Koppelungspunkt (Einrichtung für das Zusammenschalten des herangeführten Fernsehprogramms und der Zuleitung zum Teilnehmer) und stellt, wenn ein freier Koppelungspunkt verfügbar ist, das Fernsehprogramm zur Verfügung. Die Verbindung geschieht rechnergesteuert. Dabei entstehen Verbindungsdaten. Diese existieren nur bei der aktuellen Verbindung. Der Rechner verfügt über keinen externen Speicher, sondern nur über ein Zeilendisplay, auf dem aktuelle Betriebs- und Systemzustände angezeigt werden können. Bei dieser Vermittlungstechnik treten Datenschutzprobleme nur insoweit auf, als für die Dauer der Inanspruchnahme des Programms Verbindungsdaten vorhanden sind.
Beim Bildfernsprechen wird das Bild des angewählten Teilnehmers nur dann für den Anrufer sichtbar, wenn der angerufene Partner seinerseits die Bildübertragung freigibt. Es kann daher mit dem Bildfernsprecher nicht ohne Wissen und Wollen des Teilnehmers in dessen Bereich hineingesehen werden.

2.5.2.2.2 Fernwirkdienste

Auf die Absicht der Deutschen Bundespost, über das Fernsprechnetz zusätzlich Fernwirkdienste anzubieten, habe ich bereits kurz in meinem 2. TB hingewiesen. Heute kann ich ausführlicher auf den beabsichtigten Dienst eingehen, der den Arbeitstitel TEMEX trägt.

Fernwirken ist der Oberbegriff für die Begriffe Fernmessen, Fernsteuern, Fernschalten oder Fernanzeigen. „Fern" drückt dabei aus, daß Informationen zwischen räumlich auseinander liegenden Objekten, den Fernwirkstationen ausgetauscht werden. Auch heute gibt es schon Anwendungen für Fernwirken, z. B.

- Gefahrenmeldeanlagen für Brand, Einbruch, Überfall, die durch den neuen Dienst nicht substituiert, sondern in ihrer Anwendungsbreite erweitert werden sollen;
- Systeme für die Sirenensteuerung des Warndienstes;
- Überwachungssysteme für Pipeline;
- Haus-Notrufsysteme im sozialen Bereich;
- Meßstationen im Rahmen des Umweltschutzes.

Die Deutsche Bundespost realisiert solche Anwendungen mit

- Stromwegen für private Drahtfernmeldeanlagen,
- Zusatzeinrichtungen an Anschlüssen des Fernsprechnetzes, wie z. B. Automatische Wähleinrichtungen für Daten,
- Datendiensten, insbesondere Hauptanschlüsse für Direktruf (Standleitungen).

Fernwirkanwendungen werden auch in privaten (d. h. nicht zur Deutschen Bundespost gehörenden) Netzen betrieben, z. B. die Messung der Niederschlagsmenge an verschiedenen Punkten des Stadtgebiets und Steuerung von Sieleinrichtungen (Pumpen, Schieber), um erhöhten Regenwasseranfall zu bewältigen.

Für die heute vorhandenen Fernwirkanwendungen werden vorhandene, für andere Zwecke eingerichtete Techniken und Dienste „mitgenutzt"; es gibt keinen speziellen Fernwirkdienst. Die Deutsche Bundespost sieht hierfür aber einen großen Bedarf, z. B.

- persönliche Notrufe im Rahmen sozialer und medizinischer Hilfsleistungen,
- technische Alarme wie die Signalisierung von Maschinenausfällen, z. B. Fahrstuhl, Kühltruhe, Abwasserpumpen, Heizung usw.,
- Übermitteln von Meßwerten, wie im Bereich der Wasserwirtschaft, der Energieversorgung, auch von Verbrauchsgrößen, d. h. Zählerablesen,
- Übermitteln von Steuerbefehlen für Parkleitsysteme, Heizungsanlagen, Stellwerke,

und sie sieht darüber hinaus die Möglichkeit, durch eine auf die Mitbenutzung der Fernsprechleitungen konzipierte Technik eine neue, preislich attraktive Dienstleistung anzubieten. Um ihre Absichten voranzutreiben und anwendungsreife Techniken anbieten zu können, plant die Deutsche Bundespost Systemversuche in München und Ludwigshafen und Betriebsversuche mit verschiedenen Anwendern.

In den beiden Systemversuchen soll mit einer vereinfachten Vorläufertechnik ein eingeschränktes Dienstleistungsangebot gemacht werden. Es ist eingeschränkt insofern, als es sich nur um die Übermittlung zweiwertiger Fernwirkinformationen (Ja-Nein oder Gut-Schlecht-Aussagen) handelt. Damit können zunächst nur Anwendungen wie Alarmübermittlung zu sozialen und medizinischen Hilfsdiensten oder Wach- und Sicherheitsunternehmen bedient werden. Die technischen, betrieblichen und organisatorischen Vorbereitungen für den Start der Versuche in München und Ludwigshafen sind abgeschlossen; sie sollen kurzfristig begonnen werden.

Zusätzlich zu den Systemversuchen sollen Betriebsversuche mit verschiedenen Anwendern, deren Informationsübermittlung als besonders charakteristisch und somit für Tests besonders geeignet ist, durchgeführt werden. Im Unterschied zu den Systemversuchen – vorhandene, einfache Vorläufertechnik – sollen hier verschiedene Varianten der möglichen späteren Serientechnik getestet werden, damit Anbieter, Nutzer und die Industrie die für ihre Dispositionen notwendigen Informationen erhalten. Die Betriebsversuche dienen nicht nur dem sehr wichtigen Test der TEMEX-Netzkomponenten und dem Zusammenspiel mit den privaten Fernwirkeinrichtungen, sondern auch dem Test der geplanten Anwendungen, wie z. B. Verbrauchsdatenerfassung, Alarme, Zustandsmeldungen, Meßwertübermittlung, Steuerung von Parkleitsystemen, Sicherung von technischen Systemen, Altenbetreuung u. a. Da die

Betriebsversuche erst ausgeschrieben werden sollen, ist noch nicht bekannt, wo sie stattfinden werden. Es ist jedenfalls nicht auszuschließen, daß ein Betriebsversuch auch in Hamburg stattfindet.

2.5.2.2.3 Andere Dienste

Neben den eben behandelten Diensten gibt es mit TELEBOX ein Dienstangebot, das sich zwar noch im Versuchs- und Erprobungsstadium befindet, dessen Einführung sich aber konkret abzeichnet.
Dieser Dienst ermöglicht die elektronische Archivierung und Verteilung von eingegebenen Mitteilungen. Die Mitteilungen können zeit- und ortsunabhängig über ein Datenendgerät, das die entsprechenden Anschlußbedingungen erfüllt, über die öffentlichen Wählnetze (Fernsprech-, DATEX-L-, DATEX-P-NETZ) in das System eingegeben werden. Auf dieselbe Art und Weise ruft der Empfänger die an ihn adressierte Mitteilung ab. Für die Mitteilung wird dem Teilnehmer ein Speichernetz zur Verfügung gestellt, den nur er ein- und auslesen kann. Die Deutsche Bundespost hat keinen Zugang. Der Zugang ist durch Paßwort geschützt, das der Teilnehmer selbst einrichtet. Bei diesem Dienst ist die Deutsche Bundespost eine Stelle, die im Auftrag der Teilnehmer Daten verarbeitet. Sie hat daher keine eigene Verfügungsberechtigung über die Daten, sondern darf nur im Rahmen der ihr erteilten Weisungen verarbeiten. Sie ist aber verpflichtet, einen angemessenen Stand der Datensicherung zu gewährleisten.

2.5.3 Bargeld- und belegloser Zahlungsverkehr

Für den Handel und Dienstleistungsbereich zeichnet sich eine Entwicklung ab, die bisherige Zahlungsgewohnheiten nachhaltig verändern kann. Der Kunde bezahlt künftig nicht mehr mit Bargeld oder Scheck, sondern dadurch, daß seine EC-Karte maschinell gelesen wird. Für die weitere Verarbeitung ergeben sich zwei Varianten:

1) Wenn das Lesegerät off-line[1] arbeitet, ist auf der EC-Karte ein Guthaben gespeichert, das um den geschuldeten Betrag vermindert wird. Das Guthaben auf der EC-Karte kann an Geldausgabe-Automaten aufgefüllt werden. (Dieses System wird z. Z. in München in einem Pilotversuch getestet.)
2) Wenn das Lesegerät on-line[2] arbeitet, wird der geschuldete Betrag vom Bankkonto des EC-Karteninhabers abgebucht und dem Bankkonto des Geschäftspartners gutgeschrieben.

In beiden Fällen muß derjenige, der die EC-Karte benutzen will, sich durch die Eingabe einer Geheimzahl (PIN) als berechtigt ausweisen. Bei dem off-line-Lesegerät ist die Geheimzahl fest vergeben und nicht veränderbar, weil sie mit einer Zahl verglichen wird, die im Lesegerät aus Informationen gebildet wird, die auf der EC-Karte gespeichert sind. Bei dem on-line-Lesegerät kann die Geheimzahl vom Karteninhaber jederzeit verändert werden, weil sie in der (zentralen) DV-Anlage gespeichert ist, an die die on-line-Lesegeräte angeschlossen sind.
Der Sicherheitsstandard ist bei der off-line-Lösung deutlich geringer (Gefahr der Entdeckung des Algorithmus für die Bildung der Geheimzahl). Da die Lösung wegen der hohen Zahl einzubeziehender Kreditinstitute – deren Schlüssel alle in dem off-line-Gerät gespeichert werden müßten – einen europaweiten Verbund faktisch nicht erlaubt und die Echtheitsprüfung der EC-Karte sehr teuer wird, ist es wahrscheinlich, daß sich die on-line-Lösung durchsetzt.
Die on-line-Lösung sieht als wesentlichen Bestandteil eine „Evidenzzentrale" vor, an die alle Lesegeräte (EC-Karten-POS[3]-Terminals) angeschlossen sind. Die Evidenzzentrale

- prüft die Identität,
- behandelt die Eingabe falscher Geheimzahlen,
- prüft die Bonität (einschl. evtl. Sperren) und
- übernimmt und verteilt die Gutschrift- und Belastungsdatensätze.

Bis zu einem Einsatz solcher Lösungen in der Praxis sind noch viele Probleme zu lösen,

1) off-line bedeutet selbständig, ohne Verbindung mit und Steuerung durch eine zentrale DV-Anlage.
2) on-line bedeutet unselbständige Verarbeitung unter Steuerung einer zentralen DV-Anlage.
3) POS = Point of Sale

nicht zuletzt die Standardisierung (POS-Terminals, EC-Karten, Datensätze). Andererseits verspricht die Lösung beachtliche Rationalisierungserfolge, so daß mit einem starken Druck zu rechnen ist, die auftretenden Probleme bald zu lösen. Das deutsche Kreditgewerbe läßt z. Z. ein Konzept für diese Lösung erarbeiten. Ein Versuch ist für das nächste Jahr geplant.

Die Entwicklung wirft auch Fragen des Datenschutzes auf:

1) Der erste Fragenkomplex betrifft die in einer on-line-Lösung vorgesehene Evidenzzentrale. Ihre Tätigkeit hat für diejenigen, die sich des Verfahrens bedienen, gravierende, in Ausnahmefällen sogar existenzielle Bedeutung (z. B. wenn jemand sich auf die Karte verläßt und ohne Bargeld oder Schecks auf Reisen geht). Sie ist mit der Tätigkeit der Schufa vergleichbar. Daher muß sorgfältig festgelegt werden, welche Daten erhoben und gespeichert werden.
2) Der bargeld- und beleglose Zahlungsverkehr kann zu einer Aufhebung der bisher weitgehenden Anonymität wirtschaftlicher Vorgänge führen. Daher muß ein Ausgleich gefunden werden zwischen der Notwendigkeit der Speicherung von Daten über geschäftliche Vorgänge (zu Beweiszwecken) und dem Interesse des Einzelnen, daß keine Persönlichkeitsprofile entstehen.
3) Ebenso wichtig ist die Datensicherung in solchen Verfahren. Man kann nach meiner Überzeugung schon heute sagen, daß in einer off-line-Lösung kein ausreichender Stand der Datensicherung erreicht werden kann, weil die Paßworte fest vorgegeben und nicht vom Benutzer vergeben und jederzeit geändert werden können.
   Für die Datensicherung in der on-line-Lösung gibt es Maßstäbe und Erfahrungen aus dem home-banking-Verfahren über Btx. Es werden also keine grundsätzlich neuen Fragen mehr aufgeworfen, sondern es geht vielmehr darum, welches Maß an Datensicherung mit welchen Mitteln gewährleistet werden muß. Schon heute läßt sich feststellen, daß EC-Karte und (jederzeit änderbares) Paßwort allein nicht genügen.
   In diesem Zusammenhang scheint mir der allgemeine Hinweis angebracht, daß Datensicherung auch nachteilige Wirkungen für den Betroffenen haben kann. Je höher der Stand der Datensicherung ist, umso schwerer widerlegbar ist die Vermutung, daß eine Disposition auch tatsächlich von dem Berechtigten getroffen wurde; mit anderen Worten: Wenn in einem hoch gesicherten System eine Verfügung über das Vermögen eines Betroffenen getroffen worden ist, dann muß der Betroffene sich entgegenhalten lassen, daß er selbst die Verfügung getroffen hat oder das Wissen, das den Zugang zum System ermöglicht, vorsätzlich oder fahrlässig einem Dritten offenbart hat. Da aber eine absolute Datensicherung nicht erreichbar ist, wird es in dem seltenen – und m. E. auch unwahrscheinlichen – Fall, daß jemand die Sperren des System überwindet, dem Betroffenen kaum gelingen nachzuweisen, daß er bestimmte Verfügungen nicht getroffen hat.
   Dementsprechend sehen die Geschäftsbedingungen bei solchen Systemen vor, daß der Kunde allein das Risiko trägt.
4) Die letzte Frage schließlich hat zugleich auch mit Verbraucherschutz zu tun. Sie betrifft die Freiheit des Einzelnen, sich solchen Systemen anzuschließen oder nicht. Formal wird jeder Bürger sich jederzeit frei entscheiden können, ob er sich einem solchen System anschließt. Faktisch kann aber – durch eine gewollte oder eine unbewußte Entwicklung – für den Einzelnen ein Zwang entstehen, sich einem solchen System anzuschließen und damit die geschilderten Gefährdungen in Kauf zu nehmen, denen er sich nicht aussetzen möchte. Der Zwang kann darin bestehen, daß Alternativen nicht oder zu Bedingungen zur Verfügung stehen, die nicht akzeptabel sind.
   Diese unerwünschte Situation kann nur dadurch vermieden werden, daß die hier in Rede stehenden Entwicklungen rechtzeitig und in möglichst großer Öffentlichkeit diskutiert werden.
   Ich beabsichtige, das Thema „bargeld- und belegloser Zahlungsverkehr" zum Gegenstand der Beratungen der für den Datenschutz zuständigen obersten Landesbehörden zu machen, und werde vorschlagen, daß möglichst bald Gespräche mit der Kreditwirtschaft geführt werden.

3. Einzelprobleme im öffentlichen Bereich

3.1 Neue Medien

3.1.1 Bildschirmtext

Ich habe die Datenschutzprobleme, die sich beim Betrieb und bei der Nutzung von Bildschirmtext ergeben, und den Staatsvertrag über Bildschirmtext, der diese Problem bereichsspezifisch lösen soll, in meinem 2. TB ausführlich dargestellt. In Nr. 2.5.2.1 dieses TB habe ich über Erfahrungen mit dem technischen System Btx berichtet. Die folgenden Ausführungen behandeln die Umsetzung des Staatsvertrages in Bundesrecht und erste Erfahrungen aus der Überwachung.

3.1.1.1 Umsetzung des Staatsvertrages in Bundesrecht

Die Deutsche Bundespost fühlt sich als Bundesbehörde an die Bestimmungen des Staatsvertrages – als Landesrecht – nicht gebunden. Sie hat aber vor Abschluß des Staatsvertrages durch die Länder erklärt, daß im Bereich der Deutschen Bundespost beim Betrieb des Bildschirmtextes die materiellen Anforderungen des Art. 9 des Staatsvertrages beachtet würden. Es werde sichergestellt, daß sich der Vollzug nach den einschlägigen Datenschutzregelungen richten werde.
Die Datenschutzbeauftragten sind der Ansicht, daß die Deutsche Bundespost verpflichtet ist,

- alle Regelungen des Staatsvertrages, die den Betreiber Deutsche Bundespost betreffen, in Vorschriften des Bundesrechts – also nicht bloß in Verwaltungsanweisungen – umzusetzen und
- darüber hinaus die Regelungen des Staatsvertrages zu vervollständigen und zu präzisieren, soweit es aufgrund der heutigen Kenntnisse des technischen Systems Btx möglich ist.

Im Gegensatz zu herkömmlichen Medien ist das neue Medium Bildschirmtext dadurch gekennzeichnet, daß der Betrieb die Erhebung und Verarbeitung personenbezogener Daten der Nutzer in großem Umfang erfordert. Die Möglichkeit, aus den erhobenen Daten Erkenntnisse über das Teilnehmerverhalten der Nutzer zu gewinnen, stellt angesichts der Menge denkbarer Angebote ein erhebliches Gefährdungspotential dar. Eine gesetzliche Regelung durch den Bund ist gerade deshalb notwendig, weil sich die Deutsche Bundespost durch den Staatsvertrag nicht gebunden fühlt und das für diesen Fall subsidiär geltende BDSG den Datenschutzproblemen des Btx nur unzureichend begegnet (vgl. hierzu im einzelnen meinen 2. TB unter Nr. 3.1.1.4).
Auch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 stellt klar, daß wegen der denkbaren Einschränkungen der informationellen Selbstbestimmung eine dem Gebot der Normenklarheit entsprechende gesetzliche Regelung der Erhebung und Verarbeitung der Daten, die beim Betrieb von Bildschirmtext anfallen, vorhanden sein muß. Die Freiwilligkeit der Teilnahme kann dem nicht entgegengehalten werden. Denn nur die Entscheidung, am Btx teilnehmen zu wollen, ist frei; wer teilnimmt, kann den Umfang der Datenerhebung und -speicherung nicht beeinflussen. Hinzu kommt, daß das Btx-Teilnehmerverhältnis wie das Fernsprechverhältnis nicht als Vertrag ausgestaltet ist, sondern daß das Benutzungsverhältnis durch die Fernmeldeordnung geregelt ist. Schließlich kann mit zunehmender Verbreitung sozialer Druck zur Nutzung von Bildschirmtext entstehen, der die Freiwilligkeit ohnehin in Frage stellt (z. B. Kontoführung, Bestelldienste, Buchungen).
Die zu Bildschirmtext bestehenden, zum Teil konkurrierenden oder sich überschneidenden Regelungen sind für Anbieter, Teilnehmer und Betreiber nur schwer zu durchschauen. Daraus folgt die Notwendigkeit, Bildschirmtext in seiner Geamtheit so zu regeln, daß die Rechte und Pflichten der Beteiligten und ihre Rechtsbeziehungen untereinander klar und eindeutig festgelegt werden. Hierzu gehört eine Abgrenzung von Netz- und Nutzungsbereich, an die unterschiedliche Rechtsfolgen anknüpfen. Es ist fraglich, ob die Fernmeldeordnung von ihrer Konzeption her für eine solche Regelung geeignet ist.

Die Datenschutzbeauftragten der Länder haben ihren Standpunkt wiederholt der Öffentlichkeit vorgetragen und auch die Ministerpräsidenten gebeten, auf die Deutsche Bundespost einzuwirken, daß sie die Regelungen des Staatsvertrages in Bundesrecht umsetzt. Sie sind vor allem dem Argument der Deutschen Bundespost entgegengetreten, daß es genüge, wenn das tatsächliche technische System Btx den Anforderungen des Staatsvertrages entspreche. Ein technisches System kann jederzeit geändert werden. Im übrigen legt die Deutsche Bundespost – wie sie in allerjüngster Zeit mitgeteilt hat – eine wesentliche Bestimmung des Staatsvertrages, nämlich die Definition der Verbindungsdaten in Art. 9 Abs. 2 des Staatsvertrages so eng aus, daß eine große Zahl von Daten vom Staatsvertrag nicht erfaßt wird. Nach der eigenen Interpretation der Deutschen Bundespost entsteht also eine beträchtliche Regelungslücke; damit wird ihre Aussage, das technische System Btx entspreche dem Staatsvertrag, stark entwertet.
Inhaltlich ist die Verarbeitung personenbezogener Daten bisher in der Fernmeldeordnung auf ungenügende Weise geregelt. Bereichsspezifische Bestimmungen für Verbindungsdaten (Art. 9 Abs. 2 Nr. 1 Staatsvertrag) und für die Daten, die nach Ansicht der Deutschen Bundespost weder Verbindungs- noch Abrechungsdaten sind und daher vom Staatsvertrag nicht erfaßt werden, fehlen völlig, die für die Erhebung und Verarbeitung von Abrechnungsdaten (Art. 9 Abs. 2 Nr. 2 Staatsvertrag) sind unvollständig. Flankierende Bestimmungen zur Verstärkung der Kooperation bei der Kontrolle des Datenschutzes müssen hinzukommen.
Im einzelnen sind folgende Regelungen erforderlich:

1. Abschließende aufgabenbezogene Festlegung der für den Betrieb von Bildschirmtext unerläßlichen Datenarten (Daten, die nach Ansicht der Deutschen Bundespost keine Verbindungsdaten sind; Verbindungsdaten; Abrechnungsdaten = Vergütungsdaten);
2. Verbot der Speicherung der in Art. 9 Abs. 3 Satz 1 Staatsvertrag genannten Merkmale in Zusammenhang mit Abrechnungsdaten unter Berücksichtigung der mit der Zuteilung mehrerer Leitstellen verbundenen Umgehungsmöglichkeiten.
3. Festlegung der Daten, die an Anbieter übermittelt werden dürfen, einschließlich der ausschlaggebenden Bedingungen und Fristen;
4. Festlegung der Termine für die Löschung der Abrechnungsdaten;
5. Festlegung des Zeitpunktes der Löschung der Verbindungsdaten; Festlegung, welche Merkmale zur statistischen Auswertung und zur Erzeugung des Abrechnungsdatensatzes verwertet werden;
6. Regelung der Verarbeitung personenbezogener Betriebsdaten bei Mitteilungsdiensten (Speicherung, Übermittlung und Löschung der Abrechnungsdaten, Verwendung der Verbindungsdaten);
7. Verpflichtung der Deutschen Bundespost zur Auskunft, Berichtigung, Sperrung und Löschung;
8. Präzisierung der von der Deutschen Bundespost über das BDSG hinaus durchzuführenden Datensicherungsmaßnahmen (vgl. Art. 9 Abs. 8 Staatsvertrag).

3.1.1.2 Erste Erfahrungen aus der Überwachung

Das Hamburgische Gesetz zum Staatsvertrag über Bildschirmtext vom 11.4.1984 (GVBl. I S. 82) enthält die Zustimmung zum Staatsvertrag und regelt die Befugnisse der Verwaltungsbehörden, die die Einhaltung der Vorschriften des Staatsvertrages überwachen. Der Staatsvertrag über Bildschirmtext ist für Hamburg am 1.5.1984 in Kraft getreten (s. GVBl. I S. 95). Mit der Anordnung über Zuständigkeiten bei Bildschirmtext vom 25.5.1984 (Amtlicher Anzeiger S. 912) ist mir die Aufgabe übertragen worden, die Einhaltung der Datenschutzvorschriften des Staatsvertrages zu überwachen. Damit waren die rechtlichen Voraussetzungen für die Aufnahme meiner Überwachungstätigkeit erfüllt.
Auch die tatsächlichen Voraussetzungen hierfür waren zu diesem Zeitpunkt gegeben, nachdem ein Btx-Gerät beschafft und installiert war, das mir erlaubt, am Btx teilzunehmen.
Zu systematischen Prüfungen bin ich bisher nicht gekommen. Die oben beschriebene Auseinandersetzung mit der Deutschen Bundespost und die Analyse des technischen Systems Btx (vgl. Nr. 2.2.1.1) haben die verfügbaren Kräfte gebunden.

Im Berichtszeitraum habe ich
- mit der Firma Otto-Versand ihr Btx-Angebot erörtert,
- einen Anbieter abgemahnt, der sich Daten, die durch entsprechende Farbgestaltung für den Teilnehmer nicht sichbar waren, zusammen mit anderen Daten vom Teilnehmer übermitteln ließ,
- eine Prüfung des Btx-Angebots der Verbraucherbank AG begonnen.

Bei der Prüfung des Angebots der Verbraucherbank stand die Prüfung der Sicherung gegen unberechtigten Zugang im Vordergrund. Die Prüfung ist noch nicht abgeschlossen; insbesondere sind die Feststellungen zur Sicherung gegen unberechtigten Zugang noch nicht ausgewertet und das Sicherungssystem ist noch nicht bewertet worden.
Im folgenden werden daher nur erste, notwendigerweise vorläufige Überlegungen mitgeteilt.
Das System der Sicherung gegen unberechtigten Zugang hat für eine Bank, die die Kontoführung über Btx eingerichtet hat, besondere Bedeutung, weil
- dies eine zusätzliche Möglichkeit für Außenstehende eröffnet, durch unberechtigten Zugang Vermögensverhältnisse eines Dritten auszuforschen und u. U. betrügerische Verfügungen zu treffen, und
- der Zugang ohne Kontrolle durch einen Menschen zugelassen wird. Die Berechtigung zum Zugang zu einem Konto ist an die Kenntnis bestimmter Informationen geknüpft; es wird unterstellt, daß ein Dritter nur mit Wissen des Berechtigten in den Besitz der Informationen gelangen kann – von einem nachlässigen Umgang des Berechtigten mit diesen Informationen einmal abgesehen.

Die Sicherheit des Zugangs hängt daher davon ab, ob die den Zugang zum Konto eröffneten Informationen gegen Ausforschung geschützt sind.
Zum Lesen des Kontos
müssen bei der Verbraucherbank die Kontonummer und eine jederzeit veränderbare Geheimzahl (PIN) eingegeben werden; zusätzlich kann der Berechtigte vorgeben, daß für jeden Zugang eine nur einmal verwendbare, von der Verbraucherbank vorgegebene Zufallszahl (TAN = Transaktionsnummer) oder bis zu 3 – jederzeit veränderbare – Paßworte eingegeben werden müssen.
Für eine Verfügung über das Konto
muß eine TAN eingegeben werden.
Die Kontonummer ist nicht schwer zu beschaffen. Geheimzahl (PIN) und evtl. Paßworte muß der Berechtigte – vergleichbar einer EC-Karte und Scheckformularen – so aufbewahren, daß sie Dritten nicht zugänglich sind. Die TAN werden in großer Zahl (zuerst 100, dann jeweils 75) dem Berechtigten zugesandt; auch diese muß er sicher aufbewahren.
Diese Informationen werden beim home-banking über Btx aber unverschlüsselt über die Fernsprechleitung an die Btx-Vermittlungsstelle übertragen. Da die Fernsprechleitung bis zu einer Hausverteileranlage oder einem Endverzweiger ohne großen Aufwand identifizierbar ist und „angezapft" werden kann, besteht hier die Möglichkeit des Ausforschens von Kontonummer, Geheimzahl und ggf. Paßworten sowie der TAN; da jede TAN aber nur einmal benutzt werden kann, können auch nach erfolgreichem Ausforschen nur dann betrügerische Verfügungen getroffen werden, wenn ein Unberechtigter nicht nur die entsprechende Fernsprechleitung identifiziert und anzapft, sondern auch ein Gerät anschließt, mit dem er die übermittelten Informationen abfangen, verändern (andere Bankverbindung) und dann an die Btx-Vermittlungsstelle senden kann. Da die vom Teilnehmer über die Tastatur seines Btx-Gerätes eingegebenen Zeichen nicht direkt auf dem Bildschirm angezeigt, sondern von der Btx-Vermittlungsstelle nach Empfang an den Btx-Anschluß zurückgesandt und dann auf dem Bildschirm sichtbar gemacht werden („Spiegelung" oder „Echoplexen"), muß für jede betrügerische Manipulationen ein hoher Aufwand geleistet werden (Abfangen und Simulieren einer Btx-Vermittlungsstelle, Verändern der Überweisung und Senden an Btx-Vermittlungsstelle unter Simulation eines Btx-Gerätes). Bei der Verbraucherbank kommt hinzu, daß durch ein Quittungsverfahren (es wird nur ein Teil des TAN vom Teilnehmer eingegeben; den anderen Teil der TAN sendet die Verbraucherbank als Quittung zurück) der zu leistende technische Aufwand noch erheblich höher sein muß (Abfangen und Verändern auf dem Hinweg, Abfangen und Rückverändern auf dem Rückweg).

Auch wenn der Aufwand technisch realisierbar ist, erscheint jedenfalls z. Z. fraglich, ob durch betrügerische Veränderungen von Überweisungen ein so großer Vorteil erlangt werden kann, daß darüber hinaus auch die relativ hohe Gefahr der Entdeckung (durch das eingesetzte begünstigte Konto werden Spuren erzeugt) in Kauf genommen wird.
Die Schwachstelle liegt in der verhältnismäßig leichten Zugänglichkeit der Fernsprechleitungen. Die Deutsche Bundespost hat daher eine erhöhte Verantwortung:
- Sie muß zumindest die Btx-Teilnehmer über diese Risiken aufklären.
- Sie sollte die Zugangssicherung verbessern. Nach neueren Informationen beabsichtigt die Deutsche Bundespost, eine Chipkarte anzubieten, die die Sicherheit erhöht. Auch gibt es private Angebote zur Erhöhung der Sicherheit.

3.1.2 Andere Medien

Der Entwicklungsstand anderer Medien ist in Hamburg, wie überall in der Bundesrepublik, außerhalb der Kabelpilot- oder Kabelversuchsprojekte nur wenig fortgeschritten:
- Die Einführung neuer Rundfunkprogramme wird vor allem medienpolitisch diskutiert. Die gegenwärtig vorhandene Vermittlungstechnik (s. Nr. 2.5.2.2.1) sieht weder die Erhebung noch die Speicherung personenbezogener Daten über die Inanspruchnahme von Programmen vor.
- Allenfalls steht TEMEX nach Abschluß entsprechender Versuche der Deutschen Bundespost zur Verfügung, weil hier mit dem Fernsprechnetz ein Transportsystem vorhanden ist.

Die Einführung weiterer Medien ist nicht absehbar.

3.1.2.1 Vermittelte Rundfunkprogramme

Ich habe in der Diskussion über ein Landesmediengesetz Datenschutzregelungen vorgeschlagen, die vorsorglich davon ausgehen, daß bei der Verteilung von Rundfunkprogrammen künftig Verbindungs- und Abrechnungsdaten wie im Btx-System entstehen. Die Regelungen orientieren sich deshalb am Vorbild des Staatsvertrages über Bildschirmtext:
- Verbindungsdaten (Daten über die Inanspruchnahme von Programmen):
  Erhebung und Speicherung nur, soweit und solange für die Verbindung notwendig, d. h. Löschung nach Auflösung der Verbindung, soweit nicht Speicherung als Abrechnungsdaten,
  keine Datenübermittlung.
- Abrechnungsdaten (Daten über die Inanspruchnahme entgeltpflichtiger Programme):
  Erhebung und Speicherung nur, soweit und solange dies für Abrechnungszwecke erforderlich ist; i.d.R. pauschale Speicherung, detaillierte Speicherung nur mit Einverständnis des Teilnehmers;
  Löschung nach Abrechnung;
  keine Übermittlung,
- Datensicherungsmaßnahmen über die Anforderungen des BDSG hinaus.

3.1.2.2 Fernwirkdienste

Die Fernwirkdienste unter Benutzung des Fernsprechnetzes (von der Deutschen Bundespost als TEMEX bezeichnet) sind unter Nr. 2.5.2.2.2 technisch beschrieben worden. Im folgenden sollen die rechtlichen Probleme erörtert werden.
Im 2. TB habe ich darauf hingewiesen, daß Fernwirkdienste ohne Zweifel positive Aspekte z. B. für Kranke und Behinderte haben und der Rationalisierung dienen können, daß mit ihnen aber auch erhebliche Gefährdungen verbunden sein können, nämlich
- Verstöße gegen die Unverletzlichkeit der Wohnung (Art. 13 GG) und
- das Eindringen in die Privatsphäre (Art. 1 Abs. 1, 2 Abs. 1 GG)

Die neue Qualität der Fernwirkdienste – so habe ich in meinen 2. TB ausgeführt – liegt darin, daß die Kommunikation von außen gesteuert wird.

Daher halte ich es für dringend geboten, daß rechtzeitig rechtliche Vorkehrungen getroffen werden.
Es ist Sache jedes Einzelnen, ob und ggf. welche Fernwirkdienste er in Anspruch nimmt; er muß mit dem Anbieter des ihn interessierenden Dienstes einen Vertrag schließen, der die Leistungsmerkmale des Dienstes und die gegenseitigen Rechte und Pflichten beschreibt. Es ist nicht Aufgabe des Datenschutzes, den einzelnen Bürger zu bevormunden und in seinen Entscheidungen zu beeinflussen. Die wenigsten werden aber in der Lage sein, die hinter den Fernwirkdiensten stehende Technik zu übersehen, auf ihre Gefährdungen hin zu analysieren und auf vertragliche Bestimmungen hinzuwirken, die diesen Gefährdungen begegnen. Mangelnde technische Kenntnisse und mangelnde Transparenz der komplexen Technik lassen im allgemeinen keine gleichwertigen Ausgangspositionen für einen Vertragsabschluß entstehen. Datenschutzregelungen für Fernwirkdienste haben daher – ähnlich dem Gesetz über Allgemeine Geschäftsbedingungen – das Ziel, durch Setzen von Rahmenbedingungen, die den besonderen Gefährdungen von Fernwirkdiensten Rechnung tragen, „Waffengleichheit" herzustellen und einen fairen Vertrag zu ermöglichen. Nach Vorstellungen der Datenschutzbeauftragten handelt es sich um folgende Rahmenbedingungen:
- Unterrichtung des Betroffenen über Verwendungszwecke sowie Art, Umfang und Zeitraum des Einsatzes des jeweiligen Dienstes;
- schriftliche Einwilligung des Betroffenen, die nicht erzwungen werden darf (etwa durch Verweigerung einer auch auf andere Weise zu erbringende Leistung); jederzeitige Möglichkeit zum Widerruf der Einwilligung;
- Anzeige, daß und welcher Fernwirkdienst in Anspruch genommen wird;
- Möglichkeit, den Fernwirkdienst jederzeit abschalten zu können, soweit der Vertragszweck dem nicht entgegensteht.

Die Deutsche Bundespost hat den Bundesbeauftragten für den Datenschutz und die Landesbeauftragten, in deren Ländern Systemversuche durchgeführt werden, eingeladen, die von ihr beabsichtigten Versuche von Fernwirkdiensten unter Datenschutzaspekten zu begleiten und so empirische Erkenntnisse über die datenschutzrechtlichen Gefährdungen der Fernwirkdienste zu gewinnen. Ich erhoffe mir von diesem Vorgehen, das ich ausdrücklich begrüße, eine bessere Fundierung der bisher mehr theoretischen Diskussion.

3.2 Personalwesen

In der Datenschutzdiskussion nimmt das Thema Personalinformationssysteme eine beherrschende Rolle ein; in meinem 2. TB habe ich mich ausführlich mit den Personalinformationssystemen in der privaten Wirtschaft unter dem Aspekt des Arbeitnehmerdatenschutzes, insbesondere auch der Mitbestimmungsrechte des Betriebsrats befaßt (Nr. 4.8.4 im 2. TB). Die anhaltende Diskussion im privaten Bereich und gelegentliche Anfragen von Personalräten aus der hamburgischen Verwaltung haben mich veranlaßt, mich in diesem TB dem Thema „Personalinformationssystem in der hamburgischen Verwaltung" zuzuwenden.

3.2.1 Begriff des Personalinformationssystems

Anknüpfend an meine Ausführungen im 2. TB gehe ich davon aus, daß unter den Rahmenbedingungen für die öffentliche Verwaltung Systeme mit überwiegend administrativen Funktionen keine besonderen Probleme aufwerfen, und habe deshalb geprüft, ob die in der hamburgischen Verwaltung eingesetzten Verfahren folgende Merkmale enthalten, die in erster Linie Gefährdungen für die Bediensteten entstehen lassen:
a) Zusammenfassung von Daten über das Personal aus verschiedenen Anwendungsgebieten (Personalverwaltung im engeren Sinne, Personalfürsorge, Arbeitsplätze, Arbeitsleistung u. a.m.),
b) Verknüpfung über ein gemeinsames eindeutiges Kennzeichen,
c) Eignung der Verfahren zur Überwachung des Verhaltens und der Leistung des Personals sowie zur Personalsteuerung, -förderung und -planung.

3.2.2 Automatisierte Personaldatensysteme in der hamburgischen Verwaltung

Zunächst sollen die automatisierten Verfahren dargestellt werden, die behördenübergreifend personenbezogene Daten der Bediensteten der Freien und Hansestadt verarbeiten.

3.2.2.1 Stellenplan

Das automatisierte Verfahren „Stellenplan" dient der Verwaltung des beim Senatsamt geführten Stellenbestandes sowie der Erledigung von Aufgaben, die auf diesem Stellenbestand aufbauen.
In dem Verfahren wird für den Stellenbestand eine Datenbank eingerichtet, zu der Benutzerstationen über Datenfernverarbeitung im Dialog Zugang haben. Je Stelle werden bis zu etwa 30 Daten gespeichert, die mit Historik geführt werden. In die Datenbank werden auch die Strukturdaten für die Darstellung der Verwaltungsgliederungspläne (Organisationseinheiten und Aufgabenbeschreibungen) aufgenommen.
Auf der Grundlage dieses Datenbestandes sollen folgende Aufgaben automatisch erledigt werden:

- Aufstellung des Stellenplanes,
- Führung der Verwaltungsgliederungspläne (ohne Angaben über die Stellenbesetzung),
- Durchführung von Finanzierungsrechnungen,
- Auswertungen aus dem Stellenbestand.

An das Verfahren ist zunächst nur das Senatsamt angeschlossen. Im automatisierten Verfahren erhält jede Stelle und jede Größe sonstigen Personalbedarfs eine Stellennummer. Die Stellennummer ist Suchbegriff für das Auffinden im automatisierten Stellenstand; sie ist unveränderbar, d. h. sie bleibt auch nach Umwandlung oder Verlängerung einer Stelle erhalten.
Das Verfahren ist mit Rücksicht auf die Komplexität der Aufgabenstellung und den Aufwand an Zeit und Kosten für die Verfahrensentwicklung, aber auch wegen der Datenschutzprobleme, die sich bei Einbeziehung personenbezogener Daten in den Datenbestand ergäben, auf den Soll-Stellenplan und damit auf den Aufgabenbereich des Senatsamtes beschränkt worden.
Das Verfahren ist indessen so angelegt, daß ein weiterer Ausbau nicht ausgeschlossen ist. Denkbar ist eine Fortentwicklung dahingehend, daß einzelne Behörden (z. B. solche mit großer Stellenzahl) zum Datenbestand ihres Zuständigkeitsbereichs unmittelbar Zugang erhalten; damit wäre nicht nur eine dezentrale Eingabe der von diesen Behörden veranlaßten Änderungen in das Verfahren möglich, darüberhinaus könnte der Datenbestand von der jeweiligen Behörde auch zu vielfältigen Auswertungen vor Ort genutzt werden.
Eine andere mögliche Erweiterung würde in der zusätzlichen Speicherung von Daten über die Stellennutzung (Ist-Daten) bestehen.
Beide Ausbaumöglichkeiten würden wegen der erforderlichen Aktualität der Daten zwingend eine Direktverarbeitung über Datenfernverarbeitung voraussetzen. Der Aufbau eines „flächendeckenden" Datenfernverarbeitungsnetzes erscheint dem Senatsamt derzeit aber noch unwirtschaftlich, weil die Nutzungsintensität von Behörde zu Behörde sehr unterschiedlich ist, so daß eine generelle Erweiterung des Systems im skizzierten Sinn für alle Behörden gegenwärtig nicht in Betracht kommt. Die Situation kann sich in der Zukunft bei möglicherweise sinkenden Kosten für die Datenfernverarbeitung oder bei gegebener Möglichkeit der Mehrfachnutzung von Leitungen und Geräten anders darstellen.
Das Senatsamt wird die Frage einer Verfahrensausweitung weiter verfolgen und ggf. einer hieran interessierten Behörde eine Pilotanwendung vorschlagen.
Bei Aufnahme von Ist-Angaben in den Datenbestand müßte auf jeden Fall sichergestellt sein, daß auf personenbezogene Daten nur die jeweils berechtigte Behörde zugreifen kann. Im übrigen müßten vor einer solchen Verfahrensänderung die Mitbestimmungsrechte beachtet werden.

3.2.2.2 Personalabrechnung

Das automatisierte Verfahren Personalabrechnung ist sehr umfangreich, es umfaßt die Personalabrechnung für

- alle aktiven Beschäftigten (Richter, Beamte, Angestellte, Arbeiter, sonstige Beschäftigte – z. B. nebenberuflich Tätige) und
- alle Versorgungsempfänger (Pensionäre nach G131 und hamburgischem Recht, Ruhegeldempfänger).

Es ist als Stapelverfahren organisiert; lediglich die Dateneingabe und die Information des Buchhalters über das Gehalts- und Lohnkonto (einschl. Historik) sind für die aktiven Beschäftigten auf Dialogverarbeitung umgestellt worden.

Der Datenbestand umfaßt

- Angaben zur Person,
- Merkmale für Brutto- und Nettoberechnung,
- Historik der letzten 12 Abrechnungszeiträume,

er ist kompliziert aufgebaut und umfaßt maximal über 25.000 Zeichen. Ordnungsmerkmal ist eine Kennziffer, die zentral von der Besoldungs- und Versorgungsstelle (als speichernder Stelle) vergeben wird.

Das Verfahren umfaßt folgende Funktionen:

1) Die eigentliche Personalabrechnung mit
   Bruttoberechnung (Grundgehalt, -vergütung, Ortszuschlag, Zulagen, leistungsbezogene Zuschläge, z. B. Mehrarbeit, Prämien, Nachtdienst, Bereitschaftsdienst)
   Nettoberechnung (Steuerabzüge, Übermittlung von Lohnzetteln und Lohnsteuerkarten-Aufklebern an die Finanzämter, Sozialversicherungsabzüge, Übermittlung von Daten im Rahmen von DEVO/DÜVO an die Sozialversicherungsträger)
   Zahlbarmachung (Anweisung der Nettobezüge, Übermittlung von Daten an das Kreditinstitut, Vermögenswirksame Anlage, Übermittlung von Daten an den Zahlungsempfänger, Abwicklung von Vorschüssen, Zahlung von Kindergeld, Einbehaltung von Sacherträgen – Mieten, Stellplätzen –, durchlaufende Posten – Zahlung von Zehrkosten, Reisekostenvergütungen)
2) Regelmäßige Verwaltungshilfen mit Kindergeldwarnlisten (gehen an die Personalabteilungen), Wegfall von vermögenswirksamen Anlagen (geht an BVSt) vom Buchhalter gesetzten Terminen (gehen an BVSt)
3) Verwaltungshilfen im Einzelfall; (u. a. „Adreßdienst"), z. B. Adressen für die Erhebung von Nebentätigkeiten, Adressen für die Erhebung für einkommensabhängigem Kindergeld (über solche Anforderungen entscheidet i. d. R. das zuständige Referat, im Ausnahmefall die Leitung des Personalamts)
4) Verwaltungshilfen, die den Bereich der Verwaltung verlassen, Liste mit den Grunddaten der ABM-Beschäftigten für die Abrechnung mit dem Arbeitsamt (geht an die BAJS)
   Liste der Mitglieder, die am Beitragseinzugsverfahren teilnehmen, an die Betriebskrankenkasse und andere gesetzliche Krankenkassen (einmalig am 1.4.)
5) Auswertung ohne Personenbezug
   Lieferung von Statistiken, z. B. Finanzstatistik, Personalwechselstatistik, Personalbestandsstatistik;
   Personalkostentabelle;
   Beschäftigte nach Staatsangehörigkeit, Alter, Funktionsgruppen;
   Betriebskostenabrechnung;

Verfahrenserweiterungen sind gegenwärtig nicht geplant.

3.2.2.3 Personalstrukturdatei

Dieses Verfahren ist, wie aus der Bezeichnung schon erkennbar, in erster Linie nur für Auswertungen zu Untersuchungen über die Struktur des Personals der Freien und Hansestadt Hamburg angelegt. Es enthält Daten über jeden (gegenwärtigen und früheren) Beschäftigten:

- Angaben zur Person,
- Angaben zur Ausbildung,

- Angaben zum Beschäftigungsverhältnis.

Der Datenbestand enthält auch Historikdaten (ab 1978), nämlich
- Historikangaben zu jedem Beschäftigten (längstens ab 1978),
- Angaben über frühere Beschäftigte (alle nach 1978 ausgeschiedenen).

Der Datenbestand wird in sequentieller Organisation auf Magnetplatte gespeichert.
Die Daten werden aus dem automatisierten Verfahren Personalabrechnung fortgeschrieben; Verknüpfungsmerkmal ist die unter Nr. 3.2.2.2 erwähnte Kennziffer. Der Datenbestand enthält darüber hinaus wegen der unten aufgezählten Auswertungen für Verwaltungszwecke den Namen des Beschäftigten.
Der Datenbestand wird in erster Linie für Strukturuntersuchungen ausgewertet. Bedarfsträger sind verschiedene Behörden, vor allem das Personalamt, das Organisationsamt (Untersuchungen zur Personalplanung), die Leitstelle für die Gleichstellung der Frau, der Landesbetrieb Krankenhäuser. Es handelt sich um Tabellenauswertungen und graphische Darstellungen, insbesondere Alterspyramiden.
Darüber hinaus wird der Datenbestand für Verwaltungszwecke ausgewertet:
- Personalratswahlen (insbesondere Wählerlisten)
- Beförderungslisten für die Feuerwehr (neben dem Namen jeweils das Datum der Einstellung, der letzten Beförderung, des – in der Zunkunft liegenden – Ausscheidens).

3.2.2.4 Fortbildung

Nur der Vollständigkeit halber soll hier erwähnt werden, daß im Senatsamt auf einem Personalcomputer, der in erster Linie für Zwecke der Aus- und Fortbildung zur Verfügung steht, zwei kleine automatisierte Verfahren betrieben werden, mit denen personalbezogene Daten verarbeitet werden:
- Verwaltung der Teilnehmer an den zentralen Fortbildungsseminaren (z. B. Rahmenplanseminare für den höheren allgem. Verwaltungsdienst, Fremdsprachenkurse, Führungslehre-Seminare, u. a. m.),
- Speicherung der angewiesenen Honorare für die Kontrollmitteilungen an die zuständigen Finanzämter.

Es folgen die automatisierten Verfahren, die die personenbezogenen Daten der Bediensteten nur einer Behörde verarbeiten.

3.2.2.5 Bewerberdatei in der Behörde für Schule und Berufsbildung

In der Bewerberdatei werden die Daten der Bewerber für das Lehramt an Grund-, Haupt- Real- und Sonderschulen gespeichert:
- Persönliche Daten, z. B. Name, Anschrift, Geburtsdatum;
- Daten zur Ausbildung, z. B. Lehrbefähigungen, Noten der Staatsprüfung.

Die Daten werden halbjährlich durch die Personalabteilung aktualisiert und ausgewertet.

3.2.2.6 Lehrerindividualdatei in der Behörde für Schule und Berufsbildung

Die Lehrerindividualdatei enthält Daten des pädagogischen Personals an den staatlichen Schulen (mehr als 20.000 Datensätze):
- Persönliche Daten, z. B. Name, Anschrift, Geburtsdatum;
- personal- und dienstrechtliche Daten, z. B. Rechtsverhältnis, Beschäftigungsverhältnis, Amts-/Dienstbezeichnung;
- Daten zur Ausbildung, z. B. Lehrbefähigungen, Lehrämter;
- Daten zur Verwendung des Lehrers, z. B. Unterrichtsstunden.

Die persönlichen Daten und die personal- und dienstrechtlichen Daten werden von der Personalabteilung der Behörde für Schule und Berufsbildung ständig fortgeschrieben. Alle Daten werden einmal jährlich von den betroffenen Lehrern überprüft und ergänzt. Nur soweit erforderlich, findet eine neue Erhebung statt, z. B. der Unterrichtsstunden.
Die Daten werden im Stapelbetrieb verarbeitet.
Die Auswertungen dienen in erster Linie der Schulorganisation und der Planung.

Die Lehrerindividualdatei ist Gegenstand einer kürzlich bei mir eingegangenen Eingabe. Ich habe die Eingabe zum Anlaß genommen, dieses Verfahren eingehend zu prüfen. Über das Ergebnis werde ich im nächsten TB unterrichten.

3.2.2.7 Personalverwaltungssystem in der Universität

In der Universität Hamburg gibt es das automatisierte Personalverwaltungssystem. Es ist auf das wissenschaftliche Personal beschränkt und enthält folgende Daten:
- Aus- und Weiterbildungsdaten, z. B. Schulabschluß, Hochschulabschlüsse, Promotion, Habilitation;
- Beschäftigunsdaten, z. B. Dienst- und Beschäftigungsverhältnis, Bezahlung;
- Dienstdaten;
- Dienstadresse;
- Nebentätigkeiten;
- Beurlaubung;
- Lehrdeputate;
- Stellendaten.

Die Daten werden im Stapelbetrieb verarbeitet und für statistische Zwecke (inbesondere Hochschulstatistik) und für Zwecke der hochschulinternen Planung ausgewertet.

3.2.3 Gibt es in der hamburgischen Verwaltung ein integriertes Personalinformationssystem?

Auf Seite 28 sind die oben vorgestellten automatisierten Verfahren, mit denen personenbezogene Daten von Bediensteten der Freien und Hansestadt Hamburg verarbeitet werden, in einer Übersicht zusammengefaßt worden. Nach meiner Kenntnis sind z. Z. keine weiteren automatisierten Verfahren geplant, mit denen personenbezogene Daten des Personals verarbeitet werden. Die betrachteten Verfahren verfügen nicht über die Eigenschaften, die als hauptsächliche Gefährdungsmomente von Personalinformationssystemen angesehen werden. Es fehlt an der Zusammenfassung von Daten aus verschiedenen Anwendungsgebieten. Alle Verfahren bewegen sich im Anwendungsgebiet der Personalverwaltung und teilweise der Personalplanung, wobei zwar personenbezogene Daten verwendet, aber keine auf bestimmte Personen bezogene Auswertungen gemacht werden. Lediglich das Verfahren „Stellenplan" stammt aus einem anderen, immerhin der Personalverwaltung verwandten Anwendungsgebiet; z. Z. werden aber keine personenbezogene Daten verwendet. Die betrachteten automatisierten Verfahren sind – und das halte ich für den entscheidenden Punkt – nicht miteinander verknüpft, jedes Verfahren hat sein eigenes Ordnungsmerkmal und ist damit gegen die anderen isoliert. Die Ausnahme der Verknüpfung von Personalabrechnung und Personalstrukturdatei kann in diesem Zusammenhang vernachlässigt werden, weil es sich hier um weitgehend parallele Datenbestände handelt. Schließlich enthalten die Systeme auch keine Leistungs- und Beurteilungsdaten, die die Herstellung von Fähigkeits- oder Leistungsprofilen oder die Überwachung der Bediensteten gestatten würden.
Ein gemeinsames eindeutiges Ordnungsmerkmal für die Verknüpfung aller heutigen und künftigen automatisierten Verfahren wäre mit der für das Verfahren Personalabrechnung vergebenen Kennziffer vorhanden. Die Voraussetzungen für eine Verknüpfung der automatisierten Verfahren könnten dadurch geschaffen werden, daß die – auch den Personalverwaltungen in den Behörden bekannte – Kennziffer zusätzlich in alle anderen automatisierten Verfahren aufgenommen wird. Auf diese Weise könnte auch die Stellenverwaltung mit der Personalverwaltung verknüpft werden. Voraussetzung dafür wäre, daß das Verfahren für den Stellenplan um den Ist-Stellenplan erweitert und darin auch die Kennziffer gespeichert würde; das ist gegenwärtig nicht beabsichtigt.
Nach den mir vorliegenden Erklärungen des Senatsamtes soll ein umfassendes Personalinformationssystem nicht geschaffen werden. Ich habe keinen Anlaß, an diesen Erklärungen zu zweifeln. Trotzdem werde ich die weitere Entwicklung aufmerksam beobachten.
Ich habe bereits darauf hingewiesen, daß die betrachteten Verfahren nicht zur Überwachung des Verhaltens und der Leistung von Bediensteten bestimmt und schon deshalb auch nicht geeignet sind, weil sie keine dafür notwendigen Daten (die das Verhalten und die Leistung beschreiben) enthalten.

Übersicht über die z. Z. vorhandenen automatisierten Verfahren im Personalwesen im weiteren Sinne

<table>
<tr><th colspan="2">Personalverwaltung</th><th colspan="2">Stellenverwaltung</th></tr>
<tr><th>behördenbezogen</th><th>behördenübergreifend</th><th>Ist-Stellenplan</th><th>Soll-Stellenplan</th></tr>
<tr>
<td>Behörde für Schule und Berufsbildung:

Verfahren „LehrerIndividualdatei"

Personaleinsatz
Planungsauswertungen

Ordnungsmerkmal:
Name

Verfahren „Bewerberdatei"

(Grund-, Haupt-, Real- und Sonderschullehrer)

Ordnungsmerkmal:
Name

Universität Hamburg:

Verfahren „Personal-Verwaltungs-System"

(nur wissenschaftliches Personal)
Planungsausweitungen

Ordnungsmerkmal:
Personalnummer (nicht identisch mit Kennzeichen)</td>
<td>Verfahren „Personalstrukturdatei"

Verfahren „Personalabrechnung"

Fortschreibung

Auswertungen
Verwaltungshilfen, z. B.
Personalratswahlen u.
Beförderungsliste der
Feuerwehr

Ordnungsmerkmal:
Kennziffer

Personalabrechnung
Hinweislisten
Adreßlisten
Planungsauswertungen
Einzelauswertungen

Ordnungsmerkmal:
Kennziffer

Verfahren „Fortbildung"

Teilnehmerverwaltung
Kontrollmitteilungen an
das Finanzamt

Ordnungsmerkmal:
Name</td>
<td>(Erweiterung um Ist-Daten, das ist die Besetzung der Stelle, möglich, aber z. Z. nicht geplant)</td>
<td>Verfahren „Stellenplan"

Beschreibung jeder Stelle
Aufstellung des Stellenplans
Führung der Verwaltungsgliederungspläne (ohne Ist-Daten)
Finanzierungsrechnungen
Auswertungen

Ordnungsmerkmal:
Stellennummer</td>
</tr>
</table>

3.2.4 Ausblick

Auch wenn aufgrund der Struktur der vorhandenen automatisierten Verfahren und der Absichten des Senatsamtes für den Verwaltungsdienst gegenwärtig kein Grund zur Besorgnis besteht, kann ich es bei dieser Feststellung nicht bewenden lassen. Es muß Vorsorge getroffen werden, daß auch bei einer Änderung der Absichten oder auch unbeabsichtigt keine automatisierten Verfahren entwickelt werden können, die die schutzwürdigen Belange der Bediensteten beeinträchtigen.
Für mich ergeben sich 3 Tätigkeitsfelder:

3.2.4.1 Novellierung des Personalvertretungsrechts

Die Bürgerschaft hat den Senat ersucht,
ihr baldmöglichst mitzuteilen, welche Notwendigkeiten der Anpassung des Personalvertretungsgesetzes im Lichte der seit 1972 gewonnenen Erfahrungen sowie der veränderten Entwicklungen bestehen, damit die Novellierung noch in dieser Wahlperiode erfolgen kann.

Ich habe mich schon gegenüber dem Senatsamt geäußert und folgende Änderung des Personalvertretungsgesetzes vorgeschlagen:

Der Personalrat hat mitzubestimmen bei der Einführung, Anwendung sowie wesentlichen Änderung oder Ergänzung
- von Dateien und Anlagen zur automatisierten Verarbeitung personenbezogener Daten der Beschäftigten,
- von sonstigen technischen Einrichtungen, soweit diese dazu geeignet sind, das Verhalten oder die Leistung des Beschäftigten zu überwachen.

Dieser Vorschlag lehnt sich an die Formulierungen des kürzlich novellierten hessischen Personalvertretungsgesetzes an. Mit einer solchen Rechtsvorschrift würde erreicht, daß der Personalrat als die Interessenvertretung der Beschäftigten
- bei allen Automationsvorhaben beteiligt wird, mit denen personenbezogene Daten der Beschäftigten verarbeitet werden sollen, und
- bei anderen Automationsvorhaben dann beteiligt wird, wenn sie zur Überwachung geeignet sind.

3.2.4.2 Inhaltliche Gestaltung von Automationsvorhaben im Personalbereich

Die Vorschläge für eine Novellierung des Personalvertretungsgesetzes können nur an formale Eigenschaften von Automationsvorhaben anknüpfen. Es bleibt ein weiter Gestaltungsspielraum, in dem die Personalräte die Interessen der von ihnen vertretenen Beschäftigten wahren müssen. Die Erfahrungen aus der privaten Wirtschaft zeigen, daß Betriebs- und Personalräte mit dieser Aufgabe nicht allein gelassen werden dürfen. Ich stehe auch für die Beratung der Personalräte gern zur Verfügung. Mit der gesetzlichen Absicherung des Mitbetimmungsrechts der Personal- und Betriebsräte kann es im übrigen nicht sein Bewenden haben. Darüber hinaus bedarf es gesetzlicher Regelungen, die die Grundsätze der Erforderlichkeit und Zweckbindung für den Bereich der Arbeitsbeziehungen präzisieren. Meine Vorschläge für bereichsspezifische Regelungen der Verarbeitungsvoraussetzungen privatrechtlicher Arbeitsverhältnisse habe ich unter Nr. 4.7.6 noch einmal zusammengefaßt. Sie sind auf öffentlich-rechtliche Dienstverhältnisse weitgehend übertragbar.

3.2.4.3 Überwachung des Verhaltens oder der Leistung

Einen Sonderfall bilden die automatisierten Verfahren, die Daten über den Arbeitsprozeß erfassen und zugleich geeignet sind, das Verhalten oder die Leistung des Beschäftigten zu überwachen. Hierunter fallen z. B. Telefondatenerfassungssysteme, Zugangskontrollsysteme sowie alle automatisierten Verfahren im Dialogbetrieb, soweit hierbei Daten aufgezeichnet werden, die zugleich Daten über die Leistung der Benutzer sind. Hier ist besonders schwer, einen Ausgleich zwischen den Gesichtspunkten, die eine Protokollierung der Inanspruchnahme des Systems notwendig machen – hierzu gehör-

ten etwa die Kassensicherheit; aber auch der Datenschutz verlangt, daß nachträgliche Kontrollen der Datenverarbeitungsvorgänge möglich sein müssen – und den Interessen der Beschäftigten zu finden. Ob und inwieweit solche Daten erhoben und gespeichert werden müssen und wie verhindert werden kann, daß sie zugleich für Leistungsmessungen genutzt werden, läßt sich nicht abstrakt klären. Dies kann letztlich nur für jedes konkrete automatisierte Verfahren geschehen.

