BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

11. Wahlperiode

Drucksache 11/5667

24.01.86

Der Hamburgische Datenschutzbeauftragte

An den
Herrn Präsidenten der Bürgerschaft

Betr.: Vierter Tätigkeitsbericht
des Hamburgischen Datenschutzbeauftragten zum 1. Januar 1986

Gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen Vierten Tätigkeitsbericht, den ich zum 1. Januar 1986 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

Vierter Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten

Zugleich
Tätigkeitsbericht der Aufsichtsbehörde
nach §§ 30, 40 BDSG

vorgelegt zum 1. Januar 1986
Redaktionsschluß: 10. Dezember 1985

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

INHALTSVERZEICHNIS **Seite**

Abkürzungsverzeichnis

ADV	=	Automatische Datenverarbeitung
APIS	=	Arbeitsdatei PIOS Innere Sicherheit
AVAD	=	Auskunftsstelle über den Versicherungsaußendienst e.V.
BAföG	=	Bundesausbildungsförderungsgesetz
BAJS	=	Behörde für Arbeit, Jugend und Soziales
BBG	=	Bundesbeamtengesetz
bDSB	=	betrieblicher Datenschutzbeauftragter
BetrVG	=	Betriebsverfassungsgesetz
BDSG	=	Bundesdatenschutzgesetz
BfD	=	Bundesbeauftragter für den Datenschutz
BfI	=	Behörde für Inneres
BGBl	=	Bundesgesetzblatt
BGH	=	Bundesgerichtshof
BGS	=	Bundesgrenzschutz
BKA	=	Bundeskriminalamt
BKK	=	Betriebskrankenkasse
BND	=	Bundesnachrichtendienst
BSB	=	Behörde für Schule und Berufsbildung
BseuchG	=	Bundesseuchengesetz
BTM	=	Betäubungsmittel
Btx	=	Bildschirmtext
BVerfG	=	Bundesverfassungsgericht
BVerfSchG	=	Bundesverfassungsschutzgesetz
BZRG	=	Bundeszentralregister
CCC	=	Chaos Computer Club
DRS	=	Drucksache
DS	=	Datenschutz
DSB	=	Datenschutzbeauftragter
DV	=	Datenverarbeitung
DVO	=	Durchführungsverordnung
DVZ	=	Datenverarbeitungszentrale
EC-Karte	=	Eurocheque-Karte
EDV	=	Elektronische Datenverarbeitung
GewO	=	Gewerbeordnung
GG	=	Grundgesetz
GVBl	=	Gesetz- und Verordnungsblatt

HmbBG	=	Hamburgisches Beamtengesetz
HmbDSB	=	Hamburgischer Datenschutzbeauftragter
HmbDSG	=	Hamburgisches Datenschutzgesetz
HmbPersVG	=	Hamburgisches Personalvertretungsgesetz
HmbSOG	=	Hamburgisches Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
HmbVerfSchG	=	Hamburgisches Verfassungsschutzgesetz
HUK-Verband	=	Verband der Haftpflicht-, Unfall-, Auto- und Rechtsschutzversicherer e.V.
IMK	=	Konferenz der Innenminister
IuK	=	Information und Kommunikation
JVA	=	Justizvollzugsanstalt
KAN	=	Kriminalaktennachweis
KBA	=	Kraftfahrtbundesamt
KGSt	=	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KpS	=	Kriminalpolizeiliche personenbezogene Sammlung
LDSG	=	Landesdatenschutzgesetz
LID	=	Lehrerindividualdatei
MAD	=	Militärischer Abschirmdienst
ME	=	Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder
MiStra	=	Mitteilungen in Strafsachen
MittVw	=	Mitteilungen für die hamburgische Verwaltung
MiZi	=	Mitteilungen in Zivilsachen
NADIS	=	Nachrichtendienstliches Informationssystem
NJW	=	Neue Juristische Wochenschrift
NRW	=	Nordrhein-Westfalen
OFD	=	Oberfinanzdirektion
OWiG	=	Ordnungswidrigkeitengesetz
PB	=	Polizeiliche Beobachtung
PC	=	Personal Computer
PIN	=	Identifizierungsnummer
PIOS	=	Inpol-Anwendungen Personen, Institutionen, Objekte und Sachen
PIS	=	Personalinformationssystem
POLAS	=	Polizeiliches Auskunftssystem
POS	=	Point of Sale

RVO	=	Reichsversicherungsordnung
RZ	=	Rechenzentrum
Schufa	=	Schutzgemeinschaft für allgemeine Kreditsicherung
SGB	=	Sozialgesetzbuch
SOG	=	s. HmbSOG
SPUDOK	=	Spurendokumentation
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StV-Btx	=	Staatsvertrag über Bildschirmtext
StVG	=	Straßenverkehrsgesetz
StVollzG	=	Strafvollzugsgesetz
TB	=	Tätigkeitsbericht
TEMEX	=	Telemetry Exchange
UKE	=	Universitätskrankenhaus Eppendorf
VE	=	Vorentwurf
VV	=	Verwaltungsvorschift
VZ-Urteil	=	Volkszählungsurteil
WoBindG	=	Wohnungsbindungsgesetz
ZAG	=	Gesetz über die Zusammenarbeit der Dienste und der Polizei
ZAW	=	Zentralausschuß der Werbewirtschaft e.V.
ZEVIS	=	Zentrales Verkehrsinformations-System
ZPO	=	Zivilprozeßordnung

VORWORT

Ich habe bereits im 1. und 3. Tätigkeitsbericht klargestellt, daß ich über den nicht-öffentlichen Bereich nicht aufgrund von § 20 Abs. 2 Satz 2 HmbDSG berichte, daß ich dies vielmehr in meiner Eigenschaft als Aufsichtsbehörde gem. §§ 30, 40 BDSG tue.

Um die Berichterstattung über den nicht-öffentlichen Bereich und den Tätigkeitsbereich des Hamburger Datenschutzbeauftragten auch in ihrer äußerlichen Gestaltung deutlicher voneinander abzuheben, habe ich schon auf der Titelseite darauf hingewiesen, daß ich auch in meiner Funktion als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich berichte. Deshalb ist darüber hinaus der Bericht über den nicht-öffentlichen Bereich auf andersfarbigem Papier gedruckt worden.

1. Zur Lage des Datenschutzes

Auf das - aus der Sicht des Datenschutzes – sicherlich wichtigste Ereignis des Jahres warten wir heute – am 10. Dezember 1985, der Redaktionsschluß ließ sich nicht länger hinausschieben – noch immer; und es bleibt weiterhin ungewiß, ob es den Koalitionsparteien in Bonn noch gelingen wird, sich über das Paket mit den sog. „Begleitgesetzen zum Personalausweisgesetz" zu einigen. Seit einigen Monaten hatten Koalitionspolitiker angekündigt, daß es nur noch eine Frage von wenigen Tagen oder Wochen sei, bis Entwürfe für

- eine Novellierung des Bundesverfassungsschutzgesetzes, das auch die Zusammenarbeit zwischen dem Bundesamt für Verfassungsschutz und den Landesämtern regelt;
- ein MAD-Gesetz, das es bislang nicht gibt;
- ein Gesetz, das die Zusammenarbeit zwischen Nachrichtendiensten und Sicherheitsbehörden auf eine rechtlich einwandfreie Grundlage stellen will;
- ein neues Paßgesetz;
- ein Gesetz zur Änderung des Straßenverkehrsgesetzes, das vor allem den Zugriff anderer Behörden auf die Datenbestände des Kraftfahrtbundesamtes ermöglichen will;
- schließlich eine Novellierung des BDSG

im Bundestag eingebracht werden könnten und damit die Voraussetzungen für die Verabschiedung des 5. Gesetzes zur Änderung des Bundespersonalausweisgesetzes – und des 3. Anlaufs, um einen maschinenlesbaren Personalausweis einzuführen – geschaffen seien. Jetzt sieht es so aus, als ob es erst im neuen Jahr weitergehen wird. Im Januar sollen sich die Parteivorsitzenden mit den Entwürfen befassen. Auch wenn sie die in sie gesetzten Hoffnungen erfüllen, läßt sich eines heute schon voraussagen: Nur weniges von den Dingen, die die Koalition zu einem Paket zusammen geschnürt hat, kann in dieser Wahlperiode des Bundestages noch abschließend beraten werden; die Mehrzahl der Entwürfe wird der Diskontinuität anheim fallen. Wer es gut meint mit dem Datenschutz, wird hierüber indessen nicht unglücklich sein. So dringlich aus Sicht des Datenschutzes nämlich eine bereichsspezifische Regelung der Datenverarbeitung im Sicherheitsbereich erscheint, das bisherige Ergebnis der Koalitionsberatungen – soweit es der Öffentlichkeit bekannt geworden ist – ist nicht geeignet, mich sehr hoffnungsvoll zu stimmen.

CDU/CSU und FDP sind sich darüber einig, daß das Personalausweisgesetz dann vom Bundestag verabschiedet werden kann, wenn die vorparlamentarischen Verhandlungen über die „Begleitgesetze" abgeschlossen sind. Gegen diese Planung müssen folgende Einwände vorgebracht werden:

1. Der Bundestag hatte schon im Jahre 1980 ein Junktim hergestellt zwischen der Einführung eines computerlesbaren Personalausweises und der Schaffung bereichsspezifischer Datenschutzvorschriften für die Sicherheitsbehörden und sich dabei von folgenden Erwägungen leiten lassen: Der Hauptnutzer des neuen Ausweissystems, insbesondere der Verwendungsmöglichkeiten, die sich aus der Maschinenlesbarkeit ergeben, ist die Polizei. Doch die Voraussetzungen, unter denen die Polizei – mit Hilfe eines computerlesbaren Ausweises – Personenkontrollen durchführen und Personalien feststellen darf, sind nicht im Personalausweisgesetz geregelt. Dies muß in den Polizeigesetzen des Bundes und der Länder geschehen, die die Befugnisse der Polizei bei der Gefahrenabwehr regeln, und in der Strafprozeßordnung, die die polizeilichen Befugnisse bei der Strafverfolgung festlegt. Alle diese Gesetze enthalten aber entweder gar keine einschlägigen Vorschriften oder aber solche, die den verfassungsrechtlichen Prinzipien der Normenklarheit und Verhältnismäßigkeit in höchst unzureichender Weise entsprechen. Die Novellierung gerade dieser Gesetze aber hat die Koalition nicht in Angriff genommen – mit der sehr anfechtbaren Begründung, die Gesetzgebungskompetenz liege bei den Ländern. Tatsächlich ist es Sache des Bundes, z.B. die StPO, das BKA-Gesetz und das BGS-Gesetz zu novellieren und i.ü. auf die Länder einzuwirken, ihre Polizeigesetze zu ändern, um die Voraussetzungen für die nach Meinung der Koalition so dringliche Einführung eines neuen Ausweissystems zu schaffen. Das bedeutet also, die Koalition will zwar flankierende Maßnahmen ergreifen, aber es sind nicht die richtigen, wie wichtig sie – losgelöst von dem Junktim – auch sein mögen.

2. Es reicht nicht aus, daß die Koalitionsparteien sich über die Rahmenbedingungen für die Einführung eines maschinenlesbaren Personalausweises verständigen, es aber offen lassen, ob und mit welchem Inhalt sie die Entwürfe verabschieden. Vielmehr muß der Entscheidung über das Personalausweisgesetz die Feststellung vorangehen, daß ein mit der Maschinenlesbarkeit erreichbarer Sicherheitsgewinn die hiermit verbundenen Risiken für das Persönlichkeitsrecht überwiegt. Eine solche Feststellung kann der Bundestag aber erst treffen, wenn er auch abschätzen kann, wie häufig und wie intensiv mit Hilfe des maschinenlesbaren Ausweises polizeiliche Kontrollen durchgeführt werden – dies ist ihm aber nicht möglich, so lange der Inhalt der „Begleitgesetze" noch nicht festliegt.

Doch ganz abgesehen davon, daß mit den von den Regierungsparteien in Bonn vorbereiteten Gesetzentwürfen die verfassungsrechtlichen Voraussetzungen für eine Entscheidung über einen neuen Ausweis überhaupt nicht erfüllt werden können, müssen sie als ein untauglicher Versuch bewertet werden, die nötigen Konsequenzen aus dem Volkszählungsurteil zu ziehen. Wer dies will, muß zunächst einmal tragfähige, den verfassungsrechtlichen Anforderungen entsprechende Grundlagen für alle Grundrechtseingriffe schaffen, die sich aus der heute praktizierten Informationstätigkeit des Staates ergeben. Der Koalition hingegen scheint es primär darum zu gehen, künftige Nutzungen der modernen Informations- und Kommunikationstechnologie zu ermöglichen, indem sie

- einen computerlesbaren Ausweis einführt
- einen computerlesbaren Reisepaß einführt
- on-line-Zugriffe auf ZEVIS ermöglicht
- die Ausweitung des nachrichtendienstlichen Informationssystems rechtlich absichert.

Die Polizei indessen, deren automatisierte Informationssysteme schon heute einen hohen Standard erreicht haben und immer weiter ausgebaut werden, soll bis auf weiteres den Übergangsbonus strapazieren dürfen. Geregelt wird nur – und auch dies ist bezeichnend –, unter welchen Voraussetzungen sie mit und ohne Ersuchen verpflichtet und berechtigt ist, den Nachrichtendiensten Daten zu übermitteln; und vielleicht wird es sogar eine Regelung geben, die die Polizei verpflichtet, Daten zu erheben, die sie für die Erfüllung eigener Aufgaben nicht benötigt, an denen vielmehr nur die Nachrichtendienste interessiert sind.

Die einzelnen Gesetzentwürfe begegnen einer Fülle von Bedenken, die an verschiedenen Stellen dieses Berichts wiedergegeben werden. Die wesentlichen Kritikpunkte lassen sich wie folgt zusammenfassen:

1. Die gesetzgebungspolitische Reaktion auf das VZ-Urteil, wie sie in den „Begleitgesetzen" der Koalition ihren Niederschlag gefunden hat, hat der Frankfurter Staatsrechtler Erhard Denninger treffend als „gesetzesförmlichen Grundrechtsleerlauf" gekennzeichnet: Ein formal detailistischer Regelungsperfektionismus verbinde sich mit einer minimalen inhaltlichen Befugnisbegrenzung, die jedenfalls den status quo einer an der Verwaltungseffizienz orientierten Praxis absichere, wenn sie nicht vielmehr noch deren Möglichkeiten erweitere. In diesem Sinn hat der Arbeitskreis II der Innenministerkonferenz die mit dem Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes verfolgten Ziele wie folgt formuliert: „Der Entwurf stellt darauf ab, daß die Datenerhebung und Datenverarbeitung der Polizei im bisherigen Umfang zur Erfüllung der polizeilichen Aufgaben erforderlich ist und deshalb auch in Zukunft in diesem Ausmaß zulässig sein muß... Alle vorgesehenen Regelungen laufen daher im Prinzip auf eine präzisere gesetzliche Fixierung des Ist-Zustandes hinaus." In der Vorgabe des Staatssekretärs-Ausschusses für das geheime Nachrichtenwesen (zitiert in einer früheren Begründung des Vorentwurfs für die Novellierung des Bundesverfassungsschutzgesetzes) wird gefordert, daß die bisherige Praxis insbesondere der Zusammenarbeit der Sicherheitsbehörden festgeschrieben werden solle. Besser läßt sich m.E. die Tendenz der von der Koalition erarbeiteten Gesetzentwürfe nicht beschreiben.

   Das bedeutet: Eine Verwaltungspraxis, die bislang als „schlicht hoheitliche", die Grundrechtssphäre der Bürger nicht tangierende Tätigkeit angesehen wurde, soll unverändert bleiben, eher ausgeweitet werden, obwohl sie nunmehr aufgrund einer – vom Standpunkt der Verwaltung aus gesehen – radikal veränderten Rechtsanschauung als eine Beschränkung des Grundrechts auf informationelle Selbstbestimmung bewertet wird. Trotzdem sollen alle

bisherigen Aktivitäten fortgesetzt werden, ohne daß auch nur geprüft wird, ob gegen das – nicht erst im VZ-Urteil formulierte – Übermaßverbot verstoßen wird (ich habe mich mit dieser – wie ich meine – unhaltbaren Ausgangsposition unter 4.9.1 ausführlich auseinandergesetzt).

2. Die Koalitionsentwürfe werden auch dem im VZ-Urteil formulierten Grundsatz der bereichsspezifischen und präzisen Zweckbestimmung nicht gerecht, der den Gesetzgeber zwingt, die Vorstellungen von der Einheit der Staatsgewalt aufzugeben. Der auskunftsverpflichtete Bürger soll darauf vertrauen können, daß seine Daten nur für den ihm bekanntgegebenen Zweck verwendet werden. Der Austausch von Informationen innerhalb der Verwaltung soll die Ausnahme sein, die einer gesetzlichen Rechtfertigung durch überwiegende Allgemeininteressen bedarf. Das Bundesverfassungsgericht spricht davon, daß ein amtshilfefester Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote geschaffen werden müsse.

   Wie sehen nun die bisherigen Bemühungen aus, der verfassungsrechtlich gebotenen Zweckbindung genüge zu tun? Der Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes will Übermittlungen an andere als Polizeibehörden gestatten, wenn sie zu einem Zweck erfolgen, der mit dem Zweck vereinbar ist, zu dem die Polizei die Daten erhoben oder gespeichert hat. Auch der Vorentwurf zur Novellierung des Bundesverfassungsschutzgesetzes wollte in einer früheren Fassung bei Übermittlungen durch den Verfassungsschutz ohne Differenzierung nach Empfängergruppen allein darauf abstellen, ob die empfangende Behörde die Daten für Aufgaben benötigt, die mit dem Zweck des Verfassungsschutzes vereinbar sind. Da in der Praxis kaum Fälle denkbar sind, in denen eine Datenübermittlung an fehlender Zweckvereinbarkeit scheitern könnte, würde die Einführung eines Zweckvereinbarkeitsprinzips einer Aufhebung des Zweckbindungsprinzips gleichkommen.

   Nach der neuesten mir vorliegenden Fassung des Bundesverfassungsschutzgesetzes soll der Verfassungsschutz Daten übermitteln dürfen, wenn der Empfänger sie für Zwecke der öffentlichen Sicherheit einschließlich des Schutzes der freiheitlich-demokratischen Grundordnung benötigt. Die Verfasser des Zusammenarbeitsgesetzes sind davon ausgegangen, daß die Aufnahme einer besonderen Zweckbindungsregelung in das Gesetz entbehrlich sei. Das ZAG wolle die informationelle Zusammenarbeit der Sicherheitsbehörden ausschließlich auf dem diesen Behörden übertragenen Tätigkeitsgebiet des Staats- und Verfassungsschutzes regeln. In dieser Zweckbestimmung liege gleichzeitig die notwendige, aber auch ausreichende Eingrenzung des Rahmens, innerhalb dessen die Übermittlung von personenbezogenen Daten möglich und zulässig sei. Daß eine so umfassende Aufgabenumschreibung, die alle Angelegenheiten des Verfassungsschutzes, des Staatsschutzes und sogar der öffentlichen Sicherheit im weitesten Sinne einbezieht, den Anforderungen an eine präzise und konkrete Zweckbestimmung nicht gerecht wird und schon gar nicht die vom BVerfG geforderte informationelle Gewaltenteilung herstellt, bedarf wohl keiner weiteren Ausführungen. Im Gegenteil: Den Verfassern dieser Entwürfe kann bescheinigt werden, daß sie die Einheitlichkeit der Staatsgewalt nicht gefährdet haben.

   Wenn schon der Datenaustausch zwischen Nachrichtendiensten, Polizeibehörden und darüber hinaus allein dadurch gerechtfertigt wird, daß alle Übermittlungen einem Zweck dienen, ist es selbstverständlich, daß die Verfasser der Entwürfe eine Differenzierung zwischen den unterschiedlichen Aufgaben, die von einer Behörde wahrgenommen werden, gar nicht erst erwägen.

3. Für das Verhältnis zwischen den Polizeibehörden und den Nachrichtendiensten gilt das Trennungsgebot, dessen Auswirkungen auf die informationelle Zusammenarbeit der beiden Bereiche ich weiter unten (4.10.6.1) ausführlich erörtert habe. Ich komme zu dem Ergebnis, daß die bisherigen Entwürfe dem Grundgedanken des Trennungsgebots nur sehr unzureichend Rechnung tragen.

   - Es muß noch klargestellt werden, daß die Nachrichtendienste die Polizei nicht um Amtshilfe zu Maßnahmen ersuchen dürfen, zu denen sie selbst nicht befugt sind.

   - Die bisher vorgesehenen Einschränkungen für die Weitergabe von Informationen, die die Polizei unter Einsatz spezieller strafprozessualer Befugnisse (insbesondere zur Post- und Telefonkontrolle sowie zur Durchsuchung von Wohnungen) gewonnen hat, reichen nicht

aus. Es muß verhindert werden, daß die Schutzbestimmungen des G-10 unterlaufen werden.

- Vor allem aber ist es nicht hinnehmbar, daß die Informationen, die die Polizei mit besonderen Methoden der Datenerhebung (z.B. durch polizeiliche Beobachtung oder unter Einsatz technischer Mittel) gewonnen hat, ohne besondere Beschränkungen, also unter der alleinigen Voraussetzung, daß die empfangende Behörde die Daten für die Erfüllung ihrer Aufgaben benötigt, an einen Nachrichtendienst nicht nur weitergeben darf, sondern weitergeben muß.

4. Auch die Regelung des Auskunftsanspruchs gegenüber den Sicherheitsbehörden im Entwurf zur Novellierung des BDSG bleibt hinter den verfassungsrechtlichen Anforderungen weit zurück. Wann wird die Sicherheit des Bundes nicht berührt sein, wenn ein Bürger von einem der Nachrichtendienste eine Auskunft begehrt? Obendrein bedarf die Ablehnung des Auskunftsersuchens in keinem Fall einer Begründung, und nicht einmal eine interne Aufzeichnung der Gründe wird verlangt. Dem Bürger hilft es wenig, daß auf sein Verlangen dem BfD die Auskunft zu erteilen ist; der ihm seinerseits aber nur mitteilen darf, ob seine – des Bürgers – Rechte verletzt sind. Um der Rechtssprechung des Bundesverfassungsgerichts Rechnung zu tragen, wonach das Verfahrensrecht der Grundrechtsausübung nicht so hohe Hindernisse entgegensetzen darf, daß die Gefahr einer Entwertung der materiellen Grundrechtsposition entsteht, müssen die Rechte der Bürger noch wesentlich verbessert werden – und dies auch gegenüber der Polizei, deren Auskunftsverweigerungsrechte nach dem Koalitionsentwurf im Ergebnis nahezu ebenso weit reichen wie die des Verfassungsschutzes.

5. Schließlich sind die Koalitionsparteien auch nicht bereit, dem BfD die Kontrollbefugnisse zuzugestehen, die er braucht, um seine Aufgaben wirksam zu erfüllen.

   - Grundsätzlich soll er die Einhaltung von Datenschutzvorschriften nur überprüfen dürfen, wenn die Daten in Dateien verarbeitet oder unmittelbar aus Dateien benutzt werden.
   - Anders als Aufsichts- und Rechnungsprüfungsbehörden soll der BfD durch Betroffene daran gehindert werden können, Verstöße gegen besondere Datenschutzvorschriften festzustellen.
   - Im Widerspruch zum BND-Urteil des Bundesverfassungsgerichts soll die Datenverarbeitung im Rahmen des G-10 nicht der Kontrolle durch den BfD unterliegen.

   Alle diese Beschränkungen der Kontrollbefugnisse sind angesichts der Bedeutung, die das Bundesverfassungsgericht der Beteiligung unabhängiger Datenschutzbeauftragter für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung beimißt, nicht akzeptabel.

Insgesamt muß den Koalitionsparteien bescheinigt werden, daß ihre Entwürfe hinter den verfassungsrechtlichen Anforderungen deutlich zurückbleiben. Wenn es also wegen der Uneinigkeit der Partner oder wegen der vorangeschrittenen Wahlperiode des Bundestages nicht mehr zu Gesetzesbeschlüssen kommt, brauchen wir dies – wie gesagt – nicht zu bedauern.

Aber: Beim jetzigen Zustand darf es auch nicht bleiben. Seit Jahren beklagen wir uns doch darüber, daß gerade im Sicherheitsbereich tragfähige Rechtsgrundlagen für die sich ständig ausweitende Informationstätigkeit aller Behörden nicht vorhanden sind. Es kann leider keine Rede davon sein, daß in den Fällen, in denen es an gesetzlichen Befugnissen fehlt, die Datenverarbeitung auf das für die Weiterführung einer funktionsfähigen Verwaltung unerläßliche Maß reduziert wird. Ich erneuere die Forderung (3. TB, 1.3), besonders schwerwiegende Informationseingriffe, die nicht nur formalen Bedenken begegnen, bei denen Zweifel vielmehr auch an der Erforderlichkeit bestehen, nicht fortzuführen (der neue Bericht enthält weitere Beispiele). Meine Hoffnung, daß dieser Forderung entsprochen wird, ist allerdings gering.

Zu den Bemühungen des Hamburger Senats, Konsequenzen aus dem VZ-Urteil zu ziehen, gibt es kaum etwas anzumerken, weil auch nur wenig geschehen ist. Im 3. TB (1.2) hatte ich einige Gesetzgebungsvorgaben als vordringlich bezeichnet. Über den Sachstand kann ich folgendes berichten:

- SOG. Die Innenbehörde ist jetzt immerhin so weit, daß die Behördenabstimmung eingeleitet wird. Ich halte den Entwurf für beratungsreif, wenn er auch nicht immer dem Grundsatz der

Verhältnismäßigkeit gerecht wird. Die Eingriffsschwellen müssen noch bei mehreren Maßnahmen deutlich heraufgesetzt werden.

- Meldegesetz. Die Ausschußberatungen sind abgeschlossen.
- Archivgesetz. Mir liegt noch immer kein Entwurf vor.
- Verfassungsschutzgesetz. Nach Auffassung des Senats (Stellungnahme zum 3. TB) ist es für eine Auseinandersetzung mit den Forderungen des Hamburgischen Datenschutzbeauftragten auf parlamentarischer Ebene noch zu früh. Für eine Novellierung des Hamburgischen Gesetzes müsse das Ergebnis der Abstimmungsverhandlungen auf Bund-Länderebene abgewartet werden.

  Ich wiederhole: Gerade für die Datenverarbeitung des Verfassungsschutzes sind präzise gesetzliche Grundlagen erforderlich; sie greift in besonderem Maße in das Recht auf informationelle Selbstbestimmung ein, weil sie fast vollständig im geheimen und somit unter Ausschluß der Öffentlichkeit und der Kontrolle durch den Betroffenen stattfindet. Unabhängig von der weiteren Entwicklung auf Bundesebene muß das Hamburger Gesetz baldmöglichst novelliert werden.
- Gesetz über das Gesundheitswesen. Die in der Senats-Stellungnahme angekündigten Vorarbeiten für bereichsspezifische Regelungen sind im Berichtszeitraum nicht wesentlich vorangekommen. Für ebenso dringlich wie das im letzten TB geforderte Gesetz über den öffentlichen Gesundheitsdienst halte ich bereichsspezifische Regelungen für die Datenverarbeitung im Krankenhaus (siehe 4.13.1).
- Katastergesetz. Ein dringender Regelungsbedarf ist für den Senat wegen der Existenz gesetzlicher Grundlagen (Grundbuchordnung, Bodenschätzungsgesetz) nicht erkennbar. Diese Begründung verblüfft; anders als der Senat vermag ich nicht zu erkennen, daß die von ihm zitierten Vorschriften in irgendeiner Weise die Verarbeitung personenbezogener Daten für Zwecke des Liegenschaftskatasters regeln. Es bleibt bei der Einschätzung, daß Hamburg ein Gesetz für sein Kataster-(und Vermessungs-) wesen braucht, wie es alle anderen Bundesländer bereits haben.

Auch wenn die Regierungsparteien im Bund mit ihrem Vorhaben, das Bundesdatenschutzgesetz zu novellieren, erneut scheitern, sollte der Senat jetzt dem Vorbild der hessischen und der nordrhein-westfälischen Landesregierung folgen und eine Novellierung des Hamburgischen Datenschutzgesetzes einleiten. Auch in Hamburg kann nicht länger damit gewartet werden, den Geltungsbereich des Datenschutzgesetzes vom Dateibegriff loszulösen und die Beschränkung des Gesetzes auf bloß vier Phasen der Datenverarbeitung aufzugeben.

2. Entwicklung der Dienststelle

2.1 Personal

In meinem 3. TB (2.1.1, S. 5) hatte ich ausführlich über die personelle Situation in meiner Dienststelle berichtet. Der Senat hat im Stellenplan 1986 je eine neue Stelle des höheren und des gehobenen Dienstes für den Hamburgischen Datenschutzbeauftragten beantragt. Die Bürgerschaft, die ihre Beratungen über den Haushalt 1986 bei Redaktionsschluß noch nicht abgeschlossen hatte, wird diesem Antrag aller Voraussicht nach zustimmen. Hierfür bin ich sehr dankbar, weil es dadurch möglich wird, ein weiteres Referat zu bilden und den Aufgabenbereich jedes Mitarbeiters überschaubarer zu gestalten.

2.2 Eingaben

Bis zum 27.11.1985 gingen 240 Eingaben ein. Sie betrafen folgende Bereiche:

A Öffentlicher Bereich		
abgeschlossen		89
davon Sicherheitsbereich	20	
Gesundheits- und Sozialbereich	17	
übrige Bereiche	52	
nicht abgeschlossen		26
insgesamt		115
B Nicht-öffentlicher Bereich		
abgeschlossen		102
davon Versandhandel	5	
Versicherungen	13	
Kreditinstitute	10	
Sonstige des 3. Abschnitts	44	
Auskunfteien	30	
sonstige des 4. Abschnitts	–	
nicht abgeschlossen		23
insgesamt		125

2.3 Schwerpunkte der Tätigkeit meiner Dienststelle

Ich nehme diesen Bericht zum Anlaß, einmal in allgemeiner Form die verschiedenen Tätigkeitsfelder und -ebenen meiner Dienststelle zu skizzieren und dabei zu verdeutlichen, wo ich derzeitig die Schwerpunkte sehe und wo z.Z. die Hauptschwierigkeiten bei der Durchsetzung datenschutzrechtlicher Zielsetzungen in der Verwaltungspraxis liegen.