3.3 Steuerwesen

3.3.1 Novellierung der Abgabenordnung

Im Berichtsjahr sind die Arbeiten an dem Entwurf eines Steuerbereinigungsgesetzes 1985 (Änderung der Abgabenordnung und anderer Gesetze) fortgesetzt worden. Mit dem Referentenentwurf vom August 1983 hatte ich mich in meinem 2. TB auseinandergesetzt (Nr. 3.4.1). Nunmehr liegt der Entwurf der Bundesregierung vom 19.6.1984 (Bundestagsdrucksache 10/1636) vor, der sich auch zu der Stellungnahme des Bundesrats vom 18.5.1984 (Bundesratsdrucksache 140/84) äußert.
Von datenschutzrechtlicher Relevanz sind folgende Aspekte der AO-Novellierung:

- Auch der neueste Entwurf bringt keine Klarstellung hinsichtlich der Kontrollkompetenz der Datenschutzbeauftragten im Geltungsbereich des § 30 AO (Steuergeheimnis). Wie ich bereits in meinen früheren Tätigkeitsberichten (1. TB Nr. 6.3, 2. TB Nr. 3.4.1.1) dargestellt habe, ist zwischen den Datenschutzbeauftragten des Bundes und der Länder einerseits und den Steuerverwaltungen des Bundes und der Länder andererseits streitig, ob das Steuergeheimnis auch gegenüber den Datenschutzbeauftragten gilt. Hamburg hat im Bundesrat einen Vorstoß in Richtung auf eine ergänzende Regelung in der AO unternommen (BR-Drucksache 140/4/84 vom 17.5.1984), der aber erfolglos geblieben ist. Daneben habe ich für meinen Zuständigkeitsbereich nach einer von der AO-Novellierung unabhängigen Lösung des Problems gesucht (s. unten 3.3.2.1).
- Die Regelung des Kontrollmitteilungsverfahrens, die im Entwurf vom August 1983 in § 93 Abs. 7 vorgesehen war, ist nunmehr in einem § 93a AO (Entwurf) enthalten. § 93a AO (Entwurf) ermächtigt die Bundesregierung, mit Zustimmung des Bundesrates eine Rechtsverordnung zu erlassen, mit der Behörden und Rundfunkanstalten in bestimmten, in Abs. 1 abschließend aufgezählten Fällen allgemeine Mitteilungspflichten gegenüber den zuständigen Finanzbehörden auferlegt werden können. Damit sind nach dem Gesetzentwurf Kontrollmitteilungen nur zulässig, wenn und soweit sie in der Rechtsverordnung zu § 93a AO (Entwurf) konkretisiert sind. Auf allgemeine Amtshilfevorschriften können keine Kontrollmitteilungen mehr gestützt werden.
- Der Gesetzentwurf der Bundesregierung kommt der von den Datenschutzbeauftragten erhobenen Forderung, die übermittelnde Stelle gesetzlich zur Unterrichtung der Betroffenen zu verpflichten, insoweit nach, als er die „Verpflichtung zur Unterrichtung des Betroffenen" zum zwingenden Inhalt der Rechtsverordnung macht. Die Stellungnahme des Bundesrates zu § 93a Abs. 2 AO (Entwurf) sieht dagegen lediglich vor, in der Rechtsverordnung „abzugrenzen, in welchen Fällen die mitteilende Stelle verpflichtet ist, den von der Mitteilung Betroffenen zu unterrichten."
  Die Bundesregierung ist in ihrer Gegenäußerung zur Stellungnahme des Bundesrates auf diesen Vorschlag, in dem ich einen Rückschritt sehen würde, nicht eingegangen. Es bleibt zu hoffen, die Erkenntnis werde sich durchsetzen, daß Steuerpflichtige, die über Kontrollmitteilungen informiert sind, mit größter Wahrscheinlichkeit richtige und vollständige Steuererklärungen abgeben werden, weil sie durch die schriftliche Unterrichtung zwangsläufig daran gehindert werden, bestimmte steuerlich relevante Vorfälle einfach zu „vergessen". Dagegen erscheint mir die Vorstellung einiger Vertreter der Finanzbehörden, nur wenn die Steuerpflichtigen nicht genau wüßten, ob und wann Kontrollmitteilungen gefertigt werden, würden sie aus Furcht vor der Steuerfahndung „vorsorglich" alle Einnahmen angeben, wenig realistisch. Dann hätte es bis heute keine Fälle verheimlichter Einkünfte geben dürfen, denn bislang war es ja so, daß Steuerberater und Steuerpflichtige zwar von der Praxis der Kontrollmit-

teilungen wußten, sich aber zugleich im Ungewissen darüber waren, ob und wann im Einzelfall unter Berufung auf „Amtshilfe" Kontrollmitteilungen an die Finanzämter gesandt wurden. Tatsächlich sind viele Steuerpflichtige bewußt das Risiko eingegangen, aufgrund von Kontrollmitteilungen „erwischt" zu werden.
Einer Pressemeldung vom 19.10.1984 zufolge soll die AO-Novellierung aus dem Entwurf eines „Steuerbereinigungsgesetzes 1985" auf Betreiben von Bundestagsabgeordneten wieder herausgetrennt werden. Die AO-Änderungen sollen im nächsten Jahr „ohne Zeitdruck" überprüft werden. Die Argumente der Parlamentarier lassen sich wie folgt zusammenfassen: Das mit § 93a AO (Entwurf) vorgesehene Kontrollmitteilungsverfahren stelle das bisherige Ermittlunssystem des Steuerverfahrensrechts, das die Amtshilfe zwischen Behörden nur als Amtshilfe „auf Ersuchen" regele, auf den Kopf, indem es Behörden und Rundfunkanstalten verpflichte, in bestimmten Fällen von sich aus und ohne Einzelanfrage über bestimmte Zahlungen und Vorgänge zu unterrichten.
Richtig an dieser Argumentation ist, daß die AO 1977 nur die Amtshilfe, also Unterstützung im Einzelfall auf Ersuchen, nicht aber einen regelmäßigen Informationsfluß, wie es das Kontrollmitteilungsverfahren darstellt, kennt. Demgegenüber weist die Praxis aber eine Vielzahl von Kontrollmitteilungsverfahren auf. Diese seit Jahren geübte Praxis kann sich bestenfalls auf Verwaltungsvorschriften stützen, sie kennt keine Unterrichtung des Betroffenen und wurde, seit die ersten Bedenken laut wurden, mit § 111 AO 1977 (Amtshilfe) gerechtfertigt. Inzwischen ist wohl unbestritten, daß regelmäßige, anlaßunabhängige Mitteilungen nicht auf § 111 AO gestützt werden können. Wenn es nicht bald zu einer gesetzlichen Regelung des Kontrollmitteilungsverfahrens kommt, entfällt die Geschäftsgrundlage dafür, daß die Datenschutzbeauftragten die bisherige Praxis – für eine Übergangszeit – toleriert haben. Im Klartext: Wenn das Kontrollmitteilungsverfahren nicht umgehend auf eine gesetzliche Grundlage gestellt wird, müssen die z. Z. praktizierten Kontrollmitteilungen – als Eingriffe in das Recht auf informationelle Selbstbestimmung, die von Verfassungs wegen nur aufgrund präziser gesetzlicher Erlaubnistatbestände erfolgen dürfen – jedenfalls insoweit unterbunden werden, als die Betroffenen hiervon nicht unterrichtet werden.

3.3.2 Probleme in Hamburg

3.3.2.1 Steuergeheimnis im Verhältnis zur Prüfkompetenz des Datenschutzbeauftragten

Ich bin – ebenso wie die übrigen Datenschutzbeauftragten – im Gegensatz zu den Finanzbehörden der Ansicht, daß bereits die Auslegung der vorhandenen Rechtsvorschriften zu einem eindeutigen Ergebnis führt: Das Steuergeheimnis steht meiner Kontrollbefugnis nicht entgegen, sondern es stellt eine bereichsspezifische Datenschutzregelung dar, deren Einhaltung ich zu kontrollieren habe. Eine Regelung in der AO oder dem BDSG kann also nur klarstellenden Charakter haben.
Die Durchbrechung des Steuergeheimnisses zugunsten der Datenschutzkontrollbehörde läßt sich auf § 30 Abs. 4 Nr. 1 und Nr. 2 AO stützen. Ebenso wie der Rechnungshof, dem von keiner Finanzbehörde bisher das Kontrollrecht im Anwendungsbereich der AO bestritten worden ist, wird der Datenschutzbeauftragte, wenn er die Einhaltung des Steuergeheimnisses durch die Steuerverwaltung prüft, in einem Verfahren i.S. des § 30 Abs. 2 Nr. 1 lit. a AO tätig. Mithin dürfen ihm Steuerdaten gem. § 30 Abs. 4 Nr. 1 AO offenbart werden.
Ebenso wie der Rechnungshof kann sich der HmbDSB für seine Kontrolle auch auf ein Gesetz berufen, das die Offenbarung von dem Steuergeheimnis unterliegenden Daten ausdrücklich zuläßt. Nach § 20 Abs. 1 Satz 1 überwacht der HmbDSB die Einhaltung anderer Vorschriften über den Datenschutz, zu denen – worauf sich die Steuerverwaltung in anderem Zusammenhang beruft – auch das Steuergeheimnis zu rechnen ist, vgl. § 45 Satz 2 Nr. 1 BDSG.
In Anbetracht der Haltung der Finanzbehörde und der Tatsache, daß z. Z. nur geringe Chancen für eine Regelung durch den Bundesgesetzgeber bestehen, habe ich den Senat gebeten, eine Äußerung dahingehend abzugeben, daß auch nach seiner Auffassung

dem HambDSB bei der Durchführung seiner Kontrollen im Anwendungsbereich der AO das Steuergeheimnis nicht entgegengehalten werden könne.
Diesem Wunsch ist der Senat nicht gefolgt. In seiner Stellungsnahme zu meinem 2. TB (Senatsdrucksache Nr. 621 vom 5.6.1984, Nr. 4.1) stellt er vielmehr fest, das umstrittene Problem könne wegen der unveränderten Rechtsstandpunkte nur auf der Ebene des Bundesrechts geklärt werden. Gleichzeitig hat er seine Bereitschaft bekundet, im Rahmen seiner Gesetzesbindung meine Kontrolltätigkeit weitestgehend zu unterstützen. Das bedeutet, daß der HmbDSB gehindert ist, von Einzelbeschwerden losgelöste systematische Kontrollen bei der Steuerverwaltung vorzunehmen, mit denen die Kenntnisnahme von personenbezogenen Daten notwendigerweise verbunden ist.

3.3.2.2 Hundebestandsaufnahme

Im Januar löste eine Aktion des Finanzamtes Hamburg-Nord – Hundesteuerstelle – einen Sturm der Entrüstung aus, der bis heute noch nicht ganz verebbt ist. Monatelang erreichten mich Eingaben und Anrufe von Bürgern, die sich entrüstet, satirisch, sozialkritisch, polemisch, menschlich, juristisch und politisch mit dieser Aktion auseinandersetzten. Eine Reihe schriftlicher Anfragen wurden an den Senat gestellt, und die Bürgerschaftsfraktionen der CDU und der GAL brachten Anträge ein, mit denen der Senat zum Abbruch der Aktion aufgefordert werden sollte (Bürgerschaftsdrucksachen 11/1865 und 11/1866 vom 13. bzw. 18.1.1984). Zwei betroffene Bürgerinnen legten aus unterschiedlichen Gründen Verfassungsbeschwerden beim Bundesverfassungsgericht ein (1 BvR 170/84), die jedoch nicht angenommen wurden, weil sie für unzulässig bzw. aussichtslos gehalten wurden.

Was war geschehen?
Die Steuerverwaltung hatte erstmals von einer Vorschrift Gebrauch gemacht, die bereits am 9.1.1973 Gesetz geworden war. Sie hatte, zusammen mit den Grundsteuerbescheiden für das Jahr 1984, einen Fragebogen des Finanzamtes Hamburg-Nord versandt, mit dem die Grundeigentümer um Mithilfe gem. § 23 des Hundesteuergesetzes gebeten wurden. Mithelfen sollten die Grundeigentümer lt. Anschreiben zum Fragebogen dabei, die Daten der Hundesteuerstelle auf den neuesten Stand zu bringen, damit – zum Siege der Steuergerechtigkeit – ein aktueller Überblick über die Zahl der in Hamburg gehaltenen Hunde gewonnen werde. Die Grundeigentümer wurden um Angaben gebeten über die auf ihrem Grundstück gehaltenen Hunde und deren Halter. Sie sollten versichern, daß sie ihre Angaben nach bestem Wissen und Gewissen gemacht hätten. Eine Rechtsmittelbelehrung fehlte auf dem Fragebogen ebenso wie ein Hinweis auf die Folgen, mit denen bei Verweigerung der Beantwortung gerechnet werden mußte.

Ich bin bei meiner rechtlichen Prüfung der Aktion zu folgenden Feststellungen gekommen:
- Rechtsgrundlage für die Befragung der Grundeigentümer ist § 23 i. V. m. § 22 Hundesteuergesetz vom 9.1.1973. (Mit Gesetz vom 22.12.1983 wurde das Hundesteuergesetz geändert. Von dieser Änderung wurden §§ 22, 23 aber nicht berührt.). Der Umfang der Auskunftspflicht sowie das bei der Durchsetzung anzuwendende Verfahren sind nicht im Hundesteuergesetz selbst geregelt, vielmehr sind gem. § 1 des Hamburgischen Abgabengesetzes die Vorschriften der Abgabenordnung 1977 (AO) heranzuziehen, insbesondere § 93 AO.

- § 23 Hundesteuergesetz stammt aus einer Zeit, in der die heutigen Vorstellungen über das jedem zustehende Recht auf informationelle Selbstbestimmung noch nicht Allgemeingut waren. Mißt man die Vorschrift an den Maßstäben, die das Bundesverfassungsgericht mit seinem Urteil zum Volkszählungsgesetz 1983 definiert hat, so muß man zwar erkennen, daß es sich um eine bereichsspezifische Regelung für Datenerhebungen auf dem Gebiet der Hundesteuer handelt, die aber den Geboten der Normenklarheit und der Verhältnismäßigkeit nur in sehr unzulänglicher Weise entspricht.
  Gäbe es § 23 Hundesteuergesetz nicht, wäre beim Vollzug des Hundesteuergeset-

zes § 93 AO anzuwenden. Zwar wird in § 93 AO abstrakt jedem Bürger (nicht nur Grundeigentümern und Haushaltungs- sowie Betriebsvorständen) eine Auskunftspflicht auferlegt, aber diese Auskunftspflicht kann nur in einem konkreten, einzelne Personen betreffenden Steuerfall akut werden. Nach § 93 AO sollen Personen, die nicht Beteiligte eines Steuerverfahrens sind, nämlich erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung nicht zum Ziele führt oder keinen Erfolg verspricht. § 93 AO läßt also nicht – wie § 23 i. V. m. § 22 Hundesteuergesetz – eine allgemeine Erhebung über alle Hundehalter bei Nichtbeteiligten zu und statuiert keine allgemeine Auskunftspflicht. § 93 AO ermöglicht keine flächendeckende Erhebung mit der Folge, daß sich die Auskunftspflicht in der überwiegenden Zahl der Fälle – wie es bei der Erhebung nach §§ 22, 23 Hundesteuergesetz der Fall war – auf Personen bezieht, die ihren Hund angemeldet haben und ordnungsgemäß versteuern, für deren Steuerverhältnis also kein Anlaß zur Beweiserhebung und zur Inanspruchnahme von Dritten gegeben ist.

- Schwerer als die Zweifel an der Verhältnismäßigkeit des § 23 Hundesteuergesetz wiegen die Bedenken gegen die hier praktizierte Art des Verwaltungsvollzugs.
  Dazu vorweg einige Zahlen und Fakten:
  Ende 1983 waren in Hamburg rund 45.500
  Hunde gemeldet.
  Aufgrund der §§ 22, 23 Hundesteuergesetz wurden
  im Januar 1984 rund 190.000
  Fragebogen an die Eigentümer von Grundstücken in Hamburg versandt. (Ausgenommen waren die Eigentümer von Grundstücken, die im Sachwertverfahren besteuert werden, sowie die Stadt Hamburg als Grundeigentümer.) Zu den Befragten gehörten auch alle Wohnungseigentümer sowie die großen Wohnungsgesellschaften.
  Die Rücklaufquote erreichte bis Oktober 1984 mit 138.000
  beantworteten Fragebogen rund 75 %.
  In den zurückgesandten Bogen wurden rund 16.000
  Hunde benannt. Das ist etwas mehr als ein Drittel des gemeldeten Hundebestandes.
  Daß nur diese relativ geringe Zahl von Hunden benannt worden ist, ist im wesentlichen auf die Tatsache zurückzuführen, daß alle Wohnungsgesellschaften und viele Eigentümer großer Mietshäuser sich außerstande sahen, über Hundehalter in ihren Wohnungen Aussagen zu machen. Die Zahl der Haushalte in Mietwohnungen ist aber viel größer als die Zahl der Haushalte in selbstgenutzten Einfamilienhäusern oder Eigentumswohnungen. Folglich dürften auch die in Mietwohnungen gehaltenen Hunde zahlenmäßig einen wesentlichen Teil des Hundebestandes ausmachen. Gerade über diesen Teil waren aber mit der Erhebung keine Erkenntnisse zu gewinnen.
  Die in den Fragebogen benannten Hunde-/Hundehalterdaten wurden in einem automatisierten Verfahren mit den der Hundesteuerstelle bekannten Daten abgeglichen.
  Dabei wurden 1.966
  klärungsbedürftige Fälle ermittelt. Bei 800
  Fällen davon stellte sich heraus, daß die Hunde tatsächlich versteuert wurden. Die Differenzen beruhten auf abweichender Schreibweise u. ä.
  Bisher wurden 379
  nicht gemeldete Hunde „entdeckt", während ein Restbestand von 787
  Fällen noch der endgültigen Klärung bedarf.
  Nach Schätzung der Finanzbehörde sind etwa 2.500 der 4.800 bis Oktober erfolgten Neuanmeldungen wahrscheinlich unter dem Eindruck der Erhebung „freiwillig" erfolgt. Diese Schätzung basiert auf den Erfahrungswerten bzgl. der Neuanmeldungen jeweils nach Weihnachten aus den letzten Jahren.

  Ich enthalte mich einer Stellungnahme zu der Frage, ob die Aktion geeignet war, mehr Steuergerechtigkeit zu erreichen, und ob der Aufwand für dieses Mehr an Steuergerechtigkeit verhältnismäßig war. Festzustellen ist jedenfalls, daß diese Aktion erhebliche Mängel beim Verwaltungsvollzug aufwies. Aus dem Fragebogen wur-

de nicht hinreichend deutlich,
- daß das Auskunftsersuchen ein Verwaltungakt ist,
- ob die Auskunft für die eigene Besteuerung oder die Dritter verlangt wird,
- wie weit die Verpflichtung zur Auskunftserteilung geht, d. h., ob Nachforschungen, Befragungen, Besichtigungen zur Gewinnung von Erkenntnissen über tatsächliche Hundehaltung auf dem Grundstück anzustellen sind.

Außerdem fehlte eine Rechtsmittelbelehrung. Zwar ist eine Rechtsmittelbelehrung nicht notwendiger Bestandteil eines jeden Verwaltungsaktes, doch gerade bei einer so brisanten Aktion wie dieser mußte sich den Verantwortlichen die Vermutung geradezu aufdrängen, sie werde nicht von allen 190.000 Befragten unwidersprochen hingenommen werden. Schließlich wäre auch ein Hinweis auf möglicherweise geplante Erzwingungsmaßnahmen angezeigt gewesen. Das Fehlen solcher Hinweise führte in der Presse zu Spekulationen über Geldstrafen von DM 5.000 bis hin zur Erzwingungshaft.

Nach allem muß ich vermuten, die Finanzbehörde habe – zwar überzeugt davon, die Erhebung sei juristisch vertretbar und finanzpolitisch notwendig – aus Besorgnis um die politische Wirkung auf die Bürger aber bewußt vermieden, mit der notwendigen Klarheit über die Aktion zu informieren. Dies mußte zu Lasten der Konsequenz und der Transparenz des Verwaltungshandelns gehen.

3.4 Bauwesen

3.4.1 Karolinenviertel

Im September wurde von der Baubehörde im Karolinenviertel eine Erhebung durchgeführt, die erhebliche Unruhe bei den Betroffenen, den Bewohnern eines für die Sanierung vorgesehenen Altbauquartiers, ausgelöst hat, s. a. 1.2. Nach eingehender – nachträglicher – Prüfung der Rechtsgrundlagen für die „Vorbereitenden Untersuchungen nach § 4 Städtebauförderungsgesetz im Karolinenviertel" bin ich zu folgendem Ergebnis gekommen:

1. Die vorbereitende Untersuchung ist nach § 1 Abs. 2, § 3 Abs. 3 des Städtebauförderungsgesetzes zulässig.
2. Gem. § 3 Abs. 4 Städtebauförderungsgesetz sind die Betroffenen zur Auskunft über die Tatsachen verpflichtet, „deren Kenntnis zur Beurteilung der Sanierungsbedürftigkeit eines Gebietes oder zur Vorbereitung oder Durchführung der Sanierung erforderlich ist."
3. Gem. § 4 Abs. 1 des Gesetzes hat „die Gemeinde . . . Untersuchungen durchzuführen oder zu veranlassen, die erforderlich sind, um die Notwendigkeit der Sanierung, die sozialen, strukturellen und städtebaulichen Verhältnisse und Zusammenhänge sowie die anzustrebenden allgemeinen Ziele und die Durchführbarkeit der Sanierung im allgemeinen beurteilen zu können."
4. Das StBauFG beschreibt in § 1 Abs. 2 und § 3 Abs. 3 mit hinreichender Klarheit, welche Daten zur Feststellung städtebaulicher Mißstände erforderlich sind. Dagegen werden im Gesetz keine Anhaltspunkte dafür gegeben, welche Daten zur „Vorbereitung oder Durchführung der Sanierung" im einzelnen erforderlich sind. Insoweit mangelt es der Vorschrift an der nötigen Klarheit. Das hat zur Folge, daß bei Zweifeln an der Erforderlichkeit oder an der Verhältnismäßigkeit einzelner Fragen gegen die Zulässigkeit dieser Fragen entschieden werden muß. Ich halte im Ergebnis folgende Fragen für unzulässig, da für den Zweck nicht erforderlich:

   Frage 1: Wie haben Sie Ihre derzeitige Wohnung gefunden?
   Frage 27: Wie hoch ist das durchschnittliche monatliche Nettoeinkommen Ihres Haushalts?
   Frage 29: Wie setzt sich Ihr Haushalt zusammen nach Vorname, Nationalität, Geschlecht, Stellung der einzelnen Personen im Haushalt, Alter der einzelnen Personen?

Meine Bedenken und Anregungen sind für die eigentliche Befragungsaktion faktisch zu spät gekommen, denn nur die Petenten und weitere Personen, die mit der Beantwortung der Fragebogen gewartet hatten, konnten beim Ausfüllen ihrer Bogen berücksichtigen, daß sie zur Beantwortung der Fragen 1, 27, 29 nicht verpflichtet sind.
Um so größeres Gewicht muß ich auf die Kontrolle der sich nun anschließenden Auswertung der Erhebungsbogen legen. Ich habe mich eingehend informiert über das Konzept der „Vorbereitenden Untersuchung", über die Verteilung der Verantwortung und der Aufgabenerfüllung zwischen der auftraggebenden Baubehörde und der auftragnehmenden „Arbeitsgruppe Karolinenviertel", über die geplanten Abläufe bei der Datenverarbeitung, insbesondere über die definierten Auswertungskriterien. Ich habe darauf hingewiesen, daß eine Verwertung der Antworten auf die inkriminierten Fragen gem. § 5 Abs. 1 Nr. 1 zu unterbleiben hat. Dies hat zur Folge, daß die Auswertanweisung, die mit einem großen Anteil auf die Antworten zu Fragen 27 und 29 abstellt, überarbeitet werden muß. Die Verhandlungen mit der Baubehörde sind noch im Gange. Mein besonderes Augenmerk werde ich darauf richten, daß die Vorblätter rechtzeitig von den Fragebogen getrennt und die Bogen rechtzeitig vernichtet werden. Datenübermittlungen in nicht anonymisierter und nicht aggregierter Form sind ausgeschlossen. Damit kann ich die Besorgnis einiger ausländischer Mitbürger zerstreuen, daß die Ausländerbehörde Daten aus der Erhebung erhalten werde.

3.4.2 Wohnraumdatei

Im Berichtsjahr hatte ich mich damit auseinanderzusetzen, daß einerseits die Einführung der Fehlbelegungsabgabe in Hamburg immer weniger wahrscheinlich wurde, während auf der anderen Seite der Aufbau der „Wohnraumdatei" vorangetrieben wurde. Der Aufbau des Datenbestandes war ursprünglich in Vorbereitung des Verfahrens „Fehlbelegungsabgabe" erfolgt. Nunmehr soll die Wohnraumdatei dem Vollzug des Wohnungsbindungsgesetzes (WoBindG) sowie dazu dienen, Material für wohnungspolitische Maßnahmen des Senats zu liefern.
Z. Z. werden drei Modelle für die Fortführung der Wohnraumdatei diskutiert. Modell I sieht vor, die Wohnraumdatei objektbezogen als Wohnungsbestandsdatei zu führen. Die Fortschreibung würde eine ständige Übersicht über den Bestand an öffentlich geförderten Wohnungen und deren Struktur sicherstellen. Sie würde keine Informationen über die Nutzung des Sozialwohnungsbestandes (Informationen über die Mieter) liefern.
Nach Modell II sollen über die objektbezogenen Angaben hinaus auch die Namen der Wohnungsinhaber erfaßt werden. Daten über die Personenzahl der Haushalte würden jedoch nicht gespeichert.
Bei Modell III sollen außer den objektbezogenen Angaben und dem Namen des Wohnungsinhabers auch sein Alter, seine Staatsangehörigkeit und die Zahl der Haushaltsangehörigen gespeichert werden. Diese Form der Wohnraumdatei liefert aktuelle Informationen über den Wohnungsbestand, über die Wohnungsinhaber sowie über die Belegung der Sozialwohnungen.
Ursprüngliche Bedenken gegen die Modelle II und III habe ich zum Teil zurückgezogen, zu den verbliebenen steht eine Stellungnahme der Baubehörde noch aus. Die Modelle I und II sind im wesentlichen nach dem WoBindG gerechtfertigt, das folgende Aufgaben nennt:

§ 2 – Sicherung der Zweckbestimmung von Sozialwohnungen
§ 4 – Überwachung der Überlassung von Sozialwohnungen nur an Wohnberechtigte; Durchsetzung der Kündigung gegenüber Nichtwohnberechtigten
§ 6 – Sicherung vor Leerständen und unberechtigter Selbstnutzung
§ 12 – Sicherung vor Zweckentfremdung

Gegen die Speicherung des Namens des Wohnungsinhabers habe ich keine Einwände mehr, weil der Wohnungsinhaber auch nach berechtigtem Bezug der Sozialwohnung noch Mitwirkungspflichten nach dem WoBindG hat und gezielt angeschrieben werden können muß.
Die Speicherung des Namens des Untermieters halte ich dagegen nur dann für zulässig, wenn die untervermietete Wohnfläche mehr als die Hälfte der Gesamtwohnfläche ausmacht. Gem. § 21 WoBindG finden die Vorschriften dieses Gesetzes nämlich nur dann

auch auf Untermietverhältnisse Anwendung. Dieser Vorschrift trägt das Modell III noch nicht Rechnung, weil bisher undifferenziert verfahren wird, d. h. es wird in allen Fällen der Name des Untermieters gespeichert.
Der bei Modell III vorgesehene erweiterte Datenumfang ist für Aufgaben des WoBindG nicht erforderlich. Die Baubehörde begründet den Wunsch nach Speicherung der zusätzlichen Daten mit den ihr obliegenden allgemeinen Aufgaben, nämlich

- Versorgung der Hamburger Bevölkerung mit Wohnungen,
- Wohnungsplanung, Wohnungspflege,
- Erhebung und Vorhaltung aussagekräftiger Daten über den Sozialwohnungsmarkt als Entscheidungsgrundlage für wohnungspolitische Maßnahmen des Senats.

Das Geburtsjahr des Wohnungsinhabers soll Aussagen über die Altersstruktur der Einpersonenhaushalte ermöglichen, um erkennen zu können, wann in einem bestimmten Wohnquartier gehäuft in kurzer Zeit mit dem Freiwerden von Sozialwohnungen zu rechnen ist. Die Anzahl der Familienangehörigen soll Erkenntnisse über die Größe von Sozialmieterhaushalten liefern für die Planung von Neubauten oder die Zusammenlegung kleinerer Wohnungen. Das Speichern der Staatsangehörigkeit des Wohnungsinhabers wird damit begründet, daß der Senat ein neues Konzept für die Wohnungsvergabe plant, mit dem – auch – angestrebt wird, durch gezielte Vergabe von Sozialwohnungen eine gleichmäßige Verteilung der Ausländerhaushalte über das gesamte Stadtgebiet zu erreichen.
Die Daten für die Wohnraumdatei sollen durch Übermittlung aus dem Einwohnerdatenbestand gewonnen und fortgeschrieben werden. Ihre Erhebung erfolgt zwangsweise aufgrund des Meldegesetzes. Die Übermittlung aus dem Einwohnerdatenbestand an die für die Führung der Wohnraumdatei zuständigen Stellen erfolgt gem. § 3 der Hamburgischen Meldedatenübermittlungsverordnung „zur Durchführung des WoBindG". In § 3 der VO ist das Datum „Staatsangehörigkeit" nur mit aufgenommen worden, um die damals geplante Clearingstelle mit den notwendigen (so weit wie möglich aggregierten) Daten versorgen zu können. Im Hinblick auf die im Volkszählungsurteil für die Verwendung zwangsweise erhobener Daten aufgestellten Grundsätze (insbesondere Seiten 49/50) halte ich es für erforderlich, daß für die Führung einer Wohnraumdatei nach Modell III der Verwendungszweck einzelner Daten, soweit er über Zwecke nach dem WoBindG hinausgeht, bereichsspezifisch und präzise bestimmt wird. § 9 Abs. 1 reicht auf Dauer als rechtliche Grundlage für die mit Modell III geplante Datenverarbeitung nicht aus. Ohne eine präzise Beschreibung der Zwecke bleibt zweifelhaft, ob die personenbezogene Vorhaltung der Daten wirklich erforderlich ist und anonymisierte statistische Daten (z. B. vom StaLa lieferbare blockweise Aggregate) nicht ausreichen. Die Baubehörde beruft sich auf nur vage in Aussicht genommene wohnungspolitische Maßnahmen des Senats. Datenerhebung und -verarbeitung „auf Vorrat" ist aber unzulässig. Die Erfahrungen mit der Fehlbelegungsabgabe und der Clearingstelle geben zu erheblichen Bedenken gegen die zunächst nur „auf Verdacht" bereitgehaltenen Datenbestände Anlaß.

3.4.3 Katastergesetz

Das Kataster- und Vermessungswesen ist in Hamburg gesetzlich nicht geregelt. Daher fehlt es an einer rechtlichen Grundlage für die Verarbeitung der personenbezogenen Daten im Liegenschaftsbuch, das in Hamburg in einem automatisierten Verfahren geführt wird. Ich halte auch auf diesem Gebiet eine gesetzliche Regelung für erforderlich.

3.5 Schulwesen

3.5.1 Umsetzung der Datenschutzbestimmungen im Schulbereich

Seit Aufnahme meiner Tätigkeit haben sich eine Reihe von Bürgern – Schüler, Eltern und auch Lehrer – mit Fragen und kritischen Anmerkungen zur Datenverarbeitung im Schulbereich an mich gewandt. Dies führte zu einem regen Dialog mit der BSB über Datenschutz im Schulbereich und im Ergebnis zu der Erkenntnis, daß den Schulen und anderen Dienststellen der BSB zweckmäßigerweise eine Orientierungshilfe für die Anwen-

dung der abstrakt formulierten und teilweise schwer verständlichen datenschutzrechtlichen Bestimmungen gegeben werden sollte. Diese Orientierungshilfe liegt jetzt vor. Unter der Überschrift „Datenschutz-Info" will die Schulbehörde Hinweise zur Datenverarbeitung und Datensicherung in den Schulen und Dienststellen der BSB herausgeben und in das Verwaltungshandbuch für Schulen aufnehmen. Die „Datenschutz-Info" bringt die wesentlichen Erläuterungen zur Datenerhebung und Datenverarbeitung im Schulbereich. Sie erklärt die spezifischen Begriffe des Datenschutzgesetzes und wendet diese Begriffe auf Beispiele aus dem Schulbereich an. Sie benennt eine Stelle in der BSB, mit der in Zweifelsfällen Kontakt aufgenommen werden kann. Sie weist hin auf die Rechte der Betroffenen gem. § 6 und bringt in Erinnerung, daß neben dem Datenschutzgesetz auch andere Bestimmungen über den Datenschutz existieren und zu beachten sind.
Ich halte die „Datenschutz-Info" für ein geeignetes Mittel, um das Problembewußtsein beim Umgang mit personenbezogenen Daten zu wecken und auch Mitarbeitern, für die der Umgang mit Datenschutzbestimmungen nicht zum alltäglichen Geschäft gehört, zum richtigen Handeln zu befähigen. Sie ist eine wichtige Maßnahme zur Umsetzung der Datenschutzbestimmungen in die Praxis.

3.5.2 Bereichsspezifische Datenschutzbestimmungen im Schulgesetz

Mit der Schulbehörde besteht Einvernehmen, daß eine bereichsspezifische Regelung für die Datenverarbeitung im Schulbereich erforderlich ist. Inzwischen ist in allen Bundesländern die Diskussion über die Datenverarbeitung im Schulbereich angelaufen, und die Notwendigkeit einer umfassenden bereichsspezifischen Regelung in den Schulgesetzen der Länder wird allgemein anerkannt.
Im Schulverhältnis werden durch die Schulen und die Schulverwaltung personenbezogene Daten von Schülern und Eltern aus vielen Anlässen erhoben, verarbeitet und verwertet. Schon bei der Schulaufnahme sind Angaben auf den Anmeldeformularen zu machen, werden ärztliche Einschulungsuntersuchungen durchgeführt und bei Früheinschulung oder Zurückstellung sowie bei der Überweisung in Sonderschulen weitere psychologische und ärztliche Gutachten eingeholt, die eine Fülle von personenbezogenen Daten liefern. Während der Dauer des Schulverhältnisses fallen personenbezogene Daten bei Leistungsbewertungen (Noten, Prüfungsergebnisse), Verhaltensbeschreibungen und schulischen Ordnungsmaßnahmen an. Außerdem werden Daten erhoben für die Schülerversicherung, die Schulstatistik, die Schülerbeförderung, Schul- und Elternvertretungen, Schülerzeitungen, wissenschaftliche und sonstige Befragungen.
Ein Teil dieser Daten ist zweifellos für die Erfüllung des Erziehungs- und Bildungsauftrages der Schule erforderlich. Ein anderer Teil wird nur auf freiwilliger Basis erhoben und verarbeitet werden können.
Folgende Punkte müßten im Gesetz festgelegt werden, und zwar ohne Rücksicht darauf, ob die Datenverarbeitung in Dateien oder in anderer Form erfolgt:

- Die Daten, zu deren Angabe Schüler und Erziehungsberechtigte verpflichtet sind. Dabei sind Anlaß der Datenerhebung und Zweck der Datenverarbeitung zu bezeichnen. Es muß beispielsweise geregelt werden, welche Daten bei der Einschulung und der Einschulungsuntersuchung angegeben werden müssen.
- Anlaß, Zweck und Umfang der Datenerhebung und -verarbeitung für schulische Zwecke auf freiwilliger Basis, d. h. mit vorheriger Einwilligung der Betroffenen. Hierunter fällt m. E. die Regelung der schulpsychologischen Begutachtung und Beratung.
- Zulässigkeit und Umfang der Datenerhebung für statistische Zwecke sowie für wissenschaftliche Forschungsvorhaben.
- Zulässigkeit und Umfang der Übermittlung von Daten und Weitergabe von Unterlagen.

3.6 Statistik

3.6.1 Das Volkszählungsurteil und seine Konsequenzen für die Statistik

In der öffentlichen Diskussion und in den Analysen der Datenschutzbeauftragten des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 stehen die über den Streitgegenstand, die Volkszählung 1983 und die Statistik insgesamt hinausweisenden Urteilsgründe und die Auswirkungen auf den Verwaltungsvollzug im Vordergrund des Interesses. Mit der Vorbereitung einer neuen Volkszählung rücken die Aussagen des Bundesverfassungsgerichts zur Statistik wieder mehr in den Vordergrund.

3.6.1.1 Der Inhalt des Urteils

In der Presse habe ich gelegentlich gelesen, daß das Bundesverfassungsgericht die Volkszählung 1983 verboten habe. Das ist nicht richtig. Das Bundesverfassungsgericht hat den Melderegisterabgleich und die pauschalen Ermächtigungen, Einzelangaben an oberste Bundes- und Landesbehörden sowie an die Gemeinden weiterzugeben, für verfassungswidrig erklärt und darüber hinaus ergänzende verfahrensrechtliche Vorkehrungen für Durchführung und Organisation der Datenerhebung gefordert, das Volkszählungsgesetz im übrigen aber bestätigt. In der Begründung zum Urteil hat das Bundesverfassungsgericht die Bedeutung der Statistik sogar besonders hervorgehoben:
„Die Statistik hat erhebliche Bedeutung für eine staatliche Politik, die den Prinzipien und Richtlinien des Grundgesetzes verpflichtet ist. Wenn die ökonomische und soziale Entwicklung nicht als unabänderliches Schicksal hingenommen, sondern als permanente Aufgabe verstanden werden soll, bedarf es einer umfassenden, kontinuierlichen sowie laufend aktualisierten Information über die wirtschaftlichen, ökologischen und sozialen Zusammhänge. Erst die Kenntnis der relevanten Daten und die Möglichkeit, die durch sie vermittelten Informationen mit Hilfe der Chancen, die eine automatische Datenverarbeitung bietet, für die Statistik zu nutzen, schafft die für eine am Sozialstaatsprinzip orientierte staatliche Politik unentbehrliche Handlungsgrundlage . . . " (Urteil S. 49 f).
Im Gegensatz zu der generellen Forderung, daß personenbezogene Daten ausschließlich zu ganz bestimmten und im vorhinein fixierten Zwecken verwendet werden dürfen, wird der amtlichen Statistik ausdrücklich bestätigt, daß die Verwendungs- und Verknüpfungsmöglichkeiten bei statistischen Daten nicht im voraus bestimmbar sind. Zum Ausgleich dafür müssen andere Schranken für die Arbeit der Statistik festgelegt sein. Das Bundesverfassungsgericht hat dies im Volkszählungsurteil wie folgt umrissen:
„ 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."
„Der Gesetzgeber (muß) schon bei der Anordnung der Auskunftspflicht prüfen, ob die Angaben insbesondere für den Betroffenen die Gefahr der sozialen Abstempelung (etwa als Drogensüchtiger, Vorbestrafter, Geisteskranker, Asozialer) hervorrufen können und ob das Ziel der Erhebung nicht auch durch eine anonymisierte Ermittlung erreicht werden kann."
„Zur Sicherung des Rechts auf informationelle Selbstbestimmung bedarf es ferner besonderer Vorkehrungen für Durchführung und Organisation der Datenerhebung und -verarbeitung, da die Information während der Phase der Erhebung – und zum Teil auch während der Speicherung – noch individualisierbar sind; zugleich sind Löschungsregelungen für solche Angaben erforderlich, die als Hilfsangaben (Identifikationsmerkmale) verlangt wurden und die eine Deanonymisierung leicht ermöglichen würden, wie Name, Anschrift, Kennummer und Zählerliste (vgl. auch § 11 Abs. 7 Satz 1 BStatG). Von besonderer Bedeutung für statistische Erhebungen sind wirksame Abschottungsregeln nach außen."
Und schließlich: „Erst die vom Recht auf informationelle Selbstbestimmung geforderte und gesetzlich abzusichernde Abschottung der Statistik durch Anonymisierung der Daten und deren Geheimhaltung, soweit sie zeitlich begrenzt noch einen Personenbezug aufweisen, öffnet den Zugang der staatlichen Organe zu den für die Planungsaufgaben

erforderlichen Informationen. Nur unter dieser Voraussetzung kann und darf vom Bürger erwartet werden, die von ihm zwangsweise verlangten Auskünfte zu erteilen" (Urteil S. 51 ff).

3.6.1.2 Auswirkungen des Urteils auf andere statistische Erhebungen

Das Bundesverfassungsgericht hat sich im Urteilstenor nur zum Volkszählungsgesetz 1983 geäußert. Die Begründung enthält darüber hinaus aber allgemeine Aussagen zur Datenerhebung und Datenverarbeitung in der Statistik. Deshalb muß geprüft werden, welche Auswirkungen das Urteil auf andere statistische Erhebungen hat. Diese Diskussion wird nicht ganz korrekt unter der Überschrift „Umsetzungsbonus" geführt. Einen Umsetzungsbonus hat das Bundesverfassungsgericht dem Gesetzgeber in solchen Fällen gewährt, in denen es eine Rechtsvorschrift als verfassungswidrig aufgehoben, die Anwendung für eine Übergangsfrist aber zugelassen hat, soweit dies für die Weiterführung einer funktionsfähigen Verwaltung unerläßlich ist.
Soweit es sich um die Auswirkungen des Volkszählungsurteils auf andere statistische Erhebungen handelt, betrifft dies die Frage, ob die Bindungswirkung sich auch auf andere Gesetze erstreckt, die dem Volkszählungsgesetz vergleichbare verfassungsrechtliche Mängel aufweisen. Man wird sagen können, daß es im eigenen Interesse des Gesetzgebers liegt, solche Parallel-Regelungen, die von dem Urteil nicht unmittelbar erfaßt werden, sobald wie möglich anzupassen, um das Risiko zu vermeiden, daß sie demnächst als verfassungswidrig erklärt werden. Ohne diese Problematik vertiefen zu wollen, leite ich aus dem Volkszählungsurteil folgende Konsequenzen her:

- Soweit bei statistischen Erhebungen die Weitergabe von Einzelangaben ohne konkrete Zweckbestimmung vorgesehen ist, wie es das Bundesverfassungsgericht bei der Volkszählung 1983 für verfassungswidrig erklärt hat, muß eine solche Praxis sofort eingestellt werden.
- Angesichts der vom Bundesverfassungsgericht hervorgehobenen Bedeutung der Statistik für staatliches Handeln können, aber nur für eine begrenzte Übergangsfrist, statistische Erhebungen i. ü. durchgeführt werden, auch wenn die sie anordnende Rechtsvorschrift nicht den Anforderungen des Volkszählungsurteils entspricht, insbesondere die notwendigen organisatorischen und verfahrensrechtlichen Vorkehrungen gegen die Gefahr der Verletzung des Persönlichkeitsrechts noch nicht getroffen hat, wenn wenigstens folgende Voraussetzungen erfüllt sind:

Es sind Maßnahmen eingeleitet worden, neue Rechtsvorschriften zu schaffen.
Das Erhebungsprogramm und das tatsächliche Verfahren müssen den Anforderungen des Bundesverfassungsgerichts angepaßt sein.

3.6.1.3 Novellierungsbedarf

Die Auswirkungen des Volkszählungsurteils zwingen dazu,

- das Bundesstatistikgesetz – das allgemeine, für alle statistische Erhebungen geltende Vorschriften z. B. über die Geheimhaltung und das Verfahren enthält- zu novellieren und
- alle statistischen Erhebungen mit personenbezogenen Daten darauf zu überprüfen, ob ein hinreichender Grundrechtsschutz gewährleistet ist.

Dieses Arbeitsprogramm können die zuständigen Stellen nicht binnen kurzer Frist erledigen. Es müssen daher Prioritäten gesetzt werden. Gegenwärtig wird intensiv an neuen Rechtsgrundlagen für statistische Erhebungen gearbeitet, die für das Gesamtsystem der Statistik oder für den entsprechenden Politikbereich besonders dringlich sind:
die Volkszählung,
der Mikrozensus einschließlich der EG-Erhebung über Arbeitskräfte,
die Hochschulstatistik.

3.6.2 Volkszählung

3.6.2.1 Notwendigkeit und Akzeptanz

In dem Verfahren vor dem Bundesverfassungsgericht war eine der wichtigsten Fragen, ob eine Totalerhebung wie die Volkszählung überhaupt und angesichts des derzeitigen Standes der Methoden in der Statistik erforderlich ist. Die Argumente, die die Bundesregierung und einige Landesregierungen hierzu vorgetragen haben, haben sicher die Aussagen des Bundesverfassungsgerichts

zur Statistik allgemein (siehe oben 3.6.1.1),
zur Volkszählung und
zu ihrer Durchführung als Totalerhebung im besonderen (auf die ich weiter unten noch eingehen werde), beeinflußt.

Die Bundesregierung geht davon aus, daß eine Volkszählung bald durchgeführt werden soll, und bereitet daher seit geraumer Zeit einen Entwurf für ein neues Volkszählungsgesetz vor. Die Auseinandersetzung um die Volkszählung 1983 hat aber gezeigt, daß die Notwendigkeit allein nicht ausreicht, um die Mitarbeit aller Bürger der Bundesrepublik zu gewinnen, mit anderen Worten: Akzeptanz zu erzeugen, ohne die auch ein neuerlicher Versuch zum Scheitern verurteilt wäre. Voraussetzung für Akzeptanz ist, daß die Bürger von der Notwendigkeit einer Volkszählung überzeugt werden. Das ist sicher schwierig, zumal Emotionen und vorgefaßte Meinungen eine große Rolle spielen. Bislang haben sich die Bedenken eher verstärkt; die Zahl derer, die sich an einer Volkszählung nicht beteiligen wollen, scheint weiter anzusteigen. Da hilft es wenig, wenn die Bundesregierung daran erinnert, daß das Bundesverfassungsgericht die Volkszählung für zulässig hält, und darauf hinweist, daß auch das neue Gesetz Zwangsmittel zur Verfügung stellen wird.
Um Mißtrauen abzubauen, scheint es mir nicht der richtige Weg zu sein, eine Volkszählung durchzuführen, die sich im Fragenprogramm und in der Art und Weise der Durchführung von dem im Jahre 1983 gescheiterten Vorhaben nur unwesentlich unterscheidet. Ich erinnere daran, daß bei der Volkszählung 1971 für einen Teil der Fragen eine Stichprobenerhebung erfolgte. Hinzu kommt, daß die Bürger den Nutzen einer Volkszählung nach wie vor nicht erkennen können. Eine frühzeitige und umfassende Aufklärung der Bevölkerung ist aber eine ganz wesentliche Voraussetzung dafür, daß eine neuerliche Volkszählung mit einer gewissen Aussicht auf Erfolg in Angriff genommen werden kann.

3.6.2.2 Gegenwärtiger Stand der Vorbereitungen

Das Bundesministerium des Innern hat zahlreiche Entwürfe für ein neues Volkszählungsgesetz vorgelegt, z. T. im Abstand von wenigen Tagen. Diese Entwürfe sind auch den Datenschutzbeauftragten zugeleitet worden. Die Konferenz der Datenschutzbeauftragten hat die Entwürfe Mitte Oktober erörtert, von einer gemeinsamen Stellungnahme aber abgesehen, da ihr ein vollständiger Entwurf mit Begründung noch nicht vorlag. Jeder Datenschutzbeauftragte wird sich gegenüber den zuständigen Behörden in seinem Land äußern.
Kurz vor Redaktionsschluß hat die Bundesregierung einen Gesetzentwurf beschlossen. Ich habe diese Entwurfsfassung in den folgenden Ausführungen berücksichtigt.

3.6.2.3 Kritik und Forderungen an den Gesetzentwurf der Bundesregierung

Mit dem letzten, vom Bundesministerium des Innern vorgelegten Entwurfs sind erhebliche Fortschritte bei der Erfüllung der Forderungen des Bundesverfassungsgerichts erzielt worden. Es gibt nur noch wenige Bestimmungen, die hinter den Vorstellungen der Datenschutzbeauftragten zurückbleiben; diese sind zudem von relativ geringer Bedeutung, so daß ich auf eine ausführliche Behandlung in diesem Tätigkeitsbericht verzichte. Nachstehend werden einige Forderungen aufgeführt, die im weiteren Verlauf des Gesetzgebungsverfahrens noch erörtert werden müßten.

– Es fehlt eine Vorschrift, die es ausdrücklich untersagt, Personen in den Erhebungs-

stellen einzusetzen, bei denen z. B. aufgrund ihrer Berufstätigkeit zu besorgen ist, daß Erkenntnisse aus der Erhebungstätigkeit zu Lasten der Betroffenen genutzt werden.

- Im Gesetz muß bestimmt werden, daß die Zähler die ihnen bekanntgewordenen Erkenntnisse aus der Zählertätigkeit nicht für andere Zwecke nutzen dürfen.
- Die Erhebungsvordrucke sollten in einer Anlage zum Gesetz festgelegt werden, weil einerseits auf diesem Weg die tatsächlichen Belastungen der Betroffenen für alle Beteiligten besser erkennbar werden und weil andererseits bei der Volkszählung ein Entscheidungsspielraum für die Verwaltung nicht notwendig ist.
- Eine Verstärkung der Befugnisse der Zähler gegenüber dem Volkszählungsgesetz 1983 ist nicht akzeptabel. Eine Auskunftspflicht gegenüber dem Zähler kann mit der Forderung des Bundesverfassungsgerichts, dem Betroffenen eine schriftliche Beantwortung zu ermöglichen, allenfalls dann vereinbart werden, wenn sie zu der Überprüfung erforderlich ist, ob jemand seiner Auskunftspflicht genügt hat.

Im Mittelpunkt der Auseinandersetzung wird die Methodenfrage stehen. Der Gesetzentwurf des Bundesministeriums des Innern sieht eine

Totalerhebung (d. h. alle Einwohner der Bundesrepublik werden in die Erhebung einbezogen),

mit Auskunftszwang (d. h. die auskunftspflichtigen Bürger sind gesetzlich verpflichtet, die gestellten Fragen vollständig und richtig zu beantworten)

vor.

Das Volkszählungsgesetz muß neben dem Grundsatz der Normenklarheit auch dem Grundsatz der Verhältnismäßigkeit entsprechen. Dies gilt insbesondere auch für die Erhebung; eine Totalerhebung mit Auskunftszwang ist nur dann verhältnismäßig, wenn keine milderen Erhebungsformen vorhanden sind, die den Bürger weniger belasten.

Als solche kommen

Stichprobenerhebungen und

freiwillige Erhebungen

in Betracht.

Das Bundesverfassungsgericht hat im Volkszählungsurteil hierzu festgestellt:

„Es ist derzeit nicht zu beanstanden, wenn der Gesetzgeber davon ausgegangen ist, daß Erhebungen aufgrund von Stichproben auf ausnahmslos freiwilliger Basis oder eine Kombination von Voll- und Stichprobenerhebung die Volkszählung als Totalerhebung nicht zu ersetzen vermögen. Diese Alternativen zu einer Totalerhebung sind noch mit zu großen Fehlerquellen behaftet. Außerdem setzen sie verläßliche Daten über die Gesamtbevölkerung voraus, die z. T. nur periodische Volkszählungen liefern können." (S. 58 f)

Das Bundesverfassungsgericht hat allerdings hinzugefügt, daß die Würdigung auf dem gegenwärtigen Erkenntnis- und Erfahrungsstand beruht und daß daraus die Verpflichtung erwächst, bei der Anordnung einer statistischen Erhebung anhand des erreichbaren Materials zu prüfen, ob eine Totalerhebung trotz einer inzwischen fortgeschrittenen Entwicklung der statistischen und sozialwissenschaftlichen Methoden noch verhältnismäßig ist (S. 59). Das Bundesverfassungsgericht schließt seine Ausführungen zu diesem Thema mit der Feststellung ab, daß noch keine sicheren Ergebnisse vorliegen, die das Mittel der Totalerhebung schon jetzt unverhältnismäßig erscheinen lassen (S. 60).

Seit dem Urteil des Bundesverfassungsgerichts ist gerade ein Jahr vergangen, so daß nach meiner Einschätzung die Entwicklung die Aussage des Bundesverfassungsgerichts noch nicht überholt hat. Dennoch hat die Bundesregierung darzulegen, daß eine Totalerhebung mit Auskunftszwang dem Gebot der Verhältnismäßigkeit entspricht, weil es auch nach Meinung des Bundesverfassungsgerichts nicht ausreicht, lediglich darauf zu verweisen, daß Volkszählungen schon immer als Totalerhebung durchgeführt worden sind.

Im Entwurf eines Volkszählungsgesetzes wird im allgemeinen Teil der Begründung zur Notwendigkeit der Totalerhebung ausgeführt:

1. An der Einschätzung des Bundesverfassungsgerichts hat sich seither nichts geändert.
2. Auch bei Ausschöpfung aller zusätzlichen Erkenntnisquellen läßt sich kein sicheres Ergebnis dafür gewinnen, daß auf die Totalerhebung verzichtet werden könnte.

3. Dies sei auch die Auffassung des Deutschen Instituts für Wirtschaftsforschung, der Bundesanstalt für Landeskunde und Raumordnung sowie der Deutschen Gesellschaft für Soziologie.
4. Eine Vollerhebung ist nach wie vor dann erforderlich, wenn statistische Ergebnisse mit hohem Genauigkeitsgrad für die Gesamtheit der Erhebungseinheiten und in großer fachlicher und regionaler Differenzierung benötigt werden.
5. Darin liegt auch der Unterschied zwischen amtlicher Statistik und den Forschungsmethoden der Sozialwissenschaften.
6. Es sind Feststellungen über Grundgesamtheiten erforderlich, für die eine angenommene Wahrscheinlichkeit in einem bestimmten Vertrauensbereich (das wären Ergebnisse einer Stichprobe) nicht ausreicht wie z. B. bei den amtlichen Einwohnerzahlen.
7. Erst die genaue Kenntnis der Grundgesamtheiten ermöglicht es, die für Stichprobenerhebungen erforderlichen Auswahlpläne und Hochrechnungsrahmen zu erstellen.

Es wäre wünschenswert, Näheres zu den zusätzlichen Erkenntnisquellen zu erfahren, die ausgeschöpft worden sind. Den von der Bundesregierung angeführten Referenzen können andere entgegen gehalten werden, die eine gegenteilige Meinung geäußert haben. Nach meiner Ansicht sind am wichtigsten die Argumente 4. und 7.; das größte Gewicht hat dabei die Notwendigkeit von Kenntnissen der Grundgesamtheit, auf die Stichprobenergebnisse hochgerechnet werden können.

Für den gesetzlichen Auskunftszwang werden in der Begründung folgende Argumente genannt:
1. Es liegen keine sicheren Erkenntnisse vor, nach denen Erhebungen mit freiwilliger Auskunftserteilung eine ausreichende Ergebnisqualität hätten.
2. Die Ergebnisqualität hängt von der Höhe der Antwortquote ab. Aus der empirischen Sozialforschung ist bekannt, daß bei Erhebungen mit freiwilliger Auskunftserteilung auch bei Antwortanreizen wie Prämien eine erhebliche Zahl von Antwortausfällen zu verzeichnen ist.
3. Durch die zu erwartende ungleichmäßige Verteilung der Antwortausfälle sind Verzerrungen der Ergebnisse zu befürchten, deren Größe und Richtung nicht abschätzbar sind.

Auch hier hätte ich es begrüßt, wenn die Bundesregierung uns näher mit den Erkenntnissen bekannt gemacht hätte, die nach ihrer Einschätzung nicht gesichert sind. Das Argument mit den Antwortausfällen ist nicht zu widerlegen; nur wird dabei eines übersehen: Die Ergebnisqualität besteht aus Vollständigkeit und Richtigkeit. Mit einem gesetzlichen Auskunftszwang kann die Vollständigkeit vielleicht nahezu erreicht werden, aber es besteht – bei widerstrebenden Auskunftspflichtigen – keine Gewähr für die Richtigkeit der Antworten, die i. ü. nicht kontrolliert werden kann. Bei freiwilliger Auskunftserteilung wird die Vollständigkeit mit Sicherheit nicht erreicht, aber es besteht Hoffnung, daß die Antwortenden wenigstens die Wahrheit sagen. Dieses Dilemma sollte die Bundesregierung deutlich machen und ihre Entscheidung für den Auskunftszwang begründen (etwa damit, daß Auskunftspflichtige aus Bequemlichkeit doch richtige Antworten geben).
Im übrigen muß dargelegt werden, ob nicht für einzelne Erhebungseinheiten oder Erhebungsmerkmale, z. B. für die Angaben über den Lebensunterhalt, die Ausbildung, den Weg zur Arbeitsstätte und die berufliche Tätigkeit sowie für einen Teil der Angaben für die Wohnungszählung eine Repräsentativerhebung ausreicht, die auch auf freiwilliger Grundlage durchgeführt werden könnte.

3.6.3 Mikrozensus

In den Jahren 1983 und 1984 ist der Mikrozensus nicht durchgeführt worden. Der Grund für die Aussetzung in 1983 war die Aussetzung der Volkszählung durch das Bundesverfassungsgericht im April 1983; es sollte das Urteil des Bundesverfassungsgerichts abgewartet werden. 1984 ist der Mikrozensus ausgesetzt worden, weil die Durchführung aufgrund eines Gesetzes, das den im Volkszählungsgesetz aufgestellten Anforderungen nicht entspricht, mit zu großen Risiken verbunden gewesen wäre.

Das für den Mikrozensus federführende Bundesministerium des Innern hat im Oktober einen Entwurf für ein Mikrozensusgesetz vorgelegt, der nach den vorliegenden Informationen zwar einen gewissen Abschluß der Überlegungen im Ministerium darstellt, aber noch keine Begründung enthält. Dennoch habe ich ihn zur Grundlage meiner Ausführungen gemacht.

3.6.3.1 Notwendigkeit des Mikrozensus

Die Notwendigkeit des Mikrozensus zur Fortschreibung der Ergebnisse von Großzählungen und als Grundlage für Planungen und politische Entscheidungen wird – soweit ich übersehen kann – von niemandem in Frage gestellt. Umstritten ist die methodische Frage, ob er mit Auskunftszwang oder auf freiwilliger Basis durchgeführt werden soll; hierzu werde ich mich weiter unten äußern.

3.6.3.2 Kritik am Gesetzentwurf

Der vom Bundesministerium des Innern vorgelegte Gesetzentwurf trägt den Anforderungen weitgehend Rechnung, die sich aus dem Volkszählungsurteil des Bundesverfassungsgerichts ergeben. Ich habe lediglich Punkte von untergeordneter Bedeutung zu kritisieren, die ich aber gleichwohl an dieser Stelle referiere, weil damit zu rechnen ist, daß der Entwurf für ein Mikrozensusgesetz aus der Mitte des Bundestages eingebracht wird, so daß für mich keine andere Gelegenheit mehr besteht, meine Kritik in das Gesetzgebungsverfahren einzubringen.

1. Die Vorschrift über Hilfsmerkmale ist nicht vollständig. In der Aufzählung fehlen Angaben zur Organisation und Durchführung der Zählung wie z.B. Anzahl der Erhebungspapiere je Haushalt, Befragungserfolg oder Grund für fehlende Angaben, befragte Person, Teilnahme an einzelnen Erhebungsteilen. Ferner fehlt das (Hilfs-) Merkmal „Nummer des Auswahlbezirkes", das in einer anderen Vorschrift desselben Gesetzentwurfs genannt wird.

   Vor allem muß in der Vorschrift klargestellt werden, daß die Hilfsmerkmale nur von Stellen verwendet werden dürfen, die für die Durchführung des Mikrozensus zuständig sind.

2. In der Vorschrift über die Interviewer fehlen Regelungen über die Aufbewahrung der Erhebungspapiere durch den Interviewer bis zur Abgabe an das Statistische Landesamt.

3. Das Recht der Interviewer, bestimmte Angaben selbst in die Erhebungsvordrucke einzutragen, darf sich allenfalls auf die Organisationsunterlagen und nicht auf Erhebungsvordrucke beziehen, in die die für statistische Zwecke vorgesehenen Erhebungsmerkmale einzutragen sind.

4. Der Gesetzentwurf enthält keine Festlegung der Erhebungsvordrucke. Es ist unverzichtbar, daß die Erhebungsvordrucke einschl. der Hilfspapiere entweder im Gesetz (durch Anlagen) selbst oder durch eine Verordnung aufgrund einer entsprechenden Ermächtigung festgelegt werden.

5. Einzelne Erhebungsmerkmale sind zu unbestimmt (Beispiele: „Gründe für den Unterschied" zwischen der üblichen und der in der Berichtswoche geleisteten Arbeitszeit, „Art und Grund der Arbeitswoche", „Art des überwiegenden Lebensunterhalts"). Ich bezweifle, daß eine weitergehende Konkretisierung im Gesetz selbst möglich ist. Das kann nur im Fragebogen geschehen; dadurch wird aber die Notwendigkeit unterstrichen, den Fragebogen durch das Gesetz festzulegen.

3.6.3.3 Auskunftszwang oder Freiwilligkeit

Die Frage, ob die Erhebung unter Auskunftszwang oder auf freiwilliger Basis durchgeführt werden soll, ist nicht neu. Mit der Verabschiedung des z.Z. geltenden Mikrozensusgesetzes am 15. 12. 1983 hat der Bundestag die Bundesregierung u.a. aufgefordert darzulegen, „. . . in welchem Umfang Erhebungen nach dem Mikrozensusgesetz durch weniger kostenintensive und gleichwertige oder bessere Umfragemethoden ersetzt werden können. Dabei sollen auch die neuesten Erkenntnisse der empirischen Sozialforschung und die Erfahrungen mit statistischen Erhebungen im Ausland bewertet und, sofern sie auf anderen Systemen beruhen, ihre Geeignetheit für die Bundesrepublik Deutschland geprüft werden."

Ich erwarte, daß der Deutsche Bundestag die Bundesregierung bei der Beratung des Entwurfs für ein neues Mikrozensusgesetz auffordert, zumindest Teilergebnisse zu den von ihm gestellten Fragen vorzulegen. Dabei kann sich die Bundesregierung auch nicht damit herausreden, daß der Entwurf für ein neues Mikrozensusgesetz eine „Experimentierklausel" enthält, die umfangreiche Testerhebungen vorsieht. Erst wenn die Bundesregierung das heute schon vorhandene Material vorgelegt hat, kann eine Diskussion über die Frage „Auskunftszwang oder Freiwilligkeit" geführt werden, deren Klärung m.E. Voraussetzung für die Weiterführung des Mikrozensus ist.

3.6.4 EG-Stichprobenerhebung über Arbeitskräfte

Die Erhebung beruht auf der Verordnung (EWG) Nr. 276/84 des Rates vom 31. 1. 1984 zur Durchführung einer Stichprobenerhebung über Arbeitskräfte im Frühjahr 1984 (Amtsblatt der Europäischen Gemeinschaft Nr. L 32, S. 6). Nach dem Recht der Europäischen Gemeinschaft gilt diese Verordnung unmittelbar in den Mitgliedsstaaten, ohne daß es einer Übernahme durch Rechtsetzung in den einzelnen Mitgliedsstaaten bedarf.

Die EG-Stichprobenerhebung über Arbeitskräfte ist auch in früheren Jahren schon durchgeführt worden; in meinem 2. TB habe ich unter Nr. 3.7.2.2 über die Erhebung im Jahre 1983 berichtet.

Auch im Jahre 1984 habe ich mich aufgrund einiger Eingaben mit der EG-Erhebung auseinandersetzen müssen. Im Vordergrund stand dabei die Frage, ob eine Auskunftspflicht besteht.

Die Bundesregierung ist der Auffassung, daß die Auskunftspflicht durch § 12 des Bundesstatistikgesetzes i.V.m. der Verordnung der EG über die Stichprobenerhebung vorgeschrieben ist. § 12 des Bundesstatistikgesetzes bestimme, daß auch bei durch EG-Recht angeordneten statistischen Erhebungen die Vorschriften des Bundesstatistikgesetzes anzuwenden seien. Damit gelte auch § 10 Abs. 1 des Bundesstatistikgesetzes, der u.a. alle natürlichen Personen zur Beantwortung der ordnungsgemäß angeordneten Fragen verpflichtet, soweit nicht die Antwort ausdrücklich freigestellt ist.

Die Datenschutzbeauftragten sind demgegenüber der Ansicht, daß die EG als Verordnungsgeber die Regelung der Auskunftspflicht ausgeklammert und der nationalen Rechtsetzung überlassen hat. Danach ist es fraglich, ob § 10 Abs. 1 des Bundesstatistikgesetzes eine tragfähige Grundlage für die Auskunftspflicht ist. Die Bestimmung des § 10 Abs. 1 fordert von dem deutschen Gesetzgeber bei jeder Rechtsvorschrift, die eine statistische Erhebung anordnet, die Prüfung und Entscheidung der Frage, ob der Bürger einer Auskunftspflicht unterworfen werden soll; in allen Fällen, in denen der Gesetzgeber eine Auskunftspflicht anordnen will, kann er dies im Hinblick auf § 10 Abs. 1 durch Stillschweigen tun. Da die EG als Verordnungsgeber aber die Auskunftspflicht gerade nicht regelt, sondern die Regelung dem nationalen Gesetzgeber hat überlassen wollen, fehlt es an einer bewußten Entscheidung des Gesetzgebers über die Auskunftspflicht.