Allgemein kann ich die Arbeit meiner Dienststelle aufgliedern in beratende, kontrollierende und informierende Aktivitäten, die jeweils sowohl auf eigene Initiative erfolgen als auch außengesteuert sein können. Zur Beratung zähle ich etwa eigene rechtspolitische Initiativen, Stellungnahmen zu von der Verwaltung vorgelegten Gesetz-, Verordnungs- und Richtlinien-Entwürfen sowie die Bearbeitung von Anfragen, die Behörden, aber auch Bürger an mich richten. Die Kontrolltätigkeit besteht aus von mir veranlaßten Prüfungen einzelner Dienststellen sowie aus der Bearbeitung von Eingaben oder gezielten Hinweisen auf bestimmte Mißstände. Meine informierenden Tätigkeiten bestehen schließlich in der Mitwirkung an Schulungen, Ausbildungs- und Fortbildungsveranstaltungen für Behördenbedienstete, an Informations- und Diskussionsveranstaltungen, die Parteien, Verbände u.ä. Organisationen sowie – last not least – in der Herausgabe eigener Publikationen, wobei der Tätigkeitsbericht den größten Aufwand erfordert.

Die Effektivität der Aufgabenerfüllung des Datenschutzbeauftragten hängt nach meinen Erfahrungen zunächst davon ab, wieweit es mir gelingt, von außen kommende Anstöße zu bewältigen und auf eigener Initiative beruhende Aktivitäten in allen Tätigkeitsfeldern zu entwickeln. Es reicht also nicht aus, die Schaffung normativer Regelungen zu fordern und auf die Vorlage von Entwürfen zu warten, sondern ich muß eigene inhaltliche Impulse geben (vgl. 3. TB, 2.1.1, S. 5). Es reicht weiter nicht aus, nur den Mißständen nachzugehen, auf die Bürger und Bedienstete mich hinweisen, sondern ich muß selbst systematische Prüfungen einleiten (3. TB, a.a.O.). Und es reicht schließlich nicht, nur auf Einladungen zu warten, um auf gestellte Fragen Anworten zu geben, sondern ich muß selbst eine aktive Informationsarbeit betreiben, um das Interesse der Bürger an Datenschutzproblemen und das Bewußtsein der Verwaltung hierfür zu heben. Kurzum: Ohne umfassende eigene Aktivitäten wäre die Durchsetzung datenschutzrechtlicher Zielvorstellungen in der Verwaltung von Zufälligkeiten abhängig.

Es liegt auf der Hand, daß ich bei den knappen personellen Kapazitäten meiner Dienststelle Schwerpunkte setzen muß, um eigene Initiativen erfolgreich vorantreiben zu können. Diese Schwerpunkte lagen im Berichtszeitraum – stärker als in den Vorjahren – im rechtspolitischen Bereich. Dies beruht im wesentlichen auf zwei Gründen: Zum einen muß die Verwaltung immer wieder angestoßen werden, um die notwendigen Konsequenzen aus dem VZ-Urteil des Bundesverfassungsgerichts zu ziehen; sie muß bereichsspezifische Regelungen entwickeln, um ihren eigenen Handlungsrahmen zu verdeutlichen und dem Bürger den Umgang mit seinen Daten transparent zu machen. Des weiteren liegt es aber auch im Interesse einer effektiven Datenschutzkontrolle, möglichst rasch klare Regelungen für die einzelnen Verwaltungsbereiche zu schaffen, um unbestreitbare Kontrollmaßstäbe anwenden zu können. Bei systematischen Prüfungen habe ich in den letzten Jahren immer wieder die Erfahrung gemacht, daß klare Kontrollmaßstäbe fehlten und häufig ad-hoc mit großem Aufwand erst erarbeitet werden mußten (vgl. 4.9 und 4.13.2).

Diesen Schwierigkeiten Rechnung tragend, habe ich die Kräfte meiner Dienststelle schwerpunktmäßig darauf konzentriert, die Schaffung bereichsspezifischer Regelungen voranzutreiben. Über erste Ergebnisse habe ich nachstehend berichtet (insbesondere in den Bereichen Polizei, Verfassungsschutz, Justiz, Gesundheitswesen, Forschung). Ich hoffe, daß hier bald Fortschritte erzielt werden und ich bereichsspezifische Regelungen als Vorgaben erhalte, damit ich mich wieder schwerpunktmäßig meinen Kontrollfunktionen im engeren Sinne widmen kann.

2.4 Verhältnis zur Verwaltung

Ein weiteres Hauptproblem, das – neben den fehlenden konkreten Kontrollmaßstäben – die Umsetzung datenschutzrechtlicher Zielvorstellungen immer wieder schwierig macht, liegt darin, daß das Bewußtsein der Behörden für ihre eigene Verantwortlichkeit zur Sicherstellung des Datenschutzes (§ 16 HmbDSG) nach wie vor nicht so ausgeprägt ist, wie es aus der Sicht des Datenschutzes zu verlangen ist (vgl. 3. TB, 2.4., S. 8). Dies möchte ich an folgendem Beispiel verdeutlichen:

Im Berichtszeitraum habe ich bei allen meiner Kontrolle unterliegenden Behörden und sonstigen öffentlichen Stellen überprüft, wie die Führung der gem. § 16 Satz 2 Nr. 1 HmbDSG vorgeschriebenen Übersicht gehandhabt wird. Diese Übersicht soll den Behörden als Grundlage für die Sicherstellung des Datenschutzes im jeweiligen Geschäftsbereich dienen und muß – mindestens – Angaben enthalten über die Art der gespeicherten personenbezogenen Daten, über die Aufgaben, zu deren Erfüllung die Kenntnis der Daten erforderlich ist sowie über regelmäßige Empfänger von Daten.

Bei meiner Überprüfung habe ich festgestellt, daß die Übersicht bei den meisten Behörden lediglich schematisch in der Weise geführt wird, daß eine Durchschrift der gem. § 13 Abs. 4 HmbDSG erfolgten Anmeldungen zum Datenschutzregister gesammelt wird. Dies Verfahren mag zwar besonders rationell sein, zeigt aber gleichzeitig, daß diese Behörden sich ihrer Eigenverantwortlichkeit für die Sicherstellung des Datenschutzes in einer Weise zu entledigen suchen, die die Anforderungen des § 16 Satz 2 Nr. 1 HmbDSG – jedenfalls nach meiner Auffassung – nicht hinreichend erfüllt:

Während die Registermeldungen ist erster Linie Stellen außerhalb des Hauses – insbesondere den HmbDSB – und auch die Betroffenen informieren sollen, soll die interne Übersicht die Umsetzung des Datenschutzes innerhalb der speichernden Stelle gewährleisten. Es soll ein Überblick möglich werden über die gesamte Verarbeitung personenbezogener Daten.

Die Übersicht gem. § 16 Satz 2 Nr. 1 muß im Gegensatz zu den Registermeldungen nach § 13 auch sog. interne Dateien gem. § 1 Abs. 2 Satz 2 einbeziehen. Auch für interne Dateien gelten zumindest die Datensicherungspflichten nach § 8, z.T. darüber hinaus auch weitere bereichsspezifische Regelungen. Um die Einhaltung dieser Vorschriften sicherstellen zu können, darf auf die Aufnahme interner Dateien in die Dateienübersicht nicht verzichtet werden.

Die Übersicht darf sich – im Gegensatz zu den Registermeldungen – auch nicht auf die Datensammlungen beschränken, die dem Datenschutzgesetz unterliegen, sondern muß auch diejenigen enthalten, für die die sog. anderen Rechtsvorschriften gelten. Daher hat sie nicht nur Dateien, sondern z.B. auch Akten einzubeziehen. Dem § 16 ist nicht zu entnehmen, daß die verantwortlichen Stellen die Ausführung der anderen Rechtsvorschriften nur insoweit sicherzustellen haben, als sie auf in Dateien gespeicherte personenbezogene Daten anwendbar sind. Diese Verpflichtung ergibt sich im übrigen auch aus der uneingeschränkten, generellen Pflicht, die Rechtsmäßigkeit und Ordnungsmäßigkeit der Verwaltung zu gewährleisten.

Nach meiner Auffassung könnte die Übersicht die nachfolgend aufgeführten Funktionen erfüllen:

- Zulässigkeitsnachweis

  Anhand der Darstellung der Datenarten und der zugehörigen Aufgaben ist nachzuweisen, daß die Zulässigkeitsvoraussetzungen für jede Phase der Datenverarbeitung vorliegen und insbesondere die Daten nur von denen zur Kenntnis genommen werden, für die diese Kenntnis erforderlich ist.

- Auswahl von Sicherungsmaßnahmen

  Nur anhand des Nachweises über alle Standorte, Transportwege, Verarbeitungen und Zugriffsmöglichkeiten kann eine an den Datenarten und Zugänglichkeiten orientierte Risiko-Schwachstellen-Analyse durchgeführt und können die angemessenen Maßnahmen ausgewählt werden, um die Ausführung der Datenschutzvorschriften zu gewährleisten.

- Offenlegung von Verantwortlichkeiten

  Durch die Angaben des für die Datensammlung zuständigen Bearbeiters wird die Verantwortung sichtbar und damit überprüfbar gemacht.

- Verpflichtung und Schulung

  Der in der Übersicht nachgewiesene befugte Personenkreis ist auf das Datengeheimnis zu verpflichten und den Aufgaben entsprechend zu schulen. Der Nachweis des Standortes der Datenträger ermöglicht darüber hinaus die Feststellung der außerdem zu verpflichtenden Personen (z.B. Wartungstechniker, Reinigungsdienst).

- Wahrung der Rechte der Betroffenen

  Die Übersicht erleichtert die Erteilung von Auskünften an die Betroffenen, die Durchführung von Sperranträgen nach § 6 Abs. 1 Nr. 4 sowie von Berichtigungen und den Erlaß stellenspezifischer Regelungen zur sonstigen Sperrung und Löschung.

- Im Rahmen der Organisationskontrolle (Nr. 10 der Anlage zu § 8) ermöglicht die Übersicht es schließlich, Strukturen und Abläufe kritisch zu prüfen, ein umfassendes Konzept für Datenschutz und Datensicherung zu entwickeln und notwendige stellenspezifische Verfahrensregelungen einzuführen.

Meine Kritik und meine Vorschläge habe ich zunächst mit der Justizbehörde und dem Senatsamt für den Verwaltungsdienst erörtert. Dabei ergab sich, daß meine rechtliche Beurteilung (Verstoß gegen § 16 Abs. 2 Nr. 1) nicht akzeptiert wurde mit der Begründung, daß diese Regelung sich nach geltendem Recht angeblich weder auf Akten noch interne Dateien erstrecke. Übereinstimmung wurde jedoch darüber hergestellt, daß es notwendig ist, die Eigenverantwortlichkeit der Behörden stärker ins Bewußtsein des Bediensteten zu heben. Ferner bestand Einvernehmen, daß zumindest alle – auch die internen – Dateien mit personenbezogenen Daten zu erfassen und für jede dieser Dateien bestimmte Faktoren wie Standorte, Transportwege, Zugriffsberechtigungen, Rechtsgrundlagen aufzulisten sind. Auf dieser Grundlage sind Risiko-Schwachstellen-Analysen durchzuführen.

Das Senatsamt für den Verwaltungsdienst hat angekündigt, die Behörden mit einem Rundschreiben in geeigneter Weise auf die Probleme hinweisen zu wollen. Dies werde ich abwarten, bevor ich weitere Aktivitäten unternehme.

3. Beobachtung der automatisierten Datenverarbeitung (ADV)

3.1. IuK-Drucksache

Der Senat hat im Zusammenhang mit den Beratungen zum Haushalt 1986 Grundsätze für die Anwendung der neuen Informations- und Kommunikationstechnik in der Hamburger Verwaltung beschlossen, die ich wegen ihrer Bedeutung im Wortlaut wiedergebe:

Grundsätze für die künfige Anwendung der neuen IuK-Technik in der Hamburger Verwaltung

1. Die Chancen und Risiken, die der Einsatz neuer Informations- und Kommunikationstechnik in der Hamburger Verwaltung bietet, sollen aktiv gestaltet werden.
2. Die Hamburger Verwaltung soll in Zukunft die Gestaltungsmöglichkeiten der neuen IuK-Technik konsequent nutzen, um
   - im Interesse des Bürgers und zur Sicherung eines breiten Dienstleistungsangebotes die einzelne Aufgabe mit weniger Aufwand zu erfüllen und auf diese Weise die Verwaltung produktiver zu gestalten und zu rationalisieren sowie
   - die Kosten der Verwaltung und der Dienstleistungen der Stadt mit den Kostenstrukturen anderer Bundesländer und Großstädte wettbewerbsfähig zu erhalten.
   - neue Leistungen in politischen Schwerpunktbereichen (z.B. Umweltschutz) erbringen zu können.

- mit ihrer Umwelt, die die Technik gebraucht, kommunizieren zu können.

3. Beim Einsatz neuer IuK-Technik sind die qualitativen Grenzen zu wahren, die der Schutz des Bürgers, insbesondere der Datenschutz, gebietet. Der Fortentwicklung der Technik entsprechend sind diese Grenzen unter Mithilfe der dazu berufenen Institutionen, insbesondere des Datenschutzbeauftragten, stets neu zu beschreiben.

4. Auch aus Anlaß des Einsatzes neuer IuK-Technik in der Hamburger Verwaltung wird es keine Entlassungen aus dem Hamburger Staatsdienst geben.

   Allerdings werden teilweise bestehende Arbeitsplätze entfallen. Dies macht in gewissem Umfang auch einen Wechsel des Arbeitsplatzes erforderlich; hierbei sind insbesondere die Belange von Problemgruppen des Arbeitsmarktes und berufstätiger Frauen zu beachten. Durch gezielte und rechtzeitige Fortbildungs- und Umschulungsangebote soll verhindert werden, daß diese durch den Einsatz neuer IuK-Technik benachteiligt werden. Allgemein erfordern die Veränderungen am Arbeitsplatz, insbesondere die persönliche Anpassung bei einem Wechsel des Arbeitsplatzes, verstärkte Bemühungen um Fortbildung.

5. Der Einsatz neuer IuK-Technik ist so zu planen, daß

   - humane Arbeitsplätze geschaffen werden
   - die Umstellungsmaßnahmen den berechtigten Interessen der Mitarbeiterinnen und Mitarbeiter gerecht werden und dem Grundsatz der Förderung von Frauen im öffentlichen Dienst entsprechen
   - die Mitbestimmungsrechte gesichert bleiben
   - betroffene Personalräte, Mitarbeiterinnen und Mitarbeiter sowie die Bürger umfassend und rechtzeitig informiert werden.

   Soweit offene Fragen zur Folgenabschätzung des Einsatzes neuer IuK-Technik zu klären sind, sollen entsprechende Forschungsvorhaben, insbesondere des Bundes, unterstützt und in geeigneten Fällen die Begleitung Hamburger Projekte durch wissenschaftliche Forschung gefördert werden.

   Dabei soll insbesondere auch untersucht werden, durch welche Maßnahmen mögliche Benachteiligungen von Frauen verhindert und deren Berufschancen verbessert werden können.

6. Die Fähigkeit der Verwaltung, organisatorischen Wandel – unter Nutzung der neuen Informations- und Kommunikationstechnik und ausgerichtet an politisch gesetzten Zielen – zu bewältigen, muß gestärkt werden durch

   - eine Neuordnung der Verantwortungsbereiche im Sinne einer Dezentralisierung der Projektverantwortung bei gleichzeitiger qualitativer Stärkung der zentralen Steuerungsfunktionen,
   - Fortbildungs- und besondere Rekrutierungsmaßnahmen, um das notwendige Wissen auf allen Ebenen der Verwaltung zu vertiefen,
   - die Bereitstellung von personellen und finanziellen Mitteln, um den Einrichtungs- und Umstellungsaufwand abzudecken.

Die Grundsätze sind nach meiner Auffassung ein gelungener Kompromiß zwischen zwei Zielen: Einerseits die Vorteile der neuen Informations- und Kommunikationstechnik für die Steigerung der Leistungsfähigkeit der Verwaltung zu nutzen, anderseits aber die Interessen der Betroffenen – Bürger und Mitarbeiter – zu wahren. Die Grundsätze werden mir bei meiner weiteren Tätigkeit eine wichtige Hilfe sein.

Der Senat hat ferner beschlossen, die Organisation für die Anwendung neuer Informations- und Kommunikationstechnik neu zu ordnen. Ziel dieser Neuordnung sind die Dezentralisierung der Projektverantwortung und die gleichzeitige qualitative Stärkung der zentralen Steuerungsfunktionen. Dezentralisierung und Projektverantwortung bedeuten den Wegfall der bisherigen Einwirkungsrechte des Senatsamtes für den

Verwaltungsdienst bei den Projekten der Informations- und Kommunikationstechnik; die Behörden sind für ihre Projekte künftig allein verantwortlich. Das Senatsamt soll durch die Entlastung von der Projektverantwortung in den Stand versetzt werden, Richtlinien und methodische Vorgaben zu entwickeln, Aus- und Fortbildung auf dem Gebiet der Informations- und Kommunikationstechnik zu gewährleisten, zentrale Systeme vorzuhalten und die Projekte der Behörden zu koordinieren.

Die Projekte der Behörden sollen künftig über jährliche IuK-Pläne koordiniert werden, die Grundlage für die Bereitstellung der personellen und sächlichen Mittel für die Projekte sind. Nach meiner Auffassung können die IuK-Pläne eine wichtige Grundlage für meine Aufgabe sein, schon in der Entwicklungsphase auf den tätigen Datenschutz bei Informations- und Kommunikationstechnik hinzuwirken.

Der Beschlußfassung durch den Senat ist eine intensive Diskussion vorangegangen. Auch wenn die jetzige Fassung der Grundsätze meine Zustimmung findet, möchte ich einige kritische Anmerkungen hervorheben, die ich in der vorangegangenen Diskussion vorgebracht hatte.

- Die Verwaltung hat den verstärkten Einsatz der neuen Informations- und Kommunikationstechnik u.a. damit begründet, daß der Bürger einen bestimmten Standard an Verwaltungsleistungen erwartet, der nur durch den Einsatz dieser Technik erreichbar ist.

  Ich habe dem entgegengehalten, daß es sich dabei um eine einseitige Sicht der Dinge handelt; die Sorgen und Ängste vieler Bürger wegen der für sie undurchschaubaren Technik und ihren möglichen Folgen sind meistens gleichgewichtig. Erst beides zusammen ergibt ein vollständiges Bild von der Akzeptanz neuer Techniken. Zu einer staatlichen Automationspolitik gehört daher ein Konzept zur Herstellung der notwendigen Akzeptanz.

- Nach wie vor meinen einige Behörden offenbar, daß durch die Tätigkeit des Datenschutzbeauftragten und die Behandlung seiner Ergebnisse in der Verwaltung sowie in den zuständigen parlamentarischen Gremien ein ausreichender Datenschutz gewährleistet sei. Ich bin dieser Auffassung erneut entgegengetreten. Verantwortlich für die Einhaltung des Datenschutzes sind die Behörden selbst. Der Datenschutzbeauftragte hat zwar neben der Kontroll- auch eine Beratungsaufgabe; eine wirksame Beratung setzt jedoch voraus, daß die zuständigen Stellen sich mit den Problemen schon auseinandergesetzt haben.

  Bei jedem Automationsvorhaben besteht die Gelegenheit, aber auch die Notwendigkeit zu prüfen, ob den verfassungsrechtlichen Anforderungen entsprechende Rechtsgrundlagen vorhanden sind und ob der Umfang der Datenspeicherung und -verarbeitung, insbesondere der Übermittlungen, gerechtfertigt ist. Diese Prüfungen sind – um es zu wiederholen – Aufgabe der Verwaltung. Die Beteiligung des Datenschutzbeauftragten kann ihre datenschutzrechtliche Verantwortung nicht aufheben.

  Eine erhöhte Verantwortung trifft die Verwaltung beim zunehmenden Einsatz von personal computern. Auch wenn der Benutzer diese selbst programmiert, muß sichergestellt werden, daß er dabei die Grenzen der zulässigen Datenverarbeitung einhält. Schließlich erfordert die weitere Ausdehnung der dezentralen Datenverarbeitung (autonom oder als Datenfernverarbeitung) entsprechende Bemühungen um Datensicherung. Die Probleme, die die neue Entwicklung mit sich bringt, habe ich im 3. TB unter 4.7.1.2 und im vorliegenden TB unter 3.3 beschrieben. Zufriedenstellende Lösungsmöglichkeiten sind noch nicht aufgezeigt worden; entsprechende Ansätze werden diskutiert.

3.2 Bewertungen von on-line-Übermittlungen

Automatisierte Datenverarbeitung wird häufig mit großem Mißtrauen beobachtet, nicht zuletzt, weil sie in vielen Beziehungen als feindlich erfahren und weithin nicht verstanden wird (vgl. meinen 2. TB, 2.6.1). Gegenstand besonderen Mißtrauens ist die on-

line-Übermittlung. Bei der on-line-Übermittlung erhält eine Behörde, z.B. die Polizei, einen Anschluß an das automatisierte Verfahren einer anderen Behörde, z.B. des automatisierten Meldewesens der Einwohnerämter, und damit die Möglichkeit, Daten ohne Beteiligung der speichernden Stelle, in diesem Fall der Einwohnerämter, abzurufen. Dies war für mich Anlaß, die Problematik der on-line-Übermittlung grundsätzlich zu untersuchen.

Um die on-line-Übermittlung unter Datenschutzaspekten bewerten zu können, habe ich in zwei nachfolgenden Tabellen Arten der Datenweitergabe (u.a. die on-line-Übermittlung) nach Kriterien verglichen, die nach meiner Ansicht für die Bewertung wesentlich sind.

Die Tabellen zeigen kein einheitliches Ergebnis, etwa der Art, daß on-line-Übermittlungen unter Datenschutzaspekten stets besonders gefährlich sind.

Die on-line-Übermittlung hat auch aus der Sicht des Datenschutzes Vorteile:

- Möglichkeit der nachträglichen Prüfung der Zulässigkeit eines Abrufs aufgrund von Protokollierungen, auch wenn der Prüfung Grenzen gesetzt sind. Gerade bei einer hohen Zahl von Übermittlungen kann aber die automatisierte Datenverarbeitung eingesetzt werden, um trotz massenhafter Abrufe sinnvolle Kontrollen zu ermöglichen.
- Weitgehender Ausschluß der Möglichkeit, die Protokollierung – als Grundlage für die Zulässigkeitsprüfung – zu umgehen.
- Möglichkeit, den Umfang der Übermittlungen zu beschränken.

Diesen Vorteilen stehen Nachteile gegenüber:
- Schwierigkeit der Beurteilung des Grades der Datensicherheit;
- sehr großer Umfang möglicher Auswirkungen von Schwächen in der Datensicherung;
- geringer Aufwand für einen Datenabruf mit der möglichen Folge, daß Daten in großem Umfang abgerufen werden.

Dieses uneinheitliche Bild – das überdies in beträchtlichem Umfang von der tatsächlichen Gestaltung des automatisierten Verfahrens abhängt – verbietet jegliches pauschale Urteil über die on-line-Übermittlung. Vielmehr kann nur ein konkretes Verfahren der on-line-Übermittlung unter Datenschutzaspekten bewertet werden. Dafür empfiehlt sich folgendes Vorgehen:

- Verifizierung der Bewertungen in den Tabellen:
  Es muß für den konkreten Fall nachgeprüft werden, wie z.B. die maschinelle Protokollierung bei einer on-line-Übermittlung sichergestellt ist und welche Möglichkeiten bestehen, die Protokollierung zu umgehen.
- Bewertung:
  Die Bewertung einer konkreten Art der Übermittlung hängt von der Gewichtung ab, die sich wiederum nach der jeweiligen Aufgabe richtet. Mit Gewichtung ist hier gemeint, daß festgelegt wird, welche relative Bedeutung die einzelnen Vergleichskriterien für die Bewertung insgesamt haben. Danach kann anhand der verifizierten Bewertungen in den Tabellen entschieden werden, welche Übermittlungsart gewählt oder wie eine gewählte Übermittlungsart insgesamt beurteilt wird.

Die in den Tabellen zusammengefaßten Vergleichskriterien und Bewertungen basieren auf der Annahme, daß sich die Aufgabe oder die Art und Weise ihrer Erfüllung durch eine bestimmte Übermittlungsart nicht ändern, und berücksichtigen nicht explizit die Möglichkeit des Mißbrauchs. Gerade diese Argumente spielen in der Diskussion aber eine große Rolle.

- So wird z.B. vermutet, daß die anfordernde Stelle bei der Beurteilung der Erforderlichkeit für die Datenübermittlung leichter geneigt ist, die Erforderlichkeit zu bejahen als bei anderen, aufwendigeren Methoden, weil – wenn der on-line-Anschluß einmal eingerichtet ist – die on-line-Abfrage durch die anfordernde Stelle ohne großen Aufwand möglich ist.

Vergleichskriterien / Art der Datenweitergabe	Vorherige Prüfung der Übermittlungsvoraussetzungen ist möglich: durch die übermittelnde Stelle	durch Empfänger	Nachträgliche Prüfung der Zulässigkeit (tatsächlich u. rechtlich) ist möglich	Möglichkeiten, die Protokollierung zu umgehen	Möglichkeit, den Umfang der Übermittlung zu beschränken auf bestimmte: Datenfelder/ Datenarten	Datensätze/ Fälle	Entstehung zusätzlicher Informationen bei der speichernden Stelle	Durch die Technik bedingte Unsicherheit: Art des Fehlers/ Risikos	Eintrittswahrscheinlichkeit
mündlich, fernmündlich	ja Übermittlung muß angefordert werden. Bei Massengeschäften ist aber allenfalls Plausibilitätsprüfung möglich; u.U. wird nur die Authentifikation des Empfängers geprüft	ja	ja aber bei Massengeschäften praktisch nicht möglich, abhängig von der Zuverlässigkeit des Bearbeiters bei der Protokollierung	hoch angeordnete Aufzeichnungen werden – absichtlich oder versehentlich – unterlassen	ja weil Übermittlung nur durch bewußte Handlung		ja im Umfang der Protokollierung	Abhören Übertragungsfehler	selten hoch
schriftlich einschließlich TELEX			ja der Vorgang erzeugt Unterlagen	vorhanden Vorgänge verschwinden lassen				Abfangen Übertragungsfehler Verlust	selten selten selten
Datenträgeraustausch und off-line-Datenübertragung	ja, wenn von übermitt. Stelle veranlaßt. Wenn von anford. Stelle veranlaßt: Plausibilität, wenn Übermittl. begründet wird	nein, wenn von übermitt. Stelle veranlaßt; ja	ja weil maschinelle Protokollierung aber abhängig vom Umfang der Protokollierung	kaum Systemkenntnisse müssen vorhanden sein. Unterdrückung hinterläßt Spuren	ja weil der Umfang der Übermittlungen durch Programm festgelegt wird; bei der on-line-Datenübertragung kann der Zugriff auf Fälle durch Beschränkung der Suchkriterien begrenzt werden.			Verlust von Datenträgern Abhören	selten selten
Einsicht überwacht	ja aber Einschränkung wie bei mdl. Weitergabe	ja	ja aber Einschränkung wie bei mdl. Weitergabe	hoch s. mündlich	kaum	ja		keine (unmittelbare Aufnahme)	entfällt
Einsicht ohne Überwachung	nein	ja	nein	keine sinnvolle Protokollierung möglich	nein	nein	nein	s. oben	s. oben
on-line-Datenübertragung im Rahmen von Teilhabersystemen	nicht im Einzelfall (Ausnahme: Einzelfallprüfung möglich bei Abruf durch ein Programm, das zu der Prüfung in der Lage ist). Sonst: nur Prüfung, ob Zugriff im Rahmen der Berechtigung	ja	ja weil maschinelle Protokollierung, aber: vor allem beim Massengeschäft kaum möglich, weil keine ergänzenden Unterlagen, abhängig vom Umfang der Protokollierung; Problem der Bürokommunikation	wenn Protokollierung durch Systemroutinen: sehr gering, fast unwahrscheinlich Systemkenntnisse müssen vorhanden sein. Unterdrückung hinterläßt Spuren. Wenn Protokollierung der Lesezugriffe durch Anwendungsprogramme: ja, aber nicht im Einzelfall. Nachweis der generellen Ausschaltung ist abhängig von der Gestaltung	ja weil der Umfang der Übermittlung durch Programm festgelegt wird Begrenzung der Suchkriterien		ja im Umfang der Protokollierung (u.U. sensitive Datei)	Abhören Manupulationsmöglichkeiten bei komplexen Systemen	selten selten (Expertenwissen erforderlich) Wahrscheinlichkeit ist von den getroffenen Maßnahmen zur Datensicherung abhängig; außerdem unterschiedlich für Wähl- und Standleitungen

TABELLE 1

Vergleichskriterien / Art der Datenweitergabe	Grad der Datensicherheit von Dritten, insbesondere von Laien, beurteilbar	Wahrscheinlichkeit von Schwächen in der Datensicherung (praktische Erfahrungen)	Möglicher Umfang von Auswirkungen von Schwächen in der Datensicherung	Aufwand zur Abfrage von Einzelangaben		Möglichkeit einer Datenweitergabe in großen Umfang gegeben
				übermittl. Stelle	anfragende Stelle	
mündlich, fernmündlich	ja nach Schilderung der Organisation und Abwicklung	groß	groß	hoch	hoch	kaum
schriftlich einschl. TELEX		gering	gering	hoch	hoch	
Datenträgeraustausch und off-line-Datenübertragung	einigermaßen nach Schilderung der Organisation und Abwicklung		groß wegen der jeweils betroffenen Datenmengen	entfällt		ja
überwachte Einsicht	ja	sehr gering	gering	hoch	hoch	kaum
Einsicht ohne Überwachung		Wesentlicher Bestandteil der Datensicherung fehlt	sehr groß (Schwäche bekannt)	gering	hoch	ja
on-line-Datenübertragung im Rahmen von Teilhabersystemen	Ein Urteil ist dem Laien nicht möglich; der Fachmann ist erst nach aufwendiger Analyse zu einem Urteil in der Lage	groß	sehr groß Eine bestehende Schwäche kann möglicherweise über lange Zeit unerkannt bleiben; die Art der möglichen Auswirkungen ist auch bei Kenntnis des Systems kaum abschätzbar.	wenn eingerichtet: gering	gering	ja

TABELLE 2

- Ferner wird angenommen, daß bei den Bediensteten der anfordernden Stelle außerdem die „Hemmschwelle", zur Aufgabenerfüllung nicht erforderliche Daten on-line abzurufen, niedriger sein dürfte, als etwa bei der mündlichen oder schriftlichen Anfrage. Bei einem on-line-Abruf würde der Bedienstete zudem „nur" gegen eine Dienstanweisung verstoßen, in den anderen Fällen aber eine konkrete Person bewußt täuschen.