Gemessen an den Anforderungen des Bundesverfassungsgerichts mangelt es der EG-Verordnung auch an Vorschriften über die Durchführung und Organisation der Datenerhebung und -verarbeitung. Die Bundesregierung hat hierzu die Ansicht vertreten, daß die Zeit für die Schaffung entsprechender Rechtsvorschriften zu kurz gewesen sei und der vom Volkszählungsurteil des Bundesverfassungsgerichts ausgehenden Bindungswirkung auch durch Verwaltungsanweisungen Rechnung getragen werden könne, die das tatsächliche Verfahren und die tatsächliche Organisation den Anforderungen des Bundesverfassungsgerichts entsprechend regelten. Nach Ansicht der Datenschutzbeauftragten hatte die Bundesregierung ausreichend Zeit gehabt, ergänzend zur EG-Verordnung die notwendigen Vorschriften schon für die Erhebung 1984 zu erlassen.

Der Bundesbeauftragte für den Datenschutz hat die Bundesregierung auf diese rechtlichen Bedenken hingewiesen. Die Bundesregierung hat sich trotz dieser Bedenken entschlossen, die Erhebung durchzuführen.

Bei dieser Sachlage habe ich mich darauf beschränkt, das tatsächliche Verfahren der Erhebung und Verarbeitung der Daten innerhalb der EG-Stichprobenerhebung über Arbeitskräfte zu prüfen. Maßstab hierfür ist das Urteil des Bundesverfassungsgerichts über das Volkszählungsgesetz 1983, in dem gefordert wird

1. besondere Vorkehrungen für Durchführung und Organisation der Datenerhebung und -verarbeitung während der Phase, da die Angaben noch individualisierbar sind,
2. strikte Geheimhaltung der zu statistischen Zwecken erhobenen Einzelangaben,
3. eine möglichst frühzeitige faktische Anonymisierung, verbunden mit Vorkehrungen gegen eine Deanonymisierung.

Diese Forderungen sind für die EG-Stichprobenerhebung im Statistischen Landesamt erfüllt. Die Erhebungspapiere der EG-Stichprobenerhebung werden während der Bearbeitung in Räumen aufbewahrt, die nur von wenigen Bediensteten des Statistischen Landesamtes betreten werden dürfen; diese Räume sind mit besonderen Sicherheitsschlössern gesichert. Der Personenbezug der statistischen Angaben in der EG-Stichprobenerhebung wird entfernt, wenn die Erhebungspapiere für einen Auswahlbezirk vollständig und die Daten für die Übernahme auf maschinell lesbare Datenträger signiert sind. Das Verfahren hat daher nach meiner Überzeugung keinen Anlaß zur Beanstandung geboten.

Ich habe aber die Behörde für Inneres darauf hingewiesen, daß ich einer erneuten EG-Erhebung ohne ergänzende deutsche Rechtsvorschriften widersprechen würde. Hamburg hat daraufhin bei den Beratungen des Entwurfs einer EG-Verordnung für die Erhebung 1985 auf die Dringlichkeit ergänzender deutscher Rechtsvorschriften aufmerksam gemacht. Der vom Bundesministerium des Innern vorgelegte Entwurf für ein Mikrozensusgesetz schreibt die entsprechende Anwendung des Mikrozensusgesetzes vor. Nach meiner Interpretation bedeutet diese Verweisung, daß nunmehr auch für die EG-Erhebung eine Auskunftspflicht festgeschrieben wird. Es bleiben allerdings Zweifel, so daß die Begründung abgewartet werden muß. In der Begründung muß vor allem dargelegt werden, warum die Erhebung nicht – wie in anderen EG-Ländern – freiwillig sein kann.

3.6.5 Hochschulstatistik

3.6.5.1 Die gegenwärtige Regelung

Die Hochschulstatistik wird gegenwärtig durch das Bundesgesetz über eine Statistik für das Hochschulwesen (Hochschulstatistikgesetz – HStatG) in der Fassung vom 21.4.1980 geregelt. Gemessen an den Anforderungen des Bundesverfassungsgerichts im Volkszählungsurteil ergeben sich folgende wesentliche Probleme:

- Die Daten über die Studenten und Prüfungskandidaten werden personenbezogen erhoben und gespeichert, weil eine Verlaufsstatistik aufgestellt werden soll. Dabei ist die Verlaufsstatistik für Prüfungskandidaten im HStatG nicht ausdrücklich geregelt.

- § 15 Abs. 2 HStatG läßt die Weitergabe von Einzeldaten an die fachlich zuständigen obersten Bundes- und Landesbehörden sowie an die von ihnen bestimmten Stellen und Personen zu; außerdem wird die Weiterleitung von Einzelangaben für wissenschaftliche Zwecke zugelassen, ohne daß Empfänger bestimmt werden.

- § 15 Abs. 3 HStatG läßt die Verwendung von personenbezogenen Daten, die im Rahmen der Hochschulstatistik erhoben worden sind, für verwaltungsinterne Zwecke der Hochschule zu.

- Es fehlen die vom Bundesverfassungsgericht geforderten organisatorischen und verfahrensmäßigen Vorkehrungen.

3.6.5.2 Personenbezogene Erhebung und Speicherung

Die personenbezogene Erhebung und Speicherung von Daten über Studenten und Prüfungskandidaten ist ein Eingriff in das Recht auf informationelle Selbstbestimmung, der nur im überwiegenden Allgemeininteresse zulässig ist. Zweck der personenbezogenen Erhebung und Speicherung ist die Aufstellung einer Verlaufsstatistk, d.h. die erhobenen Daten werden jeweils bestimmten Personen (die zunächst Studenten, dann Prüfungskandidaten sind) zugeordnet, während der Studienzeit gespeichert und ausgewertet. Auch wenn aus den Identifikationsmerkmalen (Nachname, Vorname, Geburtsname, Geburtsdatum, Geburtsort) ein zusammengefaßter Ordnungsbegriff gebildet wird, der nicht unmittelbar die Person bezeichnet, bleiben es personenbezogene Daten, weil die dahinter stehende Person bestimmbar ist.

Im überwiegenden Allgemeininteresse liegt diese Form der Datenverarbeitung nur, wenn die Verlaufsstatistik für Planung und politische Entscheidungen im Hochschulwesen unverzichtbar ist. Daran bestehen erhebliche Zweifel.

- Der Referentenentwurf für ein neues Hochschulstatistikgesetz sieht eine Verlaufsstatistik nicht mehr vor.

  In der Begründung wird der Verzicht auf die Verlaufsstatistik mit verfassungsrechtlichen Bedenken (Verwendung eines Personenkennzeichens oder eines entsprechenden Substituts) und mit der Entwicklung der statistischen und sozialwissenschaftlichen Forschungsmethoden in den letzten Jahren begründet, die es zweifelhaft erscheinen lassen, ob die Verlaufsstatistik noch verhältnismäßig ist.

- Obwohl die Daten über Studenten und Prüfungskandidaten in der Vergangenheit personenbezogen erhoben worden sind, sind bisher keine Verlaufsstatistiken aufgestellt worden. In Hamburg ist in diesem Jahr erstmalig versucht worden, die Daten aus mehreren Semestern zusammenzuführen; dabei hat sich eine hohe Zahl von Fehlern ergeben, deren Bereinigung kaum möglich erscheint. Schon die Tatsache des faktischen Verzichts auf die Verlaufsstatistik in der Vergangenheit, ohne daß dies zum Zusammenbruch der Planung im Hochschulwesen geführt hat, spricht dafür, daß die Verlaufsstatistik nicht unverzichtbar ist.

Ich habe aus diesen Gründen die personenbezogene Erhebung und Speicherung von Daten über Studenten und Prüfungskandidaten auch vor Inkrafttreten des neuen Hochschulstatistikgesetzes für unzulässig erklärt und habe der Behörde für Inneres empfohlen, das Verfahren sofort umzustellen.

Auch die Daten über das wissenschaftliche und künstlerische Personal sind in der Vergangenheit personenbezogen erhoben, aber nicht gespeichert worden. Der Entwurf für

ein neues Hochschulstatistikgesetz sieht vor, daß die Daten künftig nicht mehr personenbezogen, sondern als Sekundärstatistik aus den Unterlagen der Hochschulen erhoben werden.

3.6.5.3 Verwendung von Einzelangaben außerhalb der Statistik

Die Vorschriften in § 15 Abs. 2 und 3 des gegenwärtig geltenden HStatG dürften verfassungswidrig sein, weil sie

- dem Gebot der Normenklarheit nicht entsprechen (Abs. 2 enthält keine präzisen Festlegungen der Empfänger und des Zwecks, für die sie zulässigerweise Daten erhalten dürfen) und

- tendenziell Unvereinbares untereinander vermischen (Abs. 3 läßt zu, daß die für Statistik erhobenen Daten auch für den Verwaltungsvollzug verwendet werden).

In Hamburg ist von der Ermächtigung des § 15 Abs. 2 HStatG kein Gebrauch gemacht worden und wird auch künftig kein Gebrauch gemacht werden.

Nach meinen Feststellungen werden die für die Hochschulstatistik erhobenen Daten nicht für den Verwaltungsvollzug genutzt, so daß auch § 15 Abs. 3 HStatG nicht angewendet wird. An der Universität Hamburg werden die Daten für den Verwaltungsvollzug und für die Hochschulstatistik zwar in einem gemeinsamen automatisierten Verfahren gespeichert, aber für die jeweiligen Zwecke getrennt verarbeitet. Diese Organisation führt dazu, daß die Daten, die für beide Zwecke erforderlich sind, nur einmal gespeichert werden. Hiergegen sind keine Bedenken zu erheben.

3.6.5.4 Organisatorische und verfahrensmäßige Vorkehrungen

Nach meinen Feststellungen entsprechen die tatsächlich geübten Verfahren der Hochschulstatistik den Anforderungen des Bundesverfassungsgerichts im Volkszählungsurteil. Es bestand daher für mich kein Anlaß, die Aussetzung der Erhebungen (mit Ausnahme der erwähnten Verlaufsstatistik) zu fordern.

3.6.5.5 Eigene Erhebungen der Hochschulen

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, daß die Hochschulen z.T. eigene statistische Erhebungen anstellen. Rechtsgrundlage hierfür ist § 142 des Hamburgischen Hochschulgesetzes (HmbHG); nach dieser Vorschrift sind eigene Erhebungen zulässig,

- wenn und soweit die Ergebnisse der Hochschulstatistik nicht ausreichen oder nicht rechtzeitig vorliegen,

- wenn die Erhebungen insbesondere für die Entwicklungsplanung der Hochschule notwendig sind und

- wenn die Behörde für Wissenschaft und Forschung die Erhebung anordnet oder eine entsprechende Anordnung des Präsidenten genehmigt.

Die Hochschule für Wirtschaft und Politik hat bei verschiedenen Erhebungen über Studenten gegen Vorschriften des Hamburgischen Datenschutzgesetzes verstoßen:

- Es fehlten die Anordnungen und Genehmigungen gem. § 142 HmbHG.

- Die Fragen drangen z.T. in nicht zu rechtfertigender Weise in die persönliche Sphäre der Betroffenen ein.

- Es fehlte an einem präzisen Nachweis, daß die Fragen erforderlich sind.

- Auf den Erhebungsvordrucken fehlte der in § 9 Abs. 2 vorgeschriebene Hinweis auf die Rechtsgrundlage.

Ich habe diese Verstöße gem. § 21 beanstandet.

3.6.6 Landesstatistikgesetz

Die amtliche, d. h. durch Rechtsvorschriften angeordnete Statistik beruht in Hamburg ausschließlich auf Bundesrecht; es gibt z. Z. keine Statistik aufgrund hamburgischen Landesrechts. Die Durchführung von durch Bundesrecht angeordneten Statistiken wird durch das Bundesstatistikgesetz und auch bundesrechtliche Vorschriften für das jeweilige statistische Vorhaben geregelt. Die im Statistischen Landesamt wahrgenommenen Landesaufgaben bestehen im wesentlichen aus weiterführenden Auswertungen von Daten, die aufgrund Bundesrecht erhoben worden sind, nach speziellen hamburgischen Interessen, aus anspruchsvollen statistischen Analysen, wie der volkswirtschaftlichen Gesamtrechnung, aus der Unterstützung der planenden Verwaltung und aus Auskünften an die Wirtschaft. Hamburg setzt sich auch nicht aus selbständigen Gemeinden zusammen, deren statistische Arbeit geregelt werden muß. Es wird sorgfältig zu prüfen sein, ob Bedarf für ein Landesstatistikgesetz besteht.

3.7 Einwohnerwesen

3.7.1 Meldewesen

3.7.1.1 Automation im Einwohnerwesen

Ich habe die Grundzüge des geplanten ADV-Verfahrens in meinem 2. TB dargestellt (Nr. 3.8.1.3, S. 65). Da sich die Planungen zwischenzeitlich geändert haben, scheint es mir notwendig, den aktuellen Sachstand mit den aus meiner Sicht problematischen Punkten näher zu erläutern.
Das automatisierte Verfahren wird nicht – wie bisher geplant – in Teilen von Schleswig-Holstein übernommen. Vielmehr entwickelt Hamburg jetzt ein eigenes Verfahren, das den besonderen Gegebenheiten der hamburgischen Meldeorganisation besser Rechnung trägt. Geplant ist der Aufbau einer Datenbank, die

- in einer ersten Stufe den Datenbestand der örtlichen Einwohnerkarteien sowie einige ergänzende Daten aus dem zentralen Personenregister und
- in einer zweiten Stufe die bisher im Personenregister des Einwohner-Zentralamtes geführten Daten aufnehmen soll.

Die Einführung der ersten Stufe soll zur Folgen haben, daß

- der Publikumsservice in den örtlichen Dienststellen verbessert werden kann,
- die im Hamburgischen Meldegesetz zugelassenen regelmäßigen Datenübermittlungen, wie z. B. für Zwecke der Familienbuchführung, zur Durchführung von allgemeinen Wahlen und für statistische Zwecke weitestgehend automatisiert erfolgen können und
- die notwendigen datenschutzrechtlichen Sicherungsmaßnahmen getroffen werden können.

Die zweite Stufe soll den örtlichen Dienststellen und dem Publikum weitere Erleichterungen z. B. für den Nachweis bestimmter personenstandsrechtlicher Daten bringen, vor allem aber die Melderegisterauskünfte erleichtern.
Die Planungen werden im Rahmen einer Projektorganisation erarbeitet, an der ich beteiligt bin. Jeder Sachbearbeiter einer Einwohnerdienststelle soll einen direkten Zugriff auf die Datenbank erhalten. „Zugriff" bedeutet

- Lesen der gespeicherten Daten,
- Eingabe erhobener neuer Daten,
- Verändern der gespeicherten Daten,

wobei die Veränderung prinzipiell nur möglich wird, wenn die Daten zuvor gelesen, d. h. auf dem Bildschirm sichtbar gemacht worden sind. Die große Zahl denkbarer Zugriffe zwingt zur Ausschöpfung aller technischen und organisatorischen Möglichkeiten, um sicherzustellen, daß sich ihr Umfang auf das Maß des Erforderlichen und Zulässigen beschränkt. Diesem Erfordernis soll durch systemeigene Vorkehrungen Rechnung getragen werden, die dem Sachbearbeiter von vornherein den Zugriff auf diejenigen Teile der

Datenbank verwehren, für die er unter regionalen oder sachlichen Gesichtspunkten nicht zuständig ist.
Eine Ausnahme hiervon soll für die innerstädtischen Umzüge gelten. Es soll nämlich bei der bisher schon für den Bürger geltenden Erleichterung bleiben, daß er sich nicht förmlich abzumelden, sondern nur bei der (neu) zuständigen Einwohnerdienststelle anzumelden braucht (vgl. § 12 HmbMG). Die (neu) zuständige Dienststelle soll in diesen Fällen auf den Datensatz des Einwohners in der Datenbank unmittelbar – lesend – zugreifen dürfen, allerdings nur unter der Voraussetzung, daß sie zuvor den Umzug in das System eingibt, und auch nur in dem Umfang, in dem sie die Daten später auf dem Mikrofilm erhalten würde.
Im täglichen Publikumsverkehr wird es aber nur ausnahmsweise zu einem Direktzugriff auf die Datenbank kommen, weil daneben eine sog. COM (Computer-output on microfilm) – Lösung geplant ist. Das bedeutet, daß dem Sachbearbeiter für die laufende Arbeit im Verkehr mit dem Publikum ein – mikroverfilmter – Auszug mit den Daten seines örtlichen Zuständigkeitsbereiches zur Verfügung stehen soll, anhand dessen er den Bürger bedienen kann. Sofern das Anliegen des Bürgers zu Änderungen des Datenbestandes führt, soll der Sachbearbeiter diese notieren und – außerhalb der Publikumszeiten, damit die Wartezeiten für den Bürger kürzer werden – in das System eingeben, wobei zur Zuordnung das aus dem Mikrofilm ersichtliche Ordnungsmerkmal (§ 3 Abs. 1 HmbMG) dient.
Dieses Ordnungsmerkmal ist – um eine Personenkennziffer zu vermeiden – regional begrenzt in der Weise, daß jede Dienststelle ihre eigenen Ordnungsmerkmale vergibt, so daß ein Umzug die Vergabe eines neuen Ordnungsmerkmals zur Folge hat.
Im übrigen soll jede in das System eingegebene Veränderung oder Hinzufügung eines Datensatzes automatisch eine entsprechende Neuverfilmung zur Ergänzung des COM-Bestandes in der zuständigen Dienststelle auslösen.
Bisher war – wie in meinem 2. TB dargestellt – geplant, nur die regionalen Einwohnerkarteien der insgesamt 28 Einwohnerdienststellen in die Datenbank zu übernehmen.
Das gegenwärtige manuelle Verfahren im Einwohner-Zentralamt sollte beibehalten werden, ein Anschluß des Einwohner-Zentralamtes an das künftige automatisierte Verfahren war nicht vorgesehen. Bei den weiteren Planungen hat sich eine wesentliche Änderung ergeben: Da das Einwohner-Zentralamt auch künftig für bestimmte Aufgaben, nämlich für

- die Eintragung von Wahlausschlußgründen,
- die Eintragung von Paßversagungsgründen,
- die Eintragung von Übermittlungssperren und
- die Abmeldung von Amts wegen

zuständig sein wird, soll es hierfür auch berechtigt sein, Daten in der beabsichtigten zentralen Einwohnerdatenbank zu lesen und zu ändern. Dies bedeutet eine Änderung des bisher vertretenen Prinzips, wonach eine Recherche für Auskünfte aus fremden Beständen technisch ausgeschlossen werden sollte.
Für die Eintragung von Wahlausschluß- und Paßversagungsgründen ist diese Regelung unter Datenschutzaspekten vorteilhaft; denn bei dieser Organisation erhalten die regionalen Einwohnerdienststellen keine Kenntnis der entsprechenden Daten, die sie zur Erfüllung ihrer Aufgaben nicht benötigen. Für die anderen Fälle sollte die Notwendigkeit einer zentralen Zuständigkeit noch eingehender begründet werden. Schließlich ist vorgesehen, künftig die regelmäßigen Datenübermittlungen aus dem Melderegister, soweit irgend möglich, aus dem maschinellen Bestand vornehmen zu lassen. Heute noch manuell ausgeführte Datenübermittlungen können dann entfallen.
Im Rahmen des Projektes waren die Datensicherungsmaßnahmen nach den Anforderungen der Anlage zu § 8 Abs. 1 ein wichtiger Diskussionspunkt. Im Ergebnis entspricht die vorgesehene Lösung diesen Anforderungen. Besonders intensiv wurden Fragen der Protokollierung erörtert. Durch die Protokollierung soll erreicht werden, daß kontrolliert werden kann, ob nur berechtigte Personen die ihnen obliegenden Operationen wie Verändern und Lesen durchgeführt haben.
Es besteht Einvernehmen darüber, daß

- beim Lesen keine Protokollierung erfolgen soll, sofern die zuständige Einwohnerdienststelle tätig wird,

- eine Protokollierung auch dann entfallen kann, wenn eine unzuständige Einwohnerdienststelle liest, sich aber eine Aktion anschließt,
- das einfache Lesen durch eine unzuständige Einwohnerdienststelle dagegen zu protokollieren ist.

Sofern eine Veränderung erfolgen soll, wird in jedem Satz, der bearbeitet worden ist, der Name des Bearbeiters und das Datum der Bearbeitung vermerkt (fallbezogene Protokollierung). Das ist auch unter Datenschutzaspekten ausreichend. Insbesondere soll auf einen Nachweis für jedes einzelne Datenfeld (feldbezogene Eingabeprotokollierung) verzichtet werden, weil weder die Aufgabenstellung des Meldewesens noch die Sensibilität der Daten dies erfordert und neue Risiken, die bei einer allzu detaillierten Protokollierung entstehen könnte, vermieden werden.
Die Zugriffe des Einwohner-Zentralamtes sind in gleicher Weise zu behandeln: Löst der Zugriff eine Aktion aus, wird nichts aufgezeichnet; ansonsten erfolgt eine Protokollierung.
Das Lesen in den COM-fiches kann aus technischen Gründen nicht protokolliert werden. Dies bedeutet, daß auch dann, wenn die Daten anderer Einwohnerdienststellen gelesen werden, eine Protokollierung nicht möglich ist.

3.7.1.2 Automationsbedingte Novellierung des Hamburgischen Meldegesetzes (HmbMG)

Die Automation im Einwohnerwesen (vgl. Nr. 3.7.1.1) erfordert einige Änderungen des HmbMG. Die Behörde für Inneres hat einen Gesetzentwurf erarbeitet, der mir zur Stellungnahme vorliegt. Der Gesetzentwurf sieht insgesamt 4 Fallgruppen vor, bei denen die Einrichtung von Verfahren zum automatischen Abruf von Daten aus dem Melderegister zugelassen werden soll:
- Zugriffe der örtlichen Meldebehörden auf ihren eigenen Bestand im Rahmen ihrer Zuständigkeit,
- Zugriff bei Umzügen innerhalb Hamburgs: Die neu zuständige Meldebehörde ruft zwecks Fortschreibung die bereits gespeicherten Daten aus dem Bestand der bisher zuständigen Meldebehörde ab,
- Abruf zu bestimmten Zwecken des im Rahmen der Aufgabenverteilung notwendigen Datenaustausches zwischen der zentralen und den örtlichen Meldebehörden,
- Abruf durch die Polizei als einzige Nicht-Meldebehörde (siehe dazu Nr. 3.7.1.3).

Auf meinen Wunsch soll im Gesetz künftig dargestellt werden, daß es in Hamburg sowohl eine zentrale Meldebehörde als auch örtliche Meldebehörden gibt. Diese Klarstellung ist notwendig, denn die Existenz mehrerer organisatorisch selbstständiger Meldebehörden zwingt zu datenschutzrechtlichen Konsequenzen.
Der für das Datenschutzrecht entwickelte funktionale Behördenbegriff eröffnet nicht etwa die Möglichkeit, die durch die Verwaltungsorganisation gezogenen Behördengrenzen zu vernachlässigen. Seine Bedeutung liegt vielmehr darin, daß die im organisationsrechtlichen Sinne einheitliche Behörde sich nach innen entsprechend ihren jeweiligen Zuständigkeiten in verschiedene Behörden im funktionalen Sinne aufteilt, zwischen denen personenbezogene Daten nur unter den Voraussetzungen des Datenschutzrechts ausgetauscht werden dürfen. Die organisatorische Abgrenzung der Behörde nach außen bleibt davon unberührt und bildet ebenfalls eine Anknüpfung für die Beschränkung der Weitergabe personenbezogener Daten.
Im Gesetzentwurf werden zwar die verschiedenen Teile des Melderegisters genannt; es bleibt jedoch unklar, wie die Aufgaben des Meldewesens zwischen der zentralen und der regionalen Ebene aufgeteilt werden. Wenngleich im Gesetz nicht alle Aufgaben im einzelnen aufgeführt werden müssen – dies kann einer Zuständigkeitsanordnung vorbehalten bleiben – sollte dennoch aus Gründen der Transparenz versucht werden, die unterschiedlichen Funktionen in allgemeiner Form zu umschreiben.

3.7.1.3 On-line-Zugriff der Polizei

Eine zentrale Bedeutung im vorliegenden Gesetzentwurf kommt dem geplanten on-line-Anschluß der Polizei an die zentrale Einwohnerdatenbank zu. Es ist vorgesehen, der Polizei die Möglichkeit zu eröffnen, für Zwecke der polizeilichen Fahndung auf bestimmte

Daten direkt zugreifen zu können, und zwar auf
- Vor- und Familiennamen,
- akademische Grade,
- Anschriften einzelner bestimmter Einwohner,
- Geburts-, Ordens- und Künstlernamen,
- Tag und Ort der Geburt.
  Sofern eine Übermittlungssperre eingetragen ist, wird auch dies der Polizei mitgeteilt.

Die Frage, in welchem Rahmen und nach welchen verfassungsrechtlichen Kriterien die vorgesehenen on-line-Anschlüsse zu beurteilen sind, ist noch nicht als abschließend geklärt anzusehen. Es ist zweifelhaft, ob die Öffnung ganzer Dateien für einen direkten Zugriff auf die vom Empfänger benötigten Einzeldaten eine Einschränkung des Rechts auf informationelle Selbstbestimmung bedeutet, der nur zulässig ist, wenn es im überwiegenden Allgemeininteresse geboten ist. Dieses Kriterium haben die Datenschutzbeauftragten bei der Einführung der Maschinenlesbarkeit von Personalausweisen in den Vordergrund gestellt.
Man könnte auch der Auffassung sein, daß der Eingriff in der Datenweitergabe liegt, ohne daß es auf die Art und Weise der Übermittlung ankommt, daß also eine bestimmte Technik der Übermittlung (z. B. ein on-line-Anschluß) sich nicht als eigenständiger Eingriff darstellt. Dann kann es gleichwohl geboten sein, den mit einer bestimmten Übermittlungsart verbundenen Risiken durch erhöhte Anforderungen an die Datensicherung zu begegnen. Damit knüpft man an die im Volkszählungsurteil ausgesprochene Verpflichtung des Gesetzgebers an, bei der Nutzung der ADV mehr als früher (angemessene) organisatorische und verfassungsrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Diese Pflicht wirkt sich nicht erst bei der Ausgestaltung, sondern auch bereits bei der Auswahl eines Übermittlungsverfahrens aus.
Ich meine, daß die skizzierte dogmatische Streitfrage an dieser Stelle nicht endgültig entschieden werden muß, da es im Ergebnis nicht darauf ankommen dürfte, ob man auf das Kriterium der „Erforderlichkeit im überwiegenden Allgemeininteresse" oder das der „Angemessenheit" abstellt. M. E. ist inhaltlich immer eine Güterabwägung zwischen der Intensität und Dringlichkeit des Informationsbedarfs der Verwaltung auf der einen und den Risiken der Verletzung der Persönlichkeitsrechte der Bürger auf der anderen Seite vorzunehmen.
Dabei gehe ich allerdings davon aus, daß der Begriff der Erforderlichkeit in diesem Zusammenhang nicht so interpretiert wird, daß eine Aufgabenerfüllung ohne on-line-Verbindung nicht möglich wäre. Das würde nämlich bedeuten, daß ein Direktanschluß niemals zugelassen werden dürfte, weil es immer Alternativen gibt.
On-line-Verfahren weisen im Vergleich zu anderen Übermittlungsverfahren bekanntlich einige Besonderheiten auf. Positiv ist zu werten, daß ein Abruf aufgrund einfacher Vorkehrungen protokolliert werden kann, daß es mithin leicht möglich ist, nachträglich zu kontrollieren, wem welche Daten übermittelt worden sind, und daß es nahezu ausgeschlossen ist, die Protokollierung und damit die Kontrolle zu umgehen. Negativ fällt demgegenüber ins Gewicht, daß bei einem on-line-Anschluß keine vorherige Kontrolle möglich ist, ob die Übermittlung zulässig ist. Selbst wenn in Betracht gezogen wird, daß einer effektiven vorherigen Kontrolle bei den anderen Übermittlungsverfahren faktisch Grenzen gesetzt sind, liegt hierin ein besonderes Risiko. Die fehlende vorherige Kontrolle begünstigt die extensive Nutzung des on-line-Anschlusses, zumal die abrufende Person darauf vertrauen kann, daß eine nachträgliche Kontrolle aufgrund der Protokolle wegen der Menge der protokollierten Daten praktisch nicht stattfindet.
Der Bedarf der Polizei, auf einen bestimmten Satz von Meldedaten schnell zuzugreifen, ist im Grundsatz anzuerkennen. Die Diskussion darüber, ob und in welchem Umfang der Polizei Meldedaten in Bruchteilen von Sekunden zur Verfügung stehen müssen, ist noch nicht abgeschlossen. Auch wenn man unterstellt, daß die Polizei eine überzeugende Begründung für eine on-line-Anbindung vorträgt, so bleibt gleichwohl zu prüfen, wie etwaige Risiken für die Persönlichkeitsrechte von Bürgern zu bewerten sind. Die Gefährlichkeit hängt u. a. davon ab, auf welche Daten die Polizei mit welchen Suchbegriffen zugreifen kann. Soweit ihr – wie bei der einfachen Melderegisterauskunft – nicht mehr als

die in § 34 Abs. 1 HmbMG genannten Grunddaten einzelner bestimmter Einwohner mitgeteilt werden (Suchbegriff: Name), ist die Gefährdung als eher gering anzusehen. Die Polizei erfährt so lediglich die Anschrift einer ihr bereits bekannten Person. Dies ist ein zweckgemäßer Einsatz des Melderegisters.
Eine Erweiterung des Zugriffs auf die nach § 34 Abs. 2 HmbMG bei einer erweiterten Melderegisterauskunft mitzuteilenden Daten über „Tag und Ort der Geburt" sowie „Geburtsnamen" erscheint mir auch noch akzeptabel, sofern sie nur für die Identifizierung einer Person genutzt werden. Problematisch wird es allerdings, wenn ein Zugriff nicht nur mit dem Namen erfolgt und somit Rasterfahndungen mit anderen Suchbegriffen (wie z. B. Anschrift) nicht ausgeschlossen werden können.
Technisch könnte ein Direktzugriff auf verschiedene Art und Weise verwirklicht werden:

1. Die Polizei erhält in eigener Verantwortlichkeit eine Kopie des Melderegisters.
2. Es erfolgt ein Direktanschluß der Polizei an das Melderegister, d. h. Aufstellung von Terminals bei der Polizei. Durch den Einbau von logischen Sicherungen wäre es möglich, der Polizei nur einen begrenzten Zugriff zu gestatten.
3. Ein Teil des Melderegisters wird physisch abgesplittet und für die Polizei zur Verfügung gestellt, bleibt aber Bestandteil des Melderegisters. Die Meldebehörde bleibt also speichernde Stelle und trägt damit für jede Übermittlung an die Polizei die Verantwortung.

Ich habe der Behörde für Inneres mitgeteilt, daß nach meiner Auffassung die Lösung 1 aus rechtlichen Erwägungen ausscheiden muß, weil es nicht zulässig ist, daß die Polizei neben der Meldebehörde ein Zweitregister errichtet. Mit der Lösung 3 läßt sich eher als mit der Lösung 2 sicherstellen, daß die Polizei auf die Daten beschränkt wird, die sie für ihre Aufgabenstellung benötigt. Weiterhin muß ich darauf bestehen, daß jeder Zugriff der Polizei ohne Ausnahme protokolliert wird. Dabei ist sicherzustellen, daß die Protokolle bei der Meldebehörde verbleiben und nicht der Polizei zur Verfügung gestellt werden, um neue Gefährdungen, die durch eine Protokollierung entstehen könnten, so weit es geht auszuschließen.
Ich habe der Verwaltung deutlich gemacht, daß für mich eine Gesamt-Nutzwert-Analyse über den geplanten on-line-Anschluß der Polizei unverzichtbar ist. Darin müssen die Vor- und Nachteile des on-line-Zugriffs (einschl. des finanziellen Aspektes) denjenigen sonstiger Übermittlungsarten (insbesondere der telefonischen Auskunft) gegenübergestellt werden.

3.7.1.4 Konsequenzen aus dem Volkszählungsurteil für das HmbMG

Das Meldewesen darf nicht die Funktion einer potentiell unbegrenzten Informati sammlung oder -bereitstellung für Aufgaben anderer Behörden übernehmen. In der Formulierung des § 1 Abs. 1 HmbMG könnte dies dadurch zum Ausdruck gebracht werden, daß die Registrierung der für Zwecke der Identitätsfeststellung und des Wohnungsnachweises nicht erforderlichen Daten nur zugelassen wird, soweit es sich um bestimmte traditionelle Mitwirkungstätigkeiten der Meldebehörde (Wahlen, Lohnsteuerkartenausstellung, Personalausweise, Wehrdienst, Familienbuch) handelt oder soweit eine eigene Datenerhebung und -speicherung durch die Behörde, die die Daten zur Erfüllung ihrer gesetzlich festgelegten Aufgaben benötigt, nur mit unverhältnismäßig hohem Aufwand möglich ist.
Die Übermittlungsvorschrift des § 31 Abs. 1 Satz 1 HmbMG übernimmt derzeit fast wörtlich die Fassung der Generalklausel des § 10 Abs. 1 und entbehrt deshalb der bereichsspezifischen Präzisierung, die das Bundesverfassungsgericht für die Verwendung zwangsweise erhobener Daten fordert. Da der im Einzelfall möglicherweise entstehende Übermittlungsbedarf nicht von vornherein ermittelt werden kann, erscheint eine Konkretisierung in der Weise, daß alle denkbaren Übermittlungsempfänger und deren Aufgaben aufgeführt werden, nicht möglich. Um gleichwohl hinreichenden Schutz gegen eine unbegrenzte Verwendung personenbezogener Daten herzustellen, muß die Zulässigkeit der Datenübermittlung davon abhängig gemacht werden, daß wenigstens die Verwendung der Daten durch den Datenempfänger bereichsspezifisch präzisiert ist. Im HmbMG ließe sich dies dadurch zum Ausdruck bringen, daß Übermittlungen nach § 31 Abs. 1 Satz 1 nur zur Erfüllung gesetzlich festgelegter Aufgaben zulässig sind.

Ich bin allerdings der Meinung, daß die durch das ungsurteil veranlaßten Gesetzesänderungen im Meldewesen bis zu einer Nov g des Melderechtsrahmengesetzes zurückgestellt werden sollten. Die nach die tscheidung gebotenen Veränderungen erfordern noch eine Reihe spezieller Prü n und Erörterungen. Es wäre m. E. besser, diese Diskussion nicht jetzt unter dem Dru der Fristen des Automationsvorhabens zu führen. Dies gilt umsomehr, als die in dem Entwurf der Behörde für Inneres gezogenen Schlußfolgerungen aus dem Volkszählungsurteil von mir nicht als gelungen angesehen werden.

3.7.1.5 Hotelmeldepflicht

Einer der Bereiche des HmbMG, die mir vordringlich regelungsbedürftig erscheinen, ist die in § 27 geregelte Hotelmeldepflicht. Hier bestehen in besonders hohem Maße Bedenken, ob sie den vom Bundesverfassungsgericht formulierten Anforderungen an die Normenklarheit und Verhältnismäßigkeit entspricht. Dem Gesetz ist derzeit nicht zu entnehmen, welche die zuständige Behörde ist, der nach § 27 Abs. 3, 4 alle Hotelmeldescheine vorzulegen sind. Dies ist nicht etwa die Meldebehörde, sondern die Polizei.
Desweiteren erscheint mir problematisch, ob es noch ein verhältnismäßiger Eingriff ist, wenn Urschriften der Hotelmeldescheine immer der Polizei zu übermitteln sind. Eine so strenge Regelung ist in keinem anderen Meldegesetz vorgesehen. Alle anderen Gesetze beschränken sich darauf, Hotelmeldescheine lediglich zur Einsichtnahme bereitzuhalten (z. B. Hessen) bzw. auf besonderes Verlangen aushändigen oder übermitteln zu lassen. Ich habe Zweifel, ob es im überwiegenden Allgemeininteresse erforderlich ist, daß in Hamburg jeder Hotelgast bei der Polizei gemeldet wird. Klärungs- und regelungsbedürftig erscheint mir ferner der Umstand, daß die Hotelmeldescheine heute nach meiner Kenntnis nicht von der Polizei nach Überprüfung vernichtet werden, sondern an das Einwohner-Zentralamt weitergegeben und dort für einen bestimmten Zeitraum gespeichert werden, auch wenn der Hotelgast Hamburg längst wieder verlassen hat. Nicht geregelt ist schließlich, in welcher Weise die Polizei die Daten von Hotelgästen nutzen darf, insbesondere unter welchen Voraussetzungen die Polizei diese Daten mit ihren Fahndungslisten abgleichen darf. Eine solche Regelung müßte zweckmäßigerweise im SOG getroffen werden.

3.7.1.6 Gruppenauskunft an Parteien

Nach § 35 Abs. 1 HmbMG darf die Meldebehörde „Parteien, anderen Trägern von Wahlvorschlägen und Wählergruppen im Zusammenhang mit allgemeinen Wahlen in den 6 der Wahl vorangehenden Monaten aus dem Melderegister über die in § 34 Abs. 1 Satz 1 HmbMG bezeichneten Daten vom Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffener bestimmend ist. Die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden."
Es handelt sich also um eine besondere Form der Gruppenauskunft, mit der die Parteien folgende Daten erhalten:
- Vor- und Familienname,
- akad. Grade und
- die Anschriften.

Das Verwaltungsgericht Berlin hat Mitte Oktober 1984 entschieden, daß derartige Gruppenauskünfte an die politischen Parteien und Wählergruppen gegen den Willen der Betroffenen unzulässig sind. Nach Ansicht des Gerichtes wird durch eine derartige Praxis, die den Parteien nur die Wahlwerbung erleichtern soll, das Recht des Einzelnen auf informationelle Selbstbestimmung verletzt. Das Gericht unterstützt damit die früher schon von den Datenschutzbeauftragten erhobene Forderung, daß hinsichtlich der Gruppenauskunft an Parteien und Wählergruppen zumindest eine Widerspruchslösung für den Bürger festgelegt werden sollte. Eine solche Regelung findet sich bereits in § 35 des Hessischen Meldegesetzes und in § 35 des Bayerischen Meldegesetzes. Der Bürger ist bei der Anmeldung auf die Widerspruchsmöglichkeit hinzuweisen.
Inzwischen hat das Oberlandesgericht Berlin zwar die Entscheidung des Verwaltungsgerichts Berlin aufgehoben, gleichwohl sollte, um Zweifel an der Verfassungsmäßigkeit des § 35 Abs. 1 HmbMG auszuräumen, die Widerspruchslösung auch in Hamburg gesetzlich festgelegt werden.

3.7.2 Paß- und Perso[illegible]swesen

In meinem 2. TB ([illegible] 3.2, S. 66 f) habe ich ausführlich über die seit Jahren betriebene Einführung eines [illegible]hinenlesbaren Personalausweises und die dabei aufgetretenen Probleme unterric[illegible]t. Seither hat die Angelegenheit folgenden Fortgang genommen: Nachdem das Bundesverfassungsgericht im Volkszählungsurteil die Forderungen bestätigt hatte, auf deren Erfüllung die Datenschutzbeauftragten in mehreren Erklärungen bestanden hatten,

- die Bundesregierung müsse darlegen, daß ein mit der Maschinenlesbarkeit möglicherweise erreichbarer Sicherheitsgewinn neue Risiken für das Persönlichkeitsrecht rechtfertige,
- die Einführung neuer maschinenlesbarer Personalausweise müsse jedenfalls so lange unterbleiben, bis die – von Verfassungs wegen unerläßlichen – gesetzlichen Regelungen für die Informationsverarbeitung der Sicherheitsbehörden in Bund und Ländern getroffen seien,
- auch das Bundespersonalausweisgesetz (BPAG) selbst müsse in einer Reihe von Vorschriften an die Gebote der Normenklarheit und Verhältnismäßigkeit angepaßt werden,

deutete sich bereits Anfang 1984 an, daß das am 25.2.1983 beschlossene 4. Gesetz zur Änderung des BPAG nicht wie geplant zum 1.11. des Jahres würde in Kraft gesetzt werden können.

Der im April 1984 vom BMI vorgelegte Vorentwurf eines 5. Gesetzes zur Änderung des BPAG ließ zahlreiche Bedenken der Datenschutzbeauftragten unberücksichtigt und warf neue Fragen auf. Im Oktober schließlich verständigten sich die Fraktionen von CDU/CSU und FDP auf eine gemeinsame Entwurfsfassung, welche kurzfristig in den Bundestag eingebracht und dort am 25.10.1984 in erster Lesung beraten wurde. Gleichzeitig wurde das 4. Gesetz zur Änderung BPAG außer Kraft gesetzt.

Die neue Gesetzesvorlage läßt den Termin des Inkrafttretens offen. Angestrebt wird dies nach der Entwurfsbegründung zum 1.1.1986, sofern bis dahin auch die erforderlichen Durchführungsgesetze der Länder vorliegen.

Beim heutigen Stand der Vorbereitungen läßt sich mit Sicherheit voraussagen, daß die von den Datenschutzbeauftragten geforderten flankierenden Maßnahmen in absehbarer Zeit nicht abgeschlossen sein werden. M. E. ist dies aber Voraussetzung dafür, daß der Bundestag über ein neues Ausweissystem entscheiden kann. Völlig ausgeschlossen ist es, daß die nunmehr offenbar auch von den Koalitionsfraktionen akzeptierten Rahmenbedingungen bis zum 1.1.1986 geschaffen sein werden. Der von ihnen für das Inkrafttreten des Personalausweisgesetzes ins Auge gefaßte Termin erscheint mithin völlig illusorisch.

Im folgenden werde ich zunächst verdeutlichen, welche zusätzlichen Zweifel an der Erforderlichkeit eines neuen, maschinenlesbaren Personalausweises entstanden sind, und sodann kritisch auf § 3a Abs. 2 des jetzt vorliegenden BPAG-Entwurfs eingehen, der die Protokollierung von Fahndungsanfragen gestattet.

3.7.2.1 Erforderlichkeit eines maschinenlesbaren Personalausweises

Bislang haben es die Verantwortlichen nicht vermocht, den konkreten Nutzen der geplanten Neuerung überzeugend darzulegen und deren Notwendigkeit hinreichend zu begründen. Die alten Zweifelsfragen bleiben bestehen: Zu einer absoluten Fälschungssicherheit wird auch das neue System nicht führen. Straftäter, die sich falscher Papiere bedienen wollen, können weiterhin auf den Reisepaß oder ausländische Dokumente ausweichen. Ferner erscheint die angekündigte Beschleunigung der Grenzabfertigung mit dem weiteren Ziel zu kollidieren, die Kontrolldichte nennenswert zu erhöhen und mehr Fahndungsaufgriffe zu ermöglichen.

Neue Zweifel an der Notwendigkeit des neuen Ausweises sind hinzugekommen, seit die Bundesregierung angekündigt hat, sich für den Abbau der innereuropäischen Grenzkontrollen einsetzen zu wollen und diese Absicht im Verhältnis zu einigen Nachbarländern bereits realisiert hat. Auch im Hinblick auf das angestrebte Ziel, mit Hilfe eines maschinenlesbaren und fälschungssicheren Ausweises bestimmte Gruppen von Straftä-

tern leichter überführen zu können, hat es eine unter dem Gesichtspunkt der Verhältnismäßigkeit bemerkenswerte Auswechslung der Argumente gegeben. Während es Ende der 70er Jahre noch hieß, in erster Linie solle Terroristen die Flucht erschwert werden – welche sich jedoch bevorzugt ausländischer Personaldokumente bedienen –, ist nunmehr die Ergreifung von Scheckbetrügern und Tätern, die Kraftfahrzeuge unter falschem Namen anbieten, in den Vordergrund gerückt.
Angesicht dieser Widersprüchlichkeiten und offenen Fragen hat es den Anschein, als ob der Beweis, daß der neue Personalausweis im überwiegenden Allgemeininteresse unverzichtbar ist, nicht geführt werden kann.

3.7.2.2 Kritik am vorliegenden Gesetzentwurf

Abgesehen von der Beweislast, die die Bundesregierung nach wie vor trifft, und den noch ausstehenden Rahmenbedingungen im Sicherheitsbereich geben auch einzelne Vorschriften des BPAG-Entwurfs, vor allem § 3a Abs. 2 Anlaß zu Bedenken.
§ 3a Abs. 2 des BPAG-Entwurfs sieht die Möglichkeit vor, unter bestimmten Voraussetzungen Fahndungsanfragen personenbezogen zu protokollieren. Da solche Aufzeichnungen zur Aufklärung und Verhütung sämtlicher 73 im Katalog des § 100a StPO aufgeführten Einzeldelikte zugelassen werden sollen, ist das Ausmaß unbemerkter Eingriffe in das Persönlichkeitsrecht breiter Bevölkerungskreise (etwa bei Razzien oder an Kontrollstellen) kaum zu überblicken. Der bloße Umstand, daß jemand in eine Ausweiskontrolle hineingeraten ist, reicht also aus, dies auch zu protokollieren. Selbst wenn es nicht sehr wahrscheinlich ist, daß jemand in kurzen Abständen mehrfach Opfer einer polizeilichen Kontrolle und einer anschließenden Protokollierung wird mit der Folge, daß umfassende Bewegungsbilder entstehen können, so ändert das nichts daran, daß mit Hilfe der durch die Verwendung des Personalausweises erlangten Daten neue Datensammlungen entstehen, die – jedenfalls für einige Zeit – gespeichert bleiben und beliebig ausgewertet werden können.
Daß das Speichern von Fahndungsanfragen unter Gesichtspunkten des überwiegenden Allgemeininteresses und der Verhältnismäßigkeit nun doch erforderlich ist, muß umsomehr in Frage gestellt werden, als der BMI bislang immer betont hatte, daß Protokollieren aus polizeilicher Sicht überflüssig seien.

3.7.2.3 Weitergabe von Lichtbildern aus dem Personalausweisregister

Veranlaßt durch eine Eingabe habe ich geprüft, ob und unter welchen Voraussetzungen Paßfotos aus dem Personalausweisregister übermittelt werden dürfen. Ich bin zu dem Ergebnis gekommen, daß es derzeit keine hinreichenden Rechtsgrundlagen für derartige Übermittlungen gibt.

Bei Paßfotos handelt es sich um personenbezogene Daten, deren Weitergabe als Eingriff in die Persönlichkeitsrechte des Betroffenen anzusehen ist. Hierfür bedarf es einer gesetzlichen Grundlage, die den Anforderungen der Verhältnismäßigkeit und Normenklarheit entspricht.

Eine solche Ermächtigungsgrundlage ist nicht vorhanden: Das geltende Hamburgische Personalausweisgesetz sieht eine Weitergabe von Daten aus dem Personalausweisregister ebenso wenig vor wie das Polizei- und das Strafverfahrensrecht. Bei einer Novellierung des Hamburgischen Personalausweisgesetzes müßte also – bei Bedarf – eine Übermittlungsregelung etwa für die Fälle geschaffen werden, in denen die gesetzlichen Voraussetzungen für die Durchführung von Identitätsfeststellungen bzw. ed-Maßnahmen beim Betroffenen selbst vorliegen (2.9 nach § 81b StPO) und der ersuchenden Behörde eine Aufgabenerfüllung auf andere Weise nicht möglich ist.

Für eine Übergangszeit – zur Anpassung des geltenden Rechts an die Anforderungen des Volkszählungsurteils – kann allenfalls unter engen Voraussetzungen eine Weitergabe von Paßfotos hingenommen werden. Voraussetzung wäre, daß sich die Weitergabe im Rahmen des Zwecks bewegt, zu dem die Fotos gespeichert wurden und daß sie im

konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Verwaltungsbetriebes unerläßlich ist.

Da die Speicherung der Fotos im Personalausweisregister dem Zweck des Nachweises über ausgestellte Personalausweise dient, käme eine Weitergabe zunächst in Betracht, wenn sie etwa der Überprüfung der Echtheit von Ausweisen dienen soll.

Eine Übermittlung zu Zwecken der Identitätsfeststellung bzw. des Fahndungs- oder Erkennungsdienstes wäre allenfalls dann zuzulassen, wenn die anfordernde Stelle (z.B. die Polizei) selbst Lichtbilder vom Betroffenen anfertigen dürfte. Der Betroffene müßte jedoch für diesen Fall über die Weitergabe der Lichtbilder unterrichtet werden.

Die Behörde für Inneres hat in ihrer Stellungnahme mitgeteilt, daß vor Weitergabe eines Lichtbildes von der anfragenden Stelle eine schriftliche Erklärung verlangt wird, die benötigten Informationen könnten nicht auf andere Weise als durch die Einsichtnahme beschafft werden. Dadurch wird zugleich die Möglichkeit eröffnet, die Zulässigkeit der Einsichtnahmen nachträglich zu kontrollieren.

Um die Notwendigkeit von Datenübermittlungen aus Personalausweis- und Paßregister empirisch zu überprüfen, hat die Polizei eine Erfassung sämtlicher Ersuchen auf Einsichtnahme in der Zeit vom 15. 10. bis 14. 12. 1984 angeordnet.

3.7.3 Ausländerverwaltung

Einer der Schwerpunkte meiner Tätigkeit im Berichtszeitraum lag auf einer umfassenden Überprüfung der Informationsverarbeitung in der Abt. Ausländerangelegenheiten des Einwohner-Zentralamtes (nachfolgend Ausländerbehörde genannt), die ich bereits in meinem 2. TB (unter Nr. 3.8.3, S. 71) angekündigt hatte. Dabei habe ich eine ganze Reihe gravierender Mängel feststellen müssen, die die Ausländerbehörde – als Teil der Landesverwaltung – jedoch nur begrenzt zu verantworten hat.

Für weite Bereiche fehlt es an hinreichenden, modernen Anforderungen entsprechenden Rechtsgrundlagen für die Informationsverarbeitung. Während es für fast alle anderen Bereiche, in denen es um eine Registrierung von Einwohnern bzw. Einwohnergruppen geht (z.B. Melderegister, Kraftfahrzeugregister, Bundeszentralregister), bereits relativ dichte Regelungen gibt, die den Umfang der staatlichen Informationstätigkeit begrenzen, fehlen entsprechende gesetzgeberische Entscheidungen auf dem Gebiet der Ausländerüberwachung fast völlig. Zwar sind die Voraussetzungen, unter denen ordnungsbehördliche Maßnahmen gegen Ausländer ergriffen werden dürfen, durch das AuslG und die dazu ergangene Rechtsprechung relativ klar begrenzt. Die Sammlung von Informationen, die der Ausländerbehörde möglicherweise bei später einmal zu treffenden Entscheidungen nutzen könnten, ist durch das AuslG aber in keiner Weise eingeengt. Anstelle gesetzlich eingeschränkter Befugnisse gibt es allerdings eine Vielzahl von größtenteils wiederum bundeseinheitlich geltenden Verwaltungsvorschriften, die einen umfassenden Informationsfluß von und zur Ausländerbehörde verlangen.

Meinen abschließenden Bericht über die Prüfung der Ausländerbehörde, dessen wesentliche Inhalte ich in den nachfolgenden Punkten zusammengefaßt wiedergebe, konnte ich der Behörde für Inneres erst im Dezember übermitteln. Eine Stellungnahme lag daher bei Redaktionsschluß noch nicht vor.

3.7.3.1 Datenerhebung bei betroffenen Ausländern

Auf den nach § 21 AuslG vom Bundesministerium des Innern vorgeschriebenen Formblättern werden zu viele Daten erhoben.

Problematisch sind die verlangten Angaben zum Zweck des Aufenthalts in der Bundesrepublik, soweit sie über eine allgemeine Beschreibung dieses Zwecks hinausgehen. So

werden z.B. Angaben über Besuch, Touristenreise, Studium, Arbeitsaufnahme usw. mit Namen der Verwandten, Ausbildungsstätte, Referenzen usw. und deren Anschriften gefordert.

In der Verordnung zur Durchführung des AuslG (DVAuslG) sind in § 1 zahlreiche Befreiungen vom Erfordernis der Aufenthaltserlaubnis vorgesehen. Danach sind die oben aufgezählten Daten z.B. für Ausländer, die sich nicht länger als 3 Monate im Geltungsbereich des AuslG aufhalten und keine Erwerbstätigkeit ausführen wollen, nicht erforderlich.

Bedenklich sind die verlangten Angaben zu Ehegatten und Kindern, sofern diese im Ausland verbleiben und der Antragsteller die Frage nach einer Miteinreise verneint. Die Datenerhebung in diesen Fällen ist erst dann erforderlich, wenn tatsächliche Anhaltspunkte für eine Miteinreise oder den Nachzug von Angehörigen vorliegen. Die Erkennbarkeit des „sozialen Umfeldes" eines Antragstellers oder der Zahl der Kinder als „Nachzugspotential" sind keine im AuslG normierten Zwecke, die eine Datenerhebung im hier beschriebenen Umfang rechtfertigen können.

Keines der Formulare enthält überdies den nach § 9 Abs. 2 HmbDSG bzw. § 9 Abs. 2 BDSG vorgeschriebenen Hinweis, aufgrund welcher Rechtsvorschrift die Daten erhoben werden, bzw. auf evtl. freiwillige Angaben in dem Formular. Wünschenswert wäre darüber hinaus ein Hinweis darauf, daß die Daten regelmäßig zumindest an das AZR übermittelt werden.

3.7.3.2 Datenanlieferungen durch dritte Stellen

Dritte Stellen (wie z.B. Meldebehörden, Polizei, Staatsanwaltschaft, Gerichte, Verfassungsschutz, Sozialleistungsträger, Grenzbehörden etc.) beliefern die Ausländerbehörde in erheblichem Umfang mit Daten. Für die Übermittlungen gibt es vielfach keine Rechtsgrundlage und sie übersteigen häufig auch das Maß dessen, was erforderlich ist, bei weitem.

- Zur Übersendung von Meldescheinen an die Ausländerbehörde auf der Grundlage von § 10 Abs. 1 der HmbMeldedaten-Übermittlungsverordnung (MeldDÜV) habe ich mich bereits in meinem letzten TB geäußert (Nr. 3.8.1.1.5, S. 63). Der Senat hat in seiner Stellungnahme leider bekräftigt, daß er meinen Forderungen nicht entsprechen wolle.

- Die Polizei teilt in allen Fällen ohne Aufforderung die Tatsache der Einleitung von Ermittlungsverfahren mit. Nach Auskunft der Ausländerbehörde werden nur solche Mitteilungen von den Sachbearbeitern in die Akten aufgenommen, die diese für „interessant" halten. Eine Tilgung der Eintragung findet nicht statt.

Gesetzliche Grundlagen für diese Mitteilungen der Polizei bestehen nicht. Sie werden gestützt auf Anl. III Ziff. 7 der AuslVwV, wo es heißt:

> „Die Polizeibehörden oder Dienststellen unterrichten die Ausländerbehörde über die Einleitung eines strafrechtlichen Ermittlungsverfahrens, wegen eines Vergehens oder eines Verbrechens. Sie unterrichten die Ausländerbehörden ferner, wenn ein Ausländer wegen erheblicher Verstöße gegen die öffentliche Sicherheit oder Ordnung in Erscheinung getreten ist. Satz 2 gilt für Ordnungsbehörden entsprechend."

Da ausländerbehördliche Maßnahmen auf die schlichte Tatsache der Einleitung polizeilicher Ermittlungen gegen einen Ausländer regelmäßig nicht gestützt werden können (vgl. BVerfG NVwZ 1983, 667), halte ich Übermittlungen im praktizierten Umfang nicht für erforderlich und somit für unzulässig.

Wie mir die Ausländerbehörde mitgeteilt hat, sieht sie selbst außer in den Fällen des Nr. 18a zu § 10 AuslVwV keine Gründe, die die unbegrenzte Aufnahme aller Mitteilungen über Ermittlungsverfahren erforderlich machen. Nr. 18a zu § 10 AuslVwV behandelt die Ausweisung vor Abschluß eines Strafverfahrens. Diese kommt dann in Betracht, wenn das öffentliche Interesse die sofortige Vollziehung der Ausweisung fordert und die Durchführung des Strafverfahrens nicht geboten erscheint. Da die Staatsanwaltschaft allein Herr des Ermittlungsverfahrens ist, liegt die Entscheidung über die Durchführung des Strafverfahrens bis zur Erhebung der öffentlichen Klage bei ihr (vgl. Nr. 18 zu § 19 AuslVwV, wonach eine Ausweisung zu unterlassen ist, sofern die StA widerspricht). Mitteilungen über Ermittlungsverfahren können daher auf die wenigen Fälle beschränkt werden, in denen die StA die Voraussetzungen des Nr. 18a zu § 10 AuslVwV bejaht. Das Mitteilungsverfahren wäre insoweit gesetzlich zu regeln.

Die Speicherung der hier fraglichen Mitteilungen in den Ausländerakten stellt eine grundrechtsverletzende Datenhaltung auf Vorrat dar, die überdies auch keinen im AuslG normierten Zweck verfolgt. Eine Einstellung dieses Verfahrens würde daher die Effizienz der Ausländerverwaltung in keiner Weise beeinträchtigen. Ziff. 7 der Anlage III zur AuslVwV – die keine Rechtsnormqualität besitzt – kann daher nicht länger herangezogen werden, um diese Mitteilungspraxis zu stützen.

In allen Fällen, in denen eine Mitteilung über eine Verurteilung erfolgt ist, sind besondere Vorkehrungen hinsichtlich der Tilgungsfristen der §§ 43 ff BZRG zu treffen, was gegenwärtig unterbleibt. Da die Länge der Tilgungsfristen in § 44 BZRG eindeutig festgelegt ist, könnte auf der Mitteilung über die Verurteilung der voraussichtliche Eintritt der Tilgungsreife vermerkt werden. Sollten Zweifel bestehen, ob die Eintragung getilgt ist, könnten diese durch eine Anfrage beim BZR ausgeräumt werden.

Sofern die Entfernung der Mitteilung über die Verurteilung organisatorisch nicht durchführbar sein sollte, müßte wenigstens der Eintritt der Tilgungsreife bzw. die vollzogene Tilgung im BZR in einer Weise vermerkt werden, die das Verwertungsverbot nach § 49 BZRG für jeden, der dienstlichen Umgang mit der Akte hat, deutlich macht.

- Mitteilungen des Verfassungsschutzes an die Ausländerbehörde erfolgen in Einzelfällen im Zusammenhang mit § 6 Abs. 2, 3 AuslG (Einschränkung und Untersagung der politischen Betätigung; unerlaubte politische Betätigung).

  Bis zur dringend notwendigen Novellierung der Verfassungsschutzgesetze (vgl. die Entschließung der Konferenz der Datenschutzbeauftragten zu den Auswirkungen des Volkszählungsurteils Ziff. 2.2) mag als Rechtsgrundlage für diese Mitteilungen § 3 Abs. 1 i.V.m. § 6 Abs. II HmbVerfSchG und § 3 Abs. 1 i.V.m. § 4 Abs. 1 BundesVerfSchG in Betracht kommen.

  Es muß aber wenigstens sichergestellt sein, daß nur gerichtsverwertbare Tatsachen, die einen unmittelbaren Bezug zum Regelungsbereich des § 6 Abs. 2, 3 AuslG haben, übermittelt werden.

- Justizbehörden teilen den Ausländerbehörden in Strafsachen gegen Ausländer gem. Nr. 42 MiStra – über die polizeilichen Mitteilungen hinaus – noch folgendes mit:

  "1. die Erhebung der öffentlichen Klage
  2. den Ausgang des Verfahrens, wenn eine Mitteilung nach 1. zu machen war.
  Bei den Mitteilungen ist auf Tatsachen hinzuweisen, aus denen sich ergibt, daß sich der Ausländer ohne die nach § 2 des AuslG erforderliche Aufenthaltserlaubnis im Bundesgebiet einschl. Berlin aufhält."

  Auch für diese Übermittlungen gibt es keine ausdrückliche gesetzliche Grundlage. Nach der übereinstimmenden Auffassung aller Datenschutzbeauftragten (vgl. Stellungnahme zur MiStra, 2. TB, Nr. 3.13.1.1, S. 94) sind die genannten Mitteilungen auf

die Fälle zu beschränken, die Maßnahmen der Ausländerbehörde begründen können. Auf die Mitteilung der Klageerhebungen ist somit, da ausländerbehördliche Maßnahmen grundsätzlich nur auf der Grundlage eines Urteils erfolgen dürfen, zu verzichten. Ausnahmen gelten nur dann, wenn begründete Anhaltspunkte dafür vorliegen, daß die Ausländerbehörde Maßnahmen nach Nr. 18a AuslVwV zu § 10 AuslG treffen muß, bevor das Verfahren abgeschlossen ist. Hier würde es allerdings ausreichen, wenn nur der Anklagesatz, nicht jedoch das wesentliche Ergebnis der Ermittlungen mitgeteilt würde.

- Von den Arbeitsämtern erhält die Ausländerbehörde zwar keine Mitteilungen über Leistungen, wohl aber Informationen über Erteilung, Widerruf und Ablehnung einer Arbeitserlaubnis. Eine Durchschrift dieser Bescheide wird zur Akte genommen.

  Die Zulässigkeit dieser Datenübermittlungen beurteilt sich, da die Arbeitsämter dem Sozialgeheimnis nach § 35 SGB-I unterliegen, nach den §§ 67 ff SGB-X.

  Nach § 71 Abs. 2 SGB-X ist die Offenbarung personenbezogener Daten eines Ausländers zulässig, um den Ausländerbehörden ausländerrechtlich zulässige Maßnahmen aufgrund der in § 10 Nr. 7, 9, 10 und § 11 des AuslG bezeichneten Umstände zu ermöglichen. In Fällen des Widerrufs und der Ablehnung der Arbeitserlaubnis kann eine Mitteilung durch § 71 Abs. 2 SGB-X somit nur dann gerechtfertigt sein, wenn die Versagungsgründe nach pflichtgemäßem Ermessen des Arbeitsamtes auch zu einer Ausweisung nach § 10 Nr. 7, 9, 10 und § 11 AuslG führen können.

  Die generelle Mitteilung von Daten zur Arbeitserlaubnis wird von § 71 Abs. 2 SGB-X indessen nicht erfaßt.

  Nach § 69 Abs. 1 Nr. 1 SGB-X ist die Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Aufgabe der Arbeitsämter als Sozialleistungsträger. Zwar ist die Erteilung der Arbeitserlaubnis abhängig vom Bestehen der Aufenthaltserlaubnis (vgl. § 5 Abs. 1 Nr. 1, § 8 Abs. 1 Nr. 1 Arbeitserlaubnis-VO). Umgekehrt hat aber die Frage, ob und in welcher Form eine Arbeitserlaubnis erteilt wurde, – außer in den in § 71 Abs. 2 SGB-X genannten Fällen – nach dem Ausländergesetz keine unmittelbare Relevanz für die Aufenthaltserlaubnis.