Diese Gesichtspunkte entziehen sich einer Bewertung in der hier gewählten Form. Ansätze für eine Berücksichtigung finden sich z.B. in den Vergleichskriterien „Aufwand für Abfrage" und „Möglichkeit, die Protokollierung zu umgehen". Gleichwohl spielen diese Gesichtspunkte eine große Rolle und müssen daher bei der Entscheidung berücksichtigt werden.

Dieses Ergebnis schließt generelle, d.h. alle on-line-Übermittlungen unterschiedslos treffende Regelungen aus. Vielmehr kann jede on-line-Übermittlung nur spezifisch nach ihrer Eigenart geregelt werden. Ich habe daher an anderer Stelle dieses Berichts (6.1) Vorschläge für eine entsprechende Novellierung des HmbDSG gemacht; Grundlage für die danach notwendige besondere rechtliche Regelung jeder konkreten on-line-Übermittlung können die Ergebnisse der oben beschriebenen Bewertung sein.

Auch die Vorschriften im BDSG für die Verarbeitung personenbezogener Daten durch Private müssen um Regelungen für on-line-Übermittlungen ergänzt werden. Die Regelungen sollten enthalten:

- Die Verpflichtung, verbindlich festzulegen, wer welche Daten für welche Zwecke abrufen darf.
- Die Verpflichtung zu angemessenen Maßnahmen der Sicherung und Kontrolle auch beim Empfänger, die insbesondere gewährleistet, daß die Daten nur für den zugelassenen Zweck abgerufen werden können und daß die Erforderlichkeit des Abrufs kontrolliert werden kann.

Die Vorschläge für zusätzliche Regelungen beschränken sich auf on-line-Übermittlungen. Für on-line-Systeme, die den Bereich einer speichernden Stelle nicht überschreiten und nur den Mitarbeitern Computerleistung am Arbeitsplatz zur Verfügung stellen, sehe ich keine Notwendigkeit für zusätzliche rechtliche Regelungen. Hier reicht es aus, durch technische und organisatorische Vorkehrungen sicherzustellen, daß jeder Mitarbeiter nur auf solche personenbezogenen Daten zugreifen kann, die für die Wahrnehmung der ihm übertragenen Aufgabe notwendig sind.

3.3 PC-Einsatz

Der PC, d.h. „Personal-Computer", „persönlicher Computer" oder „Arbeitsplatz-Computer", ist auf dem Vormarsch. Neuerdings ist auch in der hamburgischen Verwaltung – nach einer Phase der Konzentration auf automatisierte Verfahren zur Erledigung von „Massengeschäften" in einem zentralen Großrechenzentrum (der Datenverarbeitungszentrale bei der Finanzbehörde) – zunehmend eine Ausweitung der automatisierten Datenverarbeitung auch auf solche Verwaltungsaufgaben zu beobachten, die aus den verschiedensten Gründen für eine Lösung in Form eines zentralen ADV-Verfahrens nicht infrage kommen. PCs sind relativ preisgünstig und dennoch sehr leistungsstark. Sie ermöglichen in vielen Fällen eine kostengünstigere, schnellere und qualitativ bessere Aufgabenerfüllung, als dies mit herkömmlichen Mitteln möglich ist. Ihr Einsatz für eine bestimmte Verwaltungsaufgabe wird daher immer öfter von den jeweils fachlich zuständigen Stellen gefordert (z.B. von der OFD für die Personalplanung und -einsatzsteuerung, von der BfI für insgesamt sechs Aufgabenbereiche, u.a. auch für Personaleinsatzplanung). Zu einem verstärkten Einsatz von PCs wird es auch im Zuge der Realisierung des in der IuK-Drucksache zum Ausdruck gebrachten politischen Willens des Senats zur Modernisierung und Rationalisierung der Verwaltung kommen. In einigen Bereichen decken sich diese Zielvorstellungen des Senats mit den Wünschen der Mitarbeiter, während die jeweilige Behörde wegen der mit dem Einsatz verbundenen und noch nicht beherrschten Risiken diese Entwicklung noch

bremst: Z. B. im Bereich der Schulen, die PCs für den Informatikunterricht erhalten haben, wollen Lehrer diese Anlagen auch für schulinterne Verwaltungsaufgaben nutzen, wogegen die Behördenleitung den Einsatz für Verwaltungsaufgaben, bei denen personenbezogene Daten zu verarbeiten sind, nur sehr restriktiv zuläßt (s. dazu das Datenschutz-Info in MittBlSchul 1985 S. 36). In manchen Bereichen soll es Mitarbeiter geben, die sich ihre Arbeit nicht bloß mit einem einfachen Taschenrechner erleichtern wollen und die sogar schon privat angeschaffte PCs für ihre dienstlichen Aufgaben benutzen (dies wird u.a. von Lehrern und Mitarbeitern in der Steuerverwaltung behauptet).

Diese Entwicklung wird von manchen Beobachtern kritisch gesehen. Sie befürchten u.a., daß Arbeitsplätze wegrationalisiert werden könnten, daß die Arbeitsleistung und das Verhalten kontrollierbarer werden, daß Qualifikation bei den Mitarbeitern verloren gehen könnte, daß durch die Arbeit an den elektronischen Geräten gesundheitliche Schäden eintreten könnten. Auf diese soziologische Problematik will ich hier nicht eingehen. Ich beobachte die Ausweitung der dezentralen Datenverarbeitung, der individuellen DV des Sachbearbeiters vor Ort mit seinem persönlichen Computer in erster Linie unter dem Aspekt der damit verbundenen Risiken für Datensicherheit und Datenschutz.

Die Datenschutzgesetze verlangen von den Stellen, die personenbezogene Daten in automatisierten Dateien verarbeiten, die Erfüllung bestimmter Anforderungen (§§ 8, 16 HmbDSG, §§ 6, 15, 29 BDSG i.V.m. § 79 SGB X). Diese Anforderungen können jeweils nur erfüllt werden durch ein geschlossenes System aus technischen und organisatorischen Maßnahmen, das nicht nur die Einhaltung des Datenschutzes ermöglichen soll, sondern gleichzeitig auch geeignet ist, haushalts- und kassenrechtliche Sicherheit, Ordnungsmäßigkeit und Prüffähigkeit zu gewährleisten.

Für Großrechenzentren wie die DVZ sind mit erheblichem Aufwand Maßnahmen getroffen worden, die die unbefugte Nutzung des Systems und die Manipulation von Programmen und Datenbeständen verhindern. Für die physische Sicherheit ist weitestgehend gesorgt. Schließlich bietet die Entwicklung neuer automatisierter Verfahren nach den für ADV-Projekte vom Senatsamt vorgegebenen Regeln die Gewähr dafür, daß die betreffende Datenverarbeitung – jedenfalls grundsätzlich – rechtmäßig ist.

Tatsache ist nun, daß die „kleinen" PCs selbständig programmierbare Rechner sind mit eigenem Betriebssystem und autonomer Dateiverwaltung, die im Prinzip ebenso leistungsfähig sind wie die Großrechner, wenn auch nicht so schnell und so elegant. Es müßte daher der Standard, der aus Gründen der Sicherheit und Ordnungsmäßigkeit für Großrechenanlagen inzwischen als notwendig anerkannt ist, auch für PCs gefordert werden. Diese an sich naheliegende Forderung stößt aber u.a. auf folgende Einwände:

1. Bei der bisherigen Art der Aufgabenerfüllung (manuell mit Akten, Karteien, Listen usw.) wurden solche Anforderungen nicht gestellt. Worin liegt das „neue Risiko", wenn man bedenkt, daß derselbe Sachbearbeiter dieselbe Aufgabe mit denselben Daten wahrnimmt, nur eben nicht mehr nach „Altväterart", sondern per PC?
2. Ein solcher Aufwand würde die Vorteile (Kostengünstigkeit, Schnelligkeit bei der Entwicklung und Pflege des Verfahrens, Flexibilität) einschränken oder ganz zunichte machen.
3. Die im Handel erhältlichen Betriebssysteme für PC unterstützen bisher nicht die Anwendung der bei Großrechnern üblichen automatisierten Kontrollen.

Dem ersten Einwand halte ich folgendes entgegen: Das neue Risiko besteht darin, daß ein ehemals in Akten, Karteien, Listen usw. verstreuter, möglicherweise nicht oder wenig geordneter, unstrukturierter Datenbestand nunmehr in „handlicher" und verarbeitungsgerechter Form, nämlich als Datei auf einem kleinen magnetisierten Datenträger (Diskette, Cassette), vorhanden ist. In dieser Form lassen die Daten sich automatisiert verwerten, d.h. effizienter und extensiver, als es bei der alten Speicherungs-

form möglich war. Was bei der alten Speicherungsform schon allein aus zeitlichen und personellen Gründen nicht machbar war, ist mit einem automatisierten Datenbestand und einem kleinen Programm mit Hilfe des PC schnell zu realisieren. Die unter diesen Umständen mögliche Verarbeitung kann – als eigentlich schon immer zweckmäßig – wünschenswert sein und eine Verbesserung darstellen. Sie kann aber auch zu unerwünschter übermäßiger Nutzung durch die Verwaltung führen. Schließlich eröffnet sie die Möglichkeit zu mißbräuchlicher Verarbeitung, die zwar theoretisch schon immer bestanden haben mag, die aber erst durch die einfache Realisierbarkeit, durch das bessere Verhältnis von Arbeitsaufwand zu möglichem Ertrag, lohnend werden kann. Deshalb kann nicht ausgeschlossen werden, daß die neue Form der Datenhaltung sowohl Verwaltungsangehörige als auch Außenstehende zum Mißbrauch verlocken könnte.

Die beiden anderen Einwände sind beachtlich. Diese Feststellung bedeutet aber nicht, daß auf Datenschutz- und Datensicherungsmaßnahmen beim Einsatz von PCs verzichtet werden kann; vielmehr bedeutet sie, daß eine Lösung zu suchen ist, die die Anforderungen des Datenschutzes und der Datensicherheit mit denen der Wirtschaftlichkeit und der Flexibilität des PC-Einsatzes zu einem angemessenen Ausgleich bringt.

Im Kreis der Datenschutzbeauftragten sind die mit dem PC-Einsatz verbundenen Probleme schon vor einiger Zeit analysiert worden; es sind auch Lösungen erarbeitet worden (z.B. „Materialien zum Datenschutz" des Berliner Datenschutzbeauftragten, Nr. 4: Grundsätze für die organisatorischen und technischen Maßnahmen beim Einsatz isolierter ADV-Systeme). Einige große private DV-Anwender haben Lösungen für ihren eigenen praktischen Bedarf entwickelt. Die wissenschaftliche Auseinandersetzung mit dem Thema nimmt einigen Raum in der DV-Fachliteratur ein. Nunmehr hat auch das Senatsamt für den Verwaltungsdienst im Berichtsjahr begonnen, sich um das Problem zu kümmern. Die jeweiligen Lösungen – Merkblätter, Mindestanforderungen, Grundsätze für den Einsatz von Personal-Computern – sind auf die spezifischen Belange im Anwendungsbereich zugeschnitten. Für die öffentliche Verwaltung gelten z.T. andere Maßstäbe als in einem privatwirtschaftlichen Betrieb. Ich begrüße daher die Absicht des Senatsamtes, für den Einsatz isolierter ADV-Systeme (private und dienstliche PCs) in der hamburgischen Verwaltung eine eigene generelle Regelung vorzulegen. Eine Regelung in Form einer verbindlichen Verwaltungsvorschrift (wie die DS-Rahmenregelungen, die DS-Richtlinie, die Dokumentations- und die Freigaberichtlinie) würde ich einer Zusammenstellung von „Hinweisen", die nur als Handreichung zu sehen und deren Einhaltung in das Belieben der Anwender gestellt wäre, vorziehen.

Neben den Bestrebungen nach grundsätzlichen Vorgaben für den PC-Einsatz in der Verwaltung ist im Interesse aller PC-Benutzer darauf hinzuwirken, daß für PCs Betriebssoftware entwickelt wird, die möglichst das an Datensicherheit gewährleistet, was bei Betriebssystemen für Großrechner bereits zum Stand der Technik gehört.

Inzwischen werden am Markt Betriebssysteme mit entsprechenden Sicherungskomponenten sowie Datensicherungs-Module für Betriebssysteme, die noch keine Sicherungskomponenten haben, angeboten.

3.4 Datenschutz versus Datensicherung

Mit dem Staatsvertrag über Bildschirmtext (StV-Btx) ist erstmalig eine Regelung geschaffen worden, die u.a. Datenschutz und Datensicherung bei Neuen Medien gewährleisten soll. Der Staatsvertrag war Vorbild für Gesetze, die die Nutzung anderer Medien regeln, z.B. auch das Hamburgische Mediengesetz. Die bisher mit dem Bildschirmtextsystem gesammelten Erfahrungen geben Veranlassung, auf ein bisher nicht genügend wahrgenommenes grundsätzliches Problem hinzuweisen: Den Konflikt zwischen Datenschutz und Datensicherung.

Dieser Widerspruch ist auch schon in anderen Zusammenhängen aufgetreten, insbesondere bei der Verpflichtung zur Protokollierung in automatisierten Systemen, z.B.

der Zugriffe auf Auskunftssysteme (Benutzer- und Zugriffskontrolle) oder der Veränderungen von Datenbeständen in Dialogsystemen (Eingabekontrolle). Diese für Kontrollzwecke notwendigen und durch die Anlage zu § 6 BDSG in bestimmten Fällen vorgeschriebenen Protokollierungen führen zu neuen Dateien mit gelegentlich sehr sensitivem Inhalt, etwa bei der Protokollierung der Lesezugriffe auf polizeiliche Auskunftssysteme, oder zu Dateien, die die Überwachung der Leistung und des Verhaltens der betroffenen Mitarbeiter ermöglichen. Dieser Widerspruch muß durch Verwertungsverbote gelöst werden.

Bei Btx ist nach dem Wortlaut des StV-Btx schon fraglich, ob die Speicherung von Daten zu Sicherungszwecken zulässig ist. Der StV-Btx ist – aus einleuchtenden Gründen, die ich im 2. TB (S. 22 ff.) ausführlich dargestellt habe – auf einen möglichst vollkommenen Persönlichkeitsschutz angelegt. Dabei ist jedoch die Auswirkung auf Maßnahmen, die diesen Persönlichkeitsschutz sichern sollen, nicht in das Blickfeld geraten. Diese Auswirkungen sind erst später, bei der intensiven Diskussion von Detailfragen erkannt worden. Folgende Beispiele sollen diese Erfahrung veranschaulichen:

1) Bei jeder Verbindung wird auf der Begrüßungsseite – d.h. nach Identifizierung (durch Übermittlung der Hard- oder Softwarekennung) und Authentifizierung (durch Eingabe des persönlichen Kennworts) des Benutzers – angezeigt, bis wann Btx von dem Anschluß aus zuletzt genutzt wurde. Anhand von (handschriftlichen) Aufzeichnungen kann der Anschlußinhaber prüfen, ob in der Zwischenzeit ein Unberechtigter den Anschluß benutzt hat; auf andere Weise kann dies nicht festgestellt werden. Art. 9 Abs. 3 Satz 4 StV-Btx schreibt vor, Verbindungsdaten – und darum handelt es sich bei der Angabe des Zeitpunktes der letzten Benutzung – nach dem Ende der jeweiligen Verbindung zu löschen. Die Speicherung und Anzeige des Zeitpunktes der Beendigung der letzten Verbindung ist zulässig, wenn man diese Angabe nicht als Verbindungsdatum ansieht – wie dies die Deutsche Bundespost tut, die den Staatsvertrag konsequenterweise insoweit für lückenhaft hält – oder aber davon ausgeht, daß – jedenfalls für Sicherungszwecke – die letzte Verbindung erst beendet ist, wenn die nächste Verbindung aufgebaut wird. Ich halte es für dringend notwendig, dies bei nächster Gelegenheit im Staatsvertrag klarzustellen, damit eine eindeutige Rechtsgrundlage für Speicherungen zu Sicherungszwecken besteht.

2) Um die Ausforschung durch systematisches Ausprobieren zu verhindern, läßt das System für die Eingabe des persönlichen Kennworts pro Verbindungsaufbau und pro Tag eine bestimmte Anzahl von Fehlversuchen zu. Danach ist der Anschluß gesperrt. Damit diese Sperre wirksam werden kann, muß gespeichert werden, daß der Aufbau einer Verbindung versucht worden ist, daß aber diese Verbindung wegen Überschreitung der zulässigen Zahl von Versuchen, das persönliche Kennwort einzugeben, nicht zustande gekommen ist.

Bei strenger Auslegung des StV-Btx könnte man meinen, daß dies keine Verbindungsdaten sind, weil der Staatsvertrag nur erfolgreich aufgebaute Verbindungen kennt. Nach den Intentionen des Staatsvertrages müßten sie aber wie Verbindungsdaten behandelt werden, dann aber nach Beendigung des Versuchs, die Verbindung aufzubauen, gelöscht werden. Es stellt sich damit das gleiche Problem wie in dem unter 1) behandelten Fall.

3) Nach Art. 9 Abs. 6 Satz 1 StV-Btx darf ein Anbieter vom Teilnehmer personenbezogene Daten nur abfragen, soweit dies für das Erbringen der Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses erforderlich ist. Bei den Btx-Angeboten des Versandhandels besteht häufig die Möglichkeit, den Bestelldienst nur unter Angabe der Kundennummer in Anspruch zu nehmen; das Programm des Anbieters fügt die sonstigen Daten des Teilnehmers (Name, Anschrift) hinzu. Diese Möglichkeit ist von Hackern dazu genutzt worden, durch (systematisches) Probieren von Kundennummern an die Daten anderer Teilnehmer zu gelangen. Auch wenn aus dieser unberechtigten Kenntnisnahme in den meisten Fällen keine gravierenden Folgen entstehen können, insbesondere ein Vermögensschaden unwahrscheinlich ist, sollte doch die Möglichkeit bestehen, durch Datensicherungsmaßnahmen das Treiben der Hacker zu

unterbinden. Andererseits sollte aber auch der Service des Versandhandels aufrechterhalten werden.

Die Praxis hat gezeigt, daß der Bestelldienst mit bloßer Angabe der Kundennummer in Anspruch genommen werden kann, daß also – bei strenger Auslegung des Staatsvertrages – die Erhebung weiterer Daten für das Erbringen der Leistung (Zurverfügungstellung des Bestellservices) und das Abschließen eines Vertrages (Bestellung) nicht erforderlich ist. Dem Treiben der Hacker im Bestellservice könnte aber nur dadurch ein Ende gesetzt werden, daß die Deutsche Bundespost als Betreiber des Btx-Systems in die Angebotsseite, mit der die Kundennummer erfragt wird, den Namen und die Teilnehmer-Nummer des Teilnehmers einspiegelt, von dessen Anschluß aus das Angebot in Anspruch genommen wird. Damit wird die Anonymität der Benutzung aufgehoben, die bis dahin die Hacker ausgenutzt haben. Ich meine, daß diese Lösung mit Art. 9 Abs. 6 Satz 1 StV-Btx vereinbar ist. Erforderlich i.S. dieser Bestimmung ist die vollständige Identifikation, wobei ein Teil der Identifikationsdaten von der Post eingespiegelt und vom Teilnehmer durch eine eigene bewußte Entscheidung übermittelt wird.

Ich halte es für notwendig, bei allen künftigen Regelungen, die einen umfassenden Persönlichkeitsschutz gewährleisten sollen, auch die Datensicherung im Auge zu haben. Datensicherung verlangt häufig die Erhebung und Speicherung von personenbezogenen Daten, die aus der Sicht eines engen Persönlichkeitsschutzes nicht als erforderlich erscheinen.

3.5 Datensicherung in der öffentlichen Diskussion

Solange automatisierte Datenverarbeitung im wesentlichen in Rechenzentren unter der Regie von Spezialisten ablief und die Mehrheit der Bevölkerung keine klaren Vorstellungen von den Bedingungen und Möglichkeiten der EDV-Technik hatte, geschweige denn in der Lage war, sich dieser Technik selbst zu bedienen, setzten sich mit Problemen der Datensicherung nur Fachleute auseinander. Datensicherung diente anfangs nur dem Ziel, einen reibungslosen und wirtschaftlichen Betrieb zu ermöglichen. Bald schon wurde deutlich, daß sie auch notwendig ist zur Abwehr von Angriffen auf die DV-Anlagen, zur Verhinderung der unberechtigten Nutzung von Anlagen und Programmen sowie gegen finanzielle Manipulationen. Insofern war Datensicherung nun auch gegen dolose Handlungen der eigenen Mitarbeiter (Insider) sowie gegen Saboteure und Terroristen gerichtet. Seit Inkrafttreten der Datenschutzgesetze (§ 6 BDSG, § 8 HmbDSG) ist Datensicherung zum unabdingbaren Bestandteil des Datenschutzes geworden; sie wird nunmehr umfassend verstanden als die Summe aller technischen und organisatorischen Maßnahmen, die

- den störungsfreien Betrieb ermöglichen und
- jede denkbare unberechtigte Nutzung der DV-Anlagen und der Software verhindern.

Hinsichtlich der Datensicherung stimmen die Interessen der Rechenzentrumsbetreiber und die von den Datenschutzkontrollinstanzen vertretenen Belange überein. Es ist daher nicht verwunderlich, daß die Zusammenarbeit auf diesem Sektor ausgesprochen gut ist.

Inzwischen ist festzustellen, daß sich das Umfeld der elektronischen Datenverarbeitung grundlegend verändert hat:

Seit Home-Computer und Personal-Computer immer weitere Verbreitung gefunden haben, bereits den Schulkindern im Unterricht der Umgang mit Computern und Programmierkenntnisse vermittelt werden, hat sich das Wissen auf dem Gebiet der Datenverarbeitung ausgebreitet. Btx, home-banking, Geldautomaten, POS-Kassen sind eingeführt oder ihre Einführung steht unmittelbar bevor. Hinzu kommt die Preisentwicklung für Geräte und Software, die DV-Technik für private Nutzung erschwinglich werden läßt. Insgesamt haben die Bemühungen um eine (aus Benutzersicht) immer einfachere Mensch-Maschine-Kommunikation letztlich das Ziel, jedem den Zugang zur Datenverarbeitung zu eröffnen.

Wenngleich die breite Masse der Bevölkerung auch in Zukunft nicht in der Lage sein wird, fundierte Kenntnisse über die Technik und Logik der Systeme zu erlangen, so wird sich doch der Kreis derjenigen, die mit den Systemen und ihren Komponenten „umgehen" können, ständig erweitern und damit wird sich auch die Zahl der möglichen „Angreifer" auf die Systeme erhöhen. Schließlich wird die Zunahme der Datenverarbeitungssysteme und insbesondere die Ausbreitung der Datenfernverarbeitung die „Angriffsfläche" erheblich vergrößern. Ich möchte dies am Beispiel des Autos veranschaulichen: Zwar können nur wenige ein Auto entwerfen (und damit in allen einzelnen Funktionen beherrschen); noch relativ wenige können ein Auto nach vorgegebenen Plänen bauen; etliche sind in der Lage, ein Auto zu reparieren, Teile auszutauschen, einzelne Komponenten nach ihrem Geschmack zu verändern(z.B. den Motor „frisieren"). Aber unübersehbar ist die Masse der Autobesitzer und gar der Führerscheinbesitzer, die ein Auto fahren (benutzen) können und die dabei – absichtlich oder unabsichtlich – gegen Vorschriften verstoßen oder gar strafbare Handlungen begehen können. Das Beispiel ist auf die Informations- und Kommunikationstechnik übertragbar. Wie anfangs nur wenige Personen ein Auto fahren konnten, gab es am Anfang der DV-Entwicklung nur wenige, die die neue Technik beherrschten. So wie jetzt fast jeder erwachsene Bundesbürger seinen Führerschein hat, wird bald jeder Grundkenntnisse der DV haben und vor allem die Bedienung von DV-Geräten beherrschen.

Inzwischen ist Datensicherung zum öffentlich diskutierten Thema geworden, auch die Medien haben sich seiner bemächtigt. Nach meiner Beobachtung gelangte Datensicherung erstmals im Zusammenhang mit dem Verfahren über die Verfassungsbeschwerden gegen die Volkszählung 1983 in das Bewußtsein der Bürger. In der öffentlichen Anhörung vor dem Bundesverfassungsgericht gab es Sachverständige, die die Datensicherung in staatlichen Rechenzentren kritisierten, die das „Eindringen" Unbefugter in die Systeme für relativ leicht realisierbar erklärten und die nicht nur das „Anzapfen" der Dateien mit den statistischen Daten aus der Volkszählung, sondern auch deren Deanonymisierung für leicht machbar erklärten. Spektakulär wurde der Hamburger Hackerfall (s. 4.1.1.3) präsentiert. Es gab im ganzen Land kein Medium das diesen Fall nicht aufgegriffen hätte. Schließlich wurde Datensicherung im Zusammenhang mit Geldausgabeautomaten und ec-Karten „ein heißes Eisen", das in einigen Fernsehsendungen behandelt wurde.

Diese Publizität des Themas Datensicherung begrüße ich ausdrücklich; sie ist notwendig, um Datensicherheit zu erreichen. Ich habe Erkenntnisse darüber, daß selbst professionelle Anwender der Informations- und Kommunikationstechniken (Programmierer, Techniker, Vertriebs- und Vorführkräfte, Agenturen, die Unterstützung bei EDV-Anwendungen verkaufen) in der täglichen Routine die installierten Sicherungen schon mal außer Kraft setzen bzw. leerlaufen lassen (z.B. werden Warnmeldungen des Systems mit „IGNORE" übergangen, als Paßwort – etwa für den Aufbau einer Btx-Verbindung – die eigene Telefonnummer = Teilnehmernummer oder die Bezeichnung der eigenen Person/Firma/Behörde gewählt; oder es wird ganz einfach eine Tür mit automatischer Schließvorrichtung, die den unkontrollierten Zutritt zu Rechenanlagen verhindern soll, durch Arretierung am Schließen gehindert). Daß Nichtfachleute Sicherungsmaßnahmen wirkungslos machen (Beispiel: Die PIN wird auf die ec-Karte geschrieben), liegt meist daran, daß sie sich weder über das abzuwehrende Risiko noch über die Wirkungsweise der Sicherungsmaßnahmen im klaren sind. Aufklärung und Sensibilisierung sind nötig, um Abhilfe zu schaffen.

Mit meinen Mitteln – z.B. mit Beiträgen in meinen Tätigkeitsberichten („Beobachtung der ADV") – versuche ich, zur Aufklärung der Bürger beizutragen. Bei meinen Prüfungen und Beratungen weise ich auf Datensicherungsrisiken hin, mache Verbesserungsvorschläge und versuche ganz allgemein die datenverarbeitenden Stellen zu sensibilisieren. Ich erreiche natürlich nur einen begrenzten Empfängerkreis. Die weitere Verbreitung von Informationen kann nur von der Presse, dem Rundfunk, dem Fernsehen geleistet werden. Zwar leiden viele Berichte über Datensicherungsprobleme in den Medien darunter, daß sie nicht von DV-Fachleuten produziert werden. Es

wird, – manchmal auch in wesentlichen Punkten –, ungenau oder mißverständlich berichtet; häufig werden auch die Gefahren übertrieben. Selbstverständlich gehe ich allen Hinweisen auf Sicherheitsmängel nach. Gelegentlich bekomme ich aus Veröffentlichungen der Medien auch Hinweise auf mir noch nicht bekannte Risiken.

An der öffentlichen Diskussion über Defizite der Datensicherung, speziell auch in der Hamburger Verwaltung, haben sich auch Fachleute beteiligt und damit nicht nur die Öffentlichkeit beunruhigt, sondern auch mich zu eingehenden Untersuchungen veranlaßt.

Ich möchte mich an dieser Stelle mit folgenden Vorwürfen auseinandersetzen:

(1) Die Datenverarbeitungszentrale bei der Finanzbehörde (DVZ) sei schlecht gesichert. Jedem Informatikstudenten sei es möglich, in die Systeme einzudringen.

(2) Die Reidentifizierung jeder Person, deren Daten im Mikrozensus erhoben worden sind, sei technisch möglich, selbst wenn der Name, die Anschrift, die Gemeinde, das Land und der Beruf nicht zur Verfügung stünden.

(3) Diese Möglichkeit sei gerade in Hamburg sehr wohl gegeben, denn fast unbemerkt von einer großen Öffentlichkeit sei der Polizei-Rechnerkomplex inzwischen zu einem einzigen Daten-Pool geworden, wo das polizeiliche Informationssystem POLAS ebenso wie alle Daten über Hamburgs Studenten und den öffentlichen Dienst unter einem Daten-Fach vereint seien, und es würden auch die bisher dezentralen Einwohnerdaten eingespeichert.

Den ersten Vorwurf habe ich bei meiner Prüfung der DVZ nicht bestätigt gefunden (s. 3.6). Nach meinen Feststellungen bestehen in der DVZ keine Sicherheitsmängel. Das Senatsamt für den Verwaltungsdienst hatte schon vor einigen Jahren auf die Vorwürfe u.a. mit dem Angebot reagiert, einen genehmigten und überwachten Test zu ermöglichen, in dem der Beweis dafür erbracht werden sollte, daß Eindringversuche gelingen würden. Die „Herausforderer" haben dieses Angebot jedoch leider nicht angenommen, so daß die Behauptung nicht erhärtet wurde.

Zu dem zweiten Vorwurf ist folgendes zu sagen: Es wird unter Praktikern aus der Statistik und Informatikern eine Diskussion auf hoher Abstraktionsebene darüber geführt, welche Merkmale wenigstens vorhanden sein müssen, um eine Deanonymisierung bei noch vertretbarem Aufwand durchführen zu können. Es gibt Informatiker, die eine Deanoymisierung unter Ausschluß der o.g. Identifikationsmerkmale nicht nur für theoretisch möglich, sondern für relativ leicht machbar halten. Praktiker halten dies für ausgeschlossen. Für mich ist das ein akademischer Streit. Erkenntnisse für meine Arbeit hätte das von mir angebotene Experiment bringen können, mit Genehmigung der zuständigen Stellen unter meiner Aufsicht die These praktisch unter Beweis zu stellen. Das Angebot wurde nicht beantwortet.