  Es kann daher nicht festgestellt werden, daß die generelle Mitteilung von Daten zur Arbeitserlaubnis der Erfüllung der gesetzlichen Aufgabe der Arbeitsämter dient. Auch § 69 Abs. 1 Nr. 1 SGB-X stellt somit keinen Offenbarungstatbestand dar, der die Übermittlung von Daten zur Arbeitserlaubnis an die Ausländerbehörde rechtfertigen würde.

- Die Gesundheitsämter teilen den Ausländerbehörden nach der regelmäßig vor Erteilung einer Aufenthaltsgenehmigung durchgeführten amtsärztlichen Untersuchung mit, daß keine bzw. welche Bedenken gegen die Erteilung einer Aufenthaltserlaubnis bestehen.

  Die amtsärztliche Untersuchung selbst ist ebenso wie die Mitteilung des Untersuchungsergebnisses nicht im Ausländergesetz, sondern lediglich in Nr. 31 zu § 21 AuslVwV geregelt.

  Auch der Amtsarzt unterliegt der ärztlichen Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB; eine Offenbarung des Untersuchungsergebnisses ist daher nur zulässig, sofern eine besondere Befugnis hierzu besteht. Eine befugte Offenbarung liegt nach § 10 Abs. 2 AuslG in Fällen des § 10 Abs. 1 Nr. 9 vor; danach dürfen der Ausländerbehörde die erforderlichen Auskünfte mitgeteilt werden, wenn ein Ausländer wegen Gefährdung der öffentlichen Gesundheit oder Sittlichkeit ausgewiesen werden soll.

Nach dem Wortlaut des § 10 Abs. 2 i.V.m. Abs. 1 Nr. 9 AuslG erfolgt also für die Mehrheit der Fälle, in denen kein Bezug zu einer Ausweisung besteht, die Offenbarung von Daten, die der ärztlichen Schweigepflicht unterliegen, unbefugt.

Daher sollte vor Weitergabe des amtsärztlichen Untersuchungsergebnisses stets die schriftliche Schweigepflichtentbindungserklärung vom Betroffenen verlangt werden.

3.7.3.3 Speicherung der Daten/Aktenführung

Die o.g. außerordentlich vielfältigen Übermittlungen führen dazu, daß bei der Ausländerbehörde eine sehr große Anzahl unterschiedlichster Daten gespeichert wird. Es ist zwar nicht zu bestreiten, daß die Ausländerbehörde zur Erfüllung der ihr durch das AuslG zugewiesenen ordnungsbehördlichen Aufgabe der Ausländerüberwachung darauf angewiesen ist, Erkenntnisse über einzelne Ausländer zu sammeln. Doch muß der Umfang dieser Datensammlungen aus verfassungsrechtlichen Gründen begrenzt werden.

Das grundgesetzlich verbürgte allgemeine Persönlichkeitsrecht gilt – worauf ich bereits in meinem 2. TB (unter Nr. 3.8.3, S. 71) hingewiesen habe – auch für Ausländer. Auch für sie sind die Feststellungen relevant, die das BVerfG in seinem Volkszählungsurteil getroffen hat, daß nämlich ein Zwang zur Abgabe personenbezogener Daten – und dem steht die Datenweitergabe durch dritte Stellen ohne Einwilligung des Betroffenen gleich – voraussetzt, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die gesammelten Angaben für diesen Zweck geeignet und erforderlich sind.

Das BVerfG hat ferner deutlich gemacht, daß die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken mit diesen Grundsätzen nicht zu vereinbaren wäre.

Aus diesen Gründen ist die schnelle Schaffung präziser gesetzlicher Grundlagen – auf Bundesebene –, aber auch die Bereinigung der Ausländerakten von nicht erforderlichen Informationen dringend geboten.

3.7.3.4 Mitteilungen der Ausländerbehörde an dritte Stellen

– Die Ausländerbehörde übermittelt dem Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFL) Daten über jeden Asylantrag und dessen Änderungen. Nach § 8 Asylverfahrensgesetz (AsylVfG) ist ein Asylantrag bei der Ausländerbehörde zu stellen. Aus dem formlos gestellten Antrag werden die Daten formularmäßig übertragen (Niederschrift zu einem Asylbegehren). Rechtsgrundlage für die Übermittlung an das Bundesamt ist § 8 Abs. 5 AsylVfG. Problematisch an dem Formular „Niederschrift zu einem Asylbegehren" erscheinen die Fragen zu den Punkten 12 (keine Papiere) und 15 (Grenzübergang unter Umgehung der Grenzkontrollen bei . . .).

  Da nach § 47 Abs. 1 Nr. 1 AuslG die Einreise in den Geltungsbereich des AuslG ohne Paß etc., strafbar bzw. nach § 48 Abs. 1 Nr. 1 AuslG der unbefugte Grenzübertritt eine Ordnungswidrigkeit darstellt, wird hier u.U. eine nach Strafverfahrensrecht unzulässige Selbstbezichtigung verlangt.

  Die Ausländerbehörde gibt dem BAFL ferner Polizeiberichte weiter, sofern diese Hinweise darauf enthalten, daß sich ein Ausländer bereits unter anderen Personalien in der Bundesrepublik aufgehalten hat.

  Diese Übermittlungen sind zur Identitätsfeststellung durch das BAFL (vgl. § 13 Abs. 1 AsylVfG) erforderlich. Sofern keinerlei Zweifel an der Identität des Betroffenen bestehen, stellt § 13 AsylVfG allerdings keine Rechtsgrundlage für die Weitergabe des Polizeiberichts dar.

- An die Polizei erfolgen Übermittlungen nach meinen Feststellungen in folgenden Fällen:
  Die Ausländerbehörde veranlaßt eine Ausschreibung in INPOL zu Zwecken der Festnahme oder Inverwahrnahme für

  1. Ausländer, gegen die eine unanfechtbare Ausweisungs- bzw. Abschiebungsverfügung vorliegt, wenn die zum Verlassen des Bundesgebiets bestimmte Frist abgelaufen ist;
  2. Ausländer, die abgeschoben worden sind;
  3. Ausländer, bei denen die Voraussetzungen für eine Ausweisung oder Abschiebung vorliegen, wenn sie sich nicht mehr im Bundesgebiet aufhalten oder ihr Aufenthalt unbekannt ist.

  Zu Zwecken der Aufenthaltsermittlung veranlaßt sie Ausschreibungen für Ausländer, die aufgrund des Verdachts der illegalen Arbeitsaufnahme zurückgewiesen oder zurückgeschoben worden sind und bei denen zu vermuten ist, daß sie versuchen werden, aus diesem Anlaß erneut in die Bundesrepublik einzureisen.

  Auch für diese Übermittlungen erscheint mir eine präzise Gesetzesgrundlage dringend erforderlich, die die Übermittlungen auf die Zwecke „Ausschreibung zur Festnahme/Inverwahrnahme" und „Aufenthaltsermittlung" begrenzt.

  Nach Nr. 9 zu § 6 AuslVwV hat die Ausländerbehörde Verbindung mit den zuständigen Polizeibehörden oder Dienststellen aufzunehmen, wenn ihr die politische Betätigung eines Ausländers bekannt wird, die möglicherweise unzulässig ist. Auch hier fehlen gesetzliche Regelungen. Die Weitergabe der o.g. Verdachtsgründe an die Polizei kann nur dann als erforderlich angesehen werden, wenn konkrete Anhaltspunkte für eine Straftat vorliegen (Zuständigkeit der Polizei nach § 163 StPO).

  Für die Einschränkung oder Untersagung der politischen Betätigung von Ausländern nach § 6 Abs. 2 AuslG ist die Ausländerbehörde selbst ausschließlich zuständig. Auch in Fällen der unerlaubten politischen Betätigung nach § 6 Abs. 3 AuslG, die keinen Straftatbestand verwirklicht, besteht die gegenüber den allgemeinen Polizeibehörden spezielle Zuständigkeit der Ausländerbehörde, um z.B. Maßnahmen nach § 10 Abs. 1 Nr. 1 AuslG einzuleiten.

- Die Ausländerbehörde übermittelt den Sozialämtern/Sozialabteilungen der Bezirks- bzw. Ortsämter und der Ausländerstelle bzw. Leistungsstelle des Arbeitsamtes formularmäßig Daten zu negativ abgeschlossenen Asylverfahren. Das Formular enthält Angaben über Art des Abschlusses des Asylverfahrens, die Verpflichtung zur Ausreise, die Ausreisefrist und den Aufenthalt des Betroffenen. Eine gesetzliche Grundlage für diese Übermittlungen besteht nicht. Sie wäre erforderlich, um die Mitteilungen auf die Fälle zu beschränken, in denen ein unmittelbarer Bezug zu Leistungen der Sozialleistungsträger z.B. nach § 120 BSHG gegeben ist.

- Nach Mitteilung der Ausländerbehörde werden ausländischen Stellen Auskünfte melderechtlicher Art und im Zusammenhang mit der Anforderung von Paßersatzpapieren erteilt.

  Abgesehen davon, daß allein die Meldebehörden zur Erteilung melderechtlicher Auskünfte zuständig sind, ist die Übermittlung melderechtlicher Daten nur dann zulässig, wenn sie im Hamburgischen Meldegesetz ausdrücklich vorgesehen ist.

  § 31 HmbMG sieht lediglich Meldeauskünfte an Behörden oder sonstige öffentliche Stellen im Geltungsbereich des Melderechtsrahmengesetzes vor. Eine Vorschrift, die Offenbarungen an ausländische Stellen zuläßt, gibt es nicht. Entsprechende Auskünfte der Ausländerbehörde – ohne Einwilligung des Betroffenen – müssen daher unterbleiben.

Nach Ziff. 14 zu § 13 AuslVwV ist ein Ausländer, der keine gültigen Grenzübergangspapiere etc. besitzt, vor der Abschiebung anzuhalten, die notwendigen Grenzübertrittspapiere und Sichtvermerke zu beschaffen. Soweit erforderlich, haben die Ausländerbehörden den Ausländer hierbei zu unterstützen. Dies geschieht regelmäßig dadurch, daß die Ausländerbehörde Paßersatzpapiere selbst von ausländischen Stellen beschafft.

Dies bislang weder gesetzlich noch in der AusländerVwV geregelte Verfahren ist nur dann unbedenklich, wenn eine Abschiebung tatsächlich unmittelbar bevorsteht und die ausländischen Stellen dem Ersuchen zur Paßverlängerung keinerlei Indizien für die Gründe der Abschiebung (etwa im Zusammenhang mit politischer Betätigung) entnehmen können. Im Hinblick auf § 14 Abs. 1 Satz 1 AuslG, wonach eine Abschiebung unzulässig ist, sofern dem Betroffenen im Empfangsstaat Verfolgung aus rassischen, religiösen, ethnischen oder politischen Gründen droht, kann das Erfordernis eines reibungslosen Vollzugs der Abschiebung nicht in allen Fällen die mit dem Ersuchen um Paßverlängerung verbundene Datenweitergabe an ausländische Stellen rechtfertigen, da u.U. gerade durch diese Übermittlungen Gründe für die Verfolgung des Betroffenen bzw. seiner Angehörigen geschaffen werden könnten.

3.7.3.5 Zusammenarbeit mit dem Ausländerzentralregister (AZR)

Nach § 6 des Gesetzes über die Einrichtung des Bundesverwaltungsamtes wird bei dieser Stelle (in Köln) ein Ausländerzentralregister geführt. Weitere Regelungen für dieses Register fehlen vollständig. Gleichwohl wird dort – parallel zu den Datensammlungen der Landes-Ausländerbehörden – eine Vielzahl von Daten über alle in der Bundesrepublik lebenden Ausländer gespeichert.

Gespeist wird das AZR von den Ausländerbehörden der Länder. Der Verkehr der Ausländerbehörden mit dem Bundesverwaltungsamt wird in Anlage II der AuslVwV geregelt. Danach ist dem AZR über alle Ausländer, die gegenüber der Ausländerbehörde meldepflichtig sind, eine formularmäßige Mitteilung zu machen. Das entsprechende Formblatt enthält Angaben zu Staatsangehörigkeit, Namen, Vornamen, Geburtsort, Geburtsdatum, Familienstand, Geschlecht, Aufenthaltsort, Erwerbstätigkeit, Einreisedatum etc. des antragstellenden Ausländers und seines Ehegatten. Ferner sind dem AZR jeweils Änderungen zu den wichtigsten Daten sowie insbesondere hinsichtlich der Aufenthaltserlaubnis mitzuteilen. Das Ausländerzentralregister seinerseits bedient die Ausländerbehörden mit Informationen über dort bekannte Vorgänge und Erkenntnisse bezüglich einzelner Ausländer. Auch für diese Datenflüsse gibt es weder im Gesetz über die Einrichtung des Bundesverwaltungsamts noch im Ausländergesetz irgendwelche Rechtsgrundlagen. Ich habe bislang noch starke Zweifel, ob es überhaupt im überwiegenden Allgemeininteresse erforderlich ist, Ausländerdaten parallel zu den Ländern auch zentral zu registrieren.

Ich werde noch – in Zusammenarbeit mit den Datenschutzbeauftragten der anderen Länder – zu klären haben, ob – und wenn ja, inwieweit – es vertretbar ist, daß die Ausländerbehörde vor Schaffung einer einwandfreien gesetzlichen Grundlage weiterhin das Ausländerzentralregister mit Daten beliefert. Dabei wird zu berücksichtigen sein, daß die Speicherung einer Vielzahl von Daten über mehrere Millionen Einwohner der Bundesrepublik in einem automatisierten Register mit bisher noch nicht abschließend geklärten Zugriffsbefugnissen der unterschiedlichsten Stellen einen besonders gewichtigen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.

3.7.3.6 Neukonzeption des AZR

Das oben dargestellte Fehlen gesetzlicher Grundlagen hat – worauf ich schon in meinem letzten TB (unter Nr. 3.8.3, S. 71) hingewiesen habe – bereits auf Bund-Länder-Ebene zu Überlegungen zur Neukonzeption des Ausländerzentralregisters geführt. Dieses Verfahren ist allerdings bisher für die Datenschutzbeauftragten der Länder außeror-

dentlich unbefriedigend verlaufen, und zwar sowohl in inhaltlicher als auch in formaler Hinsicht.

Inhaltlich ist vor allem zu bemängeln, daß immer noch kein Gesetzentwurf vorliegt, der den Umfang der Speicherung sowie der zulässigen Datenflüsse präzise festlegt. Es wurden zwar schon die Aufgaben erörtert, an denen die Neukonzeption des AZR sich orientieren soll, nämlich

- Auskunftserteilung zur Unterstützung ausländerrechtlicher Einzelfallentscheidungen,
- Auskunftserteilung für die Sicherheitsbehörden und
- Bereitstellung ausländerpolitischer Planungsdaten.

Auch der Entwurf eines neuen, weitergehenden Datensatzes ist bereits in der Diskussion. Verfassungsrechtlich gebotene Erörterungen über eine Begrenzung der Informationseingriffe sind bislang – nach meinen Informationen – jedoch nicht angestellt worden.

In formaler Hinsicht ist zu bemängeln, daß der Bundesminister des Innern es kategorisch abgelehnt hat, Vertreter der Landesbeauftragten für den Datenschutz zu den Beratungen des Bund-Länder-Gremiums hinzuzuziehen, das die Neukonzeption des Ausländerzentralregisters vorbereitet. Begründet wurde dies mit „grundsätzlichen Erwägungen in Bezug auf unsere föderative Ordnung". Da das AZR eine Einrichtung der Bundesverwaltung sei, komme nur eine Beteiligung des Bundesbeauftragten in dem Bund-Länder-Gremium in Frage.

Diese Position ist für die Landesbeauftragten nicht hinnehmbar; denn bei dieser Neukonzeption des AZR geht es – wie oben dargelegt – neben der dringend notwendigen Schaffung einwandfreier Rechtsgrundlagen vor allem um die Klärung des Problems, welche Daten die Länder anliefern sollen und unter welchen Voraussetzungen bzw. zu welchen Zwecken andere Dienststellen diese nutzen dürfen, mithin nur Fragen, die in erster Linie das Informationsverhalten der Landesverwaltung betreffen. Für die Überwachung der informationellen Gewaltenteilung zwischen Bund und Ländern erscheint es mir somit unerläßlich, auch den Belangen des Datenschutzes auf Länderebene in einem Bund-Länder-Gremium unmittelbar Gehör zu verschaffen.

Die Zurückweisung dieses Anliegens durch den Bundesinnenminister bedeutet, daß die Durchsetzung eines effektiven Datenschutzes auf dem speziellen Gebiet der Ausländerverwaltung stark erschwert, wenn nicht verhindert wird. Im übrigen gibt diese Entscheidung wegen der grundsätzlichen Erwägungen, auf die sie gestützt wird, Anlaß zu der Befürchtung, daß der Bundesinnenminister sich auch auf anderen Gebieten, auf denen eine rege informationelle Zusammenarbeit zwischen Bundes- und Länderverwaltungen stattfinden muß, einer unmittelbaren Beteiligung der Landesdatenschutzbeauftragten verschließen wird. Dies kann dazu führen, daß bundeseinheitlich geltende normative Regelungen und Verwaltungsvorschriften erlassen werden, die Gesichtspunkten des Datenschutzes bei der Informationsverarbeitung auf Länderebene nicht hinreichend Rechnung tragen. Wenn Landesdatenschutzbeauftragte dann bei ihren nachgängigen Prüfungen möglicherweise Verwaltungsmaßnahmen zu beanstanden haben, ist die erforderliche Korrektur bei der jeweiligen Landesbehörde im Hinblick auf die bundeseinheitlich verbindlichen Vorschriften nur noch unter großen Schwierigkeiten, die vermeidbar gewesen wären, möglich.

Es liegt auf der Hand, daß der grundgesetzlich gebotene Datenschutz um so wirkungsvoller ist, je früher in einem Entscheidungsprozeß die Anliegen des Datenschutzes berücksichtigt werden und je unmittelbarer die Datenschutzbeauftragten sich in den maßgeblichen Gremien Gehör verschaffen können. Ebenfalls keiner besonderen Begründung sollte es bedürfen, daß eine solche rechtzeitige, unmittelbare Beteiligung um so wichtiger ist, je schwerwiegender der Gegenstand der Beratungen ist.

Ich habe den Präses der Behörde für Inneres von der bedenklichen Haltung des Bundesministers des Innern in Kenntnis gesetzt und ihn um Unterstützung gebeten.

Eine Reaktion lag mir bei Berichtsschluß zwar nicht vor, ich gehe aber im Hinblick auf die bisher gute Zusammenarbeit mit der Bfl bezüglich der Neukonzeption des AZR davon aus, daß er das Anliegen der Länderbeauftragten unterstützen wird.

3.7.4 Personenstandswesen

3.7.4.1 Durchführung des Transsexuellengesetzes

Bereits bei der ersten Überprüfung der sich aus dem Transsexuellengesetz (TSG) ergebenden datenschutzrechtlichen Konsequenzen hatte sich gezeigt, daß einige Gesetze und Verwaltungsvorschriften dem Grundgedanken der TSG noch besser angepaßt werden müssen (vgl. 2. TB Nr. 3.8.4.2, S. 71 f).

Nach Abschluß der Überprüfung kann ich im einzelnen folgendes feststellen:

- Gegenwärtig versendet das Gericht, das den Beschluß über die Änderung des Vornamens bzw. der Geschlechtszugehörigkeit getroffen hat, eine vollständige Ausfertigung des Beschlusses an das zuständige Standesamt. Die Begründung eines Gerichtsbeschlusses nach dem TSG enthält üblicherweise eine Schilderung des gesamten Vorlebens einer betroffenen Person mit Angaben z.T. aus dem intimen Bereich. Die Kenntnis dieser Beschlußbegründung ist für den Standesbeamten zur Erfüllung seiner Aufgaben jedoch nicht erforderlich.

- Die Dienstanweisung für Standesbeamte schreibt ferner vor, daß die Tatsache der Namens- bzw. Geschlechtsänderung in der Abstammungsurkunde, die die betroffene Person z.B. beim Rentenantrag und in Erbschaftsangelegenheiten vorlegen muß, zu vermerken ist. Diese Regelung verstößt nach meiner Auffassung gegen § 5 Abs. 1 TSG, wonach die Offenbarung des früheren Namens bzw. der Geschlechtszugehörigkeit grundsätzlich unzulässig ist. Der Schutzzweck des § 5 TSG zwingt dazu, auf die Kenntlichmachung entsprechender Vermerke in der Abstammungsurkunde zu verzichten.

- Im z.Z. noch manuell geführten Hamburger Melderegister werden zu jeder betroffenen Person 2 Karteikarten geführt: eine – entsprechend der Gerichtsentscheidung – neu angelegte, die nur die Angaben zum neuen Vornamen und Geschlecht enthält ohne Verweis auf die früheren Daten, sowie eine alte, auf der die bisher geltenden Daten mit Hinweis auf die TSG-Entscheidung vermerkt werden. Bei der Erteilung von Melderegisterauskünften, die unter Angabe der aktuell geltenden Daten gestellt werden, entstehen keine Probleme. Bei Ersuchen um eine Melderegisterauskunft, die unter dem alten Vornamen gestellt werden, greift eine Auskunftssperre ein. Routineauskünfte und Übermittlungen werden nicht vorgenommen, sondern der Sachbearbeiter hat zu prüfen, ob der Auskunft eine besondere Rechtsvorschrift entgegensteht. Die gegenwärtige Regelung, die den Sachbearbeiter auf § 5 TSG hinweisen soll, ist jedoch unbefriedigend. Das Hamburgische Meldegesetz verweist in § 34 auf das Personenstandsgesetz, dieses wiederum verweist auf das TSG, wobei in den drei Gesetzen jeweils unterschiedliche Offenbarungsbefugnisse formuliert sind. Nach meiner Auffassung müßte daher im Meldegesetz klargestellt werden, daß eine Auskunft über die alten Daten nur unter den engen Voraussetzungen von § 5 TSG zulässig ist. Dies gilt für private ebenso wie für öffentliche Stellen.

- Bei der Automatisierung des Meldewesens ist besonders darauf zu achten, daß durch technisch-organisatorische Maßnahmen dem Schutzzweck von § 5 TSG Rechnung getragen wird. Insbesondere muß ein Querverweis vom aktuellen Datensatz einer betroffenen Person auf die Angaben vor der Namens- bzw. Geschlechtsänderung ausgeschlossen werden. Ebenso ist sicherzustellen, daß auf den früher gülti-

gen Datensatz nicht routinemäßig zugegriffen werden kann, sondern nur unter den Voraussetzungen von § 5 TSG.

- Da die Daten einer betroffenen Person Vornamens- bzw. Geschlechtsänderung im Melderegister zulässig gespeichert sind, sollte bei der Neuausstellung von Personalausweisen, Pässen und Führerscheinen für die jeweiligen Register lediglich eine neue Karteikarte ohne Hinweis auf die früheren Daten angelegt und die alte Karteikarte vernichtet werden.

Diese Feststellungen habe ich der Behörde für Inneres und der Justizbehörde mit der Bitte um Prüfung und Stellungnahme übersandt. Die Diskussionen sind jedoch noch nicht abgeschlossen.

3.7.4.2 Vordruck „Sterbefallanzeige"

Die Eingabe eines Petenten hat mich veranlaßt, im Berichtszeitraum die Datenerhebung und -übermittlung im Sterbefall durch den Standesbeamten unter datenschutzrechtlichen Gesichtspunkten zu überprüfen. Im Ergebnis zeigt sich, daß nicht alle Daten, die vom Standesbeamten unter Verwendung eines Vordrucks erhoben werden, für die Erfüllung seiner Aufgaben erforderlich sind. Das gilt insbesondere für Daten, die sich auf den Nachlaß eines Verstorbenen beziehen.
Ich habe deshalb vorgeschlagen, künftig die Betroffenen darauf hinzuweisen, daß einige Angaben zwar nicht dem Standesbeamten, wohl aber z. B. dem Nachlaßgericht nach bestimmten, gesetzlichen Vorschriften erteilt werden müßten. Außerdem habe ich darum gebeten, im Vordruck den bisher fehlenden Hinweis auf die Rechtsgrundlagen für die Datenerhebung und -übermittlungen aufzunehmen.
Die Behörde für Inneres hat sich inzwischen dieser Sache angenommen und unter meiner Beteiligung einen neuen Vordruck entwickelt, der nunmehr aus datenschutzrechtlicher Sicht nicht mehr zu beanstanden ist und den Ansprüchen an eine bürgerfreundliche Verwaltung genügt.

3.8 Polizei

Bei der Polizei habe ich mich im Berichtszeitraum verstärkt mit einigen grundsätzlichen Problemen befassen müssen, die ich schon im vorigen TB angesprochen hatte. Die Klärungen, die ich mir insbesondere von den Beratungen zur SOG-Novelle versprochen hatte, sind leider nicht eingetreten, da dieser Diskussionsprozeß in der Bfl nach meinem Eindruck nicht nennenswert vorangekommen ist. Meine Vorstellungen über die notwendigen Regelungen für die Informationsverarbeitung (vgl. dazu auch Nr. 5.1.5) habe ich der Bfl bereits im Februar 1984 in einer umfangreichen Stellungnahme dargelegt.
Die Tatsache, daß die Bfl mir noch keinen neuen Entwurf für eine SOG-Novelle vorgelegt hat und daß auch nicht absehbar ist, wann ein solcher Entwurf vorliegen wird, kann m. E. nicht ohne praktische Folgen bleiben: Bestimmte, besonders schwerwiegende Informationseingriffe der Polizei, die sich nicht auf eine tragfähige Grundlage stützen können und bei denen darüber hinaus starke Zweifel an der Angemessenheit bestehen, können nicht weiter fortgeführt werden. Bis die Diskussion darüber, ob diese Aktivitäten überhaupt erforderlich sind, abgeschlossen ist und ggf. einwandfreie gesetzliche Grundlagen geschaffen sind, sind sie einzustellen. An welche Maßnahmen ich dabei denke, werde ich weiter unten ausführen.
Ein Schwerpunkt der Probleme, mit denen ich mich im Berichtszeitraum zu befassen hatte, lag bei der Weitergabe von Daten durch die Hamburger Polizei an andere Polizeibehörden und dritte Stellen (insbesondere Informationsberichte der Fachdirektion 7 – Staatsschutz –). Ich habe mich daher veranlaßt gesehen, die polizeiinternen Informationsbeziehungen (sowie die Zusammenarbeit der Polizei mit dem Verfassungsschutz) einmal näher zu prüfen (Nr. 3.8.3).
Daneben habe ich vor allem die Entwicklung der automatisierten Datenverarbeitung bei der Polizei (vgl. auch meinen 2. TB, Nr. 3.10.3, S. 79 ff) weiter beobachtet und einige Er-

kenntnisse gewonnen, die bereits bei der Novellierung des SOG berücksichtigt werden sollten (dazu Nr. 3.8.1 und 3.8.2).

3.8.1 Entwicklung der Fahndungs- und Nachweissysteme

Nachdem ich in meinem 1. TB die Grundzüge der polizeilichen Informationssysteme erläutert habe, möchte ich nunmehr daran anknüpfend den aktuellen Ausbaustand des INPOL-Verbundsystems deutlich machen und – auch im Hinblick auf die anstehende SOG-Novellierung – einige kritische Punkte ansprechen.
Zu den hier erörterten Fahndungs- und Nachweissystemen zähle ich die INPOL-Bund-Anwendungen Personenfahnung (dazu Nr. 3.8.1.2), Kriminalaktennachweis – KAN – (Nr. 3.8.1.3), Haftdatei (Nr. 3.8.1.4) sowie die Datei Erkennungsdienst (Nr. 3.8.1.5). Die Einrichtung der drei letztgenannten Anwendungen soll nach dem INPOL-Fortentwicklungskonzept aus dem Jahr 1981 bundesweit bis 1985 abgeschlossen sein.
Bevor ich auf die Problematik im einzelnen eingehe, möchte ich verdeutlichen, daß es sich bei den o. g. Anwendungen zwar um logisch voneinander getrennte Dateien handelt; diese werden jedoch in einer gemeinsamen Datenbank und verfahrenstechnisch mit einer einheitlichen Datensatz-Stuktur geführt: Die Personen- (Identifikations-) Daten („rechtmäßige Personalien") werden nur einmal in den Datenbankbereich Personen eingestellt und die zusätzlichen Informationen (Fahndung, Haft, ED etc.) werden als Datengruppe angehängt, sofern sie vorhanden sind. Wenn also zu einer bestimmten Person Fahndungsnotierungen vorliegen, werden zu dieser Person Daten in die sog. „F-Gruppe" eingestellt. Liegen überdies Hinweise auf eine Kriminalakte, auf eine Haftzeit bzw. eine erkennungsdienstliche Behandlung vor, werden entsprechende Informationen jeweils in die „U-Gruppe", die „H-Gruppe" bzw. die „E-Gruppe" eingestellt.
Da hier logisch getrennte Dateien vorliegen, darf zwar auf die jeweiligen Gruppen nur diejenige Person zugreifen, die eine erechende Zugriffsberechtigung hat. Diese Trennung wird jedoch z. T. dadurch wieder aufgehoben, daß bei der Anfrage einer bestimmten Gruppe mit den Suchbegriffen Name, Vorname, Geburtsdatum gleichzeitig ein Hinweis auf das Vorhandensein der erwähnten anderen Gruppen, bzw. einer Speicherung in einer Falldatei von bundesweiter Bedeutung gegeben wird.

3.8.1.1 Zum Problem des personengebundenen Hinweises

Ein allgemeines Problem liegt darin, daß die Datengruppe „rechtmäßige Personalien", die nur einmal besteht und jeweils mit den verschiedenen anderen Gruppen zu verknüpfen ist, nicht lediglich Identifikationsdaten, sondern – im Datenfeld PHW – auch sog. personengebundene Hinweise erhält. Dort sind z. Z. Hinweise auf folgende Umstände vorgesehen:

- bewaffnet,
- gewalttätig,
- Ausbrecher,
- Betäubungsmittel-Konsument,
- Freitodgefahr, (vgl. dazu meinen 2. TB, Nr. 3.10.5.2, S. 84 f)
- Ansteckungsgefahr,
- geisteskrank,
- geistesschwach,
- entmündigt,
- Prostitution,
- internationaler Rechtsbrecher,
- Land- oder Stadtstreicher,
- häufig wechselnder Aufenthaltsort (vgl. dazu meinen 2. TB, Nr. 3.10.5.3, S. 85 f).

Die Speicherung dieser personengebundenen Hinweise erscheint mir in mehrfacher Hinsicht problematisch. Zunächst einmal ist zu bemängeln, daß es keine Rechtsgrundlage gibt, aus der ein Bürger entnehmen kann, wann, mit welchen Inhalten und zu welchem Zweck möglicherweise Hinweise zu seiner Person im Polizeicomputer gespeichert werden.

Nach Meinung der Polizei sind die personengebundenen Hinweise erforderlich zur
- Eigensicherung des einschreitenden Beamten;
- Einleitung gezielter Fahndungsmaßnahmen;
- Unterstützung der polizeilichen Ermittlungen und
- zum Schutz des Betroffenen bei polizeilichen Maßnahmen.

Ob und unter welchen Voraussetzungen diese Zwecke eine Speicherung rechtfertigen, bedarf m. E. eingehender Überprüfungen. Ob und inwieweit einzelne Hinweise zum Schutz des Betroffenen bzw. zur Unterstützung der polizeilichen Ermittlungen erforderlich sind, halte ich für sehr zweifelhaft. Ich verweise insoweit auf meine Ausführungen im 2. TB zu den personengebundenen Hinweisen „Freitodversuch" und „häufig wechselnder Aufenthaltsort" (Nr. 3.10.5.2 und 3.10.5.3, S. 84 ff).

Anzuerkennen ist sicherlich die Notwendigkeit von Hinweisen zum Zwecke der Abwehr von Gefahren für die Sicherheit einschreitender Polizeibeamter (insbesondere etwa Hinweise auf Bewaffnung, Gewalttätigkeit und Ansteckungsgefahr). Auch diese Hinweise erscheinen mir jedoch nur im Zusammenhang mit derjenigen Datei erforderlich, die ein unmittelbares polizeiliches Einschreiten veranlassen soll, nämlich der Personenfahndung (F-Gruppe). Im Zusammenhang mit den Dateien, die lediglich als Nachweissysteme (für Kriminalakten, Haft bzw. ed-Behandlung) dienen, erscheinen diese Hinweise nicht erforderlich. Es besteht vielmehr sogar die Gefahr, daß sie den Benutzer dazu verleiten, auf eine entsprechende Nachprüfung in der Akte zu verzichten und Entscheidungen nur aufgrund der im INPOL gespeicherten Merkmale zu treffen.

Weiter erscheint mir besonders problematisch, daß die regelmäßige inhaltliche Überprüfung der Hinweise nicht sichergestellt ist. Bewertungen wie etwa „bewaffnet", „Ansteckungsgefahr" oder „Landstreicher" werden bis zu 10 Jahren im polizeilichen Informationssystem gespeichert, ohne daß jemals geprüft wird, ob die Voraussetzungen für die Zuschreibung des Merkmals zwischenzeitlich entfallen sind: Einmal Landstreicher, immer Landstreicher. Dies kann zum einen nicht im Interesse einer sachgemäßen polizeilichen Ermittlungstätigkeit liegen. Des weiteren liegt aber auch auf der Hand, daß die fortdauernde Speicherung solcher problematischen Merkmale die vom Bundesverfassungsgericht im Volkszählungsurteil hervorgehobene „Gefahr einer sozialen Abstempelung", die durch die Aufnahme dieser Kennzeichnungen in die Datenbank entstanden ist, zunehmend erhöht.

Ich habe die Bfl daher aufgefordert (und Entsprechendes haben andere Datenschutzbeauftragte auch getan), den Katalog der personengebundenen Hinweise mit dem Ziel einer Reduzierung zu überprüfen. Dabei sollte erwogen werden, PHW künftig nur noch in die F-Gruppe (= Personenfahndung) einzustellen und bei den reinen Nachweissystemen zu streichen. Ferner sind Überprüfungsfristen vorzusehen.

Die Diskussion dieser Probleme dauert noch an.

3.8.1.2 Datei Personenfahndung (F-Gruppe)

Diese Datei dient zunächst dem Nachweis von Personen, die zum Zwecke der Festnahme bzw. der Aufenthaltsermittlung ausgeschrieben sind. Insofern bestehen gegen eine Speicherung grundsätzlich keine Bedenken. Es sollte jedoch sichergestellt werden, daß die inhaltliche Richtigkeit notwendiger personengebundener Hinweise (vgl. Nr. 3.8.1.1) spätestens bei der Verlängerung einer Ausschreibung über ein Jahr hinaus überprüft wird.

Nach wie vor fehlt es allerdings an einer einwandfreien gesetzlichen Regelung der Frage, wer wann unter welchen Voraussetzungen fahndungsmäßig überprüft werden darf (vgl. Nr. 3.8.5.). Stattdessen ist immer noch ein Beschluß in Kraft, der von der Innenministerkonferenz im September 1977 im Zusammenhang mit der Terroristenbekämpfung gefaßt wurde. Nach diesem Beschluß, der inzwischen durch Presseveröffentlichungen bekannt geworden ist, sind alle Personen, deren Personalien der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden (z. B. bei Verkehrskontrollen, Unfällen, Vernehmungen etc.) in INPOL abzufragen. Von diesem Beschluß wird nach Aussagen der Polizei zwar nur mit gebotener Zurückhaltung Gebrauch gemacht. Dies ändert jedoch nichts daran, daß für eine so weit gehende Anweisung jegliche Rechtfertigung fehlt und sie daher dringend aus der Welt zu schaffen ist.

Ein weiteres besonderes Problem der Datei Personenfahndung besteht darin, daß sie auch dem Nachweis von Personen dient, die der polizeilichen Beobachtung – PB – (nach der Polizei-Dienstvorschrift 384.2) unterliegen. Hinreichende Rechtsgrundlagen für die Speicherung dieses Personenkreises gibt es jedoch nicht, worauf die Datenschutzbeauftragten wiederholt hingewiesen haben; denn die polizeiliche Beobachtung erstreckt sich auch auf Personen, gegen die kein substantieller Tatverdacht besteht und von denen auch keine konkrete Gefahr ausgeht. Die polizeiliche Beobachtung soll vorbeugend klären, ob ein Tatverdacht überhaupt besteht und gegen welche Personen er sich richtet bzw. ob eine konkrete Gefahr vorliegt und von wem sie ausgeht.
Die einschlägige Polizeidienstvorschrift grenzt zwar den zu erfassenden Personenkreis und den Anlaß der Beobachtung ein; so dürfen andere Personen nur ausgeschrieben werden, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung des Sachverhalts oder zur Ergreifung des Täters führen kann. Diese wenig präzisen Eingrenzungen können jedoch eine gesetzliche Regelung nicht ersetzen.
Unabhängig von der fehlenden gesetzlichen Grundlage erscheint mir materiell – unter Verhältnismäßigkeitsgesichtspunkten – bedenklich vor allem, daß die PB auch zur Sammlung vielfältiger Daten aus dem Umfeld des betroffenen Bürgers (z. B. aus dem Verwandten-, Freundes- und Bekanntenkreis) führt. In eine PB-Meldung sind nämlich nicht nur Angaben zur betroffenen Person (Ort, Zeit und Anlaß der Überprüfung, Reiseweg etc.) aufzunehmen, sondern auch Begleitpersonen namhaft zu machen. Ich halte es für erforderlich, daß zumindest diese Meldungen eingestellt werden, solange es an einer klaren gesetzlichen Regelung für die PB fehlt.

3.8.1.3 Kriminalaktennachweis (U-Gruppe)

Zu Einzelheiten des geplanten bundesweiten Kriminalaktennachweises habe ich mich bereits in meinem 2. TB ausführlich geäußert (Nr. 3.10.5.4, S. 86 f). Es gibt jedoch nach wie vor eine Reihe von kritischen Punkten, die von der BfI noch nicht bereinigt worden sind. Insbesondere ist nach wie vor vorgesehen, daß alle Delikte, die nach dem Kriminalpolizeilichen Meldedienst – Staatsschutz (KPMD-S), (vgl. Nr. 3.8.4.2), zu melden sind, auch wenn sie nicht in § 100a StPO aufgeführt sind, in den KAN eingestellt werden.
Am 18.1.1984 hat die Konferenz der Datenschutzbeauftragten die bisherigen Erfahrungen bei der Realisierung des KAN-Konzepts analysiert und in einem Beschluß die datenschutzrechtlichen Anforderungen an die Umsetzung der Abschichtungskriterien sowie an die praktische Handhabung erneut zusammengefaßt und weiter präzisiert. In dem Beschluß heißt es u. a.:

„1. Um eine extensive, dem KAN-Konzept zuwiderlaufende Auslegung der Abschichtungskriterien zu vermeiden und eine gleichmäßige Handhabung der Aktenauswahl in den einzelnen Ländern sicherzustellen, ist – wie in einigen Ländern (NRW, Saarland, HH) bereits anerkannt – der Erlaß von ergänzenden Durchführungsrichtlinien erforderlich.
2. In diesen Durchführungsrichtlinien sollen die Abschichtungskriterien in zwei Richtungen weiter präzisiert und somit eine bessere Handhabung durch den für die Aktenauswahl zuständigen Sachbearbeiter ermöglicht werden:
   - zum einen sollte ein Katalog derjenigen Straftaten aufgestellt werden, die in der Regel die KAN-Kriterien erfüllen;
   - zum zweiten sollten die für Einzelfall-Entscheidungen maßgeblichen Kriterien näher differenziert werden.
3. Aufnahme in den Katalog der regelmäßig KAN-relevanten Straftaten dürfen nur Verbrechen und die in § 100a StPO genannten besonders gefährlichen Vergehen finden. Die Aufnahme weiterer Regeldelikte ist durch die Errichtungsanordnung nicht gedeckt und wäre unverhältnismäßig.
   Aus gegebenem Anlaß wird darauf hingewiesen, daß insbesondere folgende Deliktsgruppen nicht pauschal, regelmäßig KAN-Kriterien erfüllen:
   - nicht als Verbrechen mit Strafe bedrohte bzw. im § 100a StPO genannte Delikte, die im Rahmen des kriminalpolizeilichen Meldedienstes – Staatsschutz zu melden sind;
   - nicht als Verbrechen mit Strafe bedrohte Sexualdelikte;

- Delikte, die lediglich in tatbestandlich nicht näher qualifizierten („besonders schweren") Fällen als Verbrechen bestraft werden;
- nicht als Verbrechen mit Strafe bedrohte bzw. in § 100a StPO genannte Delikte des Titels „Gefährdung des demokratischen Rechtsstaates" des Strafgesetzbuches.

4. In den Richtlinien ist der Gedanke zum Ausdruck zu bringen, daß Delikte, die nur einen geringen Unrechtsgehalt aufweisen, grundsätzlich nicht von überregionaler Bedeutung und damit KAN-relevant sind.
   Dies gilt sowohl für Katalog-Tatbestände, die ausnahmsweise von geringfügigem Unrechtsgehalt sein können, als auch für anhand von einzelfallbezogenen Kriterien auszuwählende Straftaten.
   Die einzelfallbezogenen Kriterien (z. B. Triebtäter, planmäßige überörtliche Begehung, gewerbsmäßige Begehung etc.) sind in den Richtlinien näher zu definieren. Insbesondere in Ballungsgebieten läßt eine Straffälligkeit auf dem Gebiet zweier Polizeibehörden nicht darauf schließen, daß die Daten überregionale (bundesweite) Bedeutung haben.
   Es ist schließlich klarzustellen, daß bei Zweifeln an der überregionalen Bedeutung keine Aufnahme in den KAN zu erfolgen hat."

Dieser Beschluß ist allen Innenministern zugeleitet worden. Der Bundesminister des Innern hat nach einem Bund-Länder-Abstimmungsverfahren nach eigenen Angaben im Einvernehmen mit den Innenministern/-senatoren der Länder mit Schreiben an den Bundesbeauftragten vom 6.6.1984 keine einzige der datenschutzrechtlichen Forderungen akzeptiert. Von der Bfl habe ich bislang keine Stellungnahme zu dem ihr mit Schreiben vom 1.2.84 übersandten Konferenz-Beschluß erhalten.
Ich halte dieses (– wie ich hoffe – Zwischen –) Ergebnis der Diskussion für außerordentlich unerfreulich, zumal deshalb, weil inzwischen immer deutlicher wird, daß der KAN mehr zu werden droht als ein reines Nachweissystem für Kriminalakten von überregionaler Bedeutung. Diese Gefahr sehe ich zum einen deshalb, weil in der praktischen Handhabung bislang nicht hinreichend sichergestellt ist, daß tatsächlich nur überregional bedeutsame Straftäter in den KAN eingespeichert werden. Entsprechende Richtlinien fehlen z. T. ganz oder aber sind – wie in Hamburg – nicht restriktiv genug.
Daß der KAN nicht nur die Funktion eines reinen Aktennachweises hat, ergibt sich ferner daraus, daß er personengebundene Hinweise enthält.
Darüberhinaus sehe ich die Gefahr, daß die Regelungen über den KAN durch die nach wie vor geltenden Regelungen über den allgemeinen Kriminalpolizeilichen Meldedienst (KPMD) unterlaufen werden. Dieser Meldedienst sieht – wie ich im einzelnen noch unter Nr. 3.8.3.1 näher erläutern werde – die Meldung diverser Delikte einschl. der Tatverdächtigen vor, die nicht von überregionaler Bedeutung i. S. der KAN-Regelungen sind. Auch in diesem Bereich muß es Beschränkungen geben.
Im Zusammenhang mit dem KAN bleibt schließlich darauf hinzuweisen, daß es nach wie vor unklar ist, wann überhaupt Kriminalakten zur vorbeugenden Verbrechensbekämpfung angelegt werden dürfen und welche Informationen darin zu sammeln sind (vgl. dazu Nr. 3.8.5). M. E. muß es von der Schwere des Delikts sowie von einer Bewertung der Wiederholungsgefahr abhängig gemacht werden, ob eine Kriminalakte angelegt werden darf, und hierfür bedarf es einer gesetzlichen Regelung.

3.8.1.4 Haftdatei (H-Gruppe)

Die Haftdatei dient dem Nachweis von Personen, die sich aufgrund richterlicher Anordnung in behördlichem Gewahrsam befinden oder befanden. Ausgenommen sind allerdings psychisch Kranke, die aufgrund der Unterbringungsgesetze der Länder freiheitsentziehenden Maßnahmen unterliegen.
Die Datensätze der Haftdatei bestehen wiederum aus dem Personengrunddaten („rechtmäßige" und andere Personalien) einschl. der personengebundenen Hinweise sowie aus den Haftnotierungen. Das sind Angaben über Vollzugsanstalt, Aufnahmetag, Einweisungsbehörde mit Aktenzeichen, Art und Anlaß der Freiheitsentziehung sowie voraussichtliches und tatsächliches Ende.
Die Rechtsgrundlage für die Einrichtung der Haftdatei findet sich in § 4 Abs. 1 BKA-G.

Dort heißt es jedoch lediglich:
„Die Landeskriminalämter unterrichten das Bundeskriminalamt unverzüglich über den Beginn, die Unterbrechung und die Beendigung von richterlich angeordneten Freiheitsentziehungen."
Nicht von § 4 BKA-G gedeckt ist somit die Speicherung der personengebundenen Hinweise. Da diese Hinweise im Rahmen der Haftdatei, die eine reine Nachweisdatei ist, auch nicht erforderlich sind, sollten sie ersatzlos entfallen.
Problematisch ist darüber hinaus die Registrierung von inaktuellen Haftmeldungen für fünf bzw. zwei Jahre über das Haftende hinaus. Diese dient der Polizei vornehmlich zur Erleichterung ihrer Ermittlungsarbeit, etwa um Alibis verdächtiger Personen leichter nachprüfen zu können.
Vom Wortlaut des § 4 BKA-G ist die Speicherung der inaktuellen Haftnotierungen ebenfalls nicht gedeckt. Sie ist überdies deswegen besonders fraglich, weil hier im besonderen Maße die Gefahr einer sozialen Abstempelung, einer Stigmatisierung des Betroffenen, besteht.
Aus meiner Sicht ist es erforderlich, die Speicherung inaktueller Haftnotierungen erheblich einzuschränken, wenn nicht ganz abzuschaffen. Solange dies nicht geschehen ist, muß auf jeden Fall sichergestellt sein, daß keine inaktuellen Haftnotierungen an Dritte übermittelt werden.

3.8.1.5 Datei Erkennungsdienst (E-Gruppe)

Die Datei Erkennungsdienst dient dem Nachweis von Fingerabdrücken (Formeln), Lichtbildern und Handschriften einschließlich der zugehörigen personenbezogenen Daten sowie der Information über durchgeführte erkennungsdienstliche Behandlungen. In dieser Datei sind also nicht die verformelten Zehnfinger- oder Einfingerabdrücke selbst gespeichert, sondern nur die Fundstellen für durchgeführte erkennungsdienstliche Behandlungen.
Die Abfragemöglichkeit für die zentrale ED-Datei soll der Hamburger Polizei ab 1985 offenstehen.
Die Datensätze der Datei Erkennungsdienst bestehen wiederum aus den „rechtmäßigen" und anderen Personalien, aus personengebundenen Hinweisen und aus Erkennungsdienstdaten. Dazu gehören
- Datum und Dienststelle der ed-Maßnahme,
- Anlaß/kriminologische Kurzbezeichnung der Straftat,
- Art der ed-Maßnahme/des Handschriftenmaterials,
- Stand/Ergebnis des Personenfeststellungsverfahrens
- ED-Hinweise sowie Sondervermerk.

Ferner soll die Datei Erkennungsdienst eine besondere Datengruppe enthalten, die Personenbeschreibungen erfaßt (sog. L-Gruppe mit Angaben zu Gestalt, Größe, Tätowierungen etc.). Neben dem Zugriff über die Personalien soll dann die Recherche mit den Merkmalen der Personenbeschreibung möglich sein.
Das Hauptproblem der ed-Datei sehe ich in der Frage, welche Daten welcher Straftäter zentral beim BKA mit direktem Zugriff für alle Polizeien des Bundesgebiets aufbewahrt werden dürfen. Beim Kriminalaktennachweis (KAN) haben die Innenminister anerkannt, daß dort nur Hinweise auf Straftäter von überregionaler Bedeutung eingestellt werden dürfen, und Abschichtungskriterien entwickelt, die eine Abtrennung dieses Personenkreises von den nur regional bedeutsamen Straftätern ermöglichen.
Die Notwendigkeit einer entsprechenden Abschichtung auch für die ed-Datei ist bislang von den Innenministern nicht akzeptiert worden. Damit besteht die Gefahr, daß mit der Datei Erkennungsdienst die für den KAN entwickelten Abschichtungskriterien unterlaufen werden (vgl. dazu meinen 1. TB, Nr. 6.7.2.1, S. 41).
Schon in meinem letzten TB (Nr. 3.10.3.2, S. 79), habe ich auf die Problematik der zunehmenden Zentralisierung der polizeilichen Datenverarbeitung auf Bundesebene hingewiesen. Ich habe deutlich gemacht, daß sich sowohl im Hinblick auf die – durch die föderalistische Struktur der Bundesrepublik begrenzten – Aufgaben des BKA („als Zentralstelle, soweit dies für eine Koordinierung der Verbrechensbekämpfung erforderlich ist") als auch im Hinblick auf das Gebot der Verhältnismäßigkeit von Grundrechtseingrif-

fen, Begrenzungen ergeben. Aus diesen Gründen ist es dringend geboten, auch für die Datei Erkennungsdienst eine Abschichtung vorzunehmen und nur Straftäter von überregionaler Bedeutung zentral zu speichern.
Die Beurteilung der Bedeutung eines Straftäters ist Sache der Länderpolizeien. Diese haben bei der Anlieferung von erkennungsdienstlichen Unterlagen deutlich zu machen, ob die Übermittlung zu Zwecken der weiteren Speicherung oder aber nur zu reinen Abgleichszwecken (mit den daktyloskopischen Unterlagen beim BKA) erfolgt.

3.8.2 Entwicklung der Aktenschließungssysteme

Neue Probleme entstehen dadurch, daß die Entwicklung der polizeilichen ADV sich nicht mehr auf umfassende Nachweissysteme beschränkt, sondern in immer stärkerem Maße darauf abzielt, auch die Erschließung und Auswertung von Akteninhalten bzw. sonstigen Informationen zu ermöglichen (vgl. dazu meinen 2. TB, Nr. 3.10.3.3, S. 79 ff).

Diese neueren Informationssysteme (PIOS,SPUDOKs) knüpfen im Gegensatz zu den – fast schon traditionellen – Nachweissystemen nicht mehr in erster Linie an die Person des Täters bzw. Verdächtigen, sondern an bestimmte Sachverhalte und Ereignisse an. Während es bei den herkömmlichen ADV-Anwendungen – wie bei den Kriminalakten – darum geht, Informationen über Verdächtige vorzuhalten, um sie damit von der Begehung künftiger Straftaten abzuschrecken bzw. Straftaten dieses Personenkreises schneller aufzuklären, werden mit den neueren Systemen – ähnlich wie bei Ermittlungs- und Spurenakten – bestimmte Ereignisse umfassend dokumentiert (SPUDOK) bzw. bestimmte Deliktsbereiche einschl. ihres Umfeldes so weit wie möglich erfaßt (PIOS).
Die neuen Probleme entstehen dadurch, daß die für die Bewertung der traditionellen Systeme entwickelten Maßstäbe für die neuen Anwendungen nicht mehr richtig passen. Die Beurteilung der vorbeugenden Speicherung von Informationen (erkennungsdienstliche Unterlagen, Kriminalakten etc.) ging davon aus, daß eine Speicherung erforderlich ist, wenn eine auf Tatsachen gestützte Prognose ergibt, daß von den Betroffenen die Begehung weiterer erheblicher Straftaten zu erwarten ist. Maßgeblich sind also die Kriterien „Schwere des Delikts" und „Wiederholungsgefahr". Diese Bewertung lehnt sich – in Ermangelung hinreichend klarer Rechtsgrundlagen – an die vom Bundesverwaltungsgericht entwickelten Zulässigkeitskriterien zur Aufbewahrung erkennungsdienstlicher Unterlagen an.
Wenn die Speicherung – wie in PIOS und SPUDOK – jedoch in erster Linie dem Zweck dient, ganze Ermittlungsverfahren zu erfassen, reichen die genannten Kriterien nicht aus. Als Aktenauswertungssysteme können diese ADV-Anwendungen nur dann ihren Zweck erfüllen, wenn mehr Personen als nur die jeweiligen „Träger" einer Kriminalakte erfaßt werden. Für die Speicherung solcher anderen Personen, die lediglich „im Zusammenhang" mit einem bestimmten Delikt (bzw. Deliktsbereich) in Erscheinung getreten sind, gibt es bislang keine rechtlich hinreichend abgesicherten Zulässigkeitskriterien (vgl. auch meinen 2. TB, Nr. 3.10.5.1, S. 83 f).
Probleme entstehen weiterhin im Zusammenhang mit der Löschung von Daten. In einem Nachweissystem kann man eine Löschung personenbezogener Daten veranlassen, wenn – ggf. unter Berücksichtigung pauschalierter Fristen – eine Wiederholungsgefahr nicht mehr anzunehmen ist. Ist aber die Speicherung von bestimmten Personen dem Zwecke der Aufklärung eines Sachverhalts untergeordnet, so ist – um den Speicherungszweck nicht zu gefährden – eine Löschung sinnvollerweise erst dann möglich, wenn ein Sachverhalt abschließend geklärt ist und sich herausgestellt hat, daß die gespeicherte Personeninformation für den – aufgeklärten – Sachverhalt keine Bedeutung hat.
Ein drittes Problem sehe ich schließlich in der Sicherung der Zweckbindung. Traditionell wurden Daten nicht-tatverdächtiger Personen nur in bestimmten Ermittlungs- und Spurenakten notiert. Ein gezielter Zugriff war Sachbearbeitern, die mit dem jeweiligen Ermittlungsverfahren nicht zu tun hatten, kaum möglich. Diese, einer Zweckbindung nahekommenden Beschränkungen, fallen bei der automatisierten Aktenerschließung weg. Insbesondere bei einer sog. „dateiübergreifenden Recherche" in mehreren PIOS- oder SPUDOK-Dateien ist die Einhaltung spezifischer Zweckbindungsvorschriften kaum

noch möglich.
Diese kurze Übersicht zeigt m. E. schon deutlich, daß es hier im technischen Bereich eine Erweiterung des polizeilichen Handlungsspielraumes gibt, die dringend neue Regelungen erfordert. Dieser Herausforderung hat sich die Polizei allerdings noch nicht gestellt.

3.8.2.1 PIOS-Dateien

In PIOS-Dateien werden regelmäßig – in unterschiedlichem Umfang – Daten aus bestimmten Ermittlungsverfahren, aus besonderen Meldediensten (vgl. Nr. 3.8.3.2) sowie Ereignisinformationen aus sonstigen Unterlagen (z. B. Zeitungsmeldungen, BKA-Berichten, nachrichtendienstlichen Mitteilungen etc.) eingestellt. Diese unterschiedlichen Informationen sollen miteinander kombiniert und verknüpft werden können. Daraus ergibt sich die Eignung von PIOS als sog. „Verdachtsverdichtungsinstrument".
Die Informationen werden bislang erfaßt in vier verschiedenen gleichberechtigten Datensäulen über – wie der Name schon sagt –:
- Personen
- Institutionen (Organisationen/Vereinigungen)
- Objekte und
- Sachen.

Die einzelnen Säulen sind wiederum gegliedert in (formatierte) Datengruppen: Personengrunddaten, Fundstellenverzeichnis, Verknüpfungshinweise sowie in freitextliche Eintragungen.
Verknüpfungshinweise, also Hinweise auf Zusammenhänge zwischen den in den anderen Datenabschnitten erfaßten Daten, müssen bislang von Sachbearbeitern selbst veranlaßt werden, was zu Fehlern führen kann.
Nach meinen Informationen soll PIOS nunmehr in der Art neu gestaltet werden, daß die Einzelinformationen (zu Personen, Personenbeschreibungen, Institutionen und Sachen) jeweils hierarchisch einem Vorgang bzw. einem Ereignis untergeordnet werden sollen, soweit dies möglich ist. Dies würde dazu führen, daß die Probleme, die ich oben (unter Nr. 3.8.2) beschrieben habe, verstärkt auftreten. Es wird schwierig, die Zulässigkeit der Speicherung einzelner Personen zu beurteilen bzw. die Löschung einzelner Personaldaten zu erreichen, wenn die Erforderlichkeit der Speicherung an die Bewertung eines bestimmten Ereignisses anknüpft.

3.8.2.2 Spurendokumentationssysteme (SPUDOK)

Das Verfahren SPUDOK (vgl. 2. TB, Nr. 3.10.3.3.3) ist das komfortabelste Verfahren, das die Polizei z. Z. betreibt. SPUDOK-Dateien ermöglichen eine weitestgehend formatfreie Datenverarbeitung. Ohne Rücksicht auf Systemkonventionen können hier Daten erfaßt und ebenso problemlos wieder zurückgewonnen werden. Die Datenerfassung erfolgt natürlich-sprachlich; es werden keine speziellen Schlüssel mehr benötigt. Ebenso einfach geschieht die Selektion; durch einfache Maßnahmen können beliebige Begriffe im Freitextbereich recherchierbar gemacht werden.
SPUDOKs können alle Spuren und Hinweise in einem oder mehreren Ermittlungsverfahren dokumentieren. Diese können nach bestimmten Kriterien selektiert, mit anderen (SPUDOK- oder PIOS-) Dateien verglichen und in andere Dateien übernommen werden. Es ist somit ein Sammelbecken für jegliche Art von Informationen, die automatisiert „gefiltert" werden können.
Es liegt auf der Hand, daß dieses Verfahren zwar ein ideales Arbeitsmittel für Spezialdienststellen und Sonderkommissionen ist (auch für parlamentarische Untersuchungsausschüsse); ebenso groß ist aber auch die Gefahr, daß die – verfassungsrechtlich gebotene – Zweckbindung der gespeicherten Informationen durchbrochen wird. Spätestens wenn SPUDOK-Daten in andere Dateien (z. B. PIOS) übernommen werden, geht der ursprünglich vorgesehene Sachzusammenhang zu bestimmten Ereignissen bzw. Ermittlungsverfahren vollständig verloren. Auf den Verlust an Kontrollierbarkeit hatte ich bereits in meinem letzten TB (a. a. O.) hingewiesen.
Wie die durch diese technischen Entwicklungen bedingten Probleme datenschutzrecht-

lich besser in den Griff zu bekommen sind, ist noch nicht geklärt. Die herkömmliche Verfahrensweise der, an die KpS-Richtlinien angelehnten Errichtungsanordnungen mit personenorientierten Aufbewahrungsfristen, wird diesem neuen Verfahren jedenfalls nicht gerecht. Wie ich bereits oben unter Nr. 3.8.2 ausgeführt habe, könnte der Zweck des speziellen SPUDOK-Verfahrens in Frage gestellt werden, wenn einzelne Spuren und Hinweise vor Abschluß eines Ermittlungsverfahrens gelöscht werden.
Auch hier ist letztlich der Gesetzgeber veranlaßt, die technischen Entwicklungen in vertretbare Bahnen zu leiten. Er muß hier modellartige Feinstrukturen entwerfen. Die Lösung muß sich nach meinen bisherigen Erfahrungen an folgenden Grundsätzen orientiern:

- Der Zweck eines SPUDOK sollte jeweils möglichst eng – an die Aufklärung bestimmter Sachverhalte angelehnt – definiert werden.
- Je enger der Zweck definiert ist, desto größer kann der Kreis derjenigen Personen sein, deren Daten (vorübergehend) automatisiert gespeichert werden.
- Die Speicherungsdauer sowie die Möglichkeiten von Übermittlungen und Abgleichen müssen – streng an Zwecke orientiert – eng begrenzt sein.

3.8.2.3 Neuere Entwicklungen

Seit neuestem gibt es Bestrebungen der Polizei, auch sog. „Massendaten" automatisiert zu verarbeiten und auszuwerten. Solche „Massendaten" fallen bei bestimmten Kontrollmaßnahmen, z. B. bei Überprüfung größerer Wohnblöcke, bei Kontrollstellen, Ringalarmfahndungen etc. an. Es kann sich etwa um Listen von Kfz-Kennzeichen handeln, die an bestimmten Punkten notiert wurden (Aktion „Gitternetz") oder um Listen der an einer Kontrollstelle überprüften Personen. Letztere sind etwa aus den Daten, die bei Fahndungsabfragen unter Verwendung eines – möglichst maschinenlesbaren – Personalausweises protokolliert werden, abzuleiten (vgl. Nr. 3.7.2.2).
Diese Massendaten werden im Gegensatz zu den – von vornherein im engeren Fallzusammenhang erfaßten – Spuren und Hinweisen nur aufgrund rein zufälliger Bezüge zum jeweiligen Tatgeschehen erhoben. Es handelt sich um Informationen, bei denen lediglich zu vermuten ist, daß die für die Fallaufklärung brauchbaren Daten darin enthalten sind. Diese Informationen sollen durch Abgleich mit anderen polizeilichen Dateien auf ihre Relevanz überprüft werden.
Rechtsgrundlagen für die Speicherung und Verwendung solcher Daten gibt es z. Z. nicht; ich halte es auch für fraglich, ob die Schaffung entsprechender Befugnisse im überwiegenden Allgemeininteresse geboten ist. Polizeiliche Maßnahmen – wie die Speicherung personenbezogener Informationen – dürfen sich nur in ganz eng zu begrenzenden Ausnahmefällen gegen Personen richten, die weder Störer noch Tatverdächtige sind. Es mag noch vertretbar sein, die Daten Nicht-Verdächtiger an Kontrollstellen und bei Razzien zu Zwecken der Identitätsfeststellung (einschl. einer Abfrage der Fahndungsdateien) zu erheben; eine weitere Speicherung von Personen, deren Identität feststeht, ist damit noch nicht gerechtfertigt.

3.8.3 Polizeiinterne Informationsbeziehungen

Neben der Zusammenarbeit der Polizeien von Bund und Ländern im Rahmen des Verbundsystems INPOL gibt es weitere, außerordentlich umfangreiche Datenflüsse unterschiedlichster Art. Diese bedürfen nach meinen ersten Überprüfungen dringend einer gründlichen Bereinigung: ich habe insbesondere Zweifel, ob sie materiell erforderlich sind, und darüber hinaus befürchte ich, daß mit diesen Datenflüssen Beschränkungen, die bei den Verbundsystemen gelten, unterlaufen werden.

3.8.3.1 Allgemeiner kriminalpolizeilicher Meldedienst (KPMD)

Nach den Richtlinien über den allgemeinen KPMD haben örtliche Polizeidienststellen bestimmte, in einem detaillierten Katalog aufgeführte Straftaten an ihr Landeskriminalamt (bzw. die jeweils zuständige Stelle) und weiter an das BKA zu melden. Erfaßt werden dabei Delikte aus fünf Deliktsklassen, nämlich aus den Bereichen

- Verbrechen gegen Leben und Freiheit und gemeingefährliche Straftaten;
- Raub und Diebstahl;
- Betrug und verwandte Erscheinungsformen;
- Straftaten in Verbindung mit Spiel, Wetten usw. sowie
- Triebverbrechen und sonstige Straftaten auf sexueller Grundlage.

Durch die Auswertung dieser Meldungen über Straftaten und Tatverdächtige sollen zum einen mögliche Straftatzusammenhänge (z. B. Serien) festgestellt und zum weiteren unaufgeklärte Straftaten gemeldeten Personen zugeordnet werden können. Die Polizei geht bei diesem Meldedienst von der Prämisse aus, daß die Arbeitsweise (modus operandi) jeweils täterspezifisch ist, und daß ein Täter dazu neigt, immer gleiche oder ähnliche Straftaten zu begehen (sog. Perseveranz).
An der Erforderlichkeit eines solchen umfangreichen Meldedienstes – jedenfalls in der vorliegenden Ausgestaltung – werden auch aus Kreisen der Polizei neuerdings wieder erhebliche fachliche Zweifel geäußert. So gibt es neue kriminologische Untersuchungen (insbesondere von einer Forschungsgruppe des LKA Bayern), die schon die Stichhaltigkeit der o. g. Perseveranz-Hypothese in Frage stellen. Schon aus diesen Gründen sollte der KPMD grundsätzlich überprüft werden. Es erscheint mir nicht vertretbar, Daten über mutmaßliche Täter bundesweit zu streuen, wenn dies die Strafverfolgung nicht nachhaltig fördert.
Hinzu kommt, daß mit dem KPMD Personengrunddaten über Straftäter an das BKA geliefert und dort gespeichert werden, die für den zentralen Kriminalaktennachweis nicht übermittelt werden dürften, weil sie nicht von überregionaler Bedeutung sind. Zwar gibt es auch in den KPMD-Richtlinien die Regelung, daß weniger schwere, speziell gekennzeichnete Delikte des Katalogs nur dann an das BKA zu melden sind, „wenn sie von überörtlichen Tätern begangen werden". Mit dieser vagen, nicht näher definierten Bestimmung ist aber nicht sichergestellt, daß tatsächlich nur Daten über überregional bedeutsame Straftäter gemeldet werden, und überdies sind im Katalog der meldepflichtigen Straftaten nach dem KPMD auch Delikte enthalten, die vom KAN-Katalog nicht erfaßt werden.
Ein weiteres Problem liegt in der unterschiedlichen Behandlung der eingehenden Meldungen durch das BKA.

3.8.3.2 Sondermeldedienste

Neben dem allgemeinen Meldedienst (KPMD) gibt es für eine Reihe von Kriminalitätsbereichen Sondermeldedienste. Zu nennen sind hier insbesondere

- Sondermeldedienst (SMD) Rauschgift
- SMD Waffen und Sprengstoff
- SMD Wirtschaftsstraftaten
- SMD Landfriedensbruch und verwandte Straftaten (an diesem Dienst nimmt Hamburg nicht teil)
- Meldedienst Staatsschutzdelikte (KPMD-S).

Aus diesen Deliktsbereichen sind regelmäßig alle Straftaten dem BKA zu melden, sie werden dort in recht unterschiedlicher Weise ausgewertet. So finden etwa Rauschgiftmeldungen Eingang in die Falldatei Rauschgift – ein Verbundsystem, an das auch die Hamburger Polizei angeschlossen ist. Auch bei den Sondermeldungen ist m. E. überprüfungsbedürftig, ob die gemeldeten Straftäter jeweils von überregionaler Bedeutung im Sinne der KAN-Kriterien sind. Zumindest bezüglich der nach dem KPMD Staatsschutz zu meldenden Delikte hege ich insofern erhebliche Zweifel.

3.8.4. Weitergabe von Lageberichten der Staatsschutzabteilung

Im Berichtszeitraum habe ich mich – veranlaßt durch diverse Eingaben – intensiv mit der Frage befassen müssen, ob die Fachdirektion Staatsschutz (FD 7) der Hamburger Polizei Lageberichte mit personenbezogenen Daten an andere Stellen weitergeben darf. Diese Angelegenheit war auch Gegenstand mehrerer Kleiner Anfragen sowie einer aktuellen Stunde in der Bürgerschaft.

Bei meinen Ermittlungen habe ich festgestellt, daß die FD 7 mehrmals wöchentlich einen sog. „Informationsbericht der FD 7-Staatsschutz ('IB')" herausgibt. Dieser enthält neben einer Darstellung der für Staatsschutzaufgaben jeweils wichtigsten Ereignisse einen – abtrennbaren – Anhang, der zu den jeweiligen Ereignissen Listen von Personen enthält. Diese Berichte sollen zum einen interne Lageauswertungen wiedergeben und darüberhinaus andere intessierte Dienststellen schnell über laufende Ermittlungsverfahren im Staatsschutzbereich informieren.
Im Sinne des Volkszählungsurteils tragfähige Rechtsgrundlagen für die Weitergabe von personenbezogenen Daten in den „IBs" gibt es kaum. Die im „IB" genannten personenbezogenen Daten werden von der Polizei regelmäßig zum Zweck der Ermittlungen wegen eines Verdachts der Begehung von Straftaten erhoben. Im vorliegenden Fall bezogen sich die Vorwürfe z. B. auf die §§ 123 (Hausfriedensbruch) und 303 (Sachbeschädigung) StGB. Soweit die Daten zu eben diesem Zweck (Betreibung des Ermittlungsverfahrens) an andere Polizeidienststellen bzw. die zuständige Staatsanwaltschaft weitergegeben werden, ist dies unbedenklich.
In den meisten Fällen dient die Weitergabe jedoch anderen Zwecken, und dies ist schon mangels ausreichender Rechtsgrundlage bedenklich. Strafprozessuale Vorschriften scheiden aus, da diese sich nur auf Übermittlungen im Zuge konkreter Ermittlungsverfahren beziehen können; aber auch die polizeiliche Generalklausel kann nicht herangezogen werden, da die Weitergabe nicht zur Abwehr einer konkreten Gefahr bestimmt ist. Rechtsgrundlagen für eine Weitergabe zur vorbeugenden Verbrechensbekämpfung gibt es – jedenfalls außerhalb des BKAG – noch nicht. Bei den meisten Empfängern des Berichts habe ich auch erhebliche Zweifel, ob die Weitergabe überhaupt für Zwecke der vorbeugenden Verbrechensbekämpfung geeignet und erforderlich ist.
Meine Nachforschungen – mit Unterstützung von anderen Kollegen aus Bund und Ländern – haben keine Gründe ergeben, die eine Übermittlung an auswärtige Polizeidienststellen (andere Landeskriminalämter, BKA) erforderten. Ich habe nicht einmal feststellen können, daß diese Berichte überhaupt sinnvoll ausgewertet werden. Auch im Hinblick auf die zahlreichen sonst bestehenden Meldedienste (s. Nr. 3.8.3) sind diese Mitteilungen daher einzustellen.
Ebenfalls problematisch erscheint mir die regelmäßige Übermittlung der im „IB" enthaltenen personenbezogenen Daten an verschiedene Dienststellen des Verfassungsschutzes. Auch diese Weitergabe ist – abgesehen von der gesetzlich nicht hinreichend abgesicherten Durchbrechung des ursprünglichen Verwendungszwecks – vielfach nicht erforderlich, denn häufig haben die vorgefallenen Straftaten bei weitem nicht das Niveau von „Bestrebungen gegen die freiheitlich-demokratische Grundordnung" i. S. von § 3 HmbVerfSchG. Die notwendige Unterrichtung des Verfassungsschutzes muß daher durch geeignetere, nämlich gezielte Maßnahmen sichergestellt werden. Weitere Dienststellen (BND, MAD, ausländische Geheimdienste) erhalten – seitdem die Bfl die Praxis im April ds. Js. eingeschränkt hat – nur noch im Einzelfall den „IB" mit personenbezogenen Daten, wenn die „Übermittlung bestimmter Daten die Zuständigkeit dieser Dienste berührt und zur Erfüllung ihrer Aufgaben erforderlich ist." Auch diese eingeschränkte Praxis halte ich jedoch für bedenklich: bei den genannten Empfängern wiegt die Durchbrechung der Zweckbindung besonders schwer, da es überhaupt keine gesetzlich geregelten Zwecke gibt, zu denen diese Dienste tätig werden. Auch für Übermittlungen an ausländische Nachrichtendienste gibt es keine hinreichend klaren Rechtsgrundlagen. Artikel 3 des Zusatzabkommens zum NATO-Truppenstatut, auf den der Senat die Übermittlungen stützen will, sieht lediglich in allgemeiner Form vor, daß die Zusammenarbeit zwischen den deutschen und den NATO-Behörden sich auch erstreckt „auf die Förderung und Wahrung der Sicherheit sowie den Schutz des Vermögens der Bundesrepublik, der Entsendestaaten und der Truppen, namentlich auf die Sammlung, den Austausch und den Schutz aller Nachrichten, die für diese Zwecke von Bedeutung sind."
Erschwerend kommt noch hinzu, daß dort eine Kontrolle darüber, was mit den übermittelten Daten geschieht und zu welchen Zwecken sie verwendet werden, überhaupt nicht mehr möglich ist und schon deshalb schutzwürdige Belange des Betroffenen gefährdet sind.
Insgesamt hat meine Prüfung daher zu dem Ergebnis geführt, daß eine Weitergabe des „IB" mit personenbezogenen Daten an Dienststellen außerhalb der Hamburger Polizei

und der zuständigen Staatsanwaltschaft eingestellt werden muß. Diese Forderung habe ich der Behörde für Inneres aber erst im Dezember mitteilen können, so daß mir eine Stellungnahme noch nicht vorliegen kann.

3.8.5 Novellierung des HmbSOG

Zu diesem Komplex gibt es leider nichts Positives zu berichten. Nachdem ich bereits in den ersten beiden Tätigkeitsberichten die Schaffung präziser Befugnisnormen für die Informationsverarbeitung der Polizei als vordringlich bezeichnet hatte, der Senat diese Forderung grundsätzlich anerkannt und die Bfl schon im Dezember 1983 den Entwurf einer SOG-Novelle in die Behördenabstimmung gegeben hat, scheint die Bfl heute weiter denn je von einem den verfassungsrechtlichen Anforderungen gerecht werdenden Gesetzesentwurf entfernt zu sein.
Ich habe der Bfl im Februar eine umfassende Stellungnahme zum vorgelegten SOG-Entwurf übermittelt, die zahlreiche Kritikpunkte, aber auch eigene Vorschläge enthielt. Die Bfl hat daraufhin die behördeninterne Diskussion wieder aufgenommen, diese Phase des Verfahrens aber bis heute noch nicht abgeschlossen. Inhaltliche Fortschritte habe ich im Laufe des Jahres nicht feststellen können. Auch die Beratungen in einem Bund-Länder-Arbeitskreis, den die Innenminister-Konferenz unter dem Eindruck des Volkszählungsurteils zur Regelung der Informationsverarbeitung im Polizeirecht eingesetzt hat, scheinen jedenfalls für die Bfl nicht sonderlich ertragreich gewesen zu sein.
Ich sehe an dieser Stelle davon ab, ausformulierte Vorschläge für eine SOG-Novelle vorzulegen. Insofern kann ich der Bfl die Verantwortung nicht abnehmen. Im übrigen verweise ich darauf, daß ich die Schwerpunkte der notwendigen gesetzlichen Regelungen bereits in meinem letzten TB (Nr. 5.1.3, S. 143 ff) skizziert habe.
An dieser Stelle möchte ich nur noch einmal die rechtspolitische Bedeutung der SOG-Novelle verdeutlichen und die wichtigsten, sich aus dem Volkszählungsurteil des Bundesverfassungsgerichts ergebenen Forderungen zusammenfassen, die ich der Bfl in meiner Stellungnahme vom Februar mitgeteilt hatte.

3.8.5.1 Zur rechtspolitischen Bedeutung

Die rechtspolitische Bedeutung der kommenden SOG-Novelle sehe ich vor allem darin, daß Grundbegriffe des traditionellen Polizeirechts zur Debatte stehen werden.
Genausowenig wie bereits der Muster-Entwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder (ME) im Jahre 1977 lediglich eine Vereinheitlichung föderalistisch zersplitterten Polizeirechts brachte, wird sich die SOG-Novelle auf eine schlichte Anpassung traditionellen Polizeirechts an neue Gegebenheiten reduzieren lassen. Vor allem für die Erhebung und sonstige Verarbeitung personenbezogener Informationen geht es auch darum, die herkömmlichen Aufgaben der Polizei sowie die nach dem allgemeinen Polizeirecht bestehenden Eingriffsbefugnisse zu erweitern.
Nach herkömmlicher Rechtslage hat die Polizei generell zwei Aufgaben zu erfüllen. Zum einen – nach hier nicht näher zu erörterndem Bundesrecht – Straftaten (§ 163 Abs. 1 StPO) sowie Ordnungswidrigkeiten (§ 53 Abs. 1 OWiG) zu erforschen; zum anderen im Einzelfall bestehende konkrete Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren, soweit andere Verwaltungsbehörden nicht rechtzeitig eingreifen können (§ 3 Abs. 2 i. V. m. Abs. 1 SOG). Zur Erfüllung dieser Aufgaben sind ihr in den jeweiligen Zuweisungsgesetzen bestimmte Eingriffsbefugnisse eingeräumt worden.
Diese gesetzlichen Eingriffsbefugnisse sollen erweitert werden für Zwecke der vorbeugenden Bekämpfung von Straftaten („Verbrechensvorbeugung"). Dieser Bereich polizeilicher Arbeit vollzieht sich im Vorfeld unmittelbar bevorstehender Gefahren. Er ist daher von der Aufgabenzuweisungsvorschrift des § 3 SOG strenggenommen nicht mehr umfaßt. Im Interesse der Rechtsklarheit sollte daher erwogen werden, die Aufgabenumschreibung für die Polizei neuzufassen. Zu denken wäre etwa an die Einfügung eines § 3 Abs. 3 SOG, in dem die Aufgabe der vorbeugenden Verbrechensbekämpfung ausdrücklich genannt wird.
Nach herkömmlichen Polizeirecht waren die Eingriffsbefugnisse der Polizei und der anderen Verwaltungsbehörden im wesentlichen durch zwei Schranken begrenzt: Zum ei-

nen waren sie an das Vorliegen einer im Einzelfall bestehenden („konkreten") Gefahr gekoppelt (vgl. §§ 3 Abs. 1, 11-16 SOG), zum anderen durften sich Maßnahmen nur gegen Störer (§§ 8, 9 SOG) sowie gegen sog. Notstandspflichtige (§ 10 SOG) richten, letztere durften jedoch nur unter sehr restriktiven Bedingungen in Anspruch genommen werden. Nach den Vorstellungen der Polizei sollen diese Hindernisse insbesondere für die Informationsverarbeitung abgebaut werden. Um Mißverständnissen vorzubeugen, möchte ich deutlich machen, daß gegen die Erweiterung polizeilicher Befugnisse durch den Gesetzgeber aus Sicht des Datenschutzes grundsätzliche Bedenken nicht zu erheben sind. Es gibt triftige Gründe dafür, schon das Entstehen schwerwiegender Gefahren von vornherein zu verhindern und nicht erst entstandene Gefahren zu bewältigen bzw. gefährdete Personen vor einer Straffälligkeit zu bewahren und sie nicht erst nach Tatbegehung zu fassen und dann einzusperren. Selbstverständlich darf die Polizei auch nicht darauf verwiesen werden, auf neue Gefahrensituationen nur mit alten, z. T. untauglichen Gegenmitteln reagieren zu dürfen. Die grundlegenden Veränderungen des Polizeirechts müssen jedoch klar ausgesprochen und deutlich begründet werden, um ihre Relevanz für den verfassungsrechtlichen Freiheits- und Persönlichkeitsschutz der Bürger in den Gesetzesberatungen ihrer Bedeutung entsprechend würdigen zu können.
Andererseits muß aber auch darauf hingewiesen werden, daß die Novellierung nicht nur dem Zweck dienen kann, die jetzige Polizeipraxis gesetzlich abzusichern. Insbesondere der Verhältnismäßigkeitsgrundsatz gebietet es, die Befugnisse der Polizei einschränkend zu regeln. Wichtig ist ferner, daß das durch die Nutzung neuer Technik entstehende Gefährdungspotential durch restriktive Gesetzesbestimmungen aufgefangen wird.

3.8.5.2 Konsequenzen aus dem Volkszählungsurteil für die SOG-Novelle

Das Bundesverfassungsgericht hat in den Gründen des Volkszählungsurteils eine Reihe von Maßstäben geliefert, an denen sich auch grundrechtsbeschränkende gesetzliche Regelungen der polizeilichen Befugnisse zu orientieren haben. Grundsätzlich muß der Einzelne Beschränkungen seines Rechts auf informationelle Selbstbestimmung danach nur im überwiegenden Allgemeininteresse hinnehmen. Dieses überwiegende Allgemeininteresse muß bei einzelnen Regelungen in der Begründung zum SOG-Entwurf näher dargelegt werden. Das Bundesverfassungsgericht weist darauf hin, daß ein solches überwiegendes Allgemeininteresse regelmäßig nur an Daten mit Sozialbezug bestehen kann, unter Ausschluß unzumutbarer intimer Angaben und von Selbstbezichtigungen.
Soweit eine Beschränkung nach dieser Maßgabe in Betracht kommt, hat sich ihre gesetzliche Ausgestaltung vor allem an folgenden Maßstäben zu orientieren:
- dem Gebot der Normenklarheit
- dem Grundsatz der Verhältnismäßigkeit
- der Pflicht zu (organisatorischen und) verfahrensrechtlichen Schutzvorkehrungen.

Diese Grundsätze gelten für die Erhebung, Speicherung, Weitergabe und sonstige Verwendung von personenbezogenen Daten. Bevor ich jedoch den Regelungsbedarf für die genannten Verarbeitungsphasen näher darstelle, möchte ich mich mit einem Lösungsvorschlag auseinandersetzen, den ich generell nicht für sachdienlich halte.
In den bisherigen Diskussionen hat sich gezeigt, daß die Polizei dazu neigt, die zu schaffenden Eingriffsbefugnisse lediglich an die Erfüllung weitgefaßter Generalklauseln zu binden. Diskutiert wurde etwa die – auch in den Datenschutzgesetzen verwendete – „Erforderlichkeit zur rechtmäßigen Aufgabenerfüllung". Wird der Aufgabenbereich dann ebenfalls nur mit sehr allgemeinen Klauseln umschrieben – wie „Gefahrenabwehr" oder „vorbeugender Schutz vor Straftaten" –, dann kann von Normenklarheit nicht mehr die Rede sein. Dieses Gebot b den Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil, daß der Bürger die Voraussetzungen und den Umfang der Beschränkungen seines Rechts auf informationelle Selbstbestimmung aus der gesetzlichen Eingriffsgrundlage klar und deutlich erkennen kann. Es muß also – für den Bürger erkennbar – präzise und bereichspezifisch geregelt werden, zu welchem Zweck Daten über ihn ggf. verwendet und – falls dies beabsichtigt ist – zu welchem Zweck sie an Dritte übermittelt werden dürfen.
Ich erkenne nicht, daß es für den Gesetzgeber gerade im Bereich der vorbeugenden Verbrechensbekämpfung nicht leicht ist, zu einer größeren Genauigkeit der Regelungen

zu gelangen, ohne gleichzeitig in eine lückenhafte Kasuistik zu verfallen. Wo eine solche Kasuistik – etwa durch Anknüpfung an bestimmte Straftatenkataloge – ausgeschlossen erscheint, müssen andere Eingrenzungsmerkmale zum Zuge kommen. Zu denken wäre etwa an ein Abstellen auf Einzelfälle, Beschränkung auf wenige Einzeldaten, näher definierte Erforderlichkeitsmaßstäbe sowie zusätzliche verfahrensrechtliche Sicherungen. Mangel an Transparenz kann schließlich – auch hierauf hat das Bundesverfassungsgericht hingewiesen – durch ein erheblich verbessertes Auskunftsverhalten gegenüber dem Bürger zumindest teilweise ausgeglichen werden.
Eine weitere generelle Gefahr bei der laufenden Novellierungsdiskussion sehe ich darin, daß z. T. der Versuchung nachgegeben wird, den Forderungen nach einer „Vergesetzlichung" zwar in formaler Weise Genüge zu tun, in der Sache jedoch lediglich die von der Polizei behaupteten Sachzwänge normativ nachzuzeichnen. Ich habe Zweifel (vgl. Nr. 3.8), ob alle von der Polizei z. Z. betriebenen und für notwendig erachteten Maßnahmen der Datenverarbeitung im „überwiegenden Allgemeininteresse" gerechtfertigt und verhältnismäßig sind. Der Grundsatz der Verhältnismäßigkeit von Informationseingriffen besagt vor allem, daß die jeweilige Informationsverarbeitung für einen bestimmten Zweck geeignet und erforderlich sein muß. Insbesondere eine Sammlung nicht anonymisierter Daten auf Vorrat – und darum geht es bei vielen polizeilichen Dateien – zu unbestimmten oder noch nicht bestimmbaren Zwecken ist unzulässig. Es muß also per Gesetz verhindert werden, daß Daten „einfach drauflos" gesammelt und „für alle Fälle" gespeichert werden, ohne daß ein aktueller oder künftiger Bedarfsfall gesetzlich umschrieben ist. Einzelfallbezogene, wenngleich typisierende Abwägungen und konkrete Zweckvorstellungen für Befugnisregelungen sind unabdingbar.

3.8.5.3 Polizeiliche Erhebung von Informationen

Als typische polizeiliche Informationserhebungen, die die Schwelle eines Eingriffs überschreiten und somit einer präzisen, bereichsspezifischen Befugnisnorm bedürfen, sind insbesondere zu nennen:

a) Personalüberprüfungen bzw. Identitätsfeststellungen (insbesondere bei Razzien und an Kontrollstellen),
b) erkennungsdienstliche Behandlung,
c) Befragung von Personen (Verdächtigen, Zeugen, nichtbeteiligten Dritten), soweit eine Auskunftspflicht der Befragten besteht,
d) gezieltes offenes oder heimliches Beobachten (insbesondere „polizeiliche Beobachtung" und „verdeckte Observation"),
e) Auswertung von bei der Polizei oder bei anderen Behörden vorhandenem Informationsmaterial, soweit damit eine Zweckentfremdung der Informationen verbunden ist.

Diese Befugnisse sind, falls sie als unabdingbar anerkannt werden sollten, klar und dem Verhältnismäßigkeitsprinzip entsprechend zu regeln. Insbesondere soweit traditionell bestehende polizeirechtliche Schranken (Gefahr und Polizeipflichtigkeit vgl. Nr. 3.8.5.1) aus Gründen der vorbeugenden Verbrechensbekämpfung durchbrochen werden sollen, ist zu bedenken: Nicht erst seit dem Volkszählungsurteil gilt der Grundsatz, daß die polizeiliche Inanspruchnahme von Nicht-Störern nur als ultima ratio in Betracht kommt.
Maßnahmen gegenüber Nicht-Störern/Nicht-Verdächtigen dürfen daher nur zugelassen werden, wenn sie der Verminderung besonders schwerwiegender Gefahren dienen. Ich erinnere daran, daß die Polizei nach dem Menschenbild des Grundgesetzes nicht jedermann als potentiellen Rechtsbrecher betrachten darf, d. h. daß der einzelne Bürger nicht damit zu rechnen braucht, ohne schwerwiegenden Grund wie ein Rechtsbrecher oder auch nur wie ein Verdächtiger behandelt zu werden. Zwar soll die Polizei einerseits nach Möglichkeit die Verletzung von Rechtsgütern von vorherein verhindern, der Rechtsstaat leistet sich aber andererseits bewußt Beschränkungen einer effektiven Gefahrenbekämpfung. Er nimmt in Kauf, daß nicht alle Gefahren bekämpft und alle Straftäter gefaßt werden, weil andernfalls der Verlust an Freiheitlichkeit für alle zu hoch wäre.
Bei der Formulierung der tatbestandlichen Voraussetzungen für die genannten Maßnahmen hat der Gesetzgeber einen Gestaltungsspielraum. Ich plädiere – je nach der Schwere des Eingriffs – für einen abgestuften Katalog von Voraussetzungen. Für beson-

ders problematisch halte ich – insbesondere im Hinblick auf die Tatsache, daß die Polizei im Gegensatz zu Nachrichtendiensten grundsätzlich offen arbeitet – heimliche Informationserhebungen durch die Polizei. Dies gilt ganz besonders, wenn auch nichtverdächtige Personen erfaßt werden. Solche Maßnahmen können, wenn überhaupt, nur bei Vorliegen besonders schwerwiegender, in einem abschließenden Katalog aufzuzählender Verdachtsgründe zulässig sein. Zu denken ist hier etwa an den Straftatenkatalog des § 129a StGB (und nicht gleich an den sehr viel weiteren des § 100a StPO).
Je stärker ein Eingriff an einen vorhandenen Tatverdacht bzw. eine konkrete Gefahr anknüpft, je offener die Maßnahme und je überschaubarer ihre Folgen für den Betroffenen sind, desto weiter können die Voraussetzungen für einen Eingriff gefaßt sein: d. h. offene Maßnahmen gegen tatverdächtige Personen könnten z. B. von der Schwere des Verdachts bzw. einer zu prognostizierenden Wiederholungsgefahr abhängig gemacht werden, ohne daß die in Betracht kommenden Straftaten eng zu umgrenzen wären.
Einer besonderen Regelung bedarf die Informationserhebung in Versammlungen. Das Bundesverfassungsgericht weist im Volkszählungsurteil ausdrücklich auf die besondere Problematik hin, die darin liegt, daß etwa die Teilnahme an einer Versammlung oder an einer Bürgerinitiative behördlich registriert wird und dazu führen kann, daß die Bürger auf die Ausübung ihrer Grundrechte nach Art. 8, 9 GG verzichten. Hier muß sichergestellt werden, daß zumindest heimliche Erhebungen, mit denen Bürger nicht zu rechnen haben, nur bei konkreten Gefahren mit erheblichem Gewicht in Betracht kommen können. Schließlich sollte nicht unerwähnt bleiben, daß die Ausforschung nicht-öffentlicher Versammlungen nicht nur wegen des Rechts auf informationelle Selbstbestimmung und des Versammlungsrechts, sondern auch wegen der Unverletzlichkeit der Wohnung auf engste verfassungsrechtliche Grenzen stößt. Ein besonderes Problem, das einer speziellen Regelung bedarf, entsteht schließlich, wenn die Informationserhebung durch die Polizei nicht auf das bloße Hören und Sehen beschränkt werden soll, sondern zusätzliche technische Hilfsmittel (wie z. B. Fotoapparate, Videokameras, Tonbandgeräte) zur Anwendung kommen. Wenn solche Aufzeichnungsgeräte gezielt zur Erhebung personenbezogener Informationen eingesetzt werden mit der Absicht, diese für einen bestimmten Zeitraum auch zu speichern und ggf. auszuwerten, müssen m. E. die gleichen tatbestandlichen Voraussetzungen gelten wie etwa bei einer erkennungsdienstlichen Behandlung. Sollen solche technischen Mittel gar verdeckt eingesetzt werden, ist die Schaffung ähnlicher Voraussetzungen nötig wie in § 100a StPO für eine Telefonüberwachung.
Einer besonderen Rechtgrundlage für die Erhebung bedarf es nur dann nicht, wenn technische Geräte zu Zwecken eingesetzt werden, die nicht auf die Erhebung personenbezogener Daten zielen (z. B. Verkehrsüberwachung, Gebäudeüberwachung). Diese Unterlagen dürfen allerdings nicht personenbezogen ausgewertet werden. In diesem Fall läge wiederum ein Eingriff vor, der einer einschränkenden Rechtsgrundlage (Grundlage könnten z. B. der Katalog des § 129a oder allenfalls der des § 138 StGB sein) bedarf.

3.8.5.4 Polizeiliche Speicherung von Informationen

Das Bundesverfassungsgericht hat im Volkszählungsurteil die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken für verfassungsrechtlich unzulässig erklärt. Es ist daher erforderlich, die Zweckbestimmungen der unterschiedlichen polizeilichen Datensammlungen einmal genau zu überprüfen sowie die zulässigen Zwecke einschließlich der sich daraus ergebenen Konsequenzen (Voraussetzung, Inhalt und Dauer der Informationsspeicherung) genau festzulegen.
Nach meinen Erfahrungen mit polizeilichen Datensammlungen, die ich in meinem ersten TB schon ausführlich geschildert habe, ist es wichtig, daß zwischen der Speicherung in sog. „Kriminalpolizeilichen personenbezogenen Sammlungen" (KpS) und Speicherungen zu sonstigen Zwecken (Vorgangsnachweise, Dokumentation etc.) unterschieden wird.
Innerhalb der KpS ist weiter zu unterscheiden zwischen solchen Informationen, die zur Durchführung konkreter Strafverfahren verarbeitet werden (z. B. Ermittlungsakten, Personenfahndungsdaten, z. T. auch Spurendokumentationssysteme) und anderen Unter-

lagen, die ohne Bezug zu einem laufenden Ermittlungsverfahren lediglich zur vorbeugenden Bekämpfung von Straftaten aufbewahrt werden. Dazu gehören z. B. erkennungsdienstliche Unterlagen, Kriminalakten, Aktennachweissysteme wie KAN und ED-Datei, manuelle Straftäterdateien, Falldateien sowie Aktenerschließungssysteme wie PIOS und SPUDOK's.
Die zuerst genannten Sammlungen kann ich im hier interessierenden Zusammenhang vernachlässigen. Sie sollten im Zusammenhang mit der strafprozessualen Informationsverarbeitung der Staatsanwaltschaft und der Strafgerichte geregelt werden (vgl. Nr. 3.12.1). Bei den Datensammlungen zu Zwecken der vorbeugenden Verbrechensbekämpfung sollte nach meiner Auffassung ein abgestuftes System von Speicherbefugnissen entwickelt werden. Die Entscheidung, welche Daten zu diesem Zweck wie und unter welchen konkreten Voraussetzungen gespeichert werden dürfen, hängt – worauf auch das Bundesverfassungsgericht abstellt – entscheidend ab von ihrer Nutzbarkeit und ihren Verwendungsmöglichkeiten. Wesentlich sind also die der jeweiligen Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten. Daraus folgt:

- Kriminalakten, erkennungsdienstliche Unterlagen klassischer Prägung und manuelle Straftäterdateien dürfen angelegt werden, wenn es sich um erhebliche Straftaten handelt und aufgrund tatsächlicher Anhaltspunkte die Gefahr der Wiederholung erheblicher Straftaten mit hinreichender Sicherheit anzunehmen ist.
- Bei der Erschließung solcher Unterlagen durch automatisierte Systeme ist zweierlei zu beachten: ein überregionaler Zugriff darf nur möglich sein auf Täter, die auch von überregionaler Bedeutung sind (vgl. Nr. 3.8.1.3 und 3.8.1.5). Die Speicherung sollte auf den Zweck des System – nämlich den Nachweis von Unterlagen – begrenzt werden (vgl. Nr. 3.8.1.1).
- Die weitgehendsten Verarbeitungs- und Verknüpfungsmöglichkeiten werden der Polizei derzeit durch Systeme wie PIOS und SPUDOK eröffnet. Der Nutzbarkeit der Daten sind kaum Grenzen gesetzt. Der Gesetzgeber muß hier m. E. genau festlegen, daß solche Systeme nur zur vorbeugenden Bekämpfung besonders erheblicher Straftaten und mit strengen verfahrensrechtlichen Sicherungen betrieben werden dürfen (vgl. Nr. 3.8.2).

Für Datensicherungen jeglicher Art muß klargestellt werden, daß nur Informationen, die die Polizei in rechtmäßiger Weise erhoben hat, gespeichert (und anderweitig verwertet) werden dürfen. Zusätzlich sind besondere Sicherungen für die Fälle vorzusehen, in denen die Polizei Bewertungen, also sog. „weiche" Informationen, speichert. Es liegt in der Natur der Sache, daß die Polizei häufig mit Informationen umzugehen hat, die auf subjektiven Beurteilungen beruhen: z. B. Verdächtigungen, Einschätzungen einer Gefahr, Prognosen. Für die betroffenen Bürger wie für die Polizei ist es gleichermaßen wichtig, daß solche „weichen" Informationen wegen ihrer besonderen Risiken (Unrichtigkeiten, subjektive Wertungen) überprüfbar bleiben. Daher muß durch entsprechende Hinweise klargestellt werden, daß jederzeit eine Beziehung zur Tatsachenbasis der Wertungen herstellbar ist. Dies gilt umso mehr, wenn über Informationssysteme Personen Zugriff auf die Daten nehmen, die den der Speicherung zugrundeliegenden Sachverhalt nicht kennen können.
Schließlich ist daran zu erinnern, daß in engem Zusammenhang mit der Befugnis zur Speicherung von Informationen auch Verpflichtungen zur Bereinigung und Löschung von Informationen zu sehen sind. Auch hier ist der Gesetzgeber gefordert, typisierte Prüf- und Löschungsregelungen – differenziert nach den verschiedenen Arten der Speicherung – zu treffen.

3.8.5.5 Weitergabe von Daten durch die Polizei

Bei der Regelung der Weitergabe ist von dem Grundsatz auszugehen, daß die Verwendung von Daten auf den gesetzlich bestimmten Zweck zu begrenzen ist. Das Bundesverfassungsgericht verlangt im Volkszählungsurteil ausdrücklich, daß insbesondere angesichts der Gefahren der automatisierten Datenverarbeitung ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich ist.

Daher ist klar zu regeln, aus welchen Arten von Datensammlungen, die die Polizei zur vorbeugenden Bekämpfung von Straftaten unterhält, Informationen weitergegeben werden dürfen. Grundsätzlich sollten als Empfänger solcher Datenübermittlungen nur andere Polizeibehörden in Betracht kommen, da nur dort eine zweckgerechte Verwendung der Daten gewährleistet erscheint.
Eine spezielle Problematik im Hinblick auf das Trennungsgebot gibt es für die Weitergabe polizeilicher Daten an den Verfassungsschutz (vgl. Nr. 3.10.2).

3.8.5.6 Sonstige Verwendung polizeilicher Daten

Das Bundesverfassungsgericht hat im Volkszählungsurteil klargestellt, daß nicht nur die Erhebung, Speicherung und Weitergabe, sondern auch die (sonstige) Verwendung personenbezogener Informationen das Recht auf informationelle Selbstbestimmung berührt. Die Polizei kann also mit den Daten, die sie rechtmäßig gespeichert hat, nicht nach Gutdünken verfahren, sondern muß sich stets am gesetzlich festgelegten Zweck orientieren.
In der Vergangenheit haben sich dabei vor allem drei Bereiche als besonders problematisch und regelungsbedürftig erwiesen:
- der Abgleich erhobener Daten mit eigenen Dateien;
- der Abgleich polizeilicher Daten mit Beständen anderer staatlicher Stellen, insbesondere Melderegister und Zentrales Fahrzeugregister (ZEVIS);
- der Abgleich mit Datenbeständen privater Stellen.

Aus verfassungsrechtlicher Sicht ist zunächst zu betonen, daß ein Abgleich neu erhobener mit bereits gespeicherten eigenen Daten der Polizei nur zulässig ist, wenn er vom Zweck der Erhebung sowie vom Zweck der Speicherung umfaßt wird. Schon nach geltendem Recht ist daher ein Abgleich der im Rahmen von Identitätsfeststellungen gewonnenen Daten in den polizeilichen Fahndungsdateien zulässig, denn die Identitätsfeststellung dient u. a. der Prüfung, ob eine bekannte Person mit einer gesuchten identisch ist.
Ich betone aber, daß die Voraussetzungen für eine Identitätsfeststellung vorliegen müssen. Abgleiche mit den Fahndungsdateien dürfen nicht zu jedem beliebigen Anlaß (wie routinemäßiges Abfragen bei Verkehrsunfällen, Verkehrskontrollen nach der StVZO, Aufnahme von Anzeigen und Fundmeldungen etc.) vorgenommen werden.
Problematisch ist es ferner, wenn z. B. Daten einer Person, die zufällig etwa in eine Kontrollstelle geriet, mit speziellen Datensammlungen wie PIOS und SPUDOK abgeglichen werden sollen. Hier bedarf es einer klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen ein Bürger eine solche Maßnahme dulden muß (vgl. auch Nr. 3.8.2.3 zum Stichwort „Massendatenverarbeitung").
Ein weiterer Problemkomplex läuft in der öffentlichen Diskussion unter dem Stichwort „Rasterfahndung". Bei dieser Methode geht es – im Gegensatz zur herkömmlichen Personen- oder Sachfahndung aufgrund konkreter tat- bzw. täterbezogener Verdachtsmerkmale – um eine systematische automatisierte Suche nach Personen und Sachen, bei der wegen der technischen Möglichkeiten ein praktisch unbegrenzter Kreis zunächst nichtverdächtiger Personen auf das Vorliegen oder Nichtvorliegen bestimmter Einzelmerkmale überprüft wird, um so schrittweise einen immer enger werdenden Personenkreis herauszufiltern, auf den immer mehr, für den Täter als charakteristisch angenommene Einzelmerkmale zutreffen. Auf diesem Wege hofft man, ermittlungsfähige Einzelspuren zu gewinnen.
Diese neuartige Fahndungsmethode bedarf aus zwei Gründen einer einschränkenden gesetzlichen Regelung: Zum einen werden bei der Rasterfahndung massenhaft Nicht-Verdächtige in Anspruch genommen. Desweiteren werden dabei regelmäßig Dateien ausgewertet, die zu ganz anderen Zwecken angelegt wurden. Es ist daher dringend geboten, die näheren Voraussetzungen für die Zulässigkeit eines Datenabgleichs z. B. näher zu umreißen. So könnte auf den Grad der Gefahr oder das Gewicht der aufzuklärenden Verbrechen abgestellt werden.
Wichtig sind hier auch besondere verfahrensrechtliche Sicherungen. So sollte die Entscheidung über die Durchführung einer Rasterfahndung auf die höchste, politisch verantwortliche Verwaltungsebene verlagert werden. „Ausgerasterte" Datenbestände und

Unterlagen sind sofort von Amts wegen zu löschen bzw. zu vernichten. Die Vernichtung muß protokolliert werden. Der Datenschutzbeauftragte ist über die Anforderung von Daten für Zwecke der Rasterfahndung zu unterrichten.
Schließlich bedarf es einer klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen Datensammlungen wie das Melderegister oder das Zentrale Fahrzeugregister für einen Abgleich mit Fahndungsdaten der Polizei zweckentfremdet werden dürfen. Ein solcher Abgleich kommt im Ergebnis der Einrichtung einer permanenten Kontrollstelle für einen bestimmten Personenkreis gleich. Für die Bewertung der Qualität eines Informationseingriffs kommt es nicht darauf an, ob Daten zu Zwecken einer Fahndungsabfrage direkt bei einem betroffenen Nicht-Störer bzw. Nicht-Verdächtigen erhoben werden (wie bei Razzien und Kontrollstellen) oder aber ob sie – sozusagen im Wege der Ersatzvornahme – bei der Meldebehörde abgefordert werden.
Im übrigen weise ich darauf hin, daß auch ein Abgleich zum Zwecke der Aktualisierung von KpS-Unterlagen unverhältnismäßig sein dürfte. Genausowenig wie sie zu diesem Zweck einen unverdächtigen, nicht polizeipflichtigen Bürger anhalten und seine Personalien feststellen darf, ist ein solcher Eingriff im Wege der Ersatzvornahme durch die Nutzung von Meldedaten zulässig.

3.8.5.7 Auskunftsrecht des Betroffenen

Die gegenwärtig gegenüber den Sicherheitsbehörden geltenden Einschränkungen des Auskunftsanspruchs sind nach dem Urteil des Bundesverfassungsgerichts nicht mehr zu halten. Ich sehe mich vielmehr in meiner Forderung nach Aufhebung des § 14 Abs. 2 Nr. 1 und Angleichung des Auskunftsanspruchs gegenüber der Polizei an den allgemeinen Auskunftsanspruch bestätigt (vgl. 2. TB, Nr. 3.9.2.4, S. 76 f).

3.9 Straßenverkehrswesen

Einer der Schwerpunkte meiner Tätigkeit im Berichtszeitraum lag im Bereich des Straßenverkehrswesens. Zum einen wird z.Z. eine umfangreiche Änderung des Straßenverkehrsgesetzes (StVG) im Zusammenhang mit der Einführung des Zentralen Verkehrs-Informationssystems (ZEVIS) beim Kraftfahrtbundesamt (KBA) in Flensburg vorbereitet (vgl. auch meinen 2. TB, Nr. 3.10.6.3, S. 89). Des weiteren habe ich die Umorganisation der Landesverkehrsverwaltung (bisher Fachdirektion 8) der Polizei zum Anlaß genommen, einmal die Informationsverarbeitung in dieser Dienststelle zu überprüfen.

3.9.1 Überprüfung der Landesverkehrsverwaltung (LVV)

Bei der Landesverkehrsverwaltung werden personenbezogene Daten vornehmlich bei der Zulassungsstelle für Verkehrsteilnehmer (Führerscheinstelle) sowie bei der Zulassungsstelle für Kraftfahrzeuge verarbeitet. Beide Dienststellen habe ich im Sommer dieses Jahres besucht. Die Ergebnisse meiner Überprüfungen habe ich nachfolgend kurz zusammengefaßt dargestellt. Da ich sie der Behörde für Inneres erst im Oktober mitteilen konnte, lag eine Stellungnahme bei Berichtsschluß noch nicht vor.

3.9.1.1 Führerscheinstelle

Die Führerscheinstelle hat die Aufgabe zu prüfen, ob die nach der Straßenverkehrs-Zulassung-Ordnung (StVZO) geforderten Voraussetzungen für die Erteilung bzw. Entziehung eines Führerscheins vorliegen. Über die ausgehändigten Führerscheine führt sie zu diesen Zwecken die sog. Führerscheinkartei (§ 10 StVZO).

Abgesehen davon, daß einige bereichsspezifische Regelungen zur Erhebung, Speicherung und Weitergabe der in der Führerscheinkartei enthaltenen Daten fehlen, habe ich hier in einigen Fällen spezielle Verletzungen datenschutzrechtlicher Bestimmungen feststellen müssen.

- Es werden zu viele Daten erhoben:
  Der Betroffene (Antragsteller) hat regelmäßig anhand von Formularen beim Antrag auf eine reguläre Fahrerlaubnis, auf Umschreibung einer ausländischen Fahrerlaubnis, auf eine Fahrerlaubnis zur Fahrgastbeförderung sowie auf einen Ersatzführerschein zahlreiche personenbezogene Daten anzugeben. Es werden der Name, Vorname, Geburtstag und Geburtsort, die Staatsangehörigkeit, die Anschrift und der Geburtsname der Mutter sowie der Beruf erfragt. Zusätzlich muß der Antragsteller angeben, ob er Brillenträger oder körperbehindert ist.

  Die Richtigkeit dieser Angaben wird mit Hilfe des Personalausweises, Passes oder einer Anmeldebestätigung der Meldebehörde bezüglich der Personenidentität und mit Hilfe eines Nachweises über eine Sehprüfung bzw. eines augenärztlichen Gutachtens bezüglich der Brillenträgereigenschaft überprüft. Als Rechtsgrundlagen für die Erhebungen können generell die §§ 8, 15, 15e der StVZO herangezogen werden. Für die Angabe des Berufs ist allerdings eine Rechtsgrundlage nicht erkennbar. Gleiches gilt für die Angabe des Geburtsnamens der Mutter. Angesichts der übrigen erfragten Identifikationsmerkmale, d.h. des Namens, Vornamens, Geburtstages, Geburtsortes und der Adresse sind diese Angaben auch nicht erforderlich. Eine Identitätsfeststellung ist mit Hilfe der übrigen Daten ohne weiteres möglich, zumal auch in dem zur Kontrolle der Angaben einzusehenden Personalausweis eine Angabe dieses Datums nicht erscheint.

  Für die Entbehrlichkeit dieser Angaben spricht schließlich auch, daß sie in der nach § 10 Abs. 2 Satz 2 StVZO geführten Kartei nicht mit enthalten sind. Ich habe der Behörde für Inneres daher empfohlen, diese Daten künftig gar nicht erst zu erheben.

- Der auf den Erhebungsformularen enthaltene Datenschutzhinweis entspricht nicht den Anforderungen des § 9 Abs. 2. Aus ihm geht nicht hervor, aufgrund welcher Rechtsvorschrift die Daten erhoben werden. Der Hinweis ist daher neu zu fassen. Dafür käme – je nachdem, um welchen Antrag es sich handelt – etwa folgender Wortlaut in Betracht:

  „Die vorstehenden Daten werden erhoben aufgrund des § 8/§ 15/§ 15e StVZO".

  Um die Datenverarbeitung für den Betroffenen möglichst transparent zu machen, könnte hinzugefügt werden:

  „Sie werden nach Maßgabe des § 10 Abs. 2 StVZO von der Zulassungsstelle in einer Kartei gespeichert".

- Nach § 15 Abs. 1 Satz 1 StVZO hat die Straßenverkehrsbehörde Personen die Fahrerlaubnis zu entziehen, die sich als ungeeignet zum Führen von Kraftfahrzeugen erweisen. Zur Erfüllung dieser Aufgabe werden der LVV von diversen öffentlichen Stellen regelmäßig Informationen übermittelt, z.B. über strafbare Verhaltensweisen, psychische Störungen etc. Ausdrückliche Rechtsgrundlagen für derartige Übermittlungen fehlen nach meinen Informationen. Regelungen finden sich z.Z. nur in diversen Verwaltungsvorschriften.

  Zu nennen sind hier die
  - Allgemeine Verwaltungsvorschrift (AVwV) zu § 15b StVZO, wonach das Kraftfahrtbundesamt eine Mitteilung über Eintragungen im Verkehrszentralregister von 9 Punkten aufwärts an die Zulassungsstelle meldet;

  - Anordnung über Mitteilungen in Strafsachen (MiStra), wonach die Staatsanwaltschaft der Zulassungsstelle die Einstellung von Strafverfahren in Straßenverkehrssachen mitteilt, wenn für die Landesverkehrsverwaltung Anlaß bestehen könnte, die Fahrerlaubnis zu entziehen;

- Nr. VI der Anordnung über Mitteilungen in Zivilsachen, wonach die Gerichte Beschlüsse und Urteile in Entmündigungs- oder Pflegschaftsverfahren mitzuteilen haben.

- Ferner gibt es noch mehr oder weniger regelmäßig Mitteilungen von Gesundheitsämtern, Versorgungsämtern, Krankenhäusern und ähnlichen Einrichtungen.

Ich erkenne grundsätzlich an, daß die Zulassungsstelle auf Mitteilungen über Eignungsmängel angewiesen ist, um ihre Aufgabe nach § 15b StVZO zu erfüllen; aus verfassungsrechtlichen Gründen ist jedoch auf die Schaffung hinreichender Eingriffsgrundlagen für derartige Übermittlungen hinzuwirken. Zu denken wäre hier etwa an eine Ergänzung des StVG, die öffentliche Stellen unter bestimmten Voraussetzungen berechtigt bzw. verpflichtet, die Straßenverkehrsbehörde über Eignungsmängel in Kenntnis zu setzen.

- Im Falle der Ausstellung eines Ersatzführerscheins wird bei der ausstellenden Behörde des alten Führerscheins zunächst telefonisch und dann durch Übersendung einer Karteikartenabschrift der dort vorhandene Datenbestand abgefragt. Dieses Vorgehen rechtfertigt sich dadurch, daß eine Zentrale Führerscheinkartei nicht existiert und die Aufgabe der Zulassungsstelle im Rahmen von § 15b StVZO und die ordnungsgemäße Überprüfung der Angaben andernfalls nicht möglich wäre.

  Gleichwohl ist auch in diesem Fall auf die Schaffung einer Rechtsgrundlage für die Nachfrage hinzuwirken. Solange eine solche nicht besteht, sollte eine Nachfrage nur mit Einwilligung des Antragstellers erfolgen. Diese sollte in das entsprechende Antragsformular aufgenommen werden.

Die laufende Novellierung des StVG bezieht bislang ergänzende Regelungen für die Informationsverarbeitung in den Führerscheinstellen nicht mit ein. Ich habe der Behörde für Inneres mitgeteilt, daß ich es für zweckmäßig halte, diesen Bereich im anstehenden Gesetzgebungsverfahren sogleich mitzuregeln, und auch die anderen Datenschutzbeauftragten um Unterstützung gebeten.

3.9.1.2 Kfz-Zulassungsstelle

Die Kfz-Zulassungsstelle hat nach der StVZO die Aufgabe, die Voraussetzungen für die Zulassung von Fahrzeugen zum Straßenverkehr zu überwachen. Zum Nachweis der zugelassenen Fahrzeuge führt sie das örtliche Fahrzeugregister nach § 26 StVZO.

Die Informationsverarbeitung entspricht, soweit ich das überprüft habe, weitgehend den geltenden Vorschriften. Festzustellen war allerdings, daß auch die von der Kfz-Zulassungsstelle benutzten Formulare den Anforderungen des § 9 Abs. 2 nicht gerecht werden. Sie enthalten insbesondere keinen Hinweis auf die §§ 23, 27 StVZO, die derzeit noch den Umfang dedung bzw. Änderungsmeldungen zu erhebenden Daten regeln.

Nicht überprüfen konnte ich im Berichtszeitraum die örtlich zuständigen Zulassungsstellen (Verkehrsabteilungen der Wirtschafts- und Ordnungsämter) in Harburg und Bergedorf. Dies soll umgehend nachgeholt werden.

Im übrigen ist die Erhebung, Speicherung, Weitergabe und sonstige Verwendung von Kfz-Registerdaten gegenwärtig Gegenstand umfangreicher Neuregelungen des StVG. In einem eigenen Abschnitt des StVG soll – statt wie bisher in der StVZO – auch für die örtlichen Fahrzeugregister bereichsspezifisch präzise festgelegt werden, welche Informationseingriffe die Kfz-Zulassungsstellen vornehmen dürfen. Die vorgeschlagenen Regelungen sind, soweit sie den öffentlichen Bereich betreffen, weitgehend akzeptabel. Auf Probleme insbesondere im Zusammenhang mit der Einführung von ZEVIS gehe ich weiter unten ein. Ein Punkt soll allerdings bereits an dieser Stelle erörtert werden.

Der Gesetzentwurf sieht vor, daß das Kfz-Register grundsätzlich nur zum Zweck der Identifizierung von Kraftfahrzeugen und Kraftfahrzeughaltern genutzt werden darf. Das Zweckentfremdungsverbot soll allerdings durch zu weit gehende Ausnahmeregelungen durchbrochen werden. Die Datenschutzbeauftragten haben wiederholt darauf hingewiesen, daß eine Nutzung der Registerdaten, die sich nicht an der Eigenschaft der betroffenen Personen als Fahrzeughalter orientiert, also z.B. zur Anschriftenermittlung für andere Zwecke, faktisch zu einer Art Bundes-Adreß-Register für die Mehrheit der erwachsenen Bevölkerung führt. Eine solche Durchbrechung des Zweckbindungsprinzips kann allenfalls ausnahmsweise für genau eingegrenzte Fallgruppen zugelassen werden, soweit es im überwiegenden Allgemeininteresse zulässig ist. Eine pauschale Auflösung der Zweckbindung, „um die Strafverfolgung, die Strafvollstreckung, die Abwehr von Gefahren für die Öffentliche Sicherheit oder Ordnung oder die Erfüllung der den Behörden für den Verfassungsschutz obliegenden Aufgaben zu gewährleisten", ist verfassungsrechtlich bedenklich.

Notwendig erscheinen daher auch hier präzise, einschränkende Regelungen der Voraussetzungen, unter denen Polizei und Verfassungsschutz Registerdaten – zweckentfremdet – nutzen dürfen.

3.9.2 Einführung von ZEVIS

Wie ich bereits in meinem 2. TB (Nr. 3.10.6.3) dargestellt habe, will das KBA ein Zentrales-Verkehrs-Informationssystem einführen, mit dem örtliche Zulassungsstellen, die Polizei sowie Zollfahndungsdienststellen im Wege des Direktabrufs Daten aus dem Zentralen Fahrzeugregister sowie dem Verkehrszentralregister sollen abfragen können.

Ein Teil von ZEVIS ist bereits in Betrieb, obwohl die allseits für erforderlich gehaltenen gesetzlichen Grundlagen noch nicht einmal in das Gesetzgebungsverfahren eingebracht worden sind. Datenbestände zahlreicher Zulassungsbezirke können bereits im ZEVIS abgefragt werden. Die Bestände der Hamburger Zulassungsstellen sind jedoch noch nicht überspielt worden. Der Hamburger Polizei stehen jedoch bereits Datenstationen für die ZEVIS-Abfrage zur Verfügung. Ich habe der Behörde für Inneres mehrfach meine Bedenken gegen die geplanten on-line-Anbindungen insbesondere für die Polizei dargelegt (vgl. Nr. 3.9.2.1). Darüber hinaus halte ich insbesondere – die nach dem StVG-Entwurf vorgesehene – Einstellung von Steckbriefnachrichten, Suchvermerken sowie die Durchführung von Fahndungsabgleichen für problematisch.

3.9.2.1 On-line-Zugriff auf ZEVIS

Bei der Bewertung von on-line-Zugriffen ist – wie ich oben im Zusammenhang mit den on-line-Zugriffen der Polizei auf das Melderegister (Nr. 3.7.1.3) bereits dargelegt habe – eine Güterabwägung zwischen der Intensität und Dringlichkeit des Informationsbedarfs der Verwaltung auf der einen und den Risiken einer Verletzung von Persönlichkeitsrechten der Bürger auf der anderen Seite vorzunehmen. Bei der Problematik des on-line-Zugriffs auf zentrale bundesweite Register erscheint mir die Gefahr einer extensiven Nutzung besonders gravierend. Das Zentrale Fahrzeugregister könnte sich – wenn die in der bisherigen Praxis zu übersteigenden Schwellen wegfallen – zu einer Art Bundes-Adreß-Register entwickeln. Es ist zu befürchten, daß insbesondere die Polizei angesichts des gegenwärtigen – bei vielen Gemeinden noch nicht weit fortgeschrittenen – Ausbaustandes des automatisierten Meldewesens, aber auch um die bisweilen hinderliche kommunale Begrenzung der Melderegister zu überwinden, die Gelegenheit wahrnimmt, sich Auskünfte, die von den Meldebehörden nur mit Schwierigkeiten zu holen sind, vom BKA zu beschaffen.

Der Entwurf zur Änderung des StVG sieht on-line-Anschlüsse außer für polizeiliche Dienststellen auch für örtliche Zulassungsstellen, Bußgeldstellen und für das Zoll-Kriminalinstitut (ZKI) vor. Eine Analyse der Angemessenheit im Hinblick auch auf diese geplanten Anschlüsse ist bisher nicht erfolgt. Nach meinen Informationen ist bisher we-

der die Intensität noch die Dringlichkeit des Informationsbedarfs hinreichend belegt worden. Die Hamburger Landesverkehrsverwaltung etwa schätzt den Bedarf der Zulassungsstellen eher gering ein. Auch eine Nutzwert-Analyse des on-line-Verfahrens im Vergleich zu anderen Übermittlungsverfahren steht nach meiner Kenntnis aus. Dementsprechend gibt es auch keine Abwägung der verschiedenen Gesichtspunkte.

Jegliche Information fehlt bislang im Hinblick auf eine Angemessenheit des Anschlusses für das ZKI. Vertieft diskutiert worden sind bislang nur die geplanten on-line-Anschlüsse für polizeiliche Dienststellen. Bei der Beurteilung dieser Zugriffsmöglichkeiten ist nach verschiedenen Zwecken zu differenzieren:

- Anfragen, die der Identifizierung unbekannter Fahrzeuge dienen (1);
- Anfragen mit Halterdaten zu anderen Zwecken (2);
- Anfragen an das VZR.

(1) Bei der Halter-Identifikations-Anfrage geht es darum, anhand des amtlichen Kennzeichens oder von Teilen eines Kennzeichens zu ermitteln, welche Halterdaten zu einem bestimmten Fahrzeug gespeichert sind. Diese Anfrage entspricht den eigentlichen Zwecken des Fahrzeugregisters.

Die Intensität und Dringlichkeit eines schnellen Zugriffs der Polizei dürfte im Grundsatz anzuerkennen sein. Nach der Begründung zum StVG-E werden täglich ca. 16.000 Anfragen von Polizei- und Justizbehörden beantwortet. Es handelt sich also um ein Massengeschäft. Dieses Bedürfnis kann auch nicht durch einen Zugriff auf die Register der örtlichen Zulassungsstellen befriedigt werden, es sei denn, jede abfrageberechtigte Stelle hätte unmittelbaren Zugriff auf jedes Register. Schließlich dürfte anzuerkennen sein, daß die Polizei in sehr vielen Fällen auch schnelle Auskünfte über den Halter eines Wagens benötigt.

Abzuwägen gegenüber dem anzuerkennenden Informationsbedarf sind die mit dem on-line-Anschluß verbundenen besonderen Risiken. Das besondere Risiko ist vor allem darin zu sehen, 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. Die Annahme, daß praktische Fälle eines latenten polizeilichen Informationsbedarfs, der bei konventioneller Technik nicht, bei einem on-line-Zugriff jedoch sehr wohl befriedigt wird, nicht ersichtlich sind, kann ich nicht bestätigen. Kontrollmaßnahmen wie z.B. die „Aktion Gitternetz" in Rheinland-Pfalz oder – was in der Praxis schon häufiger vorgekommen ist – die Überprüfung aller abgestellten Kraftfahrzeuge in der Umgebung einer Demonstration bzw. eines Versammlungslokals machen deutlich, wo die Polizei die Kontrolldichte erhöhen möchte. Diese Absichten werden noch dadurch unterstrichen, daß die Polizei immer wieder betont, welche wichtige Rolle Kraftfahrzeuge bei der Begehung von Straftaten spielen.

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"). Die „H-Anfrage" ist hervorragend geeignet, Bewegungsbilder herzustellen.

Gegenüber diesen technischen Möglichkeiten sind Rechtsgrundlagen für derartige Kontrollmaßnahmen allenfalls rudimentär vorhanden. In § 36 Abs. 5 StVO ist lediglich bestimmt, daß Polizeibeamte Verkehrsteilnehmer zur Verkehrskontrolle anhalten dürfen. Insbesondere Befugnisse zur heimlichen Halterfeststellung gibt es nicht. Die Vorschriften der StPO zur Errichtung von Kontrollstellen (§ 111) bzw. zur Identitäts-

feststellung (§ 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.

Diese eng begrenzten rechtlichen Befugnisse haben die Polizei in der Vergangenheit jedoch nicht gehindert, wesentlich weitergehende Kontrollmaßnahmen durchzuführen. Ich räume ein, daß der Gesetzgeber die Polizei zu einer angemessen effektiven Aufgabenerfüllung – vor allem zur vorbeugender Bekämpfung schwerer Straftaten – möglicherweise mit weitergehenden Befugnissen ausstatten müßte.

Ich halte es jedoch für bedenklich, der Polizei erheblich erweiterte technische Kontrollmöglichkeiten zu geben, ohne daß der Gesetzgeber zuvor eindeutig festlegt, welches Ausmaß an Kontrollen er der Bevölkerung zumuten will. Die Einführung der H-Anfrage im on-line-Zugriff auf das BKA muß daher von der Schaffung klarer Erhebungsbefugnisse für die Polizei abhängig gemacht werden.

(2) Neben der Halter-Identifikation ist ferner vorgesehen, daß die Polizei das zentrale Fahrzeugregister auch zu sonstigen Zwecken benutzen darf, die mit dem eigentlichen Zweck nichts zu tun haben („erweiterte Verwertung"). Mit der sog. P-Anfrage sollen der Polizei zum einen Fahrzeugdaten (einschl. der amtlichen Kennzeichen) sowie darüber hinaus sämtliche anderen gespeicherten Personendaten (wie Adresse, Geburtsdatum, Geburtsort etc.) zur Verfügung gestellt werden.

Bereits die Intensität und Dringlichkeit des Bedarfs für die on-line-P-Anfrage erscheint mir zweifelhaft. Zunächst einmal ist der quantitative Bedarf bislang völlig offen. Wenn man – nach den vorliegenden Zahlen – von 1.600 P-Anfragen im Monat ausgeht und diese auf die diversen Polizeidienststellen in Bund und Ländern verteilt, so kann man – auch im Vergleich zur H-Anfrage – eindeutig feststellen, daß es nicht um die Bewältigung eines Massengeschäfts geht.

Auch in einer Stellungnahme des BKA, die an zahlreichen Beispielen die Dringlichkeit aus polizeilicher Sicht darzulegen versucht, ist – von wenigen sehr theoretischen Ausnahmefällen abgesehen – nicht belegt worden, daß die mit der P-Anfrage zu erlangenden Informationen im einstelligen Sekundenbereich vorliegen müssen. In aller Regel dürfte eine Beantwortung innerhalb weniger Sekunden bis Minuten – was auch auf telefonischem Wege erreicht werden kann – nicht zu wesentlichen Behinderungen führen.

Im Ergebnis bin ich daher der Auffassung, daß das polizeiliche Informationsbedürfnis bislang nicht dargelegt ist und somit eine ausreichende Beurteilungsgrundlage nicht besteht. Das bedeutet, daß dem StVG-Änderungs-Entwurf, soweit er die P-Anfrage gestattet, schon deshalb nicht zugestimmt werden kann, weil der Informationsbedarf der Polizei ein solches Verfahren nicht trägt, ohne daß es auf das Ergebnis einer Risiko-Analyse und einer anschließenden Gegenüberstellung von Risiken und Informationsbedarf noch ankommt.