Die mit dem dritten Vorwurf kritisierten „besonderen Verhältnisse" in der DVZ sind durch Organisation und technische Vorkehrungen derart geregelt, daß ich bei meiner Prüfung (s. 3.6) zu der Feststellung gekommen bin, die sich aus der Anlage zu § 8 HmbDSG ergebenden Sicherheitsanforderungen sind erfüllt. Zu den besonderen Verhältnissen im einzelnen:

Es ist nicht richtig, daß Daten des Statistischen Landesamtes und der Polizei auf derselben Rechnergruppe verarbeitet werden.

Hierzu zunächst eine Vorbemerkung: Für den Betrieb der Rechner in der DVZ erstellt das Senatsamt für den Verwaltungsdienst unter Beteiligung der DVZ jeweils ein „Betriebsmodell", das bei Bedarf (z.B. bei Veränderungen der Maschinenausstattung) fortgeschrieben wird. Das jeweilige Betriebsmodell wird im wesentlichen von den Faktoren Kapazitätsbedarf, Arbeitsbedingungen in der DVZ und Datensicherung bestimmt. Die DVZ ist als Stelle, die Datenverarbeitung im Auftrag betreibt, für Umsetzung und Durchführung des Betriebsmodells verantwortlich. Die zum Senatsamt gehörende Systemprogrammierung implementiert die erforderlichen Betriebssysteme entsprechend dem jeweiligen Betriebsmodell. Die Anwender (Behörden der

hamburgischen Verwaltung) als Auftraggeber der DVZ gestalten ihre Verfahren entsprechend dem Betriebsmodell, d.h., ihre Programme sind so programmiert, daß sie auf der Hardware und unter der Software ablauffähig sind, die nach dem Betriebsmodell der jeweiligen Fachbehörde zur Verfügung stehen. Programme, die z.B. für die Verarbeitung auf Siemens-Rechnern unter dem Betriebssystem BS 1000 konzipiert sind, können nicht unter dem Betriebssystem BS 2000 ablaufen, schon gar nicht können sie auf IBM-Anlagen unter dem Betriebssystem MVS ablaufen. Umgekehrt laufen für IBM/MVS angelegte Verfahren nicht auf Siemens-Anlagen unter BS 1000/BS 2000.

Die Anwender gestalten ihre Verfahren i.ü. entsprechend den Anforderungen der zu lösenden Fachaufgabe als Stapelverfahren oder als Dialogverfahren. Auf Dateien von Dialogverfahren kann während der Betriebszeiten von den Berechtigten zugegriffen werden, sie sind „resident". Dateien von Stapelverarbeitungen sind nur dann in der Anlage, wenn die geplante Verarbeitung (im Batch-Betrieb) gerade läuft. Von außen kann auf solche Dateien nicht zugegriffen werden. Auch ist der Zeitpunkt ihrer Verarbeitung – und nur dann befinden sich die Daten „in der Maschine" – auch Insidern gewöhnlich nicht bekannt.

Nun aber konkret zu dem Vorwurf:

Die gesamte Datenverarbeitung des Statistischen Landesamtes läuft im IBM-Bereich ab, die Datenverarbeitung der Polizei dagegen ausschließlich im Siemens-Bereich. Die Anwendungen erfolgen mithin nicht auf derselben Rechnergruppe. Sie sind in der gegenwärtigen Form auch gar nicht geeignet, auf derselben Anlage abzulaufen, weil die Systeme nicht kompatibel sind. Die Programme müßten also jeweils für das andere Rechnersystem umgestellt werden, was erfahrungsgemäß Monate, wenn nicht Jahre in Anspruch nehmen würde. Die Daten des Statistischen Landesamtes werden im übrigen ausschließlich im Stapelbetrieb verarbeitet und stehen auch deshalb nicht für den Zugriff über Datenfernverarbeitungsleitungen der Polizei zur Verfügung.

Es ist auch nicht richtig, daß die Polizei auf Daten der Studenten zugreifen kann.

Heute läuft die Datenverarbeitung der Universität – insbesondere das SOS-Verfahren (Studenten-Operations-System) – bis auf geringe Restanten nicht mehr im Siemens-, sondern im IBM-Bereich.

Früher wurden zwar beide Anwendungen auf einer Siemens-Anlage unter BS 1000 abgewickelt, jedoch konnte auch damals aus dem Polizei-Bereich nicht auf die Dateien der Universität zugegriffen werden:

(1) Die Uni-Dateien waren nicht resident, sondern nur temporär für den Batch-Betrieb im System erreichbar. Der Polizei waren die Verarbeitungszeiten der Dateien der Universität gar nicht bekannt.

(2) Die – sorgfältig getesteten, freigegebenen und vor Manipulationen geschützten – Programme der Polizei enthalten keine Komponenten, die einen Zugriff auf Daten anderer Anwendungen vorsehen oder ermöglichen. Anwender des Polizeiverfahrens (Polizeibeamte in den Revierwachen über Terminals/Datenfernverarbeitung) konnten daher nur die Daten abfragen, die ihnen das Polizeisystem zur Verfügung stellt, also nicht die Daten der Uni.

(3) Das von der Systemprogrammierung (zum Senatsamt für den Verwaltungsdienst gehörend) generierte Betriebssystem verhinderte versehentliche Übergriffe von einer Anwendung auf die andere. Zwar muß eingeräumt werden, daß das Betriebssystem BS 1000 nicht genügend Sicherheit bietet gegen absichtliche Übergriffe durch Personen mit Systemprogrammierkenntnissen und -befugnissen, doch wurde diesem Mangel durch organisatorische Maßnahmen begegnet (Funktionstrennung zwischen Systemprogrammierung, Programmierung der Polizeiverfahren, Programmierung der Uni-Verfahren, Operating und Archiv; physisch getrennte Anlagen für Programmentwicklung/Test und Produktion; Freigabeverfahren für die in der Produktion eingesetzten Programme und deren Schutz gegen Veränderungen). Gleichwohl wäre als Ergänzung zum BS 1000 die Einführung von Siche-

rungssoftware auch in diesem Bereich unumgänglich geworden, wenn nicht die Änderung des Betriebsmodells (Umstellung der Siemens-Anwendungen – außer Polizei – vom BS 1000 – Bereich auf IBM/MVS das Problem weitgehend erledigt hätte.

Ebensowenig ist es richtig, daß der Polizeirechner zu einem riesigen Datenpool geworden ist, in dem sich auch die Daten der BVSt befinden:

Die Daten der Bediensteten der FHH werden durch die BVSt auf IBM-Rechnern verarbeitet. Auch sie stehen dem Polizeiverfahren also nicht zur Verfügung.

Auch stimmt es nicht, daß die Einwohnerdienststellen auf die Daten des Statistischen Landesamts zugreifen können:

Die Einwohnerdienststellen haben gegenwärtig noch keine Terminals; sie können schon aus diesem Grund nicht auf Daten des Statistischen Landesamtes zugreifen. I. ü. werden die Daten des Statistischen Landesamtes im Stapelbetrieb verarbeitet und sind überhaupt nur temporär im Zugriff.

Schließlich hat bei der öffentlichen Anhörung zum Mikrozensusgesetz ein Sachverständiger sogar behauptet, ein Eindringversuch in ein Rechenzentrum sei bereits gelungen; ihm lägen Beweise vor. Leider konnte ich die Behauptung ohne einen Anhaltspunkt über Zeitpunkt und angegriffenes System oder den benutzten Weg (Fernübertragungsleitung, physisches Eindringen, Einschleusen von Material?) nicht nachprüfen. Meine mehrfach geäußerten schriftlichen Bitten um nähere Angaben wurden nicht beantwortet.

Ich finde es wenig hilfreich, wenn behauptet wird, ein DV-System weise Schwachstellen auf und diese seien sogar ausgenutzt worden, den zuständigen Stellen die nötigen Hinweise, die zu einer Schließung der Lücke beitragen könnten, aber verweigert werden.

3.6 Datenverarbeitungszentrale (DVZ)

Im Berichtsjahr habe ich die 1984 begonnene Prüfung des Datensicherungssystems der DVZ (s. 2.5.1 im 3. TB) fortgesetzt und abgeschlossen. Die DVZ hat sich während der Prüfung stets kooperativ verhalten und jede gewünschte Unterstützung gewährt, insbesondere alle Fragen bereitwillig beantwortet.

Gegenstand der Prüfung waren die technischen und organisatorischen Maßnahmen, die die DVZ als Stelle, die Daten im Auftrag verarbeitet, gem. § 8 Abs. 1 HmbDSG zu treffen hat. Die Datensicherungsmaßnahmen haben zu gewährleisten, daß personenbezogene Daten nur entsprechend den Weisungen der speichernden Stelle (Auftraggeber) verarbeitet werden. Die geforderten Datensicherungsmaßnahmen sollen möglichst Fehlern und absichtlichen Verstößen gegen Weisungen der Auftraggeber vorbeugen oder wenigstens die Aufklärung ermöglichen; sie umfassen die Betriebssicherung i.S. der DS-Richtlinie (MittVw 1977 S. 205). Gegenstand meiner Prüfung war nicht die Sicherung der einzelnen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden (Verfahrenssicherheit und Dateisicherung i.S. der DS-Richtlinie).

Selbst ein umfassendes Sicherungssystem kann in seiner Wirksamkeit beeinträchtigt werden, wenn die einzelnen Komponenten des Systems bekannt sind. Anders ausgedrückt: Die Geheimhaltung ist eine der Sicherheitskomponenten. Es liegt daher auf der Hand, daß ich über das Prüfungsergebnis nur in allgemeiner Form berichten kann.

Die Prüfung lief in folgenden drei Phasen ab:

(1) Risikoanalyse

Auf Grundlage insbesondere der Empfehlungen der KGSt habe ich alle denkbaren Risiken zusammengestellt und für jedes Risiko die Eintrittswahrscheinlichkeit sowie Art und Umfang des möglichen Schadens beschrieben. Die Risiken Krieg, Terroranschlag, katastrophale Naturereignisse sowie vergleichbare schwere

Unfälle und technische Defekte habe ich relativ grob dargestellt. Sehr detailliert beschrieben habe ich dagegen die Risiken, deren Beherrschung durch die DVZ mein besonderes Augenmerk galt. Es sind dies personelles Versagen sowie kriminelles Handeln durch Personal der DVZ, sonstiges Personal der FHH, Mitarbeiter von beauftragten Firmen, sonstige Personen. Eine Unterlage dieser Art gab es in der DVZ bisher noch nicht.

(2) Bestandsaufnahme der Datensicherungsmaßnahmen

Die Datensicherungsmaßnahmen wurden für jedes Risiko getrennt nach Funktions- bzw. Arbeitsbereichen aufgenommen, und zwar nahezu ausschließlich der Sollzustand; nur stichprobenweise wurde auch der Istzustand geprüft.

(3) Bewertung der Datensicherungsmaßnahmen

Die festgestellten Datensicherungsmaßnahmen sind für jedes Risiko und ggf. für jeden Arbeitsbereich bzw. jede Funktion bewertet worden. Maßstab war dabei – wie bereits im 2. TB (S. 19) ausgeführt –, ob die versehentliche unberechtigte Nutzung fremder Daten so gut wie ausgeschlossen und die Schwelle für die absichtliche unberechtigte Nutzung fremder Daten (der eigentliche Mißbrauch) so hoch liegt, daß der mögliche Ertrag aus dem Mißbrauch den Aufwand für die Überwindung der Datensicherungsmaßnahmen nicht lohnt.

Diese Bewertung beruht auf den Erfahrungen, die die Prüfer selbst bei früheren Untersuchungen gesammelt haben, und auf den Erkenntnissen, die andere Fachleute bei entsprechenden Untersuchungen gewonnen und veröffentlich haben. In die Bewertung sind eingeflossen die bekanntgewordenen Informationen über DV-Unfälle und kriminelle Handlungen sowie Statistiken über Computerkriminalität. Ein analytisches Bewertungsverfahren stand nicht zur Verfügung.

In meinem Prüfbericht kam ich zu der Schlußfeststellung, daß die in der DVZ getroffenen Sicherungsmaßnahmen als System einen angemessenen Stand der Datensicherung gewährleisten und daß bei keinem Risiko gravierende oder ernsthafte Lücken bestehen. Ich sehe allerdings Möglichkeiten, die Datensicherung noch zu erhöhen, und habe einige konkrete Hinweise gegeben. Diese Hinweise betrafen folgende Gegenstände:

- Der Dienstaufsicht kommt eine besondere Bedeutung zu. Insbesondere in bestimmten Bereichen der DVZ stellt sie sich als ständige Aufgabe der Vorgesetzten dar.
- Es ist deutlich geworden, daß einer Reihe von Risiken nur mit verfahrensspezifischen Kontrollen begegnet werden kann. Für Verfahren mit Haushalts- und Kassenwirksamkeit (also wenn es "ums Geld" geht) gibt es allgemeine Standards, die auf Anforderungen des Rechnungshofes zurückgehen. Für andere Verfahren gibt es solche Vorgaben noch nicht, sie sollten aber entwickelt werden, damit auch in Verfahren mit „nur" personenbezogenen Daten ein entsprechend hoher Schutz gegen Manipulation in die Verfahren eingebaut wird.
- Der Einsatz von Sicherungssoftware nach neuestem Stand sollte auf alle Systeme der DVZ ausgedehnt werden.
- Der Einsatz automatisierter Verfahren zur Unterstützung der Produktion (Bandverwaltung, Datenbestandsverwaltung, Arbeitsvorbereitung) sollte ausgeweitet werden.
- Angestrebt werden sollte die Einführung automatisierter RZ-Steuerung.

Der Automatisierung der Rechenzentrumssteuerung (Planung und Produktion) messe ich unter Sicherheitsaspekten eine erhebliche Bedeutung zu. Die DVZ ist in dieser Hinsicht nicht besonders fortschrittlich. Abgesehen von Produkten zur Bandverwaltung, zur Datenbestandsverwaltung, zur Betriebsabrechnung und einem System für die Arbeitsvorbereitung (Eigenentwicklung der DVZ) gibt es keine automatisierten Verfahren. Auch wenn die DVZ hierin der Mehrzahl der Rechenzentren gleicht (s. z.B. Kellerbach: RZ-Produktion steht oft auf wackeligen

Beinen, Computerwoche vom 7.6.1985, S. 12), sollten alle Anstrengungen unternommen werden, den RZ-Betrieb so weit wie möglich zu automatisieren. Wie ich bei der Prüfung eines anderen – privaten – Rechenzentrums feststellen konnte, sind vorbildliche Lösungen für folgende Aufgaben gefunden und bereits im Einsatz:

- Verwaltung von Programmen in den Stadien Entwicklung (Programmierung), Abnahmetest, Produktion, Archivierung;
- Produktionsplanung (Maschinenbelegung) und -überwachung (Ist-Kontrolle);
- zeitgleiche Erstellung von Dokumentation und Produkt, mit der Wirkung, daß das Jobcontrolling nur aus der Dokumentation (automatisiert) entwickelt werden kann.