3.9.2.2 Fahndungsabgleich sowie Einstellung von Suchvermerken und Steckbriefnachrichten

Im Entwurf des StVG-Änderungsgesetzes ist vorgesehen, daß die Polizei – zusätzlich zu regulären Auskünften und der Möglichkeit eines Direktabrufverfahrens – im zentralen Fahrzeugregister Suchvermerke und Steckbriefnachrichten über Personen (Zeugen, Beschuldigte, Verurteilte), deren Aufenthalt unbekannt ist, niederlegen sowie darüber hinaus einen Datenabgleich zwischen dem Fahndungsbestand des BKA (beschränkt auf mit Haftbefehl oder mit Steckbrief gesuchte Personen) und den Halterdaten des Kraftfahrtbundesamtes veranlassen darf.

Zwar kann nach dem jetzigen Stand der Rechtsprechung nicht festgestellt werden, daß eine solche Zweckentfremdung bei ausdrücklicher gesetzlicher Regelung, wie sie in Abs. 4 vorgesehen ist, mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG unvereinbar wäre. Jedoch ist darauf hinzuweisen, daß das Bundesverfassungsgericht gerade in der Verknüpfung von verschiedenen Zwecken eine Gefahr für das Recht auf informationelle Selbstbestimmung gesehen und die informationelle Gewaltenteilung für einen wichtigen Schutz des einzelnen erachtet hat.

Da der einzelne heute häufig auf ein eigenes Kraftfahrzeug und damit auf die Angabe der im Kraftfahrzeugregister gespeicherten Daten angewiesen ist, bedarf jede Zweckentfremdung besonders sorgfältiger Prüfung und einer Rechtfertigung durch eindeutig überwiegende Belange des Gemeinwohls.

(1) Gegen die Niederlegung von Steckbriefnachrichten durch die hierfür zuständigen Behörden ist grundsätzlich nichts einzuwenden. Die Voraussetzungen für eine steckbriefliche Verfolgung gesuchter Personen sind in § 131 StPO eingehend umschrieben, und auch im Bundeszentralregister ist die Niederlegung von Steckbriefen vorgesehen (§ 25 BZRG).

Die Behandlung von Steckbriefen beim KBA muß allerdings deutlicher und eingeschränkter geregelt werden. Nach § 40 Abs. 3 Satz 2 hat das KBA der niederlegenden Behörde die Halter- und erforderlichen Fahrzeugdaten zu übermitteln, wenn das Register eine Eintragung über die gesuchte Person „enthält". Ungeklärt ist, was zu geschehen hat, wenn das Register neue Mitteilungen über einen Betroffenen enthält. Für diese Fälle dürfte eine Regelung analog § 26 BZRG angemessen sein.

Unbefriedigend ist bislang auch die Dauer der Aufbewahrung von Steckbriefnachrichten geregelt. Eine Löschung ist, falls vorher keine Erledigung mitgeteilt wird, erst nach Ablauf von 3 Jahren seit der Niederlegung vorgesehen. Durch diese Regelung, die dem § 27 BZRG entspricht, ist m.E. nicht hinreichend sichergestellt, daß Betroffene von ungerechtfertigten Diskriminierungen verschont bleiben. Um eine bessere Überprüfung der Tatsache, ob die Voraussetzungen für eine steckbriefliche Verfolgung noch vorliegen, zu gewährleisten, erscheint mir eine Regelung, die den Vorschriften für die INPOL-Personenfahndung entspricht, notwendig zu sein. Danach sind Fahndungsausschreibungen nur für 3 Monate gültig und müssen dann – bei Bedarf – erneuert werden.

(2) Im Gegensatz zum Erlaß von Steckbriefnachrichten sind die Voraussetzungen für den Erlaß von Suchvermerken nirgends gesetzlich geregelt. Zwar erwähnt § 25 BZRG auch die Niederlegung von Suchvermerken; was diese enthalten dürfen und welche Stellen sie unter welchen Voraussetzungen erlassen dürfen, ist völlig offen. Solange es keine gesetzlichen Befugnisse zum Erlaß von Suchvermerken gibt, muß darauf verzichtet werden, diese in ZEVIS einzustellen.

(3) Es ist nicht nachvollziehbar, warum über den Erlaß von Steckbriefnachrichten hinaus auch noch der eingangs beschriebene Fahndungsabgleich erforderlich sein soll. Im übrigen ist darauf hinzuweisen, daß es auch eine Befugnis des BKA zur Übermittlung von großen Teilen des INPOL-Fahndungsbestandes an das KBA nicht gibt. Die Vorschriften der StPO decken ein solches Massenverfahren jedenfalls nicht ab. Auch auf den Fahndungsabgleich ist daher zu verzichten.

3.10 Landesamt für Verfassungsschutz

Beim Verfassungsschutz habe ich im Berichtszeitraum erneut nur Einzelfälle prüfen können. Anlaß zu Beanstandungen war in diesen Fällen nicht gegeben. Eine von mir beabsichtigte Querschnittsprüfung für einzelne Arbeitsbereiche des Landesamts mußte ich aus Kapazitätsgründen leider zurückstellen. Durch das Volkszählungsurteil sehen sich

die Datenschutzbeauftragten in ihrer Forderung bestätigt, auch die Informationstätigkeit des Verfassungsschutzes bereichsspezifisch und präzise zu regeln. Die Novellierung des Hamburgischen Verfassungsschutzgesetzes (HmbVerfSchG) scheint mir eine der vordringlichen Maßnahmen zu sein, die der hamburgische Gesetzgeber in Angriff zu nehmen hat.
Die Behörde, die die Verfassung schützen soll, ist in besonderem Maße berufen, ihre Tätigkeit auf verfassungskonforme Grundlagen zu stellen. Gerade sie darf sich den Forderungen des Bundesverfassungsgerichts nach präzisen bereichsspezifischen gesetzlichen Grundlagen für die Informationsverarbeitung nicht entziehen. Gerade beim Verfassungsschutz, dessen Tätigkeit ihrem Wesen nach kaum einer Kontrolle durch die Öffentlichkeit zugänglich ist, sind klare Festlegungen seiner Aufgaben und gesetzliche Begrenzungen seiner Befugnisse nötig, um sowohl der Behörde selbst wie auch den zu ihrer Kontrolle berufenen Einrichtungen eindeutige Maßstäbe für die Beurteilung der Zulässigkeit von geheimen Maßnahmen an die Hand zu geben. Die Einrichtung von Kontrollinstanzen nützt relativ wenig, wenn die Maßstäbe der Kontrolle unklar sind. Im Frühjahr habe ich auf einer Arbeitstagung des Landesamts für Verfassungsschutz bereits eine Reihe von Konsequenzen formuliert, die sich aus dem Volkszählungsurteil für dessen Arbeit ergeben. Die Reaktion war zunächst eher zurückhaltend. Doch ich habe den Eindruck, daß der Verfassungsschutz inzwischen bereit ist, mit den Vorbereitungen für eine Änderung des Gesetzes zu beginnen. Auch ein ad-hoc-Ausschuß des Arbeitskreises IV der Innenminister-Konferenz hat bereits mit der Erarbeitung eines Vorschlages zur Novellierung des „(Bundes-) Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes" begonnen. Ich nehme diesen Bericht zum Anlaß, zusammenfassend die bestehenden Regelungsdefizite aufzuzeigen und meine Forderungen zu formulieren. Dabei gehe ich davon aus, daß die Formulierung von Regelungen in Gesetzesform dem Verfassungsschutz keine unüberwindlichen Schwierigkeiten bereitet. In vielen Bereichen geht es lediglich darum, die gängige Praxis – die z. Z. durch interne Verwaltungsrichtlinien gesteuert wird – zu verrechtlichen und für den Bürger – soweit es nach den besonderen Gegebenheiten vertretbar ist – transparenter zu machen.

3.10.1 Präzisierung der Aufgabenstellung

Zunächst ist der Katalog der Aufgaben des Verfassungsschutzes (§ 3 VerfSchG) nach Möglichkeit so zu präzisieren, daß sich bereits hieraus ergibt, in welchem Umfang jeweils die Verarbeitung personenbezogener Informationen erforderlich sein kann. Dabei ist klar nach den unterschiedlichen Zwecken der Datenverarbeitung zu trennen, um eine strenge Einhaltung des Grundsatzes der Zweckbindung zu ermöglichen. Nach meinen Erfahrungen ist die Sammlung und Auswertung personenbezogener Daten für die folgenden, differenziert zu behandelnden Aufgaben des Verfassungsschutzes in unterschiedlichem Umfang notwendig:

- Extremismusbeobachtung,
- Spionageabwehr und
- Mitwirkung bei Sicherheitsüberprüfungen.

Die Befugnisse des Verfassungsschutzes zu Informationseingriffen sind den jeweiligen Zwecken entsprechend zu regeln, wobei die zu unterschiedlichen Zwecken angefallenen Datenmengen gegeneinander abzuschotten sind. In diesem Zusammenhang erinnere ich daran, daß der Grundsatz „Kenntnis, nur wenn nötig" schon heute, nicht nur aus Gründen des Datenschutzes, vom LfV strikt praktiziert wird.

3.10.2 Klarere Erhebungsbefugnisse

Es ist wesentlich klarer zu regeln, welche Informationen der Verfassungsschutz zu welchen Zwecken mit welchen Mitteln erheben darf. Dabei ist auch zu berücksichtigen, daß der Verfassungsschutz neben den Erhebungen, die er – verdeckt oder offen – beim Betroffenen oder bei Befragung dritter Personen vornimmt, häufig auch Informationen von anderen staatlichen Stellen benötigt. Auch hierfür ist festzustellen, unter welchen Voraussetzungen und zu welchen Zwecken der Verfassungsschutz von anderen Behörden

die Weitergabe von personenbezogenen Unterlagen verlangen darf und wann andere Behörden (insbesondere die Polizei) verpflichtet sind, von sich aus den Verfassungsschutz zu unterrichten.
So muß hinsichtlich der Aufgabe „Extremismusbekämpfung" berücksichtigt werden, daß die Tätigkeit des Verfassungsschutzes in erster Linie der Regierung einen Überblick, eine Einschätzung der „Sicherheitslage" (sowie die Einleitung von Verfahren nach den Artn. 9 Abs. 2, 18 und 21 Abs. 2 GG vor dem Bundesverfassungsgericht) ermöglichen soll. Die Beobachtung der im Verfassungsschutzgesetz genannten „Bestrebungen" zielt primär also auf Vereinigungen und Organisationen, nicht aber auf einzelne Personen – etwa einfache Mitglieder dieser Organisationen – ab. Wenn auch Erkenntnisse über Verbände nicht durchgehend von solchen über einzelne Aktivisten („Träger" von Bestrebungen) getrennt werden können, weil Informationen über Einzelpersonen auch Rückschlüsse auf Organisationsstrukturen und Ziele zulassen mögen, so ist gleichwohl der Ansatzpunkt der Informationssammlung im „Staatsschutz"bereich – in Abgrenzung zur polizeilichen Aufgabenerfüllung (Aufklärung von Staatsschutzdelikten – Verfolgung einzelner Straftäter) – klarer herauszustellen.
Ferner ist transparenter zu machen, von welcher Schwelle an Aktivitäten bestimmter „Betrebungen" Informationseingriffe des Verfassungsschutzes rechtfertigen. Die im VerfSchG genannten Schutzgüter (etwa „auswärtige Belange" und „freiheitlich-demokratische Grundordnung") sind einer weiten Interpretation zugänglich, so daß weder Juristen noch weniger aber betroffene Bürger erkennen können, welcher Grad – über regierungskritische Gesinnung hinausgehender – verfassungsfeindlicher Aktivitäten überschritten sein muß, um Maßnahmen des Verfassungsschutzes zu veranlassen. Formulierungshilfen lassen sich möglicherweise aus dem „SRP-Urteil" und dem „KPD-Urteil" des Bundesverfassungsgerichts gewinnen.
Zu Zwecken der Spionageabwehr ist nach meinen Erfahrungen in stärkerem Maße die Auswertung personenbezogener Unterlagen, etwa des Melderegisters, notwendig. Da hier möglicherweise schon bei relativ vagen Anhaltspunkten Erhebungsbefugnisse anzuerkennen sein dürften, die allerdings ebenfalls gesetzlich zu regeln sind, ist es besonders wichtig, daß diese Informationen ausschließlich zum Zwecke der Spionageabwehr verwendet und auch – wie es heute bereits üblich ist – innerhalb des LfV nicht anderen Mitarbeitern zugänglich gemacht werden.
Auch der gesamte Komplex der Mitwirkung des Verfassungsschutzes an Sicherheitsüberprüfungen ist für die Betroffenen transparenter zu gestalten. Die hierzu bestehende interne Regelung in den Sicherheitsrichtlinien reicht nicht aus.
Es ist sicherzustellen, daß das LfV nur tätig wird, wenn solche Überprüfungen dem betroffenen Bürger bekannt gemacht worden sind und daß Befragungen dritter Personen zu diesem Zweck nur zulässig sind, wenn der Betroffene eingewilligt hat.
Auch die derzeitige Regelung des Einsatzes „nachrichtendienstlicher Mittel" entspricht nicht den Anforderungen der Normenklarheit. Die Einschätzung, daß eine Präzisierung dieses Begriffes untunlich sei, dürfte sich heute kaum mehr halten lassen. Wenigstens sollten die zulässigen nachrichtendienstlichen Mittel im Gesetz beispielhaft aufgezählt werden (etwa Observation, Einschleusung von V-Leuten etc.). Daneben sollte geregelt werden, ob und wann der Einsatz technischer Mittel zur Aufzeichnung von Informationen (außerhalb des Anwendungsbereiches des G 10) zulässig sein soll (etwa Einsatz von Video-Geräten etc.). Die Voraussetzungen für den Einsatz nachrichtendienstlicher Mittel sollten abschließend und stärker an die jeweiligen Verarbeitungszwecke angelehnt formuliert werden. Dringend klärungsbedürftig erscheint mir ferner die vieldiskutierte Frage, ob der Verfassungsschutz auf der Grundlage des Art. 13 Abs. 3, 1. Alternative GG tätig werden und personenbezogene Informationen verarbeiten darf. Nach meiner Auffassung ist eine „gemeine Gefahr" i. S. dieser Vorschrift nicht vom Verfassungsschutz, sondern nur von der Polizei zu bekämpfen.
Ausdrücklich klargestellt werden sollte auch, daß dem Verfassungsschutz keine polizeilichen Befugnisse zustehen und daß er die Polizei nicht im Wege der Amtshilfe um Maßnahmen ersuchen darf, zu denen er selbst nicht befugt ist (vgl. § 4 Abs. 4 BremVerfSchG). Dem Gebot der Trennung von Polizei und Verfassungsschutzbehörden muß ferner durch eine strenge Handhabung des Zweckbindungsgrundsatzes Rechnung getragen werden. Dies gilt nicht nur für Informationen, die die Polizei aus Telefonüber-

wachungsmaßnahmen gem. §§ 100a, 100b StPO gewonnen hat. Hier besteht Einigkeit, daß der Verfassungsschutz solche Informationen von der Polizei nicht erhalten darf (vgl. 2. TB, Nr. 3.11., S. 90). Dies gilt vielmehr generell für Informationen, die die Polizei aufgrund nur ihr zustehender spezieller Befugnisse für Zwecke des Strafverfahrens (z. B. § 108, 110 StPO) gewonnen hat. Es ist nicht vertretbar, daß die Polizei mit strafprozessualen Mitteln gewonnene Daten routinemäßig an das LfV weitergibt und es damit an polizeilichen Instrumenten teilhaben läßt, die ihm selbst von Gesetzes wegen nicht zustehen.
Ich erkenne zwar an, daß das Trennungsgebot die informationelle Zusammenarbeit zwischen Polizei und Verfassungsschutz nicht schlechthin verbietet; andererseits darf sie auch nicht als ein Prinzip möglichst effektiver Arbeitsteilung mißverstanden werden. Deshalb darf der Datenaustausch nicht zu einem Massengeschäft ausarten, das eine sorgfältige Prüfung des Einzelfalles ausschließt. Als Maßstab für eine Lösung bietet sich § 7 Abs. 3 G 10 an; dort hat der Gesetzgeber diejenigen Rechtsgüter beschrieben, deren Schutz ihm wichtiger erscheint als das ansonsten – gerade bei Telefon- und Post-Überwachungsmaßnahmen – sehr bedeutsame Zweckbindungsprinzip.

3.10.3 Speicherung und Löschung

Genau wie bei der Erhebung kommt es auch bei der Speicherung von Informationen auf eine klare Differenzierung nach den verschiedenen Zwecken an. Für alle Aufgabenbereiche klarzustellen ist zunächst, daß nur solche personenbezogenen Informationen gespeichert werden dürfen, die auf rechtmäßige Weise erhoben wurden.
Differenziert zu behandeln sind die Löschungspflichten für die gespeicherten Informationen. Nach meinen Erfahrungen sind langjährige Aufbewahrungsfristen (15-20 Jahre) – bei strenger Zweckbindung – allenfalls im Bereich der Spionageabwehr anzuerkennen. Im Bereich der Extremismusbeobachtung sind erhebliche kürzere Überprüfungs- und Löschungsfristen vorzusehen, da sowohl der Grad der Gefährlichkeit von Organisationen als auch die politische Haltung und Aktivität von einzelnen Personen im Laufe der Zeit häufig einem bedeutsamen Wandel unterlegen ist. Besonderer Einschränkungen bedarf die Speicherung von Informationen über Minderjährige, da hier die Gefahr besteht, daß einzelne lebenslang mit Jugendsünden abgestempelt werden. Ich weise darauf hin, daß etwa § 5 Abs. 1 Satz 1 des BremVerfSchG von 1981 hier bereits besondere Einschränkungen vorsieht.
Auch für die Mitwirkung an Sicherheitsüberprüfungen ist deutlich zu machen, welche Informationen der Verfassungsschutz unter welchen Voraussetzungen wie lange vorhalten darf. Klärungsbedürftig erscheinen mir z. B. folgende Fragen:

- Wann darf der Verfassungsschutz Angaben zu einer Person speichern, zu der er auf Antrag einer berechtigten Stelle seine vorhandenen Informationssammlungen abgefragt hat? Darf er die Tatsache, daß eine solche Anfrage an ihn gerichtet wurde, auch dann speichern, wenn keine Erkenntnisse vorlagen?
- Darf der Verfassungsschutz allein die Tatsache speichern, daß eine Person in einem sicherheitsempfindlichen Bereich arbeitet?
- Wie lange dürfen Informationen über Personen gespeichert werden, denen der Umgang mit Verschlußsachen erlaubt ist? Ist eine Weiterspeicherung zulässig, wenn die Ermächtigung zum Umgang mit Verschlußsachen nicht mehr fortbesteht?

Schließlich muß, wenn Bewertungen/Einschätzungen über einen Betroffenen gespeichert werden, erkennbar sein, wer die Bewertung vorgenommen hat und wo die Informationen gespeichert sind, die der Bewertung zugrundeliegen (vgl. § 5 Abs. 2 BremVerfSchG). Diese Forderung wird vor allem dann von Bedeutung sein, wenn der Verfassungsschutz dazu übergehen sollte, im NADIS oder in anderen automatisierten Dateien nicht mehr nur Hinweise auf andere Vorgänge, sondern auch Akteninhalte selbst (wie etwa bei PIOS und SPUDOK) zu speichern.

3.10.4 Weitergabe von Erkenntnissen durch den Verfassungsschutz

Es dürfte kaum noch zweifelhaft sein, daß die z. Z. in § 5 HmbVerfSchG statuierte Pflicht zur gegenseitigen Rechts- und Amtshilfe keine hinreichende Befugnis zur Weitergabe

personenbezogener Daten begründen kann. Nach dem Volkszählungsurteil muß die Zweckbindung von Daten „amtshilfefest" sein. Die Weitergabe von Daten ist daher unter Berücksichtigung des Zwecks der Datenspeicherung beim Verfassungsschutz sowie der Aufgabenerfüllung des Empfängers konkret zu regeln. Erwägenswert erscheinen mir etwa folgende Abstufungen:

- Ergebnisse von Sicherheitsüberprüfungen dürfen nur an die Stellen gegeben werden, die berechtigterweise die Überprüfung veranlaßt haben.
- Informationen, die zu Zwecken der Spionageabwehr gesammelt wurden, dürfen nur an Strafverfolgungsbehörden weitergegeben werden, und das nur dann, wenn ein Verdacht sich so sehr verdichtet hat, daß die Veranlassung von Strafermittlungsverfahren geboten erscheint. Bestehende Verwertungsgebote – etwa nach dem G 10 – bleiben selbstverständlich unberührt.
- Für Informationen aus der Extremismusbeobachtung, die an Strafverfolgungsbehörden übermittelt werden sollen, gilt das gleiche. An Einstellungsbehörden dürfen solche Daten allenfalls in begründeten Ausnahmefällen weitergegeben werden. Die Weitergabe muß sich auf gerichtsverwertbare Tatsachen beschränken. Auf jeden Fall ist sicherzustellen, daß keine routinemäßige Belieferung an Einstellungsbehörden stattfindet.
- Schließlich bedarf es einer Befugnisnorm für die Weitergabe von Erkenntnissen an andere Verfassungsschutzämter sowie sonstige Geheimdienste, soweit deren Zuständigkeitsbereich berührt ist. Auch hier ist jedoch sicherzustellen, daß der Grundsatz der Zweckbindung eingehalten wird. Um erforderlichenfalls eine Berichtigung bzw. Löschung weitergegebener Informationen nachmelden zu können und eine Kontrolle der Weitergabe zu ermöglichen, sind Empfänger und Anlaß einer Übermittlung aufzuzeichnen.

3.10.5 Bürgerrechte gegenüber dem Verfassungsschutz

Die geltende weitgehende Beschränkung von Bürgerrechten auf Auskunft über personenbezogene Informationen und die Erschwerung ihrer Löschung kann nach dem Volkszählungsurteil nicht mehr aufrechterhalten bleiben. Es ist zwar anzuerkennen, daß der Verfassungsschutz in der Lage sein muß, Versuche zur Ausforschung seiner Tätigkeit zu verhindern. Gleichwohl darf dies nicht dazu führen, daß Betroffene praktisch nicht in der Lage sind, sich gegenüber unzulässigen Informationseingriffen zur Wehr zu setzen. Dies wäre mit der Rechtsweggarantie des Art. 19 Abs. 4 GG, die viele als „Krönung des Rechtsstaates" oder aber als „formelles Hauptgrundrecht" bezeichnen, nicht vereinbar. Eine Lösung des Konfliks sollte m. E. in der Weise gefunden werden, daß Bürger einerseits über den Einsatz nachrichtendienstlicher Mittel (wie im G 10) im Nachhinein informiert werden; auch ein Auskunfts- und Löschungsrecht muß ihnen grundsätzlich zuerkannt werden, wobei mir abgestufte Einschränkungen – differenziert nach den verschiedenen Speicherungszwecken – vertretbar erscheinen. Es dürfte auf der Hand liegen, daß die Gefahr einer Ausforschung bei der Spionageabwehr ungleich schwerwiegender sein dürfte als bei der Extremismusbeobachtung bzw. der Sicherheitsüberprüfung.

3.11 Staatsanwaltschaft

3.11.1 Zentralkartei (ZK)

Nachdem zwischenzeitlich geklärt worden ist, welche Art von Hardware bei der Automatisation der ZK zum Einsatz kommen soll, hat die Justizbehörde nunmehr auch – von mir akzeptierte – Vorschläge zu differenzierten Löschungs- und Sperrfristen gemacht.

Die einvernehmlich erarbeitete Lösung geht davon aus, daß die ZK für die Staatsanwaltschaft eine doppelte Funktion zu erfüllen hat:

- zum einen als internes Indexsystem zum Wiederauffinden der von der StA selbst aufzubewahrenden Vorgänge,

- desweiteren als aktueller Auskunftsdienst, um vornehmlich Verfahrensbeteiligte über die Aktenzeichen laufender staatsanwaltschaftlicher Verfahren informieren zu können.

Datenschutzrechtliche Probleme stellen sich vornehmlich bei der Nutzung der ZK als externer Auskunftsdienst; diese Probleme sollen wie folgt gelöst werden:

(1) Konventionelle Altbestände: Die alte Handkartei soll zunächst grob bereinigt und sodann für jeglichen Auskunftsverkehr mit dritten Stellen gesperrt werden:

- Vor Umstellung der Zentralkartei auf das automatisierte Verfahren werden in der Zeit vom Dezember 1984 bis Frühjahr 1985 alle Karteikarten entfernt, deren Eintragungen ausschließlich Amtsanwaltschaftssachen und/oder Verkehrsdelikte betreffen und deren letzte Eintragung aus den Jahren vor 1980 datiert. Durch diese Maßnahme wird die Zahl der Karteikarten der ZK bereits um 15% – 20% verringert.
- Bei der Datenersterfassung werden aus der auf diese Weise bereinigten ZK nur die Vorgänge der letzten 4 Jahre (in Anlehnung an die Bestimmungen des § 15 Abs. 4; berechnet ab Ende des Eintragungsjahres) in das ADV-Verfahren übernommen. Sämtliche älteren Vorgänge werden unabhängig vom Tatvorwurf nicht übernommen, sondern verbleiben als gesperrter Bestand (d.h. sie stehen für den Auskunftsdienst nicht mehr zur Verfügung) in der konventionellen Kartei.
- die konventionelle Kartei gilt als eine interne Datei i.S. des HmbDSG.
  Sie wird aus den Geschäftsräumen der ZK ausgelagert und ist nur einem noch näher zu bestimmenden engen Kreis von Bediensteten zugänglich. Sie steht der StA damit ausschließlich als Index für archivierte Akten pp. zur Verfügung.

(2) ADV-Zentralkartei

Die in die ADV-Datei als Erstbestand übernommenen und die im Laufe des Betriebes neu eingegebenen Datensätze sollen genereil nach Ablauf von 4 Jahren (in Anlehnung an die Überprüfungsfrist des § 15 Abs. 4) unabhängig vom Tatvorwurf programmgesteuert gesperrt werden.

Die Berechnung der 4-Jahresfrist erfolgt

- bei den übernommenen Vorgängen aufgrund der Jahrgangszahl des Aktenzeichens,
- bei den neuen Eingängen aufgrund des tatsächlichen Speicherungsdatums.

Nach Sperrung der Datensätze werden diese im Auskunftsprogramm nicht angezeigt. Der Zugriff ist nur über ein besonderes Programm möglich.

Darüber hinaus habe ich gefordert:

- Auch vor Ablauf von 4 Jahren muß eine Sperrung der Daten mit der Eingabe der Erledigung in den Fällen erfolgen, in denen das Verfahren eingestellt wurde bzw. ein Freispruch erfolgte, weil
  - die Tat unter keinen Straftatbestand fällt oder
  - der Beschuldigte nicht der Täter ist.

  Ein abschließendes Gespräch über diese Forderungen steht noch aus.
- Die Löschung der Datensätze in der ADV-Kartei erfolgt programmgesteuert nach den Fristen der Aufbewahrungsbestimmungen. Die Löschungsfristen werden systemintern durch eine Verknüpfung des Deliktes und der Erledigungsart sowie des Erledigungsdatums berechnet. Es wird organisatorisch sichergestellt, daß jede Änderung der für die Berechnung relevanten Daten der Zentralkartei mitgeteilt wird.

3.11.2 Auskunftspraxis der Staatsanwaltschaft

Leider hatte ich die Auskunftspraxis der Staatsanwaltschaft im Berichtszeitraum zu bemängeln. Entgegen den Ausführungen in meinem 2. TB (Nr. 3.9.2.3, S. 76) stellte sich heraus, daß die Staatsanwaltschaft, wenn Betroffene selbst bei ihr Auskunftsanträge stellen, kategorisch unter Hinweis auf § 14 Abs. 2 eine Auskunft verweigert.
Ich habe der Staatsanwaltschaft mitgeteilt, daß ich diese Praxis für nicht zulässig halte, und deutlich gemacht, welchen Wert ein möglichst umfassendes und uneingeschränktes Auskunftsrecht für die Realisierung des vom Bundesverfassungsgericht ausdrücklich anerkannten Rechts auf informationelle Selbstbestimmung hat.
Eine Reaktion stand bei Abschluß des Berichts noch aus.

3.12 Justizverwaltung und Strafvollzug

3.12.1 Schaffung von Rechtsgrundlagen für die Datenverarbeitung im Strafverfahren

Ich hatte in meinen ersten beiden Tätigkeitsberichten herausgearbeitet, daß auch bei der Justiz in den unterschiedlichsten Zusammenhängen große Mengen von z. T. außerordentlich sensiblen personenbezogenen Daten anfallen, die in diversen Aktensammlungen und Registern gespeichert werden. Ferner hatte ich dargestellt, wie gerichtliche Entscheidungen aufgrund diverser Verwaltungsvorschriften, z. B. der Anordnung über Mitteilungen in Strafsachen (MiStra), der Anordnung über Mitteilungen in Zivilsachen (MiZi) oder der Richtlinien für das Straf- und Bußgeldverfahren regelmäßig einem weiten Kreis von Empfängern mitgeteilt werden.
Seit dem Volkszählungsurteil können sich die Justizverwaltungen den Forderungen nach Schaffung einwandfreier bereichsspezifischer Rechtsgrundlagen für die genannten Informationseingriffe nicht mehr entziehen. Beratungen zur Überprüfung der Rechtsgrundlagen für die genannten Verwaltungsvorschriften laufen. Greifbare Ergebnisse sind jedoch noch nicht ersichtlich.
Ich meine, daß die Justizverwaltungen in dieser Situation darüber nachdenken sollten, ob nicht, statt an bestehende Regelungen jeweils eine Vorschrift über Datenverarbeitung anzuflicken, ein Querschnittsgesetz die geeignetere Lösung wäre, das zumindest für den gesamten strafprozessualen Bereich die gebotenen Regelungen klar und übersichtlich zusammenfaßt.
Strafprozeßdaten werden in den Ermittlungs- und Handakten der Kriminalpolizei, in den Ermittlungsakten der Staatsanwaltschaft, in den Gerichtsakten sowie schließlich im Bundes- und Verkehrs-Zentralregister gespeichert. Die Aufbewahrungsfristen in diesen Datensammlungen (einschl. der jeweiligen Nachweis-Systeme) sind z. Z. überhaupt nicht aufeinander abgestimmt, was zur Folge hat, daß etwa Verurteilungen, die nach dem BZRG längst gelöscht wurden, in anderen Unterlagen noch lange vorhanden sind. Die Gefahren für den Betroffenen, die durch das Verwertungsgebot des § 49 BZRG ausgeschlossen werden sollten, liegen auf der Hand.
Ebensowenig aufeinander abgestimmt sind die derzeit geltenden Mitteilungspflichten der verschiedenen Stellen in unterschiedlichen Phasen des Strafverfahrens. So kommt es z. Z., daß die Ausländerbehörde über ein und dasselbe Verfahren sowohl von der Polizei als auch von der Staatsanwaltschaft und Gerichten unterrichtet wird (vgl. Nr. 3.7.3.2).
Diese Ungereimtheiten lassen sich nach meiner Einschätzung nur dann mit der gebotenen Klarheit und Transparenz für den Bürger beseitigen, wenn für die Daten, die von unterschiedlichen Stellen für letztlich ein und denselben Zweck – nämlich Verfolgung einer bestimmten Straftat – verarbeitet werden, eine einheitliche zusammenhängende Regelung erarbeitet wird.
Mir ist bewußt, daß der Gesetzgeber mit einer solchen Regelung Neuland betreten würde. Gleichwohl meine ich, daß die Justizverwaltungen auch angesichts der Bedeutung, die die automatisierte Datenverarbeitung gerade auf dem Gebiet der Strafverfolgung erlangt hat, sich dieser Herausforderung nicht entziehen sollten.

3.12.2 Strafvollzug: Schriftwechsel mit Gefangenen

Aus dem Bereich des Strafvollzugs ist erfreulicherweise zu berichten, daß das Strafvollzugsamt eine neue Allgemeine Verfügung zum Problem der Überwachung des Schriftwechsels von Gefangenen erlassen hat. Nunmehr ist – auf meinen Wunsch hin – zunächst sichergestellt worden, daß zum einen Schreiben eines Gefangenen an den Datenschutzbeauftragten nicht mehr von der Justizvollzugsanstalt überwacht werden. Auf diese Weise wird gewährleistet, daß Gefangene ohne Furcht vor Benachteiligungen von ihrem Anrufungsrecht nach § 22 Gebrauch machen können.
Ferner konnte ich erreichen, daß auch Schreiben des Datenschutzbeauftragten an einen Gefangenen sowie Schreiben hamburgischer Behörden, die Auskünfte nach § 14 enthalten, nicht mehr überwacht werden. Zugleich sind geeignete Vorkehrungen getroffen worden, die mißbräuchliche Mitteilungen unberechtigter Dritter ausschließen sollen.

3.13 Gesundheitswesen

3.13.1 Prüfung eines Bezirksgesundheitsamtes

Im Frühjahr habe ich die erste Querschnitts-Prüfung einer Dienststelle des öffentlichen Gesundheitswesens – bei einem Bezirksgesundheitamt – begonnen. Die Prüfung konnte wegen verschiedener Verzögerungen zwar noch nicht abgeschlossen werden, einige wesentliche Zwischenergebnisse kann ich jedoch schon in diesem Bericht mitteilen.
Nach meinen Feststellungen sammeln sich in den Bezirksgesundheitsämtern außerordentlich große Mengen personenbezogener Informationen an, und zwar in zweifacher Hinsicht: zum einen gibt es hier Informationen über fast alle Einwohner eines Bezirks – von Säuglingen und Schulkindern angefangen bis hin zu Verstorbenen. Desweiteren werden z. Z. weit in die geschützte Privatsphäre hinreichende Daten über eine Vielzahl von Sachverhalten verarbeitet: Angaben über Säuglinge und Mütter, über Behinderte und Drogensüchtige, Röntgenbefunde, Untersuchungsberichte, Meldungen nach dem Bundesseuchengesetz etc. Die anfallenden Datenmengen verarbeitet das Gesundheitamt zu den unterschiedlichsten Zwecken, die in der Praxis nicht immer klar gegeneinander abgegrenzt werden und für die es auch kaum modernen Anforderungen entsprechende, bereichsspezifische gesetzliche Grundlagen gibt.
Nach meinen Feststellungen sind grundsätzlich drei, sich stark unterscheidende Verwendungszwecke der Informationsverarbeitung zu unterscheiden:

- gutachterliche Zwecke: duldungspflichtige oder nicht duldungspflichtige Gutachtertätigkeit etwa im Rahmen des PsychKG, der Überwachung von Lebensmittelbetrieben, der Erteilung von Aufenthaltserlaubnissen etc,;
- hoheitlich-sicherheitsrechtliche Zwecke: Vollzug des Bundesseuchengesetz, Tuberkulosefürsorge, Durchführung von Röntgen-Reihen-Untersuchungen, Aufsicht über Medizinalpersonen etc,;
- Beratungszwecke: Beratungstätigkeit auf freiwilliger Basis (z. B. Mütterberatung, Suchtkrankenberatung, sozialpsychiatrischer Dienst etc.).

Es liegt auf der Hand, daß ein Bürger für die genannten Verwendungszwecke in ganz unterschiedlichem Umfang Einschränkungen seines Rechts auf informationelle Selbstbestimmung in Kauf nehmen muß. Es gibt z. Z. allerdings keine Gesetze, die ihn klar erkennen lassen, welche seiner Daten jeweils erhoben, gespeichert, weitergegeben oder sonst verwendet werden dürfen.
Ein besonderes Problem sehe ich in der Frage, inwieweit Informationen, die für einen der o. g. Aufgabenbereiche des Gesundheitsamtes erhoben werden, auch beim Vollzug in einem anderen Bereich verwendet werden. Es liegt m. E. auf der Hand, daß etwa Befunde und Angaben aus der Mütter- und Suchtkrankenberatung im Zusammenhang etwa mit einem Gutachten zu einem ganz anderen Zweck verwendbar sein dürfen.
Es gibt auch keine Rechtsvorschriften, die eine Verknüpfung von – zu unterschiedlichen Daten gewonnenen – Informationen zulassen. Gleichwohl ist eine solche Zusammenführung von Daten im Gesundheitsamt heute ohne große Schwierigkeiten möglich. Jedes Gesundheitsamt führt eine alphabetisch, nach den Namen von Klienten aufgebaute Zentralkartei, die zur Auffindung der meisten im Gesundheitsamt vorhandenen perso-

nenbezogenen Unterlagen dient. Auf einer Karteikarte können sich somit z. B. sowohl Hinweise auf Vorgänge beim sozialpsychiatrischen Dienst als auch auf Gutachten finden. Ich habe erhebliche Zweifel, ob die Zentralkartei in dieser Form weitergeführt werden sollte, da die Zweckbindung der verschiedenen Daten zu leicht unterlaufen werden könnte.
Das Gespräch in dieser Angelegenheit dauert jedoch noch an. Über den Abschluß der Prüfung werde ich in meinem nächsten TB berichten.

3.13.2 Geburtsbescheinigungen

Aufgrund einer Eingabe habe ich mich im Berichtzeitraum mit den Datenübermittlungen befaßt, die anläßlich der Geburt eines Kindes erfolgen. Dabei stellte ich fest, daß in einem solchen Fall von den Krankenhäusern bis zu 6 verschiedene Vordrucke gleichzeitig zur Datenweitergabe an mehrere Behörden (z. B. Standesamt, Gesundheitsamt, Jugendamt) verwendet werden. Ich habe den Eindruck gewonnen, daß es dabei zu einer Reihe von Parallelinformationen kommt, die nach meiner Auffassung entbehrlich sind.
Deshalb habe ich angeregt, das System der Datenübermittlungen – einschl. des Vordruckwesens – in diesem Bereich einmal gründlich zu überarbeiten und den datenschutzrechtlichen Erfordernissen anzupassen.
Die Gesundheitsbehörde hat diesen Vorschlag aufgenommen und damit begonnen, die Vordrucke im Gesundheitswesen insgesamt einer datenschutzrechtlichen Prüfung zu unterziehen.
Der Vordruckausschuß der bezirklichen Gesundheitsämter hat inzwischen unter meiner Mitarbeit eine Neufassung des Vordrucks „Geburtsbescheinigung" entwickelt. Dieser Vordruck wird im Kreißsaal des Krankenhauses innerhalb von 48 Stunden nach der Geburt eines Kindes von der Hebamme ausgefüllt und enthält Angaben, die

- der Standesbeamte für die Erteilung der Geburtsurkunde benötigt,
- das Gesundheitamt zur Klärung der Frage benötigt, ob der Mutter ein Angebot zur Unterstützung im Rahmen der Mütterberatung unterbreitet werden soll,
- das Statistische Landesamt zur Fortschreibung der Bevölkerungsstatistik benötigt.

Der Vordruck wird über das Standesamt an das Gesundheitsamt gesandt. Die Angaben, die das Gesundheitsamt benötigt, befinden sich in einem verschlossenen, inneren Teil, der nur vom Gesundheitsamt geöffnet werden darf.
Nach meiner Auffassung sind die zahlreichen und sehr detailierten medizinischen Angaben im verschlossenen Teil des Vordrucks in der überwiegenden Zahl für das Gesundheitsamt zur Entscheidung darüber, ob ein Angebot zur Mütterberatung unterbreitet werden soll, nicht erforderlich. Ich habe deshalb erreichen können, daß in der Neufassung des Vordrucks auf die meisten medizinischen Daten verzichtet wird.
Außerdem ist verabredet worden, daß die jetzt erarbeitete und bereits verwendete Neufassung des Vordrucks lediglich eine Übergangslösung ist. Im Zusammenhang mit der Prüfung aller Datenübermittlungen anläßlich der Geburt soll der Vordruck dann in die Form gekleidet werden, die voll und ganz datenschutzrechtlichen Erfordernissen entspricht.

3.13.3 Rechtsgrundlagen für den öffentlichen Gesundheitsdienst

Rechtsgrundlagen – auch für die informationelle Tätigkeit der Gesundheitsämter – finden sich heute noch vornehmlich im (hamburgischen) „Gesetz über das Gesundheitswesen" (GwG) vom 15.3.1920 mit den dazu erlassenen „Ausführungsbestimmungen" vom 27.8.1920 sowie im (Reichs-) „Gesetz über die Vereinheitlichung des Gesundheitswesens" (GVGw) vom 3.7.1937 mit den dazu erlassenen drei „Durchführungsverordnungen" aus dem Jahr 1935. Diese – zwischenzeitlich nur teilweise aufgehobenen – Vorschriften enthalten im wesentlichen nur Aufgaben-, jedoch keine Befugnisnormen. Sie sind nicht nur aus Gründen des Datenschutzes dringend novellierungsbedürftig. Andere Länder haben dies bereits erkannt: so ist das GVGw in den Ländern Schleswig-Holstein und Berlin durch neue Gesundheitsdienstgesetze abgelöst worden. In einigen anderen Ländern laufen entsprechende Vorhaben. Ich meine, daß auch Hamburg nun sehr bald nachziehen sollte.

3.14 Wissenschaft und Forschung

Der in meinem letzten TB (Nr. 3.16.1, S. 103) skizzierte Zielkonflikt zwischen Datenschutz und wissenschaftlicher Forschung war weiterhin Gegenstand häufiger Erörterungen. Zwar konnten bislang in allen Fällen pragmatische, zweckgerechte Lösungen gefunden werden. Z.T. war dies aber nur mit gerade noch vertretbaren Auslegungen geltender Rechtsnormen möglich. Ich möchte dies exemplarisch am Beispiel des Forschungsvorhabens „Dioxin und frühkindliche Mißbildungen" darstellen und anschließend Konsequenzen deutlich machen.

3.14.1 Forschungsprojekt „Dioxin und frühkindliche Mißbildungen"

Die Gesundheitsbehörde führt – mit Unterstützung des Bremer Instituts für Präventivforschung und Sozialmedizin (BIPS) – ein Forschungsprojekt über etwaige Zusammenhänge zwischen der Emission von Dioxin und frühkindlichen Mißbildungen durch. Die Notwendigkeit und Dringlichkeit eines solchen Forschungsprojekts wird von mir nicht bestritten. Bislang gibt es keine Forschungsergebnisse zu diesem Thema. Da andere auswertbare Datenbestände nicht zur Verfügung stehen, beabsichtigt die Gesundheitsbehörde im Rahmen dieses Projekts, Daten aus Unterlagen der Gesundheitsämter (Geburtsbescheinigungen, Todesbescheinigungen) sowie aus Klinikunterlagen (Geburtenregister etc.) auszuwerten. Als Ausgangspunkt für die Beurteilung der Datenübermittlung von den Gesundheitsämtern bzw. Kliniken habe ich § 11 des Gesetzes über das Gesundheitswesen (GWG) vom 15. 3. 1920 angesehen. Nach diesem § 11 ist die Gesundheitsbehörde verpflichtet,

> „alle Einrichtungen und Zustände, die für die öffentliche Gesundheits- und Krankenpflege von Bedeutung sind, zu überwachen, bei drohenden oder eingetretenen Gefahren für die Volksgesundheit, insbesondere bei Seuchen, schleunigst die möglichen Ermittlungen anzustellen, die erforderlichen Anordnungen zu treffen und das weiter Notwendige bei den zuständigen Stellen zu beantragen."

Bei wohlwollender Betrachtungsweise kann die Pflicht zur Anstellung „der örtlichen Ermittlungen" als Grundlage für die (zwangsweise) Erhebung personenbezogener Daten durch die Gesundheitsbehörde angesehen werden. Diese Erhebung kann auch im Wege der Ersatzvornahme durch Beiziehung von personenbezogenen Daten aus anderen Stellen geschehen. § 11 gilt insofern auch als Befugnisnorm zur Offenbarung von Daten durch diese Stellen.

Ich habe darauf hingewiesen, daß die Heranziehung des § 11 als Befugnisnorm nur noch als Notbehelf für eine Übergangszeit vertretbar ist. Den Anforderungen des BVerfG an eine moderne normenklare Eingriffsgrundlage wird diese Regelung offensichtlich nicht gerecht.

Unter der Prämisse, daß § 11 GWG eine Befugnis zur Offenbarung von Daten (im Rahmen der Abwehr von Gefahren für die Volksgesundheit) enthält, ist sie auch als Rechtfertigungsgrund für die Durchbrechung der ärztlichen Schweigepflicht nach § 203 StGB anzusehen. Unter den Voraussetzungen des § 11 GWG werden Patientengeheimnisse nicht „unbefugt" offenbart.

Die Datenübermittlungen von den Gesundheitsämtern bzw. Kliniken sind auch nach § 11 GWG durch den Grundsatz der Erforderlichkeit begrenzt („nötige Ermittlungen"). Daraus folgt, daß die Gesundheitsbehörde nur Unterlagen solcher Personen erhält, bei denen Anhaltspunkte dafür bestehen, daß sie zur Errichtung des Forschungszwecks notwendig sind, d.h. nur solcher Personen, bei denen Mißbildungen, die auf dem Einfluß von Dioxin beruhen können, aufgetreten sind. Entsprechende Vorsortierungen sind von den Lieferanten der Unterlagen vorzunehmen.

Das BIPS verarbeitet die der Gesundheitsbehörde gelieferten Daten in deren Auftrag nach § 3 Abs. 1.

Die Begründung eines Auftragsverhältnisses setzt voraus, daß die Verfügungsgewalt und die Verantwortlichkeit des Auftraggebers ungeschmälert bleiben. Es darf kein grundlegender Unterschied gegenüber der Verarbeitung im Hause bestehen. Der Auftragnehmer ist streng an Weisungen des Auftraggebers gebunden. Nach § 3 Abs. 1 Satz 2 ist der Auftragnehmer unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Datensicherungsmaßnahmen sorgfältig auszuwählen.

Diese Bestimmung ist so auszulegen, daß sie verfassungsrechtlichen Anforderungen genügt. Aus der Verpflichtung der Behörden zum Schutz der Grundrechte folgt, daß die Einschaltung von Auftragnehmern nicht zu einer vermeidbaren Gefährdung schutzwürdiger Belange der Betroffenen führen darf. Solche Gefährdungen dürften – bei den sensiblen Patientendaten – dann vermieden sein, wenn die Auftragsvergabe an den Bestimmungen des § 80 SGB-X orientiert wird und der Auftragnehmer sich vertraglich der Kontrolle durch den HmbDSB unterwirft.

Dies bedeutet, daß die Gesundheitsbehörde bei der Zusammenarbeit mit dem BIPS folgendes zu beachten hat:

- Es muß sorgfältig nach zwei Stufen der Zusammenarbeit differenziert werden. Zunächst geht es um die Erarbeitung eines detaillierten Konzepts für die Durchführung der epidemiologischen Studie, um die Herstellung eines vollständigen Forschungsdesigns. Davon muß die Vergabe des eigentlichen Auftrags entsprechend § 3 Abs. 1 sauber unterschieden werden. Diese beiden Ziele sollten Gegenstand verschiedener Verträge sein,

- Bei der Vergabe des eigentlichen DV-Auftrages sind präzise Weisungen zu erteilen. Das vollständige Forschungsdesign sowie die Unterwerfung unter die Kontrolle des HmbDSB muß zum Bestandteil der Weisungen im Rahmen des Auftragsverhältnisses werden. An der Abstimmung dieser Weisungen wird der HmbDSB beteiligt.
  Die Gesundheitsbehörde hat meine Position zu dem o.g. Forschungsvorhaben akzeptiert und meine Forderungen bei der Umsetzung berücksichtigt.

3.14.2 Forderungen an den Gesetzgeber

Ungeachtet der oben skizzierten Lösung wird doch immer deutlicher, daß der Zielkonflikt zwischen Forschung und Datenschutz einer generellen Lösung durch den Gesetzgeber bedarf. Welche Regelungsmodelle sich hierfür anbieten, habe ich bereits ausgeführt (vgl. 2. TB unter Nr. 3.16, S. 103). Vordringlich erscheint mir eine spezialgesetzliche Regelung für die Forschungs- und Gesundheitsdaten, möglicherweise im Zusammenhang mit der Novellierung des Gesetzes über das Gesundheitswesen.

3.15 Datenschutz und Umweltschutz

Im Berichtszeitraum wurde immer deutlicher, daß die Intentionen der Umweltpolitik – nämlich Zusammenarbeit aller Beteiligten beim Umsetzen des Umweltkonzepts in die Praxis – u. U. mit Datenschutzinteressen einzelner Beteiligter kollidieren könnten: immer häufiger werden Überwachungs- und Genehmigungsbehörden aufgefordert, anderen öffentlichen Stellen, Abgeordneten, Bürgern und Umweltschutzorganisationen über Umweltgefahren und Umweltverstöße sowie über deren Verursacher oder die Verantwortlichen zuverlässige und klare Angaben zu machen. Dieses Interesse steht nicht selten den Belangen derjenigen entgegen, deren Umweltverhalten zur Debatte steht. Meistens handelt es sich bei den für Umweltgefahren und Umweltverstöße Verantwortlichen nicht um natürliche Personen, sondern um Kapitalgesellschaften, Konzerne, öffentliche Un-

ternehmen usw. Doch können als Verursacher und Verantwortliche bei Umweltverstößen auch „bestimmte oder bestimmbare natürliche Personen (Betroffene)", auf deren Daten der Schutz der Datenschutzgesetze beschränkt ist, auftreten. Soweit sich das Interesse der Öffentlichkeit auf die durch Umweltverstöße geschädigten oder gefährdeten Arbeitnehmer, Anlieger, Kinder usw. bezieht, ist in allen Fällen zu beachten, daß deren personenbezogene Daten durch die Datenschutzgesetze geschützt sind.
Wichtig ist mir andererseits die Feststellung, daß Datenschutz nicht dazu mißbraucht werden darf, Umweltverstöße zu vertuschen und Umweltsünder zu decken.
Vor diesem Hintergrund sind die nachfolgend genannten Beratungen und Beteiligungen zu sehen, die im Berichtszeitraum stattfanden:

- Die BBNU bat mich um Stellungnahme zu zwei Datenübermittlungsersuchen im Zusammenhang mit Überwachungsaufgaben nach dem Altölgesetz.
- Ein Bezirksamt bat um Prüfung, ob die Übermittlung von Daten aus dem im Aufbau befindlichen regionalen Altablagerungskataster an das zentrale Altablagerungskataster bei der BBNU unbedenklich ist.
- In einem Behördenabstimmungsverfahren, dessen Gegenstand die Einrichtung des Altablagerungskatasters war, habe ich aus datenschutzrechtlicher Sicht Stellung genommen.
- Ebenfalls war ich an den Überlegungen beteiligt, eine Untersuchung über die möglichen Ursachen der im Osten Hamburgs gehäuft auftretenden kindlichen Mißbildungen durchzuführen (s. Nr. 3.15.1).
- Über den Fortgang der Arbeiten am „automatisierten Emissionskataster (Luft) für Hamburg" habe ich folgendes zu berichten:
  Die Anregungen, die ich im Jahre 1983 zum Emissionskataster gegeben hatte, sind bei der Entwicklung des automatisierten Verfahrens berücksichtigt worden. Seit Juni 1984 läuft die Eingabe der Daten der Quellengruppe „ Industrie" in das automatisierte Verfahren (Datenerfassung). Grundlage sind die von den Betrieben freiwillig abgegebenen einfachen und erweiterten Emissionserklärungen. Mit der Datenerhebung (durch Befragung) hinsichtlich der Quellengruppe „Kleingewerbe" ist im Januar 1984 gegonnen worden. Bei der späteren Einspeicherung der Emissionsdaten dieser Gruppe in das automatisierte Verfahren werden weder Name noch Adresse der Betreiber miterfaßt. Zur Identifikation werden der Rechts-/Hochwert (kartographische Koordinaten) sowie die beiden ersten Stellen des achtstelligen Schlüssels für die Art des Betriebes benutzt.

3.16 Landesarchivgesetz

In meinem 2. TB hatte ich auf die Dringlichkeit eines Landesarchivgesetzes hingewiesen. Inzwischen hat die Bundesregierung den Entwurf für ein Bundesarchivgesetz in die parlamentarische Beratung gebracht. Auch in Hamburg soll demnächst ein an den Entwurf des Bundes angelehnter Entwurf für ein Landesarchivgesetz vorgelegt werden.

4. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

4.1 Handel

4.1.1 Versandhandel

Wie bereits in meinem 1. TB (Nr. 4.2.2, Beispiel 5, S. 21) und 2. TB (Nr. 4.1.2, S. 109) erwähnt, fragt der Versandhandel mit einem sog. Erstbestellschein personenbezogene Daten des Interessenten ab, um sich von der Bonität des künftigen Vertragspartners ein Bild machen zu können, bevor er ihm ein Konto als Einzelbesteller oder als Sammelbesteller (d.h. auch für andere Personen als Mitbesteller) einrichtet. Vom Ergebnis dieser Bonitätsprüfung hängt die Höhe des Einkaufskreditlimits ab, das dem Kunden gewährt wird. Bei Bestellungen, die die Kreditgrenze von DM 200,– überschreiten und in den Fällen, in denen Interesse an der Errichtung eines Sammelbestellerkontos besteht, wird regelmäßig bei der Schufa nachgefragt. Der Versandhandel fragt im Erstbestellschein nach der Berufstätigkeit, dem Familienstand, der Ausländereigenschaft und der Aufenthaltsdauer. Diese Daten sind eine wesentliche Grundlage für die Entscheidung, ob und in welcher Höhe ein erster Kredit gewährt wird (bei Ausländern ist beispielsweise die Dauer des Aufenthalts in der Bundesrepublik von großer Bedeutung). Sie werden nicht in die Stammdaten des Kontos übernommen oder zu weiteren Zwecken genutzt. Nach dieser ersten Bonitätsprüfung werden die Erstbestellscheine nur noch für später mögliche Kontrollen und aufgrund von handels- und steuerrechtlichen Aufbewahrungsvorschriften aufbewahrt.
Da der neue Kunde diese Angaben im Rahmen des vorvertraglichen Vertrauensverhältnisses und unter keinem rechtlichen Zwang hergibt, kann aus der Sicht des Datenschutzes die Praxis des Versandhandels insoweit nicht kritisiert werden.
Der Versandhandel erhebt allerdings auch personenbezogene Daten des Ehegatten und fragt über ihn bei der Schufa nach. Der Versandhandel rechtfertigt Erhebung, Speicherung und Übermittlung mit § 1357 BGB, da es sich bei einem Kauf per Versandhandel i.d.R. um ein Geschäft zur angemessenen Deckung des Lebensbedarfs der Familie handele, das mit Wirkung auch für den anderen Ehegatten besorgt werde. Deshalb dürften auch dessen personenbezogene Daten auf dem Erstbestellschein erhoben werden, ohne daß es seiner Einwilligung bedürfe.

Mit den einschlägigen BGB-Kommentierungen hingegen gehe ich davon aus, daß es sich bei einer Vielzahl von Geschäften aus dem breitgefächerten Angebot des Versandhandels nicht um solche zur angemessenen Deckung des Lebensbedarfs handelt, die auch für den anderen Ehegatten besorgt werden.

Erst recht ist zweifelhaft, ob für die Dauervertragsverhältnisse des Versandhandels § 1357 BGB generell Anwendung finden kann. Der Versandhandel schließt mit seinen Kunden nur in seltenen Fällen Einzelkaufverträge ab, die dann auch noch ggf. per Nachnahme abgewickelt werden. In der Regel wird ein Dauervertragsverhältnis angestrebt, bei dem die Kunden – Bonität vorausgesetzt – gleich zu Beginn der Vertragsbeziehung entweder als Einzelbesteller oder als Sammelbesteller einen Kredit in Höhe von DM 2.000,– bis DM 3.000,– eingeräumt bekommen. Das Vertragsverhältnis mit Sammelbestellern ist mit Sicherheit nicht von § 1357 BGB gedeckt; aber auch bei Einzelbestellern werden die rechnerisch zusammengefaßten Einzelbestellungen in der Regel einen Umfang erreichen, der eine vorherige Verständigung der Ehegatten voraussetzt, so daß die Anwendung von § 1357 BGB ausgeschlossen ist. Selbst wenn man aber zum Ergebnis käme, daß nur ein geringer Teil der Geschäfte von § 1357 BGB nicht gedeckt ist, müßte doch, auch um diese wenigen Fälle auszusondern, in jedem Einzelfall geprüft werden,

- ob es sich um ein Geschäft größeren Umfangs handelt, das ohne Schwierigkeiten zurückgestellt werden kann,

- ob der jeweilige andere Ehegatte ebenfalls erwerbstätig ist,
- ob es sich um ein Geschäft handelt, das die wirtschaftlichen Verhältnisse der Familie übersteigt.

Hierzu wäre es notwendig, Einblick in die beruflichen, wirtschaftlichen, finanziellen und familiären Verhältnisse zu gewinnen und die erhobenen Daten in Beziehung zum beabsichtigten Rechtsgeschäft zu setzen.

Darüber hinaus ist zu berücksichtigen, daß die Voraussetzungen des § 1357 BGB nur dann gegeben sind, wenn vor dem Abschluß eines Geschäfts eine Verständigung zwischen den Ehegatten gewöhnlich als nicht notwendig angesehen wird und hierüber auch keine vorherige Abstimmung stattfindet. Dies richtet sich nach den Anschauungen des Lebenskreises, dem die Ehegatten angehören.

Wenn eine solche individuell-konkrete Abwägung der berechtigten Interessen des Versandhandelsunternehmens gegen die schutzwürdigen Belange der Kunden nicht stattfindet, kann nicht davon ausgegangen werden, daß in allen Fällen die Voraussetzungen der §§ 23, 24 BDSG gegeben sind.

Der Versandhandel weist darauf hin, daß der Ehegatte bei Geschäften, die nach seiner Ansicht das Familieneinkommen zu stark belasten, die Möglichkeit hat, die Bestellung nach § 1b AGzG zu widerrufen oder von dem bis zu 14 Tage dauernden Rückgaberecht Gebrauch zu machen.
In Gesprächen mit dem Versandhandel ist zu klären, ob dies ein Ansatz für eine Lösung ist, die nicht auf die Einwilligung des Ehegatten abstellt.

4.1.2 Direktwerbung

Der Adreßhandel sorgt von Zeit zu Zeit immer wieder für Schlagzeilen. Während Anfang des Jahres bekannt wurde, daß die Deutsche Postreklame GmbH private Adressen von Soldaten weitergegeben hatte, wurde in Hamburg die Öffentlichkeit darauf aufmerksam, daß bei einer direkt adressierten Werbung für einen „Erotic-Guide" auch jugendliche Mitglieder eines Sportvereins angeschrieben worden waren. Hierzu war es auf folgende Weise gekommen: Der Sportverein hatte ein auf Direktwerbung und Adressenverwaltung spezialisiertes Unternehmen beauftragt, alle Anschriften seiner Vereinsmitglieder zu speichern, Rundschreiben zu adressieren und zu versenden. Von einem anderen Kunden hatte dieses Unternehmen den Auftrag zur Direktwerbung für den „Erotic-Guide" erhalten und dazu nach Zielgruppen ausgewählte Anschriften angemietet. Bei der praktischen Verarbeitung hatte sich ein Bedienungsfehler eingeschlichen. Einige Adressen vom Stapel der Vereinsmitglieder wurden zusätzlich für den Direktwerbe-Auftrag verwendet. Aufgrund einer fehlerhaften Kontroll-Routine konnte dieser Fehler nicht sofort entdeckt werden. Im Schlußgespräch nach meiner Überprüfung dieses Falles habe ich Vorschläge zur Verbesserung der Sicherheitsmaßnahmen gemacht.

Durch eine andere Beschwerde erfuhr ich, daß ein Unternehmen dem Betroffenen nicht mitteilen wollte, aus welcher Quelle die für die direkt adressierte Werbung genutzte Adresse stammte. Als ich selbst mir die Herkunft der Adresse und die für die Werbemaßnahme vorgegebenen Auswahlkriterien nennen lassen wollte, gab mir die Firma zur Antwort, daß sie über den Betroffenen keinerlei Daten gespeichert habe. Sie berief sich darauf, daß eine Übermittlung personenbezogener Daten an sie nicht stattgefunden habe, da sie nur das Werbematerial zur Verfügung gestellt habe, welches erst ein Vermittler mit den von anderer Seite gelieferten Adressen versehen und zur Post aufgegeben habe. Andere Daten des Betroffenen seien auch nicht gespeichert, so daß das BDSG auf diesen Vorgang nicht anwendbar sei.

Ich bin der Meinung, daß der Betroffene sehr wohl einen Anspruch darauf hat, die Quelle seiner genutzten Adresse zu erfahren.

Fühlt sich jemand durch das unaufgeforderte Zusenden von Werbematerial in seinem Persönlichkeitsrecht beeinträchtigt, so wird er verhindern wollen, daß ihm weitere Werbesendungen zugehen. Dazu muß er sich an den Adressen-Eigentümer wenden. Er muß also versuchen, die Herkunft der Adresse in Erfahrung zu bringen. Als möglicher Ansprechpartner kommt für ihn allein der Werbende (Adressen-Mieter) in Betracht, da ihm gegenüber nur dieser namentlich in Erscheinung getreten ist.
Wendet er sich jedoch an den Werbenden, so offenbart er diesem, in welcher Eigenschaft er umworben wurde. Die Datenschutz-Aufsichtsbehörden haben seit jeher den Standpunkt vertreten, daß bei der Adressenvermietung und -mittlung immer dann eine Übermittlung vorliegt, wenn der Adressen-Mieter durch die Reaktion des Betroffenen (Antwort auf das Werbeschreiben) Kenntnis von dessen personenbezogenen Daten erlangt. Ausschlaggebend für diese Bewertung ist, daß der Betroffene in diesen Fällen unbewußt Informationen über sich preisgibt, die zwangsläufig aus den vom Adressenkunden festgelegten Selektionskriterien folgen. Der Betroffene handelt damit praktisch als „Werkzeug" dessen, der die Daten verkauft oder vermietet. Dieser Vorgang ist daher dem Adressenmieter als Übermittlung zuzurechnen. Wenn sich ein Betroffener über eine Werbesendung beschwert, ist der Übermittlungstatbestand genauso erfüllt, wie wenn er aufgrund der Werbesendung bestellt.
Die Daten des Betroffenen sind dem werbenden Unternehmen mithin übermittelt worden. Ich gehe allerdings davon aus, daß die Firma die Daten nicht in einer Datei i.S. des BDSG gespeichert hat. Aus dem BDSG ergibt sich daher kein gegen sie gerichteter Auskunftsanspruch.

Wohl aber läßt sich ein Anspruch des Betroffenen auf Auskunft über die Herkunft seiner Daten aus einer analogen Anwendung der §§ 1004, 823 BGB herleiten.
§ 1004 BGB stellt zunächst einmal nur auf eine Beeinträchtigung des Eigentums ab, gewährt Rechtsschutz aber auch zugunsten anderer absoluter Rechte, zu denen heute auch das allgemeine Persönlichkeitsrecht gezählt wird. Dies geschieht in Form eines Beseitigungsanspruchs bei einmaliger Beeinträchtigung sowie in Form eines Unterlassungsanspruchs, wenn weitere Beeinträchtigungen zu erwarten sind.
Für den vorliegenden Fall ist festzustellen, daß durch das unaufgeforderte Zusenden von Werbematerial eine Beeinträchtigung des Persönlichkeitsrechts hervorgerufen wird. Grundsätzlich darf zwar von der Zulässigkeit unaufgeforderten Zusendens von Werbematerial ausgegangen werden. Etwas anderes gilt jedoch, wenn der Betroffene der Verwendung seiner Adresse zu Werbezwecken widerspricht. Der Widerspruch ist als Indiz zu werten, daß schutzwürdige Belange des Betroffenen beeinträchtigt sind. Die Weiterspeicherung ist mithin nach § 23 BDSG unzulässig geworden, und die Adresse darf zu Werbezwecken nicht mehr verwendet werden. Jede durch das BDSG nicht gedeckte Verwendung personenbezogener Daten stellt eine Verletzung des allgemeinen Persönlichkeitsrechts dar (vgl. BGH-Urteil vom 7. 7. 1983 in NJW 1984, S. 436; BGH, Urteil vom 22. 5. 1984 – VI ZR 105/82). Da derartige Beeinträchtigungen auch in Zukunft zu erwarten sind, steht dem Betroffenen ein Unterlassungsanspruch zu.
Der zivilrechtliche Anspruch richtet sich einmal gegen die speichernde Stelle, also den Adressen-Eigentümer. Die Gefahr der weiteren unzulässigen Verwendung zu Werbezwecken geht von ihm aus. Gegen ihn kann der Betroffene seinen Anspruch aber nicht durchsetzen, solange er ihm unbekannt ist.
Da die werbende Firma die Beeinträchtigung durch den Adressen-Eigentümer mitverantworten hat, muß sie nun mitwirken, die Störungsquelle zu beseitigen. Ihr Beitrag zur Vermeidung der Wiederholungsgefahr besteht in der Auskunft über Namen und Anschrift des Adressen-Eigentümers.

Auch dieser Vorfall zeigt im übrigen, daß die vor Jahren zwischen den Datenschutz-Aufsichtsbehörden und dem Allgemeinen Direktwerbe- und Direktmarketing-Verband e.V. (ADV) getroffenen Vereinbarungen (vgl. 1. TB Nr. 7.3) nicht umgesetzt worden sind.

Ich habe mir einige Vertragstexte für Direktwerbe-Aufträge vorlegen lassen und feststellen müssen, daß sie keine der vereinbarten Regelungen übernommen haben. Eine Kontrolle wird allerdings dadurch erschwert, daß in der Branche der Adreßvermittler und

Letter-Shops (dies gilt jedenfalls für die meisten kleinen und mittleren Unternehmen) durchweg nicht mit schriftlichen Verträgen gearbeitet wird.
Offensichtlich konnten die Mitglieder des ADV die vom Verband akzeptierten Regeln bei ihren Auftraggebern (den Adreß-Mietern) nicht durchsetzen. Einzig und allein die auf freiwilliger Basis und der Werbewirtschaft Porto sparende „Robinsonliste" funktioniert halbwegs. Dabei ist jedoch anzumerken, daß sie weiterhin nur halbjährlich aktualisiert wird. Auch bietet sie keinen absoluten Schutz vor ungebetener Direktwerbung, wenn in die Vermittler-Maschinerie Namens-Varianten geraten, die nicht in der Robinsonliste verzeichnet sind.

Das Verfahren der Direktwerbung wurde bewußt so kompliziert gestaltet, um das werbende Unternehmen aus dem Anwendungsbereich des BDSG auszugrenzen.
In der Praxis wird Direktwerbung so durchgeführt, daß keiner der Beteiligten (Adressen-Eigentümer, Adressen-Verwalter, Vermittler, Letter-Shop oder Adressen-Mieter) prüft, ob nicht schutzwürdige Belange eines Umworbenen einer Verwendung seiner Daten für die Werbeaktion entgegenstehen. Dem Betroffenen werden bestenfalls im Nachhinein die Zusammenhänge erklärt, und es werden ihm die Quelle oder aber nur der Vermittler und die Selektionskriterien genannt. Weniger gutwillige Unternehmen (s.o.) gehen auf Einwendungen der umworbenen Personen überhaupt nicht ein.

Deshalb halte ich es für dringend notwendig, bei der bevorstehenden Novellierung des BDSG dafür zu sorgen, daß alle an der Direktwerbung Beteiligten dem 4. Abschnitt des BDSG und damit der ständigen Überwachung durch die Aufsichtsbehörde unterworfen werden.

Ob es zu einer Novellierung des BDSG in absehbarer Zeit kommen wird, ist ungewiß. Vordringlich ist ein Gespräch mit dem Zentralausschuß der Werbewirtschaft e.V. (ZAW), in dem nicht nur die mit dem ADV vereinbarten Regeln bestätigt, sondern weitergehende, sich an dem z.Z. diskutierten Vorschlag für eine Empfehlung des Europarats zum Schutz personenbezogener Daten bei der Verwendung zum Zwecke der Direktwerbung orientierende Verbesserungen der Position des Betroffenen erreicht werden sollten.

Auch über die Europarats-Initiative berichtete ich bereits in meinem 1. TB (vgl. Nr. 7.3). Der dort erwähnte Vorentwurf liegt inzwischen leicht verändert, aber noch sehr datenschutzfreundlich dem Lenkungsausschuß für rechtliche Zusammenarbeit beim Europarat zur Beschlußfassung vor.

Über einen besonderen Zweig des Direktmarketing – das Angebot von Adressen nach Bewertungskategorien von Auskunfteien – wird unter Nr. 4.4.1 berichtet.

4.2 Kreditwirtschaft

4.2.1 Erteilung von Bankauskünften

Durch die von Banken und Sparkassen zum 1. 1. 1984 vorgenommene Änderung der Allgemeinen Geschäftsbedingungen (AGB) hat die Frage, unter welchen Voraussetzungen Bankauskünfte erteilt werden dürfen, in der Öffentlichkeit große Beachtung gefunden.
Zum Jahreswechsel 1983/1984 wiesen zahlreiche Kreditinstitute in Zeitungsanzeigen, durch Aushang in den Geschäftsstellen oder mit persönlichen Anschreiben ihre Kunden darauf hin, daß sie ihre AGB geändert hätten. Die AGB enthielten nunmehr einen ausdrücklichen Hinweis darauf, daß das Kreditinstitut bankmäßige Auskünfte über die Kreditwürdigkeit und die Zahlungsfähigkeit des Kunden erteilen könne. Hiermit war keine Ausdehnung des bisherigen Verfahrens beabsichtigt. Die Kreditinstitute wollten lediglich ihre – insbesondere von den Datenschutzbehörden angegriffene – Auskunftspraxis rechtlich absichern.

Die Datenschutz-Kontrollinstanzen hatten in der Vergangenheit mehrfach darauf hingewiesen, daß die Erteilung von Bankauskünften über natürliche Personen in aller Regel unzulässig sei, da es an einer ausdrücklichen Einwilligung des Kontoinhabers fehle. Eine Verletzung des Bankgeheimnisses bzw. – in der Terminologie des Datenschutzes – die Beeinträchtigung schutzwürdiger Belange des Bankkunden ließe sich nur vermeiden, wenn dieser eine Einwilligungsklausel ähnlich wie die Schufa-Klausel unterzeichnet habe (vgl. 2. TB Nr. 4.2.1) Erst durch die Beschwerden einiger Bankkunden erfuhren die Datenschutzbehörden von der Änderung der AGB; sie hatten neue Einwände. Die Konferenz der Datenschutzbeauftragten veröffentlichte eine Entschließung, in der es hieß, die neue AGB-Bestimmung über die Zulässigkeit von Bankauskünften sei gemäß § 9 Abs. 1 und 2 Nr. 1 AGB-Gesetz unwirksam, da sie mit wesentlichen Grundgedanken der Datenschutzgesetze, insbesondere mit dem Grundsatz der Selbstbestimmung des Kunden über seine Daten nicht zu vereinbaren sei und ihn entgegen dem Geist von Treu und Glauben unangemessen benachteilige. Die Kreditinstitute dürften daher auch dann nicht nach der Neuregelung in den AGB verfahren, wenn ein Kunde von seinem Widerspruchsrecht keinen Gebrauch gemacht habe.
Diese Presseerklärung löste eine Flut von Widersprüchen beunruhigter Bankkunden aus. Ende Januar kamen Vertreter der Datenschutzbehörden und der Kreditwirtschaft mit dem Ziel zusammen, die bestehenden Meinungsverschiedenheiten so schnell wie möglich zu beseitigen, die datenschutzrechtlichen Voraussetzungen und Grenzen des Bankauskunftsverfahrens zu präzisieren, die Kunden über Inhalt und Zweck dieses Verfahrens umfassend zu unterrichten und sie auf ihre Rechte hinzuweisen.
Für die Übergangszeit bis zum Abschluß der Gespräche wurde beschlossen, daß Bankauskünfte über Privatkunden nur erteilt werden sollten, wenn die ausdrückliche Zustimmung des Kunden vorliegt. Bankauskünfte über Geschäftskunden sollten – vorbehaltlich anderer Weisungen des Kunden – im bisher üblichen Umfang erteilt werden (vgl. Bekanntmachung Nr. 11/84 des Bundeskartellamtes über die Anmeldung eines Beschlusses zur vorläufigen Behandlung der Erteilung von Bankauskünften im Rahmen der Allgemeinen Geschäftsbedingungen von Kreditinstituten vom 7. 2. 84, Bundesanzeiger vom 16. 2. 84).

Im Oktober veröffentlichten der Kreditausschuß, der „Düsseldorfer Kreis" und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein „Gemeinsames Kommuniqué über das Bankauskunftsverfahren", das für das Bankauskunftsverfahren folgende Regeln enthält:

1. Das Kreditinstitut ist berechtigt, über Geschäftskunden (juristische Personen und Kaufleute) Bankauskünfte zu erteilen, sofern ihm keine anderslautende Weisung des Kunden vorliegt.
2. Bankauskünfte über Privatkunden erteilt das Kreditinstitut nur dann, wenn diese allgemein oder im Einzelfall ausdrücklich zugestimmt haben.
3. Bankauskünfte sind allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse des Kunden, seine Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Sparguthaben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditinanspruchnahmen werden nicht gemacht.
4. Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute für deren eigene Zwecke und die ihrer Kunden; sie werden nur dann erteilt, wenn der Anfragende ein berechtigtes Interesse an der gewünschten Auskunft glaubhaft darlegt.

Über diese Neuregelung unterrichtet die Kundeninformation „Bankauskunftsverfahren", die in den Kreditinstituten aushängt. Später sollen die Regeln in die Allgemeinen Geschäftsbedingungen der Banken und Sparkassen aufgenommen werden. Einvernehmen wurde auch über folgende Einzelheiten der praktischen Durchführung des Bankauskunftsverfahrens erzielt:

„1. Die Auskunftsverweigerung wegen fehlender Einwilligung ist so zu formulieren, daß sie nicht als negative Auskunft verstanden werden kann. Liegt bei Privatkunden eine

Einwilligung nicht vor oder hat bei Geschäftskunden der Kunde die Erteilung einer Auskunft untersagt oder hat die angefragte Stelle keinen Einblick in die wirtschaftlichen Verhältnisse des Kunden, ist dies in der Antwort deutlich zum Ausdruck zu bringen.
2. Die Auskunft darf sich nur auf die wirtschaftlichen Verhältnisse des Kunden und sein Verhalten im Geschäftsleben beziehen.
3. Bankauskünfte werden nur aufgrund von Erkenntnissen erteilt, die der auskunftgebenden Stelle vorliegen. Es werden keine Recherchen (etwa mit Hilfe von Wirtschaftsauskunfteien) angestellt.
4. Hat das Kreditinstitut eine von Anfang an unrichtige Auskunft erteilt, so ist es zur Richtigstellung gegenüber dem Auskunftsempfänger verpflichtet.
5. Der Kunde, der eine Auskunft erhält, ist ausdrücklich darauf hinzuweisen, daß er empfangene Informationen nur für den angegebenen Zweck verwenden und nicht an Dritte weitergeben darf.
6. Mündlich erteilte Bankauskünfte werden dokumentiert und sollen in der Regel schriftlich bestätigt werden.
7. Auf Verlangen des Betroffenen hat das Kreditinstitut den Inhalt einer erteilten Auskunft mitzuteilen.
8. Wirtschaftsauskunfteien erhalten keine Bankauskünfte."

Gegenstand der Gespräche war auch das Schufa-Auskunftsverfahren. Es bestand Einvernehmen darüber, daß auch die sog. Schufa-Klausel geändert werden soll, die von jedem Bankkunden bei der Eröffnung eines Girokontos, der Aufnahme von Kleinkrediten und der Übernahme von Bürgschaftsverpflichtungen unterzeichnet wird. Ohne eine sehr viel ausführlichere und deutlichere Unterrichtung des Kunden über die Aufgabe der Schufa, die Vertragspartner des Schufa-Auskunftsverfahrens und die Datenflüsse zwischen den Beteiligten liegt nach Meinung der Datenschutz-Aufsichtsbehörden eine wirksame Einwilligung des Kunden nicht vor, so daß Schufa-Auskünfte über ihn nicht erteilt werden dürfen. Beide Seiten sind sich jedoch einig, daß zunächst der Ausgang eines beim BGH schwebenden Rechtsstreits abgewartet werden soll, der über die Wirksamkeit der Schufa-Klausel geführt wird (vgl. Nr. 4.4.3.3).

4.3 Versicherungswirtschaft

4.3.1 Schweigepflichtentbindungsklausel

Möchte jemand seine Altersvorsorge durch eine Lebensversicherung treffen oder erweitern oder sich privat gegen Krankheitsrisiken absichern, so wird von ihm verlangt, daß er eine Vielzahl von persönlichen Daten, vor allem Gesundheitsdaten, über sich selbst, seine Eltern und seine Geschwister angibt bzw. das Versicherungsunternehmen ermächtigt, diese Auskünfte von Dritten einzuholen. Hierfür verwenden die Versicherungsunternehmen sog. „Schweigepflichtentbindungsklauseln". Bei Lebensversicherungsunternehmen wird z. Z. die nachstehende Schweigepflichtentbindungsklausel bei Anträgen auf Abschluß eines Versicherungsvertrages verwendet:

„Ich ermächtige den Versicherer zur Nachprüfung und Verwertung der von mir über meine Gesundheitsverhältnisse gemachten Angaben, alle Ärzte, Krankenhäuser und sonstigen Krankenanstalten, bei denen ich in Behandlung war oder sein werde, sowie andere Personenversicherer und Behörden über meine Gesundheitsverhältnisse zu befragen.
Dies gilt nur für die Zeit vor der Antragsannahme und die nächsten 3 Jahre nach der Antragsannahme. Der Versicherer darf auch die Ärzte, die die Todesursache feststellen, und die Ärzte, die mich im letzten Jahr vor meinem Tod untersuchen oder behandeln werden, über die Todesursachen oder die Krankheiten, die zum Tode geführt haben, befragen.
Insoweit entbinde ich alle, die hiernach befragt werden, von der Schweigepflicht auch über meinen Tod hinaus."

Gegen die Verwendung dieser Klausel, die wohl auch als datenschutzrechtliche Einwilligung in die Übermittlung der angeforderten Daten durch die genannten Personen und Stellen zu verstehen ist, bestehen aus der Sicht des Datenschutzes erhebliche Bedenken.
Zunächst kommt es darauf an, daß die „Schweigepflichtentbindungsklausel" die an die Einwilligung gem. § 3 Nr. 2 BDSG zu stellenden Anforderungen erfüllen muß. Eine Einwilligung i. S. dieser Vorschrift ist aber nur dann wirksam, wenn sie hinreichend bestimmt ist. Das läßt sich bei einer Ermächtigung, die sich nicht nach konkreten, versicherungsrechtlich erheblichen Kriterien richtet und sich damit einer Blankoeinwilligung nähert, kaum annehmen. Die Anforderungen an die Bestimmtheit müssen um so strenger gefaßt werden, je sensitiver die Daten sind, auf die sich die Erklärung bezieht. Eine Erklärung, die so weit gefaßt, ist wie die in den Antragsformularen der Lebensversicherungen enthaltene Klausel, entspricht diesen Anforderungen nicht. Da der Betroffene nicht weiß, worauf er sich bei der Unterzeichnung einläßt, reicht die Klausel jedenfalls insoweit nicht, als sie sich auf in der Zukunft liegende, ärztliche Behandlungen bezieht. Für in der Zukunft liegende Umstände kann der Betroffene eine wirksame Einwilligung nur erteilen, wenn die zukünftigen Umstände für ihn vorhersehbar sind. Da niemand in der Lage ist, seinen künftigen Gesundheitszustand vorherzusehen, können darauf bezogene Erklärungen mithin nicht als hinreichend bestimmt angesehen werden.
In diesem Zusammenhang ist darauf hinzuweisen, daß nach einer Entscheidung des 85. Deutschen Ärztetages (12.-15.5.1982 in Münster) zu „Fragen der ärztlichen Schweigepflicht und Probleme des Datenschutzes" sich Sozialleistungsträger, Privatversicherer, Gerichte und Behörden bei Arztanfragen nicht sollen darauf berufen können, daß der Patient pauschal einer Befreiung von der ärztlichen Schweigepflicht zugestimmt hat.

Die Lebensversicherer halten es hingegen – und zwar auch im Interesse der Versicherungsnehmer – für erforderlich, daß die Schweigepflichtentbindungsklausel auch in die Zukunft gerichtet ist. So sei der Lebensversicherer von der Zahlung der Versicherungssumme befreit, wenn der Versicherte innerhalb von 3 Jahren nach Vertragsannahme Selbstmord verübe. Wenn sich aber aufgrund der Auskunft der von der Schweigepflicht entbundenen Stellen herausstelle, daß sich der Versicherte schon einige Zeit vor dem Selbstmord in einem psychisch labilen Zustand befunden hat, müsse die Versicherung gleichwohl zahlen.
Weitere Bedenken gegen die Schweigepflichtentbindungsklausel ergeben sich daraus, daß nach deren Text die Ermächtigung auch gegenüber „Behörden" gilt. Mit „Behörden" i. S. der Klausel sind vor allem die Sozialversicherungsträger gemeint. Für diese bestimmt jedoch § 67 Satz 1 SGB X ausdrücklich, daß der Betroffene „im Einzelfall" in eine Offenbarung eingewilligt haben muß, soweit nicht eine gesetzliche Offenbarungsbefugnis nach den §§ 68-77 SGB X vorliegt. Diesen gesetzlichen Anforderungen wird die z. Z. verwendete Schweigepflichtentbindungsklausel gegenüber den in §§ 18-29 SGB I genannten Stellen nicht gerecht. Das bedeutet, daß die Sozialleistungsträger aufgrund der Klausel keine Sozialdaten an Versicherungen weitergeben dürfen.
Weiter ist zu prüfen, ob die Informationswünsche der Versicherer von ihrem Umfang her gerechtfertigt sind. Das Problem liegt – z. B. bei Krankenhausentlassungsberichten – darin, daß in den Berichten sehr häufig noch weitergehende Informationen angeführt sind, die die Gesundheitsverhältnisse meist nicht einmal mittelbar berühren, deren Kenntnis aber gleichwohl für nachbehandelnde Ärzte wichtig sein können, nämlich z. B. Informationen über Probleme im beruflichen Bereich, über Schwierigkeiten in der Ehe, Angaben über sexuelle Verhaltenweisen bzw. Abartigkeiten sowie Angaben zu Lebensgewohnheiten u. ä. Meines Erachtens braucht eine Versicherung nicht alles zu wissen, was der Arzt für Zwecke der Nachbehandlung erfährt.
Diese Auffassung ist mit den anderen Aufsichtsbehörden abgestimmt. Die Aufsichtsbehörden werden möglichst bald mit der Versicherungswirtschaft über die oben skizzierten Probleme sprechen. Ein Termin ist allerdings noch nicht vereinbart. Die Weiterverwendung der jetzigen Klausel bringt insbesondere die Sozialleistungsträger in Konflikte.

4.3.2 Zentrale Dateien der Versicherungsverbände

Über die Übermittlungen aus den zentralen Dateien der Versicherungsverbände habe ich ausführlich in meinem 2. TB (Nr. 4.3.1) berichtet. Meiner Auffassung, die ich im 2. TB begründet habe, hat die Versicherungswirtschaft lediglich wirtschaftliche und praktische Erwägungen entgegengesetzt. Ich habe weitere Vorschläge zu einer datenschutzgerechten Ausgestaltung der Verfahren gemacht und meine rechtlichen Bedenken konkretisiert. Die Versicherungswirtschaft hat bisher nichts unternommen, die – nach Meinung aller Datenschutzaufsichtsbehörden gegen Vorschriften des Datenschutzes verstoßenden – Verfahren der zentralen Registrierstelle Rechtsschutz beim HUK-Verband und der Sonderwagnisdatei der Lebensversicherer zu ändern. Ich habe den Gesamtverband der Deutschen Versicherungswirtschaft nochmals gebeten, er möge die Initiative ergreifen und dafür sorgen, daß ein rechtmäßiger Zustand hergestellt wird.

4.4 Auskunfteien

4.4.1 Angebot von bonitätsgeprüften Adressen durch Handels- und Wirtschaftsauskunfteien

Kürzlich wurde mir bekannt, daß eine Auskunftei sich zur Hilfe bei zielgerichteter Kundensuche anbot. Zur Auswahl potentieller Kunden wurden Adressen angeboten, die „nach von Ihnen vorzugebenden Merkmalen" aus den „ umfangreichen elektronischen Archiven" herausgsucht würden. In dem Angebot hieß es:

> „Ihre Anforderung kann so zum Beispiel lauten, daß die zu findenden Kunden entweder bundesweit oder in bestimmten Regionen ansässig sind, über ein bestimmtes Alter verfügen, bestimmte Rechtsformen aufweisen, eine zu definierende Umsatzgrößenordnung und ein bestimmtes Zahlungsverhalten besitzen. Nach Ihren Vorgaben suchen wir bundesweit oder in dem von Ihnen vorgegebenen Gebiet diejenigen Firmen, auf die exakt diese Merkmale zutreffen. Bei der Lieferung der entsprechenden Anschriften können sie weitere, ebenfalls vorher bestimmbare Daten über das einzelne Unternehmen erhalten. So können wir Ihnen beispielsweise auf Wunsch die Anzahl der Mitarbeiter, den Umsatz in DM, den Namen des Geschäftsführers oder Inhabers oder das tatsächliche Zahlungsverhalten bekanntgeben.
>
> Um Ihnen einen Überblick über die möglichen Auswahlkriterien zu geben, überlassen wir Ihnen anbei unseren Katalog der Auskunftsmerkmale. Wir fügen ebenfalls eine Auflistung unserer Bonitätsklassen zur Zahlungsweise bei, nach der Sie Ihre zukünftigen Kunden von uns suchen lassen können."

Beigefügt war eine Liste, die u. a. folgende Selektionsmerkmale zur Zielgruppenbeschreibung enthielt: Auftragslage, Krediturteil, Unternehmensentwicklung und Zahlungsweise.

Die Weitergabe sog. „bonitätsgeprüfter Marketing-Adressen" wirft zunächst einmal die Frage auf, ob es sich dabei in erster Linie um einen Adressenhandel im weitesten Sinne oder die Erteilung von Auskünften zu Zahlungswürdigkeit und Bonität handelt.

Grundlage für die automatisierte Marketing-Adressenselektion sind Datenbestände, die zu Zwecken der Kreditauskunft angelegt wurden und bisher ausschließlich in diesem Rahmen Verwendung gefunden haben. Die Besonderheit der angebotenen Adressen liegt gerade darin, daß sie z. B. Umsatzzahlen und Zahlungsverhalten – also kreditrelevante Merkmale – zum Auswahlkriterium haben; die Aufnahme bzw. Nichtaufnahme in die Marketing-Adressenliste bedeutet somit auch eine Auskunft über die Kreditwürdigkeit des Betroffenen.

Das Marketing-Adressen-Angebot stellt daher eine erweiterte Form der Kreditauskunft dar. Die Einordnung in den Bereich des bloßen Adressenhandels würde dem zugrundeliegenden Sachverhalt nicht gerecht werden und darüber hinaus zahlreiche Probleme etwa bei der Zweckbeschreibung der verarbeitenden Stelle nach § 39 Abs. 2 Nr. 4 BDSG oder der Zulässigkeit der Speicherung zu nicht eindeutig im voraus beschriebenen Zwecken aufwerfen.

Die Zulässigkeit der Übermittlung der im Angebot näher bezeichneten Daten richtet sich nach § 32 Abs. 2 BDSG.

Problematisch erscheint hierbei zunächst, ob es überhaupt Empfänger gibt, die ein berechtigtes Interesse an der Übermittlung von nach Umsatz und Kreditwürdigkeitskriterien ausgewählten Marketing-Adressenlisten glaubhaft darlegen können. Dazu bedarf es m. E. eines spezifizierten Interesses an ganz bestimmten Daten für im einzelnen zu benennende Ziele oder Geschäftszwecke; globale Verweisungen genügen nicht. Ein berechtigtes Interesse an Angaben z. B. über die Kreditwürdigkeit haben nur solche Unternehmen oder Personen, die mit dem Betroffenen tatsächlich in Geschäftsverbindungen stehen oder eintreten wollen.
Das Erfordernis der glaubhaften Darlegung des berechtigten Interesses im Einzelfall und der Protokollierung nach § 32 Abs. 2 Satz 2 BDSG schließt die listenmäßige Übermittlung aus, selbst wenn man davon ausgeht, daß nicht eine sog. „schwarze Liste", sondern ein Verzeichnis von potentiellen Kunden mit „positiver Zahlungsweise" übersandt wird. Da diese Merkmale an einen Interessentenkreis weitergegeben werden, der in der Mehrzahl der Fälle dem von ihm anvisierten Markt nicht völlig ohne Kenntnisse gegenüber stehen wird, stellt die Nichtaufnahme bestimmter Unternehmen in die Marketing-Adressenverzeichnisse inzident auch eine negativ zu wertende Kreditauskunft über sie dar.
Meines Erachtens sind die Zulässigkeitsvoraussetzungen für eine Datenübermittlung nach § 32 Abs. 2 BDSG nicht erfüllt.

4.4.2 Auskunftstelle über den Versicherungsaußendienst e.V. (AVAD)

Ich beziehe mich auf den 2. TB, in dem ich unter Nr. 4.4.2 über meine Vorschläge berichtet hatte, das Auskunftsverfahren der AVAD transparenter zu gestalten. Erfreulicherweise ist es in diesem Jahr zu einer Einigung mit der Versicherungswirtschaft gekommen.
Das neue Verfahren sieht so aus, daß ein Außendienstmitarbeiter künftig zu Beginn seiner Beschäftigung (als Angestellter oder Handelsvertreter) über die Tätigkeit der AVAD unterrichtet wird. Die Zustimmung zum AVAD-Auskunftsverfahren wird Gegenstand des Vertrages.
Beim Ausscheiden wird die Auskunft für die AVAD gefertigt und abgesandt. Gleichzeitig wird dem Betroffenen eine Kopie ausgehändigt, damit er so früh wie möglich seine Einwände gegen den Inhalt der Auskunft und/oder das Speichern bei der AVAD vortragen kann.
Wehrt sich der Betroffene und liefert er Anhaltspunkte, die Zweifel an der Richtigkeit der Auskunft aufkommen lassen, wird die AVAD bei Abforderung der Auskunft durch eine andere Gesellschaft nur die identifizierenden Angaben, eine Beschreibung der Tätigkeit und die zweifelsfrei richtigen Daten übermitteln; sie wird sich außerdem bei der Gesellschaft, die die Auskunft erstellt hat, nach der Richtigkeit und Aktualität der gemeldeten Angaben erkundigen.
Greift der Betroffene die Auskunft pauschal und ohne eine spezifizierte Begründung an, so entsteht noch kein Anspruch auf Sperrung. Die AVAD muß den Betroffenen darüber aufklären, daß sie die Daten nicht sperrt und weiterhin Auskünfte erteilt, oder daß sie trotz der Intervention zumindest die Identifizierungs- und Tätigkeitsangaben weitergibt.
Bei diesen Verfahren ist sichergestellt, daß der Schutzzweck der AVAD – dafür zu sorgen, daß nur vertrauenswürdige Personen im Versicherungsaußendienst eingesetzt werden – nicht eingeengt wird. Andererseits ist gewährleistet, daß der ausscheidende Mitarbeiter nicht erst eine Benachrichtigung durch die AVAD und die auf seinen Antrag erteilte Selbstauskunft abwarten muß, bevor er sich gegen irgendwelche Aussagen in der Auskunft wenden kann. Er hat die Möglichkeit, unverzüglich sowohl gegenüber der AVAD als auch gegenüber der absendenden Gesellschaft zu reagieren, wenn ihm Unrichtigkeiten oder Ungenauigkeiten auffallen.

4.4.3 Schufa

4.4.3.1 Eingaben

Auch in diesem Jahr gab es wieder Beschwerden darüber, daß Vertragspartner der Schufa mit dem Anfragemerkmal „AV" (Anfrage wegen Vorleistung oder Leistung mit

kreditorischem oder geschäftlichem Risiko) bei der Schufa anfragen und die übermittelten Informationen ausschließlich für private Zwecke nutzen, was eindeutig gegen die vertraglichen Abmachungen verstößt und in aller Regel auch nach dem BDSG unzulässig ist. In einem – m. E. eindeutigen – Fall hat ein Betroffener Strafantrag wegen unzulässiger Datenübermittlung gestellt. Die staatsanwaltlichen Ermittlungen sind noch nicht abgeschlossen.
Das Problem dieser Datenübermittlungen liegt darin, daß die Schufa nicht erkennen kann, ob der Anfrage das angegebene berechtigte Intresse tatsächlich zugrundeliegt. Schon heute geht die Schufa jedem Hinweis auf eine möglicherweise unzulässige Nutzung der von ihr übermittelten Information nach. Im Zuge meiner Prüfung (vgl. Nr. 4.4.3.2) habe ich Vorschläge gemacht, die die Voraussetzungen für die nachgehende Kontrolle verbessern sollen.

4.4.3.2 Schufa-Auskunftsverfahren

4.4.3.2.1 Geschäftszweck der Schufa

Im Laufe des Berichtszeitraums habe ich die Schufa GmbH Hamburg geprüft.
In der nachfolgenden Betrachtung gehe ich aber nur auf grundsätzliche Probleme ein, die alle oder die sieben am SCHABS-Verfahren beteiligten Schufa-Gesellschaften betreffen.
Die Schufa sammelt, speichert und übermittelt Angaben über die Kreditfähigkeit und Kreditwürdigkeit von Einzelpersonen.
Sie sieht es als ihre Aufgabe an, die kreditgebende Wirtschaft vor Verlusten zu schützen, aber auch den Verbraucher vor übermäßiger Verschuldung zu bewahren. Sie arbeitet nach dem Grundsatz der Gegenseitigkeit.
Die Anschlußfirmen sind von sehr unterschiedlicher Struktur. Es lassen sich dabei drei Gruppen unterscheiden. Einmal sind hier vor allem die Kreditinstitute zu nennen, auf die über 80 % der Schufa-Auskünfte entfallen. Zum anderen sind große Versandhandelsunternehmen, Waren- und Kaufhäuser und zum dritten kleinere Wirtschafts- und Handelsunternehmen Anschlußfirmen der Schufa. Der Informationsbedarf ist bei diesen Gruppen unterschiedlich; deshalb haben sie auch unterschiedliche Schufa-Anschlußverträge mit unterschiedlichen Rechten und Pflichten.
Kreditinstitute und ihre Zweigstellen, die für eigene Rechnung Kredite herauslegen und selbst bis zur Erledigung überwachen, sowie Einzelhandels- und Versandhandelsunternehmen, Waren- und Kaufhäuser und Wirtschaftsunternehmen, die geschäftsmäßig in nennenswertem Umfang aus eigenen Mitteln Kredite an Privatpersonen herauslegen und selbst bis zur Erledigung überwachen (sog. A-Vertragspartner), melden die Daten über die Aufnahme und Abwicklung der Kredite, über die Übernahme von Bürgschaftsverpflichtungen, über die Eröffnung eines Girokontos und ggf. Unregelmäßigkeiten bei der Kontoführung (aber keine Bestände oder Umsätze). Dafür erhalten sie auch sämtliche Auskunfts- und Beobachtungsmerkmale, also auch positive bzw. neutrale Feststellungen (Vollauskünfte), aber keine Auskünfte darüber, wer die Daten eingemeldet hat.
Einzelhandels- und Versandhandelsunternehmen, Waren- und Kaufhäuser und Wirtschaftsunternehmen, die wegen eigener Vorleistung oder eigener Lieferung ein Kreditrisiko tragen (sog. B-Vertragspartner), melden nur etwaige Daten bei vertragswidriger Abwicklung des Warenkredites (Negativdaten); sie erhalten daher auch nur Schufa-Auskünfte über vorhandene Negativmerkmale, nicht jedoch über aufgenommene Kredite oder bestehende Bürgschaftsverpflichtungen.
Daneben gibt es auch Anschlußfirmen, die keine Geld- oder Warenkredite einräumen, aber Risiken aus wirtschaftlichen Vorleistungen übernehmen. Dazu gehören z. B. Möbelhändler, die hochwertige Möbel nach Maß anfertigen lassen, oder Handwerksbetriebe, die individuelle Einzelanfertigungen erstellen, aber auch Wohnungsunternehmen und Autovermieter. Sie erhalten dieselben eingeschränkten Auskünfte (nur Negativdaten) wie z. B. Handelsunternehmen, die Warenkredite gewähren.
Näheres regeln die Verträge mit den Anschlußunternehmen sowie die „Technische Abwicklung des Auskunfts- und Meldeverfahrens" (TA), die Bestandteil dieser Verträge ist.
Von Ende 1982 bis August 1983 wurde das vorher manuell betriebene Auskunftsverfah-

ren der Schufa GmbH Hamburg in die automatisierte Datenverarbeitung übernommen; und zwar beteiligt sie sich am sog. SCHUFA-Auskunfts- und Beobachtungs-System (SCHABS), an das noch sechs weitere Regional-Schufa-Gesellschaften angeschlossen sind. Nachdem die richtige Übernahme der Daten kontrolliert worden war, wurden die vorher verwendeten Karteikarten vollständig vernichtet.
Die Umstellung der manuell geführten Schufa-Kartei auf die automatisierte Datenverarbeitung führte einerseits zu einem Schufa-Verbund-System, das zwar dezentralisiert ist, faktisch aber wie eine einzige Bundes-SCHABS-Datei wirkt. Andererseits ist festzustellen, daß alle Löschungsprobleme mit manuell geführten Karteikarten beseitigt sind. Auch haben sich mit Hilfe der Automation eine Reihe von zusätzlichen – allerdings auch notwendigen – Datensicherungsmaßnahmen realisieren lassen.
Jede der Schufa-Gesellschaften verwaltet ihren eigenen Datenbestand. Die Nutzung der Datenbestände erfolgt jedoch nicht nur durch die regional tätige Schufa. In den Schufa-Anschlußverträgen ist geregelt, daß im überörtlichen Auskunfts-, Beobachtungs- und Meldeverfahren jede Schufa in Vollmacht für alle anderen Schufa-Gesellschaften handelt. Jede Schufa im SCHABS-Verfahren ist mithin berechtigt, unter bestimmten Voraussetzungen die Datenbestände aller anderen SCHABS-Partner zu lesen. Veränderungen sind jedoch nur durch die jeweils den Datensatz verwaltende Schufa möglich. Wegen weiterer Einzelheiten wird auf Nr. 4.4.3.3 verwiesen.

4.4.3.2.2 Dateien

Die Schufa-Gesellschaften im SCHABS-Verbund führen für ihre Auskunftstätigkeit drei ADV-Dateien, und zwar eine Haupt-, eine Negativ- und eine Suchdatei.

- Hauptdatei
  In dieser Datei werden die Personalstammdaten sowie Anfrage-, Auskunfts- und Beobachtungsmerkmale nach Namen, Vornamen, Geburtsdatum und voller Anschrift (Straße, Hausnummer, Postleitzahl und Zustellbezirk) des Betroffenen gespeichert. Es wird versucht, nur solche Angaben zu erfassen, die mit Hilfe des Geburtsdatums eindeutig einer Person zuzuordnen sind; nur ein ganz geringer Teil des Datenbestandes ist ohne Geburtsdatum.
  Ehepartner sind nicht in einem gemeinsamen Datensatz gespeichert. Die Datensätze enthalten jedoch gegenseitige Hinweise.
- Negativdatei
  In dieser Datei sind Eidesstattliche Versicherungen (EV) und Haftbefehle zur Erzwingung einer EV aus dem Schuldnerverzeichnis nach Namen, Vornamen, vollständiger Anschrift des Betroffenen gespeichert. Vom Schuldnerverzeichnis werden in ca. 90% aller Fälle Haftbefehle ohne Geburtsdatum gemeldet.
- Suchdatei
  In dieser Datei sind Suchaufträge von den Vertragsfirmen aller Schufa-Gesellschaften gespeichert, wenn ein Schuldner unbekannt verzogen ist. Es werden Name, Vorname, Geburtsdatum und die der Schufa als letzte bekanntgewordene volle Anschrift des Schuldners erfaßt. Suchaufträge ohne Geburtsdatum werden nicht aufgenommen.

4.4.3.2.3 Datenverarbeitung

Die Schufa-Anschlußfirmen haben die Möglichkeit, Anfragen telefonisch, schriftlich, über Telex oder als sog. DATA-Anfrage im automatisierten Verfahren an die Schufa zu richten.

- Telefonische Auskünfte
  Bei Anrufen, mit denen Auskünfte abgefordert werden, gibt eine Mitarbeiterin Namen und Kennziffer des Anfragenden, das Anfragemerkmal sowie Namen, Vornamen, Geburtsdatum und Anschrift des Betroffenen in das System ein.
  Seit Anfang 1984 werden alle telefonischen Auskünfte schriftlich bestätigt. Sofern sich die Identität des Betroffenen nicht eindeutig feststellen läßt, enthalten die schriftlichen Bestätigungen einen besonderen Hinweis hierauf.

Wegen der nicht nur theoretischen Mißbrauchsmöglichkeiten der Schufa-Kennziffer insbesondere im Telefonverkehr ist es bedenklich, daß für jeden Vertragspartner nur eine Kennziffer vergeben wird. Bei Vertragspartnern mit einer Vielzahl von Anfrageberechtigten erscheint eine Kontrolle im Fall eines Mißbrauchs nahezu unmöglich.
In solchen Fällen ist die Vergabe mehrerer Kennziffern unbedingt erforderlich. Auch ein Wechsel der Kennziffer nach einem bestimmten Zeitraum sollte erwogen werden.
Die seit Anfang 1984 von allen Schufa-Gesellschaften praktizierte obligatorische schriftliche Bestätigung aller telefonischen Anfragen relativiert das Kontrolldefizit, sofern es sich um Vertragspartner mit einer geringen Zahl Anfrageberechtigter handelt. Denn bei kleineren überschaubaren Unternehmen ist davon auszugehen, daß es ihnen auffällt, wenn sie eine Bestätigung für eine nicht angeforderte telefonische Auskunft erhalten und diese auch noch bezahlen sollen.
In diesen Fällen schließt sich sowohl bei der Schufa als auch beim Vertragspartner eine genauere Prüfung an. Wenn die Schufa in allen Fällen, in denen der Verdacht eines Mißbrauchs besteht, sofort eine Kennzifferänderung vornimmt, bietet die obligatorische schriftliche Bestätigung wenigstens bei Vertragspartnern mit wenigen Anfrageberechtigten hinreichenden Schutz vor mißbräuchlichen Anfragen.

- Schriftliche Auskünfte
  Sofern sich die Identität des Betroffenen nicht eindeutig feststellen läßt (insbesondere bei Nachmeldungen von Eintragungen ohne Geburtsdatum, Mitteilung anhand von Suchaufträgen), enthalten alle schriftlichen Auskünfte einen besonderen Hinweis und die Aufforderung an den Vertragspartner, unbedingt eine Identitätsprüfung vorzunehmen.
  Jeder schriftlichen Auskunft ist zudem ein Rücklaufformular angefügt, das vom Vertragspartner für die nachfolgende Meldung an die Schufa verwendet werden kann, wenn eine Kreditentscheidung getroffen worden ist. Er kann seiner Pflicht zur Meldung auch auf anderem Wege nachkommen.
  Auf jeden Fall muß der Vertragspartner das Ergebnis seiner Identitätsprüfung mitteilen. Sobald aufgrund der Rückmeldung eine eindeutige Zuordnung möglich ist, wird diese in dem betreffenden Datensatz vorgenommen. Andernfalls wird ein (wechselseitiger) Hinweis aufgenommen, daß keine Personenidentität besteht.
- Telexauskünfte
  Das Verfahren der Telex-Anfragen entspricht dem der schriftlichen Anfragen. Die fernschriftlichen Anfragen und Auskünfte werden zudem protokolliert.
- DATA-Auskünfte
  Für Großkunden wurde das DATA-Verfahren entwickelt. Bisher nutzten hauptsächlich Versandhäuser diese Möglichkeit für Sammelanfragen. Hierbei werden die Anfragen teils per Standleitung, teils auf Band gespeichert dem Rechenzentrum zugeleitet; dort werden sie zwischengespeichert und im Stapel-Verfahren in Stundenabständen eingelesen. Wenn eine vollständige Identität zwischen den Angaben des Vertragspartners und denen in einem von der Schufa gespeicherten Datensatz besteht, stellt das Rechenzentrum die entsprechende Auskunft dem Schufa-Vertragspartner auf dem gleichen Wege zur Verfügung. Die übrigen Anfragen werden an die jeweils verwaltende Schufa-Geschäftsstelle weitergeleitet und dort von den Mitarbeitern geprüft. Die angeschlossenen Vertragspartner haben also keinen on-line-Zugriff auf den Datenbestand der Schufa. Ähnlich wie bei einer on-line-Lösung liegt das Problem einer DATA-Anfrage aber darin, daß der Vertragspartner – bei eindeutiger Identitätsfeststellung – ohne Einschalten eines Sachbearbeiters der Schufa direkt Daten aus dem Bestand der Schufa abrufen kann. Wie bei einem on-line-Verfahren kann mehr übermittelt werden, als der Vertragspartner tatsächlich benötigt, und ist der übermittelnden Stelle eine vorherige Prüfung nicht möglich, ob die Übermittlung zulässig ist. Schon bevor eine gesetzliche on-line-Regelung ähnlich dem § 6a des Referentenentwurfs des Bundesinnenminsteriums zur Änderung des BDSG vom 23.6.1983 in Kraft tritt, sollte die Schufa mit ihren Vertragspartnern detaillierte verfahrenssichernde Vereinbarungen treffen, die an diese strengere Anforderungen angepaßt sind, um wenigstens die nachgehende Kontrolle zu erleichtern.

4.4.3.2.4 Prüfung des berechtigten Interesses

Monatlich wird in 10 Fällen das Vorliegen eines berechtigten Interesses für eine Anfrage nachträglich überprüft.
Zur Stichprobenprüfung wird den betreffenden Vertragspartnern ein Vordruck zugesandt, der vom Datenschutzbeauftragten oder der Revisionsabteilung des Vertragspartners auszufüllen und der Schufa zurückzureichen ist.
Nur solche Vertragspartner, die weder über eine Revision noch über einen bDSB verfügen, prüfen nicht selbst, sondern müssen ihre Unterlagen der Schufa vorlegen.
M. E. sollten – mit Ausnahme der Kreditinstitute, soweit sich deren Anfragen auf die Gewährung von Krediten oder die Eröffnung von Girokonten beziehen – alle Vertragspartner, auch wenn sie einen bDSB bestellt oder eine Revision eingesetzt haben, der Schufa die Prüfung des berechtigten Interesses überlassen und ihr hierfür beweiskräftige Unterlagen übersenden.
Die Praxis, monatlich in nur 10 Fällen das berechtigte Interesse zu überprüfen, entspricht zwar den Vereinbarungen zwischen Aufsichtsbehörden und Schufa-Gesellschaften; die Zahl von 120 Rückfragen jährlich für alle Geschäftsstellen einer Schufa-Gesellschaft steht jedoch in einem krassen Mißverhältnis zu den über 360.000 Auskünften, die beispielsweise die SCHUFA GmbH Hamburg im Jahre 1983 erteilt hatte. M. E. muß eine wesentlich höhere Kontrolldichte erreicht werden.

4.4.3.2.5 Daten aus dem Schuldnerverzeichnis

Nach den Bestimmungen des § 915 ZPO und den aufgrund dieser Bestimmungen erlassenen Allgemeinen Vorschriften des Bundesministers der Justiz vom 1.8.1955 (Bundesanzeiger Nr. 156 vom 16.8.1955) müssen Haftanordnungen und Eidesstattliche Versicherungen im Einzelfall gelöscht werden, wenn das Vollstreckungsgericht dies angeordnet hat. Im übrigen sind derartige Eintragungen spätestens nach drei Jahren, gerechnet vom Schluß des Jahres der Eintragung an, zu löschen.
Die TA der Schufa sieht eine Löschung aller von ihr gespeicherten Angaben nicht erst – wie § 35 Abs. 2 BDSG es verlangt – nach Ablauf von fünf, sondern bereits nach drei vollen Kalenderjahren vor; diese Löschung erfolgt programmgesteuert. Wird eine Löschung im Schuldnerregister vorgenommen, so wird diese bei der Schufa nachvollzogen, sobald die monatlich erscheinenden „Vertraulichen Mitteilungen" diese Löschung melden. Eine vorzeitige Löschung auf Antrag des Betroffenen ist möglich, wenn er seine schriftliche Bestätigung des Amtsgerichts – Abt. Schuldnerregister – vorlegt.
Die verfahrensmäßigen Risiken, die dadurch entstehen, daß das Geburtsdatum vom Amtsgericht nicht in allen Fällen gemeldet wird, gleicht die Schufa dadurch aus, daß sie auf Zweifel an der Identität und die Rückmeldepflichten der Vertragspartner hinweist.
Zur Gewährleistung eines korrekten Verfahrens haben sich die Aufsichtsbehörden der Länder mit den Schufa-Gesellschaften verständigt, daß

- das bloße Behaupten des Betroffenen, die Angaben seien im Schuldnerverzeichnis vorzeitig gelöscht worden, für eine Löschung nicht ausreicht,
- die betreffenden Daten unverzüglich zu löschen sind, wenn das Gericht eine Löschungsurkunde ausgestellt hat und diese vorgelegt wird,
- sofern der Betroffene eine Urkunde nicht vorlegen kann, seine Angaben jedoch glaubhaft erscheinen, die Schufa beim zuständigen Gericht anrufen soll.

4.4.3.2.6 Datensicherungsmaßnahmen

Die Datensicherungsmaßnahmen der Schufa Hamburg sind unter den Aspekten

- Zu- und Abgangskontrolle,
- Speicherkontrolle,
- Benutzer-, Zugriffs-, Übermittlungs- und Eingabekontrolle,
- Auftragskontrolle,
- Transportkontrolle,
- Organisationskontrolle

geprüft worden.

Die von der Schufa getroffenen Sicherungsmaßnahmen können auch in ihrer Summe nicht jedes Risiko ausschließen. Auch wenn also Restrisiken verbleiben, haben die Datensicherungsmaßnahmen der Schufa generell doch einen hohen Standard. Auf noch bestehende Schwachstellen habe ich die Schufa hingewiesen und konkrete Empfehlungen gegeben, wie diese beseitigt werden können.

4.4.3.3 Schufa-Klausel

Schon in meinem 2. TB habe ich auf die mit der Schufa-Klausel verbundenen datenschutzrechtlichen Probleme hingewiesen (vgl. Nr. 4.4.3.3, S. 126 ff).
Das Hanseatische Oberlandesgericht bestätigte am 23.11.1983 die Entscheidung des Landgerichts Hamburg vom 27.8.1982, wonach die Schufa-Klausel in dem Kreditantrag einer Teilzahlungsbank nicht nur eine bloße Unterrichtung des Kunden über die Datenverarbeitung der Schufa darstelle, sondern daß das Kreditinstitut in Wahrheit eine formularmäßige Einwilligung des Kunden nach § 3 BDSG erwirken wolle. Damit bestätigte das Gericht zugleich die Auffassung, die die Aufsichtsbehörden der Länder schon 1979 in Gesprächen mit der Kreditwirtschaft zur Gestaltung der Schufa-Klausel geäußert hatten. Die Spitzenverbände der Kreditwirtschaft waren hingegen der Meinung, daß sowohl die Anfragen an die Schufa, die Antworten, weitere Meldungen an die Schufa, das dortige Speichern und die anschließenden möglichen Datenübermittlungen an andere Anschlußfirmen ohne die Einwilligung des Betroffenen zulässig seien. Die Übermittlungen von der Schufa an anfragende Firmen seien immer durch bestehende Vertragsverhältnisse gedeckt. Auch die weiteren Datenübermittlungen seien nach § 24 oder § 32 Abs. 2 BDSG zulässig, weil ein berechtigtes Interesse des Empfängers vorliege, dem schutzwürdige Belange des Betroffenen nicht entgegenstünden.
Dieser Meinung widersprachen die Aufsichtsbehörden mit der Begründung, daß in einzelnen Fällen sehr wohl schutzwürdige Belange beeinträchtigt sein könnten, und dies müsse in jedem Einzelfall gesondert geprüft werden. Eine Einzelfallprüfung sei aber bei einem Massengeschäft wie dem Schufa-Auskunftsverfahren praktisch nicht möglich; im übrigen ließen die Verträge der Schufa Differenzierungen auch nicht zu, weil die Anschlußfirmen generell zur Meldung verpflichtet seien. Um sicher zu gehen, daß das Speichern bei der Schufa und die vielen nachfolgenden Datenübermittlungen in allen Fällen zulässig seien, müsse die Einwilligung des Betroffenen in diese Datenverarbeitung eingeholt werden.
Der schließlich als Kompromiß akzeptierte Text der Schufa-Klausel ließ diese Meinungsverschiedenheiten offen. Die Kreditwirtschaft ging auch weiterhin davon aus, daß die Klausel nur die Bedeutung einer qualifizierten Benachrichtigung habe, während die Aufsichtsbehörden meinten, sie erfasse von ihrem objektiven Erklärungswert her die Absicht, die Zustimmung des Kunden zu erreichen. Deshalb sei sie als Einwilligungsklausel zu werten.
Nach den allgemeinen Grundsätzen zur Einwilligung sei für ihre Wirksamkeit jedoch Voraussetzung, daß der Betroffene die der Einwilligung zugrundeliegenden relevanten Umstände kenne. Der Erklärungsempfänger habe also eine entsprechende Pflicht zur Aufklärung.
Wenn jetzt alle Beteiligten aufgrund der Rechtsprechung der beiden hamburgischen Gerichte davon ausgehen müssen, daß eine ausdrückliche Einwilligungserklärung notwendig ist, bedarf es einer Umgestaltung der Schufa-Klausel.
Die Aufsichtsbehörden erwarten, daß der Betroffene detailliert über das gesamte Schufa-Auskunftssystem aufgeklärt wird. Er muß wissen, welche Daten seine Bank zu welchem Zweck an die Schufa übermittelt und welche Daten die Schufa unter welchen Voraussetzungen zu welchen Zwecken an welche Anschlußfirmen – auch außerhalb der Kreditwirtschaft – weitergibt.
Eines ist jedoch zu berücksichtigen: Auch der BGH hat sich bereits in verschiedenen Entscheidungen mit den Meldungen an die Schufa befaßt und z. B. in seinem Urteil vom 7.7.1983 (Az.: III ZR 159/82) ausgeführt, daß die übermittelnde Stelle (das Kreditinstitut) in jedem Einzelfall nach dem Verhältnismäßigkeitsgrundsatz eine Abwägung zwischen ihren berechtigten Interessen bzw. denen der Schufa oder der Allgemeinheit auf der ei-

nen Seite und den schutzwürdigen Belangen des Betroffenen auf der anderen Seite vorzunehmen habe, bevor sie die Daten übermittele. Dieses Abwägungsgebot schließe es indes nicht aus, daß in bestimmten Fällen eine Datenübermittlung regelmäßig zulässig sein werde, weil den für eine Datenübermittlung sprechenden berechtigten Interessen ein solches Gewicht zukomme, daß die Belange des Betroffenen zurücktreten müßten. So würden 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. In anderen Fällen werde im Einzelfall sorgfältig zu prüfen sein, welches Gewicht den berechtigten Interessen an der Datenübermittlung zukomme, inwieweit die Übermittlung schutzwürdige Belange des Betroffenen berühre und welcher Wert diesen Belangen zukomme.
Auch nach der BGH-Rechtsprechung muß also eine Abwägung vorgenommen und hierbei den schutzwürdigen Belangen des Betroffenen der Vorzug gegeben werden, wenn die der Schufa zu meldenden Daten eine gewisse Relevanzschwelle nicht überschreiten. Die pauschale Übermittlung z. B. einer Bank über die Aufnahme und Abwicklung eines Kredits ist also nur zulässig, wenn die Einwilligung des Betroffenen vorliegt. Nach dem BGH gilt dies nicht für die bloße Weitergabe von eindeutig negativen Merkmalen. Doch muß m. E. wenigstens die Übermittlung der folgenden „weichen" Schufa-Merkmale auf jeden Fall von der Einwilligung abhängig gemacht werden:

KL – Klage erhoben
LM – letzte außergerichtliche Mahnung
MB – beantragter Mahnbescheid.

Zur Aussagekraft von Negativmerkmalen habe ich mich im vorigen TB (vgl. Nr. 4.4.3.3) geäußert. Die dort zitierte Entscheidung vom OLG Hamm ist vom BGH nicht bestätigt worden (Urteil vom 15.12.83, NJW 1984, S. 1889).
Wie unter Nr. 4.4.3.2.1 bereits geschildert, kann man die Anschlußfirmen der Schufa in drei Gruppen einteilen.
Die A-Vertragspartner müssen die von den Gerichten beanstandete Schufa-Klausel in der oben beschriebenen Weise ändern (und ein Merkblatt für ihre Kunden bereithalten).
Mit der Kreditwirtschaft besteht Übereinstimmung, daß zunächst aber das Ergebnis des beim BGH schwebenden Revisionsverfahrens gegen die Entscheidung des Hanseatischen Oberlandesgerichtes abgewartet werden soll, bevor eine endgültige Fassung der Schufa-Klausel und der Umfang zusätzlicher Informationen vereinbart werden.
Die B-Vertragspartner verwenden bislang keine Schufa-Klausel. Sie nehmen nur eingeschränkt am Schufa-Verkehr teil und erhalten auf ihre Anfrage nur eine Identitätsbestätigung und etwa vorhandene Negativmerkmale. Andererseits melden sie auch nur vertragswidriges Verhalten und/oder Gesetzesverstöße. Dazu nutzen sie allerdings das volle Spektrum der von der Schufa durch ihre Merkmale vorgegebenen Möglichkeiten, melden also auch die oben erwähnten „weichen" Merkmale. Die Schufa und ihre B-Vertragspartner sind davon ausgegangen, daß diese Informationsflüsse entweder in einer Beziehung zu einem Vertragszwecke stehen oder aber schutzwürdige Belange der Betroffenen nicht beeinträchtigen. M. E. muß diese Praxis geändert werden. Wenn die B-Vertragspartner weiterhin eine Einwilligung nicht einholen, können sie zwar die „weichen" Negativ-Merkmale empfangen, die auf der Basis einer Einwilligung ins Schufa-Auskunftssystem gelangt sind, dürfen aber selbst solche Daten nicht an die Schufa übermitteln.
Aus der Gruppe der sonstigen Vertragspartner habe ich im 2. TB (vgl. Nr. 4.5.2.1)die vertraglichen Beziehungen mit den Wohnungsvermietern als Beispiel beschrieben und ausgeführt, daß ein Schufa-Anschluß überhaupt nicht gerechtfertigt sei. Zu dieser Gruppe zählen weiter Hotels, Kfz-Vermieter, Kreditvermittler und Immobilien-Makler. Sie alle können nicht von sich behaupten, daß sie Kredite gewähren.
Das Einspeisen in die Schufa-Dateien und die umfangreichen Nutzungsmöglichkeiten gehen weit über das hinaus, was diese Stellen überschauen können. Sie sind faktisch nicht in der Lage zu prüfen, ob im Einzelfall nicht doch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Aus diesem Grund ist § 24 BDSG keine ausreichende Rechsgrundlage für eine Weitergabe an die Schufa.

Mithin dürfen diese Anschlußfirmen Schufa-Auskünfte nur erhalten, wenn sie eine gesonderte Einwilligung ihres Kunden zur Datenabfrage bei der Schufa und zur Einmeldung von Negativ-Merkmalen bekommen haben. Unter dieser Bedingung dürften sie dieselben eingeschränkten Auskünfte (nur Negativ-Daten) wie B-Vertragspartner erhalten. Selbstverständlich sind für die Wirksamkeit der Einwilligung genauere Informationen nötig. Diese Unternehmen müssen ihren Kunden ihre besondere Interessenlage genau beschreiben. Wer in diesen Branchen als Kunde einen Vertrag schließt, wird in aller Regel nicht wissen, daß der Schufa Informationen gegeben werden und welche davon durch die Schufa an wen weitergeleitet werden.

4.5 Markt- und Meinungsforschung

4.5.1 Sachlage

Marktforschung ist eine freie, zweckgerichtete Tätigkeit, die mit angemessenen, wissenschaftlich gesicherten und überprüfbaren Methoden und Verfahrensweisen durchgeführt wird mit dem Ziel, Informationen über Märkte und Bevölkerungsgruppen, d.h. über wirtschaftliche, soziale und sozialpsychologische Tatbestände, Zusammenhänge und Entwicklungen zu gewinnen. Sie bedient sich dabei zweckentsprechender Verfahren der Primär- und Sekundär-Analyse. Unter den Erhebungsmethoden sind vor allem die strukturierten mündlichen Befragungen (= Interviews) und Repräsentativ-Erhebungen, daneben auch die Methoden der Beobachtung sowie des Experiments/Tests zu nennen.
In der Regel werden also für den Auftraggeber personenbezogene Daten von Angehörigen bestimmter Zielgruppen erhoben, gespeichert und anschließend anonymisiert übermittelt. Zu diesem Zweck sind in Hamburg eine ganze Reihe von Instituten der Markt-, Meinungs- und Sozialforschung (MSI) tätig, von denen sich 30 als Stellen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiten, bei mir zum Register (§ 39 BDSG) gemeldet haben.
Bei der Verarbeitung personenbezogener Daten zu den o.b. Zwecken sind die Bestimmungen des BDSG zu beachten. Hinsichtlich der Frage, ob die Verarbeitung personenbezogener Daten nur mit schriftlicher Einwilligung des Betroffenen zulässig ist (§ 3 BDSG), sind die obersten Aufsichtsbehörden für den Datenschutz – je nachdem, um welche Fallgruppe es sich bei der Befragung handelt – zu folgenden Ergebnissen gelangt, die mit den Verbänden der Markt- und Sozialforschungsinstitute abgestimmt worden sind:
Einmal-Befragungen (Interviews)
In diese Gruppe fallen Befragungen, bei denen der Betroffene – möglicherweise auch mehrmals – befragt wird (z.B. Produktbefragungen), das Ergebnis der Befragung vom Interviewer jedoch erst nach Abschluß aller Phasen der Befragung an das MSI weitergegeben wird.
Für den manuellen Teil der nun folgenden Datenverarbeitung gilt folgendes:
Unmittelbar nach Eingang der Fragebogen im MSI müssen Adreßteil und Fragenteil des Fragebogens voneinander getrennt und separat aufbewahrt werden. Eine Zusammenführung von Adreß- und Fragenteil erfolgt nur zum Zweck der Interviewer-Kontrolle. Nach Abschluß dieser Kontrollen, spätestens bei Beginn der automatisierten Verarbeitung der Fragenteile, d.h. der Erfassung der Daten, sind die Adreßteile zu vernichten. Dem steht es gleich, wenn die Möglichkeit, beide Teile aufeinander zu beziehen, beseitigt wird. Die Adreßteile sollen so bald als möglich vernichtet werden. Ein genauer Zeitraum kann allerdings nicht bestimmt werden, da die einzelnen Befragungen unterschiedlich ablaufen.
Unter diesen Voraussetzungen kann davon ausgegangen werden, daß der Betroffene mit Hilfe der zum Fragenteil gehörenden Daten nicht mehr bestimmt werden kann und daß es sich insoweit nicht mehr um personenbezogene Daten i.S. des § 2 Abs. 1 BDSG handelt. Ferner kann davon ausgegangen werden, daß die Daten – solange sie manuell verarbeitet werden – in einer internen Datei i.S. des § 1 Abs. 2 Satz 2 BDSG gespeichert sind. Solange die Daten nicht automatisiert verarbeitet werden, ist somit für die Datenverarbeitung eine Einwilligung i.S. des § 3 BDSG nicht erforderlich. Es gelten aber die Vorschriften über die Datensicherung nach § 6 BDSG.

Wiederholungs-Befragungen (Paneluntersuchungen)
In diesen Fällen werden Adreßteil und Fragenteil getrennt voneinander in automatisierten Verfahren gespeichert; zum Zwecke des Vergleichs der Befragungsergebnisse oder einer erneuten Befragung kann zwischen Fragen- und Adreßteil jedoch immer der Bezug hergestellt werden. Für Mehrfachbefragungen gilt:
Werden die vertraglichen Vereinbarungen über eine regelmäßige Befragung zwischen dem MSI und dem Betroffenen schriftlich geschlossen, ist auch eine ausdrückliche schriftliche Einwilligung nach § 3 Satz 1 Nr. 2 BDSG erforderlich. Das gleiche gilt, wenn der Betroffene auf Fragebogen selbst seinen Namen einsetzt oder den Fragebogen unterschreibt.
In allen anderen Fällen gehen die Aufsichtsbehörden davon aus, daß auch bei Mehrfachbefragungen besondere Umstände i.S. des § 3 Satz 2 1. Halbsatz vorliegen, die die Schriftform der Einwilligung entbehrlich machen, wenn die folgenden Voraussetzungen erfüllt sind:
Der Betroffene wird bei Beginn der Befragung über die Freiwilligkeit seiner Angaben belehrt.
Spätestens am Ende der Befragung ist dem Betroffenen ein Merkblatt auszuhändigen. Dieses muß Umfang und Zweck der geplanten Verarbeitung deutlich machen. Die Freiwilligkeit der Angaben ist besonders hervorzuheben. Mit den Aufsichtsbehörden abgestimmte Mustermerkblätter sind bei den Berufsverbänden erhältlich. Nach Aushändigung des Merkblattes muß dem Betroffenen genügend Bedenkzeit verbleiben, damit er ggf. die Möglichkeit hat, die „Löschung" seiner Daten zu verlangen.
Werden dem Betroffenen Fragebogen vorgelegt, so müssen auch diese einen ausdrücklichen Hinweis auf die Freiwilligkeit der Angaben enthalten.

Zur Konkretisierung der aus § 36 Abs. 1 BDSG folgenden Verpflichtung zur Anonymisierung ist folgendes sicherzustellen:
Adreßteile und Fragenteile sind auch physisch voneinander getrennt aufzubewahren. Im automatisierten Verfahren sind die zur Verknüpfung benutzten Programme besonders zu sichern.
Der Datenschutzbeauftragte des MSI kontrolliert in besonderer Weise die Verknüpfung von Adreß- und Namensteilen.
Für die Auswertung der Angaben und die Verknüpfung der Adreß- und Namensteile soll nicht der gleiche Mitarbeiter verantwortlich sein.

4.5.2 Prüfungen

Ich habe im Berichtszeitraum 15 MSI überprüft. Die Prüfung erstreckte sich auf folgende Fragen: Erforderlichkeit des jeweils erhobenen Datensatzes, Form der Erhebung, Anonymisierung, Speicherung der Daten und Aufbewahrung der Unterlagen, Praxis der Datensicherung und der Interviewer-Kontrollen.

Ich habe dabei festgestellt, daß die Ergebnisse der Besprechungen zwischen Aufsichtsbehörden und den Verbänden der Markt- und Sozialforscher aus den Jahren 1979/1980 bei den Instituten nicht umgesetzt wurden, z.T. nicht einmal bekannt waren. Es bestand eine große Unsicherheit darüber, wie die Datenverarbeitung datenschutzgerecht zu gestalten ist, die ihre Ursache z.T. schon in unterschiedlichen Definitionen von Verarbeitungsvorgängen hat.

So mußte in den Prüfungsgesprächen zunächst klargestellt werden, daß das BDSG auf Markt- und Meinungsforschungsinstitute auch dann anwendbar ist, wenn nur Einmalbefragungen durchgeführt werden, da personenbezogene Daten für einen bestimmten Zeitraum gespeichert werden. Regelmäßiger Diskussionspunkt war auch die unterschiedliche Auslegung des Begriffs „anonymisieren". Es war klarzustellen, daß unter datenschutzrechtlichen Gesichtspunkten erst dann von anonymisierten Daten ausgegangen werden kann, wenn ein erneutes Zusammenführen von Adressen und entsprechenden Fragebogen theoretisch und praktisch unmöglich ist.

In aller Regel mußten die Markt- und Meinungsforschungsinstitute auch darauf hingewiesen werden, daß es nicht zulässig ist, „alte" Adressenlisten ohne Wissen der Betroffenen für die Durchführung einer neuen Studie erneut an die Interviewer auszugeben.
Zu bemängeln ist nicht nur, daß die inhaltlichen Fragen, die mit den Verbänden der Markt- und Sozialforschungsinstitute in den Jahren 1979 und 1980 besprochen worden waren, von den hamburgischen Instituten nicht umgesetzt worden sind. Die meisten von ihnen sind nicht einmal der Pflicht nachgekommen, sich zu dem bei mir geführten Register zu melden. In einigen Fällen geschah dies nicht einmal, nachdem der Bundesverband Deutscher Marktforscher e.V. (BVM-Nord) in einem Rundschreiben auf diese Verpflichtung hingewiesen hatte. Einige Institute haben sich erst nach zweimaliger Aufforderung ihrer Pflichten besonnen; in diesen Fällen wurden Bußgeldverfahren eingeleitet, die noch nicht abgeschlossen sind.

–

4.6 Datenschutz bei Verkehrsbetrieben

4.6.1 „Schwarzfahrer-Datei" der HHA

Die HHA hat das im 2. TB (vgl. Nr. 4.6.1) beschriebene Verfahren zur Durchsetzung des von „Schwarzfahrern" zu entrichtenden erhöhten Beförderungsentgelts inzwischen automatisiert. Die gesamte Abrechnung und das Mahnverfahren erfolgen ab 1.1.1984 mit Unterstützung einer Datenbank-Organisation. Im Zuge der Neugestaltung haben sich einige datenschutzrechtlich relevante Änderungen ergeben:

- Datenerhebung: Bei der neuen FP-Meldung (Feststellung durch den Fahrkartenprüfer) ist auf die Erhebung des Berufes, des Geburtsstaates und der besonderen Kennzeichen verzichtet, an der Erhebung der Personalausweis-Nr. jedoch festgehalten worden. Ich begrüße, daß der Umfang der zu erhebenden Daten reduziert wurde. Allerdings muß ich feststellen, daß die HHA meiner Empfehlung, von der Serien-Nr. des Personalausweises lediglich den Buchstaben und die letzten 4 Ziffern zu erheben und zu speichern, nicht gefolgt ist.
- Datenspeicherung: In automatisierten Tageslisten werden Name, Vorname, Anschrift, Beanstandungsort und Datum des Vorfalls gespeichert. Im on-line-Verfahren kann die Abteilung Verkehrsrechnung die entsprechenden personenbezogenen Daten abrufen.
- Aufbewahrungsdauer: An der Speicherungshöchstdauer von 2 Jahren hat sich nichts geändert. Zwölf Monate lang können die zuständigen Sachbearbeiter aktuell über Bildschirm auf die Datenbank zugreifen. Anschließend werden die Daten monatsweise mikroverfilmt und ein weiteres Jahr archiviert. Diese Daten dürfen nur noch unter den strengen Voraussetzungen für die Aufhebung einer Sperre (§ 27 Abs. 2 i. V. m. § 14 Abs. 2 BDSG) verwendet werden (z. B. zur Behebung einer bestehenden Beweisnot).
  Personenbezogene Daten sog. „Graufahrer" (also Personen, die ihre Monatskarte vergessen haben oder mit einer Zeitkarte bzw. einem Einzelfahrschein zu weit gefahren sind,) werden 3 Monate nach dem Vorfall gelöscht, wenn das Beförderungsentgelt gezahl wurde.
- Datenübermittlungen: Regelmäßige Datenübermittlungen an Dritte, insbesondere an die Polizei, sind weder geplant noch programmäßig vorgesehen.
- Mehrfachtäter-Suchprogramm: Einmal monatlich erfolgt ein Suchlauf für Schwarzfahrer-Mehrfachtäter. Die Daten solcher Personen, die innerhalb eines Jahres (gerechnet vom 1. Vorfall an) dreimal als „Schwarzfahrer" festgestellt worden sind, werden ausgedruckt. Die entsprechenden Unterlagen werden dann – wie bisher – an die Rechtsabteilung abgegeben, die die Forderung beitreibt und in gravierenden Fällen Strafantrag stellt.
  Die Automatisierung der Abrechnung und des Mahnverfahrens führt zu keinem anderen Ergebnis im Hinblick auf die grundsätzliche Zulässigkeit der Verarbeitung personenbezogener Daten von „Schwarzfahrern", so daß ich auf meine im 2. TB (vgl. Nr. 4.6.1) dargelegte Rechtsauffassung verweise.

4.7 Arbeitnehmerdatenschutz

4.7.1 Gefährdungspotential neuer Entwicklungen

Zahlreiche Anfragen im Bereich Arbeitnehmerdatenschutz bezogen sich wieder auf die mit der Einführung und Anwendung von Personalinformationssystemen (PIS) verbundenen datenschutzrechtlichen Probleme (vgl. 2. TB Nr. 4.8.4.) Ein immer stärker werdendens Interesse richtet sich auf sog. Betriebsdatenerfassungssysteme (BDE), bei denen personenbezogene bzw. auf Personen beziehbare Daten – z. T. als „Nebenprodukt" der eigentlichen Anwendung – anfallen, sowie den Einsatz von Personalcomputern (PC).

4.7.1.1 Gefährdungspotential von BDE-Systemen

Durch den planvollen Einsatz von BDE hat der Arbeitgeber die Möglichkeit, das gesamte Betriebsgeschehen, den Produktionsfluß und den Personaleinsatz zu gestalten, aber auch zu kontrollieren. Dabei fallen je nach System in unterschiedlichem Umfang Personal-, Auftrags-, Material- und Maschinendaten an. Ich habe nicht vor, alle Aspekte der betrieblichen Erfassung von Personaldaten flächendeckend abzuhandeln (z. B. auch Personalkredite, Zeitkontenführung, Gleitzeiterfassung). Über Datenschutzprobleme bei der Telefondatenerfassung berichte ich in anderem Zusammenhang (Nr. 4.7.5 dieses TB). An dieser Stelle sollen die über den Arbeits- bzw. Produktionsprozeß erhobenen Betriebsdaten, wie z. B. Beginn, Ende und Unterbrechung eines Arbeitsgangs, Art des Auftrags, Unterauftrags oder Arbeitsganges, belegte Maschine, Stillstand und Grund der Störung etc., betrachtet werden. Es ist zu unterscheiden zwischen

- Maschinenbelegungssystemen und
- Fertigungssteuerungs- und Auftragsverfolgungssystemen, die jeweils um ein automatisiertes Verfahren der Entgeltdatengewinnung und darüber hinausgehend um Dispositionsfunktionen ergänzt werden können.

Die primäre Aufgabe eines Maschinenbelegungssystems besteht darin, einen Wochen- oder Monatsplan für die Maschinen-/Anlagenbelegung unter Berücksichtigung vorgegebener Prioritäten zu erstellen. Ziel ist die optimale Maschinen-/Anlagenbelegung, also die Vermeidung von Stillständen wegen falscher Zeit- und Mengendisposition, die Beschleunigung des Durchlaufs der Aufträge.
Wenn derartige Maschinenbelegungssysteme um eine Terminverfolgung ergänzt werden, so entstehen Fertigungssteuerungs- und Auftragsverfolgungssysteme, bei denen die „Soll"-Daten der Auftragsverteilung auf die Maschinen und Anlagen mit den „Ist"-Daten des tatsächlichen Ablaufs der Arbeiten verglichen werden. Um diese Aufgabe bewältigen zu können, braucht das System Rückmeldungen aus der Produktion, die Informationen über den Auftragsfortschritt liefern. Die weitestgehende Form dieser Fertigungssteuerungs- und Auftragsverfolgungssysteme ist die lückenlose, zeitgenaue Erfassung aller Arbeitsgänge mit Beginn- und Ende-Zeitangaben der Bearbeitung, wobei dem System nach jedem Arbeitsgang die Fertigstellung mitgeteilt werden muß (automatische Beleglesung oder Eingabe in ein Bildschirmterminal). Praktisch bedeutet das, daß alle Bearbeitungszeiten im System lückenlos gespeichert werden.
Eine weitere Ausbaustufe liegt in der technischen Möglichkeit, BDE-Systeme um eine integrierte Entgeltdatengewinnung zu ergänzen. Hierbei werden gleichzeitig mit der Rückmeldung fertiggestellter Arbeitsschritte die Daten für die Entgeltabrechnung erhoben. Vor allem bei Akkord- oder Prämienlohn können mit Hilfe solcher integrierter Systeme die einmal erfaßten Daten sowohl für die Fertigungssteuerung bzw. Auftragsverfolgung als auch für die Lohnabrechnung verarbeitet werden. Bei der gemeinsamen Erfassung von Lohn- und Fertigungsdaten kennt das System Arbeits- und Personalnummer und ist somit in der Lage, die Arbeitsgangdaten, d. h. Art der Arbeit, Vorgabezeit, tatsächliche Bearbeitungszeiten, evtl. Stör-, Ausfall-, Warte- oder Wegezeiten den Personen, die die Arbeit durchgeführt haben, zuzuordnen; alle diese Daten werden damit zu personenbezogenen Daten i. S. des § 2 Abs. 1 BDSG. Von seiner Datenbasis her betrachtet, bietet das System die Möglichkeit, personenbezogene Leistungsvergleiche (reale Zeiten für denselben Arbeitsgang) anzustellen und Vorgabezeiten nach der Höhe des auf den Arbeitsgang bezogenen Leistungsgrad zu sortieren.

Eine weitere Verfeinerung der dargestellten BDE-Systeme stellen Systeme mit Dispositionsfunktionen dar, die sich nicht auf die Steuerung des Fertigungsablaufs beschränken. So kann außer dem Ablauf der Produktion beispielsweise der Einsatz von Technikern überwacht und gesteuert werden, wenn ein elektronisches Tagebuch mit der Aufzählung der eingesetzten Geräte bei den Kunden, die von den Technikern besucht werden, über den Personalnummern-Schlüssel mit den alle die Einzelarbeiten betreffenden personenbezogenen Daten gekoppelt wird. Die vorhandene Datenbasis würde Auswertungen erlauben über die Zahl der Kundenbesuche pro Techniker, Menge und Art der eingesetzten Ersatzteile pro Techniker etc.
Das BAG hat sich in seiner Entscheidung vom 14.9.1984 zu einigen in diesem Zusammenhang auftretenden Fragen geäußert und entschieden, daß diese Art von BDE-Systemen nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung des BR unterliegt (näheres siehe unter Nr. 4.7.2).
Eine weitere Einsatzmöglichkeit eines solchen Systems mit Dispositionsfunktionen läßt sich anhand des folgenden Beispiels illustrieren: Mit EDV-Unterstützung werden Hafenarbeiter in sog. Gänge zum Laden oder Löschen der Schiffe eingeteilt; gleichzeitig werden die dabei erworbenen Entlohnungsansprüche aufgrund der ausgeführten Tätigkeiten und des Schichteinsatzes festgestellt.
Allen dargestellten BDE-Systemen ist gemeinsam, daß es sich um im Produktionsprozeß anfallende Angaben handelt, die über die Personal-Nummer des Arbeitnehmers zu personenbezogenen Daten werden. Hierüber kann der Arbeitnehmer nach § 26 Abs. 2 BDSG Auskunft verlangen. Dieses Recht reicht allerdings insofern nicht aus, als ihm nach geltendem Recht Auskünfte über einzelne Verfahren der Auswertung nicht mitzuteilen sind. Um dem einzelnen Arbeitnehmer die Chance zu geben, die Verarbeitung seiner Daten genau zu verfolgen, sollte sein Auskunftsanspruch über § 26 Abs. 2 BDSG hinaus ausgedehnt werden auf alle Auswertungsprogramme bzw. Einzelauswertungen, in die seine Daten einbezogen sind.
§ 23 BDSG setzt für die Speicherung solcher Daten gewisse rechtliche Schranken. Über die Zweckbestimmung des Arbeitsverhältnisses hinaus kann die Speicherung allerdings relativ leicht mit der 3. Alternative des § 23 BDSG begründet werden.
Aber auch wenn die Speicherung von Arbeitnehmerdaten auf den Zweck des Arbeitsverhältnisses begrenzt und auch die betriebsinterne Verwendung künftig im BDSG geregelt würde, ist eine Beeinträchtigung schutzwürdiger Belange des Arbeitnehmers durch Einzelauswertungen nicht auszuschließen. Zumindest müssen Auswertungen und Verknüpfungen, wenn sie zur Herstellung eines „Persönlichkeitsbildes" der Arbeitnehmer führen, sowie die Speicherung solcher „Profile" verboten werden. Entscheidend ist, daß – ganz unabhängig von der künftigen Ausgestaltung der Rechtsstellung des einzelnen Arbeitnehmers – die BR – rechtlich und tatsächlich – in die Lage versetzt werden, durch Betriebsvereinbarungen sicherzustellen, daß personenbezogene Einzelauswertungen und Verknüpfungen, soweit sie sich überhaupt mit einem überwiegenden Interesse des Unternehmens rechtfertigen lassen, in geringstmöglichem Maß in die Persönlichkeitssphäre des Arbeitnehmers eingreifen.

4.7.1.2 Individuelle Datenverarbeitung – Gefährdungspotential einer neuen Entwicklung am Beispiel des Einsatzes von Arbeitsplatzcomputern

Die Dezentralisierung der Datenverarbeitung hat durch relativ preiswerte hardware erheblich zugenommen. Auch für die Personaldatenverarbeitung werden zunehmend Arbeitsplatzrechner und PC eingesetzt.
Wenn man sich vor Augen hält, daß Mitte der 70er Jahre, als das BDSG konzipiert wurde, viele kleinere und mittlere Rechenzentren mit derselben Kapazität auskommen mußten, die ein heutiger Hochleistungs-PC auf die Tischplatte bringen kann, so wird deutlich, welche eindrucksvollen Speicherungs- und Anwendungsmöglichkeiten diese Geräte – insbesondere bei der Personalverwaltung – bieten können.
So können PC z. B. abteilungsintern Anwendung finden, ohne daß Speicher- oder Rechenkapazitäten im Rechner des Gesamtunternehmens blockiert werden. Abteilungsleiter mit DV-Kenntnissen haben sogar die Möglichkeit, die bestehenden Personalverwaltungsprogramme um weitere eigene Auswertungen zu ergänzen, ohne daß in allen

Fällen der bDSB informiert wird. Nach den Beobachtungen vieler bDSB versäumen es die Mitarbeiter von Fachabteilungen häufig, solche Aktivitäten anzuzeigen, obwohl sie unzweifelhaft unter das BDSG fallen.
Mir ist ein Fall bekannt geworden, in dem ein Abteilungsleiter im Büro vorbereitete Disketten mit nach Hause genommen hat, wo er auf seinem privaten PC spezielle Auswertungen gemacht hat, die er dann dienstlich verwertet hat.
Die neue Sachlage ist dadurch gekennzeichnet, daß Datenverarbeitung auf der Basis autonomer Systeme weit schlechter kontrollierbar ist als in einer zentralen Groß-EDV-Anlage und daß es technisch möglich ist, die isolierten Verfahren – wenn auch heute noch in einem engen technischen Rahmen – ohne Beteiligung der DV-Abteilung miteinander zu verknüpfen.
Die konsequente Dezentralisierung, die zunehmende Verbreitung von Arbeitsplatzrechnern und PC sowie die fortschreitende Entwicklung von Multifunktionsterminals, die sämtliche Kommunikationsgeräte zusammenfassen, sind untrügliche Anzeichen dafür, daß sich innerhalb kürzester Zeit die Bedingungen für den ADV-Einsatz grundlegend geändert haben. Dadurch sind neue datenschutz- und arbeitsschutzrechtliche Probleme entstanden. So kann eine dezentralisierte Datenverarbeitung in Einzelfällen nicht nur zu einem Kontrollvollzugsdefizit führen, sondern auch die Umgehung von Betriebsvereinbarungen erleichtern, die präzise Daten- und Programmkataloge sowie die dazugehörigen Einzelheiten des Verfahren enthalten. Bei diesem Sachverhalt stellt sich darüber hinaus die Frage, wie der im allgemeinen mit mangelhaften EDV-Kenntnissen ausgestattete unmittelbar Betroffene die tatsächliche Einhaltung solcher Vereinbarungen bzw. deren Überschreitung soll kontrollieren können, wenn schon der bDSB mangels praktischer Möglichkeiten und die Aufsichtsbehörde mangels Betroffenenbeschwerde dies nicht vermögen.
Bisherige Erfahrungen mit dezentralem Einsatz von PC zeigen, daß es für dieses Problem und die in diesem Zusammenhang zu fordernde lückenlose Kontrolle z. Z. noch keine zufriedenstellenden Lösungen gibt, insbesondere wenn man bedenkt, daß sich z. T. auch unter Verwendung von Programmhilfen, die von den DV-Herstellern geliefert werden, einfache Auswertungsprogramme ohne Schwierigkeit dezentral entwickeln, unverzüglich ausführen und ebenso schnell löschen lassen.
Sowohl die Mitwirkung bei der Gestaltung (Betriebsvereinbarungen) als auch die nachträgliche Information darüber, was an Programmen vorgelegen hat, erweisen sich als überaus fragwürdig. Nur eine Verdichtung der internen Kontrolle durch bDSB und BR und ein intensiveres Zusammenwirken beider Institutionen sowie die Erweiterung der Befugnisse der Aufsichtsbehörde bieten eine reelle Chance, den negativen Auswirkungen der individuellen Datenverarbeitung entgegen zu wirken. Wegen weiterer Einzelheiten verweise ich auf Nr. 4.7.6 dieses TB.

4.7.2 Entwicklung der Rechtsprechung

4.7.2.1 Personal- und Betriebsdatenerfassungssysteme

Bereits in meinem 2. TB (vgl. Nr. 4.8.4) habe ich ausführlich über die Probleme berichtet, die sich bei der Auslegung des § 87 Abs. 1 Nr. 6 BetrVG stellen. Nach wie vor streiten Arbeitgeber und Betriebsräte in einer Fülle von Einigungsstellenverfahren und Prozessen mit wechselndem Ausgang über die Frage, ob Personalinformationssysteme „dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen". Nur dann nämlich besteht ein Mitbestimmungsrecht bei der Einführung und Anwendung.
Das BAG hatte bisher den Begriff der Überwachung in § 87 Abs. 1 Nr. 6 BetrVG nicht abschließend definiert. Es hat mit Urteilen vom 14.5.1974 (AP Nr. 1 zu § 87 BetrVG 1972) und vom 9.9.1975 (BAG 27, 256) von der „Auswertung" der durch die Überwachung gewonnenen Daten gesprochen, Überwachung also in der Ermittlung von Verhaltens- und Leistungsdaten gesehen, in einer Entscheidung vom 10.7.1979 (AP Nr. 3 zu § 87 BetrVG 1972) eine Überwachungseignung auch angenommen, wenn die Aufzeichnung und die Auswertung des Kontrollergebnisses zeitlich versetzt erfolgt. Damit hat es die Auswertung zur Überwachung gerechnet.

Mit seiner Entscheidung vom 6.12.1983 (1 ABR 43/81) hat das BAG bekräftigt, daß es bei der Entscheidung über die Frage, ob eine technische Einrichtung zur Überwachung bestimmt ist, entscheidend auf den technischen Vorgang der Erhebung ankomme. Die Frage, ob ein datenverarbeitendes System eine zur Überwachung von Leistung oder Verhalten der Arbeitnehmer bestimmte technische Einrichtung sein kann, wenn es Verhaltens- oder Leistungsdaten verarbeitet, die auf nicht-technischem Wege gewonnen und dem System lediglich zum Zwecke der Speicherung und Verarbeitung eingegeben werden, hat es auch in dem Urteil vom 6.12.1983 ausdrücklich offengelassen.
Eben mit dieser Frage hat sich das BAG in seiner neuen Entscheidung vom 14.9.1984 (1 ABR 23/82) auseinandersetzen müssen. Gegenstand des Rechtsstreits war folgender Sachverhalt:
Die beteiligte Firma verkauft und vermietet Kopierautomaten und unterhält dafür einen technischen Kundendienst. Die Kundendiensttechniker sollen nach den Plänen der Firma in einem sog. Technikerberichtssystem einen Beleg ausfüllen, in dessen 63 Belegtiteln produkt- und leistungsbezogene Angaben über die Ausführung des Auftrages gemacht werden sollen, wobei auch die Personalnummer des Kundendiensttechnikers einzutragen ist. Solche personenbezogenen Daten sind etwa die Dauer der Reisezeit für jeden Kundenbesuch, die Arbeitszeit beim Kunden selbst, die sog. Logistikzeit, das ist die Zeit für die Beschaffung eines Ersatzteiles, die Art der durchgeführten Arbeitsaufgabe u. ä. Die Angaben werden anschließend in einer EDV-Anlage ausgewertet. Dabei werden in gewissem Umfang auch Daten aus anderen Systemen verwendet bzw. durch das Technikerberichtssystem gewonnene oder aufbereitete Daten in anderen Systemen – etwa der Kundenabrechnung – verwendet.
In Fortentwicklung seiner bisherigen Rechtssprechung geht das BAG nunmehr davon aus, daß eine Überwachung von Arbeitnehmern nicht nur durch die Erhebung von verhaltens- und leistungsbezogenen Daten geschieht, sondern auch dann, wenn die auf nicht-technischem Wege gewonnenen Daten zu Aussagen über das Verhalten oder die Leistung von Arbeitnehmern ausgewertet werden. Bedient sich der Arbeitgeber hierzu einer technischen Einrichtung, so löse dies ein Mitbestimmungsrecht des BR aus. Der Gesetzgeber habe ersichtlich in der technischen Überwachung von Arbeitnehmern eine größere Gefährdung für das Persönlichkeitsrecht der Arbeitnehmer gesehen als bei einer Überwachung mit herkömmlichen Mitteln. Auch die technische Verarbeitung von Verhaltens- und Leistungsdaten führe zu einer solchen Gefährdung. Sie sei vergleichbar den Gefahren, die bei der technischen Erhebung von Verhaltens- und Leistungsdaten entstehen, wie sie das Gericht in seiner Bildschirm-Entscheidung beschrieben habe. Dieser Gefährdung zu begegnen, sei Sinn des Mitbestimmungsrechts des BR. Dieses versetze ihn in die Lage mitzuentscheiden, ob und ggf. welche Verhaltens- und Leistungsdaten erhoben und zu welchen Zwecken sie verwendet werden sollen.
Mit Entscheidung vom 14.9.1984 hat das BAG klargestellt, daß Überwachung sowohl das Sammeln von Informationen als auch das Auswerten bereits vorhandener Informationen sein kann.
Diese Entscheidung hat in einigen für die Praxis relevanten Punkten für Klarstellungen gesorgt; es bleiben allerdings doch einige Fragen offen, und sie wirft neue Fragen auf. So stellt das BAG darauf ab, ob „Leistungs- und Verhaltensdaten" verarbeitet werden, obwohl das BetrVG diese Begriffe nicht verwendet. Die Abgrenzung von Daten, die Leistungs- und Verhaltensdaten sind und solchen, die es nicht sind, ist m. E. kaum zu leisten. Denn ein abschließender Positiv-Katalog von Leistungs- und Verhaltensdaten kann – insbesondere wegen der Möglichkeit ihrer multifunktionalen Verwendung – nicht erstellt werden. Z. B. ist die Tatsache, daß ein Arbeitnehmer an einem Wochentag nicht zur Arbeit erschienen ist, primär ein Abrechnungsdatum. Gleichzeitig ist es – z. B. durch Einzelauswertungen der Fehlzeitenstatistik – auch ein Leistungs- und Verhaltensdatum. Es mag einige wenige, klar definierbare Leistungs- und Verhaltendaten geben, viele personenbezogenen Daten werden allerdings erst durch eine entsprechende Verwendung zu Leistungs- und Verhaltensdaten.
Auch das Bundesverfassungsgericht weist im Volkszählungsurteil darauf hin, daß es unter den Bedingungen der modernen Datenverarbeitung kein belangloses Datum gibt.
Es könne nicht allein auf die Art der Angaben abgestellt werden; entscheidend sei vielmehr ihre Nutzbarkeit und Verwendungsmöglichkeit.

Bereits in der schon genannten Entscheidung vom 6.12.1983 hatte das BAG ausgeführt, daß sich die Bestimmung einer technischen Einrichtung zur Erhebung von Verhaltens- und Leistungsdaten aus dem verwendeten Programm ergebe. Nur wenn nach dem verwendeten Programm Verhaltens- und Leistungsdaten erhoben und der menschlichen Wahrnehmung zugänglich gemacht würden, sei die technische Einrichtung zur Überwachung bestimmt. In seiner Entscheidung vom 14.9.1984 wendet das BAG die gleichen Grundsätze an und kommt zum Ergebnis, daß eine technische Einrichtung, die Verhaltens- und Leistungsdaten auswertet, jedenfalls auch zur Überwachung bestimmt sei, wenn diese Auswertung auf der Grundlage eines entsprechenden Programmes erfolge. In beiden Fällen stellt das BAG also auf die in einem System tatsächlich vorhandenen und verwendeten Programme ab. M. E. berücksichtigt das Gericht damit nicht hinreichend, daß alle auf dem Markt vorhandenen PIS und BDE, die zur Lohn- und Gehaltsabrechnung verwendet werden, durch Ergänzung zusätzlicher software zum Zwecke der Personalsteuerung und -planung wie auch zum Zweck der Leistungs- und Verhaltenskontrolle erweitert werden können. Der Arbeitgeber kann zunächst davon absehen, ein entsprechendes Programm einzusetzen. Die Erfahrung zeigt, daß in vielen Unternehmen die Möglichkeiten der vom Hersteller angebotenen Systeme sukzessiv ausgeschöpft werden. Wenn man aufgrund mangelnder „Unmittelbarkeit" z. B. die Anschaffung der EDV-Grundausstattung für Lohn- und Gehaltsabrechnung für mitbestimmungsfrei hält, so besteht die Gefahr, daß Mitbestimmungsrechte, die erst bei Folgeinvestitionen einsetzen, materiell entwertet sind, weil bei der Ergänzung von Einrichtungen zu solchen, die kurze Zeit später das Kriterium der unmittelbaren Eignung zur Leistungs- und Verhaltenkontrolle erfüllen, die „richtige" Entscheidung weitgehend von ökonomischen Sachzwängen diktiert sein könnte (vgl. 2. TB, Nr. 4.8.4.1).

Hieraus wird deutlich, daß auch die neuen Entscheidungen des BAG nicht geeignet sind, jeglichen Streit darüber, ob ein Verfahren, in dem Personaldaten verarbeitet werden, unmittelbar zur Überwachung des Verhaltens und der Leistung der Arbeitnehmer bestimmt ist. Das kann nur durch eine Änderung des BetrVG erreicht werden, die nur noch an der automatisierten Verarbeitung von Arbeitnehmerdaten anknüpft.

4.7.2.2 Vernichtung von Personalfragebögen

Am 6.6.1984 hat der 5. Senat des BAG entschieden, ein Bewerber habe einen Anspruch darauf, daß der Arbeitgeber den von ihm ausgefüllten Personalfragebogen nach einer erfolglos gebliebenen Bewerbung vernichte (Az.: 5 AZR 286/81). Das BAG geht zwar davon aus, daß die persönlichen Daten des Bewerbers im vorliegenden Fall nicht in einer Datei i. S. des § 2 Abs. 3 Nr. 3 BDSG gespeichert werden, rechtfertigt den Anspruch des Bewerbers auf Vernichtung des Personalfragebogens jedoch als quasi-negatorischen Beseitigungsanspruch in entsprechender Anwendung des § 1004 BGB. Die dauerhafte Aufbewahrung der dem Arbeitgeber anvertrauten persönlichen Daten stelle einen objektiv rechtswidrigen Eingriff in das Persönlichkeitsrechts des Bewerbers dar.
Wo das BDSG aufgrund formaler Anwendungsschranken keine Schutzwirkung entfalte, sei auf die Grundsätze des allgemeinen Persönlichkeitsrechts zurückzugreifen, die auch bei den durch vorvertragliche Verhandlungen entstandenen Rechtsbeziehungen zur Anwendung kämen. Das informationelle Selbstbestimmungsrecht werde beeinträchtigt, wenn ein Dritter – im vorliegenden Fall also der Arbeitgeber – die Daten des Bewerbers auf Dauer in seinem Einflußbereich belassen wolle. Die auf einem Datenträger festgehaltenen Daten könnten noch nach Jahren für dann anstehende Entscheidungen herangezogen und auch effektiver genutzt werden. Sie seien mit anderen Daten kombinierbar und leichter zu vergleichen. Infolge ihrer Gegenständlichkeit seien sie leichter dem Zugriff Dritter zugänglich. Mit der Speicherung der Daten werde also eine neue Qualität des den Bewerber betreffenden Informationsprozesses erreicht; dementsprechend erhöhe sich auch die Schutzbedürftigkeit.

Im Regelfall habe ein Arbeitgeber ein berechtigtes Interesse allenfalls daran, die Namen der erfolglosen Bewerber festzuhalten, um im Falle einer nochmaligen Bewerbung evtl. Verwaltungs- und Vorstellungskosten einzusparen. Dafür reiche es jedoch aus, wenn die die Person des Bewerbers ausreichend charakterisierenden persönlichen Daten wie Name, Anschrift und Geburtsdatum gespeichert würden. Die Aufbewahrung des Einstellungsfragebogens mit den viel weitergehenden Auskünften übersteige dagegen dieses Informationsbedürfnis des Arbeitgebers. Der Arbeitgeber könne sich schließlich nicht darauf berufen, daß der Bewerber im Personalfragebogen der Verarbeitung seiner Daten zugestimmt habe. Die Zustimmung des Bewerbers zur Datenspeicherung beziehe sich ersichtlich lediglich auf die Dauer des Bewerbungverfahrens selbst.
Das Urteil zeigt, daß nach Meinung des BAG die Ausstrahlungswirkung des allgemeinen Persönlichkeitsrechts weit genug reicht, um dem Betroffenen – im Rahmen eines Arbeitsverhältnisses oder auch bei der durch vorvertragliche Verhandlungen entstandenen Rechtsbeziehung – z. B. einen Löschungsanspruch auch dort zu gewähren, wo das BDSG aufgrund formaler Anwendungsschranken keine Schutzwirkung entfaltet. Zugleich räumt das Gericht allerdings ein, daß die Grundsätze des allgemeinen Persönlichkeitsrechts einen schwächeren Schutz gewährleisten als das BDSG. Damit bestätigt es die Auffassung der Datenschutzbeauftragten, daß die ergänzende Auslegung der bestehenden Vorschriften i. S. der Drittwirkung letztlich nicht ausreicht, um den Arbeitnehmer vor unberechtigten Eingriffen der Arbeitgeber zu schützen. Deshalb ist der Gesetzgeber aufgerufen, den Arbeitnehmerdatenschutz zu verbessern.

4.7.3 Einsicht des Betriebsrates in die Dateienübersicht des betrieblichen Datenschutzbeauftragten

Ein Betriebsrat (BR) hat mich gefragt, ob der bDSB ihm Einsicht in die nach § 29 Satz 1 Nr. 1 BDSG geführte Dateienübersicht zu gewähren hat. Ich bin zum Ergebnis gekommen, daß dem BR die Einsicht in die Dateienübersicht, in der Arbeitnehmerdaten bezeichnet sind, nicht verwehrt werden kann und habe dies wie folgt begründet:
Nach § 75 BetrVG hat der BR mit darüber zu wachen, ob die freie Entfaltung der Persönlichkeit im Betrieb gewährleistet ist. Die im Volkszählungsurteil des Budesverfassungsgerichts vorgenommene Ableitung des Datenschutzes aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG hat daher auch unmittelbare Bedeutung im Betrieb. Erst die gesetzlich abgesicherte Intervention des BR ermöglicht es den Arbeitnehmern, Verarbeitungsbedingungen durchzusetzen, die auf ihre Interessen Rücksicht nehmen. Einseitige und isolierte Entscheidungen über personenbezogene Datenverarbeitung im Betrieb verstoßen gegen das Kooperationsgebot des § 75 Abs. 2 BetrVG. Daraus ergeben sich verschiedene Rechte des BR:

1. § 80 Abs. 1 Nr. 1 BetrVG: Kontrollrechte zur Einhaltung von Datenschutzvorschriften.
   Zu diesem Zweck hat der BR Anspruch auf Unterrichtung über Art und Ziele der Verarbeitung von Arbeitnehmerdaten (Vorlage und Erläuterung der Programme der bestehenden Personaldatenbanken und deren Verknüpfung mit anderen Datenbanken). Die Kontrollmechanismen des BDSG (§§ 28 ff), ändern nichts am Kontrollrecht des BR. Für den bDSB ergibt sich daraus die Verpflichtung, seiner Kontrollfunktion auch und gerade unter Berücksichtigung der besonderen Stellung des BR nachzugehen. Der bDSB muß dem BR auch für Einzelauskünfte zur Verfügung stehen.
   Das Überwachungsrecht des BR erstreckt sich auch darauf, daß der bDSB seine Tätigkeit ordnungsgemäß und weisungsfrei ausübt.
   Da die Erstellung einer Dateienübersicht zu den gesetzlichen Aufgaben des bDSB zählt (§ 29 Abs. 1 Nr. 1 BDSG), folgt aus dem Vorhergesagten zwingend ein Einsichtsrecht des BR in die Dateienübersicht.
2. Darüber hinaus ergibt sich ein Informationsanspruch des BR auch aus § 80 Abs. 2 BetrVG. Die Möglichkeiten des BR, seine Mitbestimmungsrechte, z . B. nach §§ 87, 94 und 95 BetrVG wahrzunehmen, sind nur gewährleistet, wenn er vorher hinreichend informiert wird. Sofern mitbestimmungspflichtige Maßnahmen getroffen werden sollen, die auch einen Bezug zu den betrieblichen Dateien haben, ist u. U. auch die Einsichtnahme des BR geboten. In Fällen, in denen ein Initiativrecht des BR be-

steht (z. B. § 87 BetrVG) steht dem BR auch ein Einsichtsrecht in die Datenübersicht zu, sofern die Einsichtnahme zur Vorbereitung bzw. Durchführung der Initiative erforderlich ist.

3. Aus § 83 BetrVG ergibt sich hingegen kein eigenständiges Einsichtsrecht des BR, da hier nur Rechte des Arbeitnehmers selbst geregelt werden, der allerdings nach § 83 Abs. 1 Satz 2 BetrVG ein Mitglied des BR hinzuziehen kann.
   Da sich der Auskunftsanspruch des Arbeitnehmers auch auf die Methoden der automatisierten Datenverarbeitung erstreckt, läßt sich aus § 83 BetrVG auch ein Einsichtsrecht des Arbeitnehmers in die Dateienübersicht ableiten; die Hinzuziehung eines Betriebsratsmitgliedes nach § 83 Abs. 1 Satz 2 BetrVG gibt diesem dann ein – mittelbares – Einsichtsrecht.

4.7.4 Verpflichtung auf das Datengeheimnis

Der Streit darüber, ob Betriebsräte sich trotz ihrer Geheimhaltungspflichten nach § 79 BetrVG auch auf das Datengeheimnis nach § 5 BDSG verpflichten lassen müssen (vgl. 1. TB, Nr. 7.5.2., S. 59) hält an. Daher möchte ich meine im 1. TB dargestellte Auffassung, daß eine Verpflichtung von BR-Mitgliedern auf das Datengeheimnis geboten ist, soweit sich die Verschwiegenheitspflicht nach § 79 BetrVG nicht auf in Dateien gespeicherte personenbezogene Daten erstreckt, näher erläutern.

§ 5 Abs. 1 BDSG enthält ein unmittelbar an die bei der Datenverarbeitung beschäftigten Personen gerichtetes Verbot zweckfremder Datenverfügung und -nutzung. Die Vorschrift reguliert nicht nur den externen, sondern auch den internen Datenverkehr, bezieht also die Bekanntgabe an eine andere Abteilung, eine Zweigstelle oder einen Betrieb mit ein. Gem. § 5 Abs. 2 BDSG muß der Leiter eines Unternehmes dafür sorgen, daß der von Abs. 1 erfaßte Personenkreis auf das Datengeheimnis verpflichtet wird.

„Bei der Datenverarbeitung beschäftigt" ist eine Person nur dann, wenn der ihr übertragene oder von ihr wahrgenommene Tätigkeitskreis sie mit geschützten Daten dauernd oder regelmäßig in der Weise in Verbindung bringt, daß sie diese zur Kenntnis nehmen, verarbeiten oder sonst nutzen kann. Entscheidend ist allein die faktische Möglichkeit solcher Aktivitäten. Auch auf den Schwerpunkt der Tätigkeit kommt es nicht an. Zu diesem Personenkreis gehört auch der als Teil der speichernden Stelle anzusehende BR, der im Rahmen seiner zahlreichen Mitwirkungs- und Mitbestimmungsrechte insbesondere im personellen Bereich Anspruch auf Unterrichtung auch über vom BDSG geschützte personenbezogene Daten und auf ihre Vorlage hat. Die Verpflichtung auf das Datengeheimnis gem. § 5 Abs. 2 BDSG ist auch nicht im Hinblick auf die speziellen betriebsverfassungsrechtlichen Geheimhaltungspflichten (vgl. §§ 79 Abs. 1 Satz 1, 82 Abs. 2 Satz 3, 83, 99 Abs. 1 Satz 3, 102 Abs. 2 Satz 5 und 120 Abs. 2 BetrVG) entbehrlich. Letztere regeln nur Teilbereiche des Datenschutzes; demgegenüber schützt das BDSG wegen der Gefährdung, die mit der Verarbeitung personenbezogener Daten in Dateien verbunden ist, alle personenbezogenen Daten. So regelt § 79 Abs. 1 Satz 1 BetrVG die Offenbarung und Verwertung von Betriebs- oder Geschäftsgeheimnissen. Es sind durchaus Fälle denkbar, in denen Daten von Arbeitnehmern oder anderen Personen weder „Geschäfts- noch Betriebsgeheimnisse" darstellen. Darüber hinaus erfassen weder das „Offenbaren" noch das „Verwerten" die gleichen Tatbestände wie § 5 BDSG. Dies gilt insbesondere für den Tatbestand des Speicherns.

Da § 79 BetrVG und die anderen o. b. betriebsverfassungsrechtlichen Bestimmungen nach Anlaß und Gegenstand einen anderen Regelungsansatz haben und keine Dekkungsgleichheit vorhanden ist, sind also auch Betriebsratsmitglieder auf das Datengeheimnis zu verpflichten.

Die Geltung des § 5 Abs. 1 BDSG auch für Betriebsratsmitglieder führt nicht zu einer irgendwie gearteten Einschränkung der Betriebsratsarbeit. Denn § 5 Abs. 1 BDSG untersagt nur eine unbefugte Nutzung von personenbezogenen Daten. Ihre Nutzung zur Erfüllung der umfassenden Betriebsratsaufgaben ist jedoch nicht unbefugt.

Eine schriftliche Verpflichtung ist nach dem Wortlaut des Gesetzes nicht zwingend vorgeschrieben; sie empfiehlt sich aber, um die ordnungsgemäße Verpflichtung nachweisen zu können.

Die Verpflichtung, die von der speichernden Stelle – also vom Arbeitgeber – vorzunehmen ist, setzt eine Information über die konkrete Bedeutung des Datengeheimnisses für die Arbeit der Betriebsräte voraus. Die schlichte Wiederholung des § 5 BDSG reicht dafür ebenso wenig aus wie ein ganz allgemein gehaltener Hinweis auf die Verschwiegenheitspflicht. Für die Betriebsräte muß vielmehr erkennbar sein, warum gerade sie vom Arbeitgeber angesprochen werden, auf welche mit ihrer Tätigkeit zusammhängenden Vorgänge sich also das Datengeheimnis bezieht und wie es sich zu ihrer funktionsbedingten Schweigepflicht verhält.
Ich hätte allerdings keine Bedenken dagegen, wenn die Verpflichtung auf das Datengeheimnis so praktiziert würde, daß lediglich der Betriebsratsvorsitzende von der speichernden Stelle verpflichtet würde und dann der Betriebsratsvorsitzende seinerseits die weiteren Betriebsratsmitglieder verpflichtet.

4.7.5 Telefondatenerfassung von Arbeitnehmern

In fortschreitendem Maße werden in größeren Betrieben und Unternehmen automatische Gesprächserfassungsanlagen eingesetzt. Diese Anlagen sollen die Gebührenabrechnung bzw. die ordnungsgemäße Verrechnung der Telefongebühren erleichtern.
Bei den meisten Anlagen dieser Art werden folgende Daten der Telefongespräche erfaßt und gespeichert:

- Datum und Uhrzeit,
- Nummer der Nebenstelle,
- Nummer des angerufenen Gesprächspartners (Zielnummer),
- Gebühreneinheiten,
- ggf. Gesprächskosten.

Bei einigen Anlagen ist es möglich, durch eine spezielle betriebsinterne Vorwahl die Privatgespräche von den dienstlichen Gesprächen zu unterscheiden. Die Kosten dieser Privatgespräche werden den Arbeitnehmern dann monatlich in Rechnung gestellt. Diese Abrechnungen enthalten die vollständige ausgedruckte Zielnummer des Privatgesprächs.
Diese automatische Erfassung und Speicherung von Telefongesprächsdaten von Arbeitnehmern, insbesondere die Erfassung der Rufnummer des angewählten Teilnehmers (Zielnummer), war Gegenstand mehrerer Anfragen. Ich habe den Petenten – meist Arbeitnehmern oder Betriebsräten von Unternehmen, bei denen die Einführung einer automatischen Telefongesprächsdatenerfassung bevorstand – folgende Auffassung mitgeteilt:
Bei den erfaßten Telefondaten handelt es sich um Einzelangaben über persönliche oder sachliche Verhältnisse, die den Arbeitnehmer, aber auch den angerufenen Gesprächspartner betreffen, also um personenbezogene Daten i. S. von § 1 Abs. 1 BDSG. Speichernde Stelle i. S. des § 2 Abs. 3 Nr. 1 BDSG ist die Abrechnungsstelle des Arbeitgebers.
Zulässig ist eine solche Datenverarbeitung personenbezogener Daten nur dann, wenn das BDSG oder eine andere Rechtsvorschrift sie erlaubt (§ 3 Nr. 1 BDSG) oder der Betroffene eingewilligt hat (§ 3 Nr. 2 BDSG).
Unter datenschutzrechtlichen Aspekten wäre es möglich, in den Arbeitsverträgen eine ausdrückliche Einwilligung der Arbeitnehmer in eine automatische Erfassung der Telefondaten vorzusehen. Zumeist werden Gesprächsdaten-Erfassungsanlagen nicht in neu gegründeten Betrieben installiert, so daß eine Einwilligung nachträglich einzuholen wäre. Bei der Einführung dieser Anlagen handelt es sich gleichzeitig auch um technische Einrichtungen, die das Verhalten oder die Leistung von Arbeitnehmern überwachen. Gem. § 87 Abs. 1 Nr. 6 BetrVG steht dem Betriebsrat bei Einführung und Anwendung solcher technischen Überwachungsanlagen mithin ein Mitbestimmungsrecht zu. Falls keine Einigung über eine solche Angelegenheit zustandekommt, entscheidet die Einigungsstelle. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat (§ 87 Abs. 2 Satz 2 BetrVG). Weder der Spruch der Einigungsstelle noch die Einigung zwischen Arbeitgeber und Betriebsrat können jedoch einer Einwilligung i. S. des § 3 Nr. 2 BDSG gleichgestellt werden.

Vielmehr könnte § 23 BDSG eine Gesetzesnorm i. S. von § 3 Nr. 1 BDSG sein, die die Speicherung der Telefondaten erlaubt. Das berechtigte Interesse des Arbeitgebers kann in der Vermeidung unnötiger Telefongespräche bzw. einer korrekten Telefonbenutzung durch den Arbeitnehmer gesehen werden. Dabei muß anerkannt werden, daß der Arbeitgeber ein Interesse daran hat, die Telefonkosten möglichst niedrig zu halten. Insbesondere dann, wenn der Arbeitgeber dem Arbeitnehmer einen Amtsanschluß mit Fernwahlmöglichkeit zur Verfügung stellt, hat er ein erhebliches Kostenrisiko zu tragen. Daher ist ein berechtigtes Interesse an der Telefondatenerfassung – soweit es folgende Daten betrifft – anzuerkennen:

- Datum und Uhrzeit,
- Nebenstellennummer,
- Gebühreneinheiten.

Fraglich ist, ob die Speicherung der Zielnummer erforderlich ist. Anhand der Zielnummer kann der Arbeitgeber den Gesprächspartner des Arbeitnehmers ermitteln und damit feststellen, ob es sich um ein dienstliches oder privates Telefongespräch gehandelt hat. Dazu ist aber nicht die vollständige Zielnummer nötig.

Denn auch aus Telefonnummern, die verstümmelt sind – bei denen z. B. die letzten zwei Ziffern fehlen –, kann der Arbeitgeber i. d. R. feststellen, ob es sich um ein berechtigtes Dienstgespräch gehandelt hat. Sollten sich Rückfragen ergeben, kann der Arbeitgeber den Arbeitnehmer im Einzelfall auch auffordern, ihm anhand einer Liste mit verkürzten Zielnummern die Erforderlichkeit der Telefongespräche nachzuweisen. Der Arbeitgeber wird mit Hilfe der verkürzten Nummern den angerufenen Gesprächspartner i. d. R. rekonstruieren und so gegenüber dem Arbeitgeber Rechenschaft ablegen können. Dabei bleibt es ihm überlassen, ob er z. B. einen Informanten, den er angerufen hat, preisgibt.

In Betrieben, bei denen die Arbeitnehmer den Gesprächspartnern Vertraulichkeit garantiert haben, läßt sich eine Geheimhaltung anders nicht ermöglichen.

Auch bei den Anlagen, die eine differenzierte Abrechnung nach Privat- und Dienstgesprächen durch eine bestimmte Vorwahl ermöglichen, ist – für Abrechnungszwecke – die vollständige Erfassung der Zielnummer weder bei Privatgesprächen noch bei Dienstgesprächen erforderlich. Bei Dienstgesprächen besteht nur ein berechtigtes Interesse des Arbeitgebers, zu überprüfen, ob der Arbeitnehmer in Wahrheit ein Privatgespräch geführt, es aber als dienstliches Telefonat angegeben hat. Diese Kontrolle läßt sich aber auch anhand verkürzter Zielnummern durchführen. Nichts anderes gilt, wenn der Arbeitnehmer sich darauf berufen will, daß er ihm zur Last gelegte Privatgespräche nicht geführt hat, sein Apparat vielmehr von einem Kollegen mißbräuchlich genutzt wurde.

Wenn die Zielnummer ungekürzt gespeichert würde, besteht die Gefahr, daß der Arbeitgeber, obwohl die Speicherung nur Abrechnungszwecken dienen soll, die Zielnummer auswerten und somit ein „Telefonprofil" des einzelnen Arbeitnehmers erstellen kann.

Es liegen bereits einige Betriebsvereinbarungen über Gesprächsdatenerfassungsanlagen vor. Darin wird meistens die Erfassung der ungekürzten Zielnummer für erforderlich gehalten, um eine „ordnungsgemäße Abrechnung zu gewährleisten". Es wird versucht, dem Datenschutz zu genügen, indem entweder nur die Anzahl von Gebühreneinheiten ausgedruckt wird und nur bei auffälligen Gebührenabweichungen die Geschäftsleitung den Ausdruck sämtlicher aufgezeichneter Daten veranlaßt, um sie mit dem Mitarbeiter zu erörtern; oder es werden alle Gesprächsdaten erfaßt – incl. der Zielnummer –, um die Telefonkosten für ein bestimmtes Arbeitsprojekt zu errechnen, wobei aber die erfaßten Nebenstellen keinem konkreten Arbeitnehmer zugeordnet werden können. Allen Betriebsvereinbarungen ist gemeinsam, daß sie ausdrücklich festschreiben, die Gesprächsdatenerfassung werde nicht zur Leistungs- oder Verhaltenskontrolle der Arbeitnehmer benutzt, sondern diene ausschließlich der Abrechnung.

Einige Betriebsvereinbarungen berücksichtigen die Unabhängigkeit des Betriebsrates und räumen ihm einen externen direkten Amtsanschluß ohne Kontrollmöglichkeiten ein. Andere Betriebsvereinbarungen sehen vor, daß die Zielnummer der Betriebsrats-Nebenstelle nicht erfaßt, sondern nur nach Gebühreneinheiten abgerechnet wird.

Datenschutzrechtlich ist bei dem Abschluß von Betriebsvereinbarungen zu berücksichtigen, daß – wie oben erörtert – eine vollständige Erfassung der Zielnummer unzulässig ist.

Es sollte daher in Betriebsvereinbarungen nur geregelt werden, wie die Erfassung der verkürzten Zielnummern gehandhabt wird. In Betracht käme danach
- die Speicherung einer generell verkürzten Zielnummer oder
- die Speicherung einer – verkürzten – Zielnummer nur bei Ferngesprächen oder
- die Speicherung der verkürzten Zielnummer nur dann, wenn bei Orts- und Ferngesprächen oder nur bei Ferngesprächen eine auffällige Gebührenabweichung festgestellt oder eine vereinbarte Kostenschwelle überschritten worden ist.

Die Betriebsvereinbarungen sollten vor allem die Dauer der Speicherung zu Abrechnungszwecken regeln. Anzustreben sind möglichst kurze Speicherzeiten. Nach dem Ausdruck der Abrechnungsbelege müssen personenbezogene Daten unverzüglich gelöscht werden, sofern nicht längere gesetzliche Aufbewahrungsfristen entgegenstehen.
Die Erfassung der Zielnummer stellt zugleich eine Verarbeitung der personenbezogenen Daten des Gesprächspartners dar. Eine Einwilligung des Angerufenen in die Speicherung seiner Gesprächsdaten ist nicht mehr möglich, weil in dem Moment, in dem die Telefonverbindung hergestellt worden ist, die Speicherung bereits vorgenommen wurde.
Wer sich einen Telefonanschluß einrichten läßt, ist i. d. R. sicherlich damit einverstanden, daß seine Telefonnummer anderen bekannt wird. Doch wird man nicht von einer generellen Einwilligung in die Speicherung seiner Nummer in der Gesprächserfassungsanlage eines ihm möglicherweise gar nicht bekannten Unternehmens ausgehen können. Auch kann aus der Tatsache, daß er einen Anruf annimmt, nicht gefolgert werden, er sei damit einverstanden, daß Dritte von dem Telefonat Kenntnis erhalten. Schließlich kann die Einwilligung des Gesprächspartners auch nicht durch die Einwilligung des Arbeitnehmers in die Telefondatenerfassung ersetzt werden.
Somit könnte die Speicherung nur zulässig sein, wenn sie zur Wahrung berechtigter Interessen der speichernden Stelle – Arbeitgeber – erforderlich ist und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Angerufenen beeinträchtigt werden. Wie bereits oben aufgezeigt, ist die vollständige Speicherung der gesammten Zielnummer zu Abrechnungszwecken aber nicht erforderlich. Außerdem sind die schutzwürdigen Belange des Angerufenen beeinträchtigt, denn er kann nicht kontrollieren, wer seine Telefondaten wann erfaßt und auswertet, auch wenn die gespeicherten Daten unverzüglich nach Erstellen einer Abrechnung gelöscht werden.
Die Zulässigkeit der Speicherung personenbezogener Daten des Angerufenen wird von Betriebsvereinbarungen nicht tangiert. Wenn allerdings die Betriebsvereinbarung davon ausgeht, daß nur die verkürzte Zielnummer erfaßt werden darf, so dürften in aller Regel auch die schutzwürdigen Belange des Betroffenen gewahrt bleiben.
Kürzlich ist ein Beschluß des Arbeitsgerichts Hamburg vom 3.10.1984 (23 BV 6/84) veröffentlicht worden. Darin ist das Arbeitsgericht Hamburg unter besonderer Berücksichtigung des presserechtlichen Informationsschutzes bzw. des publizistischen Zeugnisverweigerungsrechts zum gleichen Ergebnis gekommen.
Eine andere Auffassung vertritt das LAG Düsseldorf in seiner Entscheidung vom 30.4.1984 (Az.: 10 TaBV 10/84); auch diese Entscheidung ist noch nicht rechtskräftig geworden. In Kürze ist also mit einer Grundsatzentscheidung des BAG zu diesem Problem zu rechnen.

4.7.6 Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts

Das VZ-Urteil hat Konsequenzen auch für die Datenverarbeitung im nicht-öffentlichen Bereich. Die vom BVerfG beschriebenen Gefährdungen des Rechts auf informationelle Selbstbestimmung ergeben sich nicht nur aus der Datenverarbeitung staatlicher Stellen. Undurchschaubarkeit der Verarbeitung, Zusammenfügung zu Persönlichkeitsbildern, Erweiterung der Einflußmöglichkeiten auf den Einzelnen kennzeichnen auch die Datensammlungen privater Unternehmen.
Gerade der Personalbereich der Betriebe bildet einen Schwerpunkt zunehmender Automatisierung. Moderne Personalinformationsssysteme liefern die Möglichkeit zu einer umfassenden Normung und Kontrolle des Verhaltens und der Leistung der Beschäftigten. Angesichts dieser Gefährdungen des Rechts auf informationelle Selbstbestimmung bedarf die Verarbeitung von Arbeitnehmerdaten einer speziellen gesetzlichen Schutzre-

gelung; eine korrigierende Auslegung bestehender Vorschriften i. S. der Drittwirkung reicht zur Gewährleistung des Grundrechts nicht aus. Wegen der Abhängigkeit des Arbeitnehmers von Arbeitsplatz und Einkommen zur Sicherung seiner Existenz stellt sich für ihn generell die Pflicht zur Angabe seiner Daten als zwangsweise Erhebung i. S. des BVerfG-Urteils dar. Hieraus ergibt sich für das Beschäftigungsverhältnis die Notwendigkeit einer bereichsspezifischen und präzisen Bestimmung der Verwendungszwecke der erhobenen Daten, des Schutzes vor Zweckentfremdung durch Weitergabe- und Verwertungsverbot sowie der Beschränkung auf das zur Zweckerreichung erforderliche Datenminimum. Die Bestimmungen der §§ 23 ff BDSG genügen – auch im Zusammenwirken mit Regelungen des sonstigen arbeitsrechtlichen Informationsschutzes – den Anforderungen an Zweckbindung und Normenklarheit nicht. Insbesondere die Verarbeitungsbefugnis aufgrund „berechtigter Interessen" des Arbeitgebers muß entfallen. Da die Gefahr einer Beeinträchtigung des Persönlichkeitsrechts bei jeder Ausgestaltung der Datenverarbeitung und Datennutzung besteht, darf es auch bei dem auf Dateien abstellenden Regelungsansatz des BDSG nicht verbleiben.

Durch Gesetz muß festgelegt werden:

- Speicherung, Auswertung und Übermittlung von Arbeitnehmerdaten sind – unabhängig von der Form der Verarbeitung – auf die Fälle gesetzlicher Verarbeitungspflichten und der Durchführung der Arbeits- bzw. Dienstverhältnisse zu beschränken.
  Auch mit Einwilligung des Betroffenen darf die Verarbeitung über diesen Rahmen nicht hinausgehen, da die typische Abhängigkeit des Arbeitnehmers einer freien und gleichberechtigten Gestaltung der Informationsbeziehungen sowohl bei der Bewerbung als auch bei bestehenden Arbeitsverhältnissen entgegensteht.
- Auswertungen und Verknüpfungen, die zur Herstellung eines „Persönlichkeitsbildes" der Arbeitnehmer führen, sowie die Speicherung solcher „Profile" sind grundsätzlich unzulässig.

Als verfahrensrechtliche Schutzvorkehrungen fordert das Gericht die Festlegung von Aufklärungs-, Auskunfts- und Löschungspflichten, um Datentransparenz herzustellen bzw. die Zweckbindung zu verstärken.

- Der Auskunftsanspruch des Arbeitnehmers ist daher über § 26 Abs. 2 BDSG hinaus auszudehnen auf alle, nicht nur die regelmäßigen Datenempfänger, sowie die Auswertungsprogramme bzw. Einzelauswertungen, in die seine Daten einbezogen sind.
- Die Auskunftseinschränkungen nach Nrn. 4 und 5 von § 26 Abs. 4 BDSG (bei Daten aus allgemein zugänglichen Quellen und bei gesperrten Daten) müssen entfallen.
- Daten müssen – vergleichbar der Regelung in § 84 SGB X – gelöscht und nicht nur gesperrt werden, wenn sie zur Durchführung des Arbeitsverhältnisses nicht mehr erforderlich sind und durch die Löschung schutzwürdige Belange des Beschäftigten nicht beeinträchtigt werden.

Im Bereich der Arbeitsbeziehungen kann die Sicherung und Durchsetzung von Grundrechten des Arbeitnehmers nicht ausschließlich individuell erfolgen. Um Abhängigkeit und Fremdbestimmung des einzelnen Beschäftigten und die daraus resultierende Möglichkeit der Beeinträchtigung seines Selbstbestimmungsrechts jedenfalls teilweise zu kompensieren, bedarf es wirksamer Beteiligungs- und Kontrollrechte der Betriebs- und Personalräte.

Der BR hat das Persönlichkeitsrecht der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern (§ 75 Abs. 2 BetrVG). Seine Rechte sind in bezug auf die Verarbeitung von Arbeitnehmerdaten im Lichte des Grundrechts auf informationelle Selbstbestimmung zu interpretieren. Doch reicht dies für ein effizientes kontrollierendes Gegengewicht gegen die Verfügungsmöglichkeiten des Arbeitgebers nicht aus.

Noch immer wird darüber gestritten, ob Verfahren, in denen Personaldaten verarbeitet werden, „dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen", weil hiervon nach dem BetrVG (und auch nach dem Hamb. Personalvertretungsgesetz) die Mitbestimmungsrechte der Betriebs- und Personalräte abhängig sind. Diese Anknüpfung muß für Personaldatensysteme aufgegeben werden, während bei sonstigen technischen Einrichtungen weiterhin auf die Überwachungsmöglichkeit abgestellt werden sollte. Über die bisherigen gesetzlichen Regelungen hinaus und in Anlehnung an das neu gefaßte Hessische Personalvertretungsgesetz müssen die Be-

triebs- und Personalräte also ein eindeutiges Mitbestimmungsrecht haben bei der Einführung und Anwendung sowie bei wesentlichen Änderungen oder Ergänzungen

- von Dateien und Anlagen zur automatisierten Verarbeitung personenbezogener Daten der Beschäftigten,
- von sonstigen technischen Einrichtungen, soweit diese dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.

Schließlich trägt es zur Verbesserung des Datenschutzes auch für die Arbeitnehmer (wie für alle anderen Betroffenen) bei, wenn die Stellung des bDSB gestärkt und die Befugnisse der Aufsichtsbehörde erweitert werden. Auf die Nrn. 5.2.2 und 5.2.3 meines 2. TB, unter denen ich meine Empfehlungen zur Novellierung des BDSG zusammengefaßt habe, weise ich hin.

Hamburg, den 31.12.1984
Claus Henning Schapper