Die Vorteile dieser weitgehenden Automatisierung liegen auf der Hand: Menschliche Einwirkungsmöglichkeiten und hiermit eine Möglichkeit von Fehlern und dolosen Handlungen werden vermieden. Angesichts auf dem Markt vorhandener Produkte stehen der anzustrebenden Ausweitung der Automatisierung des Rechenzentrumsbetriebs nach Aussagen der DVZ nur die fehlende Normierung für die in der DVZ ablaufenden, in den einzelnen Behörden entwickelten Verfahren entgegen. Dies sollte für das Senatsamt für den Verwaltungsdienst Veranlassung sein, entschiedene Schritte in Richtung auf eine umfassende Normierung zu unternehmen.

4. Einzelprobleme im öffentlichen Bereich

4.1 Neue Medien

4.1.1 Bildschirmtext

Ich habe über Datenschutzprobleme bei Bildschirmtext im 2. und 3. TB ausführlich berichtet. In diesem Tätigkeitsbericht kann ich mich daher auf kurze Sachstandsberichte beschränken.

4.1.1.1 Entwicklung des Dienstes

Die Entwicklung des Bildschirmtextdienstes ist weit hinter den Erwartungen der Deutschen Bundespost zurückgeblieben. Das betrifft zum einen die Zahl der angeschlossenen Teilnehmer (ca. 39.000) als auch die Zusammensetzung der Teilnehmer. Der Durchbruch zu einer breiten Nutzung in den privaten Haushalten ist bisher ausgeblieben. Die Post unternimmt daher große Anstrengungen, um Teilnehmer insbesondere im privaten Bereich zu gewinnen. So wurde z.B. 1985 in Hamburg erstmalig eine Btx-Werbewoche durchgeführt.

4.1.1.2 Umsetzung des Staatsvertrages in Bundesrecht

Im 3. TB (S. 19 f) habe ich ausführlich über den Konflikt zwischen der Deutschen Bundespost und den Datenschutzbeauftragten in der Frage der Umsetzung des Staatsvertrages in Bundesrecht berichtet. Der Sachstand ist unverändert: Die Post hat bisher nichts unternommen, um die Forderungen der Datenschutzbeauftragten zu erfüllen. Sie begründet dies damit, daß der Bundesbeauftragte – und ich habe mich dem angeschlossen – festgestellt habe, das technische System Btx werde den Anforderungen des Datenschutzes im wesentlichen gerecht. Sie stellt allerdings in Aussicht, daß sie die benutzungsrechtlichen Vorschriften überarbeiten werde, sobald hinreichende Erfahrungen mit der neuen Systemtechnik vorliegen (s. Bundestagsdrucksache 10/2857). Im Geschäftsbericht 1984 der Deutschen Bundespost heißt es hierzu, daß die bisherigen organisatorischen, technischen und rechtlichen Maßnahmen und Regelungen – wenn auch im Einzelfall evtl. verbesserungsfähig – für die erste Phase des Btx-Dienstes ausreichend seien und erforderliche Regelungen und Maßnahmen getroffen werden, wenn in der Zukunft ein zusätzlicher datenschutzrechtlicher Regelungsbedarf auftreten sollte (Geschäftsbericht S. 24).

Wie die Datenschutzbeauftragten nachgewiesen haben, besteht ein zusätzlicher datenschutzrechtlicher Regelungsbedarf bereits heute. In Anbetracht der Akzeptanzschwierigkeiten des Bildschirmtextes wäre die Post m.E. gut beraten, wenn sie unfruchtbare Auseinandersetzungen mit den Datenschutzbeauftragten vermiede. Die Datenschutzbeauftragten werden jedenfalls ihre Bemühungen fortsetzen, die Deutsche Bundespost zu einer Änderung ihrer Haltung zu bewegen.

4.1.1.3 Btx – ein unsicheres Medium?

In meinem 3. TB hatte ich darüber berichtet, daß die Datenschutzbeauftragten des Bundes und der Länder es unternommen hatten, sich vollständige und zutreffende Kenntnisse über das technische System von Btx zu verschaffen, um zu einer Würdigung dieses Dienstes zu gelangen. Dieses Vorhaben konnte noch nicht abgeschlossen werden. Mit den nachfolgenden Ausführungen knüpfe ich an meine Ausführungen im 3. TB (2.5.2.1) über die Sicherheitsdefizite des Systems an.

Eines der vermuteten Sicherheitsrisiken hatte sich im November 1984 mit dem „Hamburger Hackerfall" konkretisiert: Einem Teilnehmer war es gelungen, unbefugt unter dem Namen eines anderen Teilnehmers das System zu benutzen. Diesen Fall habe ich im Berichtsjahr eingehend untersucht, u.a. um die offenbar bestehende Sicherheitslücke exakt zu lokalisieren und den wilden Spekulationen in der Öffentlichkeit Fakten entgegenhalten zu können. Zur Erinnerung:

Der Fall wurde bekannt unter dem Schlagwort „Bankraub per Btx" oder auch „elektronischer Bankraub". Hauptakteure des „Coup" waren zwei Mitglieder des in Hamburg agierenden Chaos-Computer-Clubs (CCC), einer „chaotischen Vereinigung" jugendlicher Hacker. Betroffen waren die Deutsche Bundespost als Betreiber von Btx, ein Hamburger Kreditinstitut als Btx-Teilnehmer und -Anbieter sowie meine Dienststelle als Schauplatz einer Demonstration der CCC-Leute für Pressevertreter.

Die Ermittlungsarbeit hat sich als sehr langwierig erwiesen, nicht zuletzt deshalb, weil meine Anfragen an die Deutsche Bundespost zur Programmlogik der Editier- und Verbindungsaufbauroutinen nur schleppend beantwortet wurden und ich für die Recherchen in Programmen des Btx-Systems auf die Amtshilfe des für die Bundespost zuständigen BfD angewiesen war. Wie sich am Ende herausgestellt hat, ist erst dadurch, daß der BfD anhand der Programmunterlagen der Post selbst intensiv in die Programmlogik eingestiegen ist, der wesentliche Schritt zur Aufklärung des Sachverhalts getan worden. Die Post hat von sich aus zur Klärung nur wenig beigetragen.

Der Fall:

Zwei Mitglieder des CCC, deren eines Anbieter und Teilnehmer am Btx ist, hatten ein eigenes entgeltpflichtiges Angebot unbefugt unter dem Namen eines anderen Teilnehmers – und damit zu dessen (Gebühren-)Lasten – aus dem Btx-System abgerufen. Sie hatten unter Benutzung von Anschlußkennung und Kennwort des anderen Teilnehmers eine Verbindung zum Btx-System aufgebaut und – mit Hilfe eines entsprechend programmierten Mikrocomputers – ihre eigene Seite mehrere Stunden lang in schneller Folge abgerufen, wodurch ihrem Vergütungskonto ungefähr DM 135.000,– gutgeschrieben und das Btx-Gebührenkonto des Kreditinstituts mit dem entsprechenden Betrag belastet wurde.

Als der Coup gelungen war, gaben sie unter der Überschrift „Kennwort: Bankraub" eine Presseerklärung heraus, mit der sie die Öffentlichkeit auf Sicherheitsmängel im Btx-System hinweisen wollten.

Der mißbrauchte Anschluß:

Der von den CCC-Mitgliedern mißbrauchte Btx-Anschluß des Kreditinstituts ermöglichte zu keiner Zeit den Zugriff auf irgendwelche Bankkonten. Es handelte sich vielmehr um einen ausschließlich für Demonstrationszwecke eingerichteten und genutzten Anschluß. Er war nicht mit der Anschlußbox D-BT03, sondern mit einem Datenübertragungsmodem ausgestattet, bei dem die Anschlußkennung vom Benutzer über eine Tastatur eingegeben werden muß. Der Anschluß war anfangs nicht freizügig

geschaltet. Die hierüber abgewickelten Demonstrationen des Btx-Systems fanden während der Geschäftszeiten und – für geladene Gäste – in den Abendstunden in verschiedenen Zweigstellen des Kreditinstituts statt.

Untersuchungsergebnis:

Nach dem Vorbringen der CCC-Mitglieder und der ersten Verlautbarung der Deutschen Bundespost zum Fall sah es anfänglich so aus, als hätten die Hacker, weil die Post insoweit ihrer Aufklärungspflicht nicht nachkam, die Öffentlichkeit auf einen gravierenden datenschutz- und eigentumsgefährdenden Sicherheitsmangel im Btx-System hingewiesen (1).

Nach der Darstellung, die die Post mir auf meine Fragen gab, sah es dann allerdings so aus, als hätten die Mitglieder des Chaos-Computer-Clubs einen zwar vorhandenen Programmfehler, der jedoch nicht die behaupteten Auswirkungen haben konnte, zum Vorwand genommen für einen massiven Angriff auf die Deutsche Bundespost und das Btx-System sowie zu einer die Öffentlichkeit irreführenden Darstellung der Risiken von Btx. Hiernach hätten sie der Öffentlichkeit ein Risiko, das so tatsächlich nicht bestand, nur vorgegaukelt (2).

Nach den Feststellungen des BfD lagen die unter (2) dargestellten Überlegungen neben der Sache, weil die betreffenden Programmroutinen für den Fall gar keine Rolle spielten. Relevant sind ganz andere Programmroutinen, und diese könnten bei dem damaligen Fehler im Editierprogramm die von den Hackern behaupteten Auswirkungen haben (3).

(1) Die CCC-Mitglieder haben folgende Darstellung gegeben:

Bei ihren Aktivitäten als Anbieter und Teilnehmer im Btx-System seien sie wiederholt auf Fehler gestoßen, die z.T. die Sicherheit des Systems beeinträchtigen. Die Deutsche Bundespost, die sie auf diese Sicherheitsmängel und andere Fehler hingewiesen hätten, habe auf ihre Hinweise und Mängelrügen nur zögerlich, z.T. unwillig reagiert.

Beim Austesten der Editierfunktionen seien sie schließlich auf folgenden Fehler gestoßen: Wenn bei der Eingabe von Decoderinformationen (das sind die Informationen, die ein Anbieter für den graphischen Aufbau einer Btx-Seite eingeben muß) genau die Anzahl an Informationen eingegeben wurde, die von der Post für maximal zulässig angegeben worden war, machte sich ein Programmfehler bemerkbar, der bewirkte, daß am Bildschirm anstelle der editierten Seite verstümmelte Daten, z.T. aus der eigenen bearbeiteten Seite, z.T. ganz fremde Daten, angezeigt wurden.

Da sie in diesem Fehler ein Sicherheitsrisiko vermuteten, hätten sie durch entsprechende Eingaben immer wieder die Fehlerkonstellation in der Erwartung erzeugt, daß unter den verstreut angezeigten Fremddaten auch einmal Identifikationsmerkmale anderer Anbieter oder Teilnehmer sein würden.

Bei ihren Versuchen hätten sie schließlich Daten auf den Bildschirm bekommen, die sie für Teilnehmerdaten gehalten und daher notiert hätten. Als sie das, was sie für eine manuell einzugebende Anschlußkennung hielten, beim Verbindungsaufbau von ihrem zumindest für diesen Zweck freizügig geschalteten Teilnehmeranschluß eingegeben hätten, sei in der Begrüßungsseite eine Teilnehmernummer erschienen; diese hätten sie als Adressat in eine Mitteilung im Btx eingetragen und auf diese Weise den Inhaber des Anschlusses erfahren. Sie hätten dann ein weiteres notiertes Datum als Kennwort erkannt; als sie mit Hilfe der so gewonnenen Daten versucht hätten, unter fremdem Namen eine Verbindung aufzubauen, sei ihnen dies gelungen.

Sie hätten dann den fremden Anschluß freizügig geschaltet, das Paßwort „USD70000" in „Bankraub" geändert und schließlich durch per Mikrocomputer gesteuerten automatischen Aufruf ihrer eigenen gebührenpflichtigen Angebotsseite eine Gebührenbelastung für den fremden Teilnehmer in Höhe von ca. DM 135.000,– bewirkt. Durch die Eingabe des neuen, nur ihnen bekannten

Kennwortes hätten sie sichergestellt, daß keine Veränderungen von Seiten des berechtigten Anschlußinhabers hätten vorgenommen werden können, bevor sie ihre Entdeckung der Öffentlichkeit bekanntgemacht hätten.

(2) Die Darstellungen der Post ergaben folgendes Bild:

In einer ersten Stellungnahme hatte sie erklärt, es sei richtig, daß durch einen Programmfehler Teile anderer als der bearbeiteten Btx-Seiten, sogar Daten fremder Teilnehmer auf dem Bildschirm hätten angezeigt werden können. Dabei war sie von der Annahme ausgegangen, daß der Anschluß des Kreditinstituts von diesem freizügig geschaltet und daher für den Verbindungsaufbau nur die Kenntnis des Kenntwortes erforderlich gewesen war. (Der Programmfehler wurde nach Bekanntwerden umgehend behoben.)

Als die Post jedoch erfuhr, daß der Anschluß von dem Kreditinstitut nicht freizügig geschaltet und für den Systemzugang sowohl die Anschlußkennung als auch das persönliche Kennwort des Kreditinstitutes benutzt worden waren, schloß sie aus, daß diese beiden fremden Kennungsdaten zusammen durch den Fehler im Btx-System offenbart worden sein könnten. Aufgrund der Programmlogik sei es zu keiner Zeit zu einer gleichzeitigen Abspeicherung beider Daten in dem während einer Sitzung für die Abwicklung der betreffenden Verbindung benutzten Speicherbereich im Rechner gekommen. Wenn – wegen des Programmfehlers – Daten aus einem solchen Speicherbereich unkontrolliert auf dem Bildschirm erschienen seien, so könne jedenfalls nicht mehr angezeigt worden sein, als im Arbeitsspeicherbereich vorhanden war.

Nach der Programmlogik wurde und wird beim Verbindungsaufbau im Hauptspeicher des Teilnehmerrechners in der Btx-Vermittlungsstelle ein Arbeitsspeicherbereich eingerichtet, der während der Dauer einer Verbindung für den Aufbau und die Abwicklung dieser Verbindung benutzt wird. Zu Beginn des Verbindungsaufbaues wird die Anschlußkennung unter einer bestimmten Adresse in diesem Speicherbereich gespeichert. Im weiteren Verlauf des Verbindungsaufbaues wird, wenn in der Btx-Leitzentrale zu der im Speicherbereich abgelegten Anschlußkennung ein Anschlußsatz (definierte Folge von Daten, die den Teilnehmeranschluß beschreiben) vorhanden ist, ein Sessionsatz (definierte Folge aller Daten, die im Verlauf der Verbindung gespeichert werden) angelegt. Die Stelle, an der die Anschlußkennung gespeichert wird, befindet sich innerhalb des Bereichs, der im weiteren Verlauf des Verbindungsaufbaues vom Sessionsatz eingenommen wird. Die für die Anschlußkennung reservierte Speicherstelle wird beim Anlegen des Sessionsatzes frühzeitig mit Daten überschrieben, die für den weiteren Verbindungsaufbau benötigt werden. Erst nachdem die Anschlußkennung auf diese Weise zu einem wesentlichen Teil durch Überschreiben mit neuen Daten zerstört worden ist, wird das Kennwort vom Teilnehmer abgefragt und in den Hauptspeicher und dort in den Speicherbereich für die Verbindung übernommen. Das Kennwort wird zur Prüfung an die Btx-Leitzentrale übersandt. War das Kennwort richtig, überträgt die Btx-Leitzentrale den Mitbenutzersatz (definierte Folge der Daten, die den Teilnehmer oder Mitbenutzer beschreiben) an den Teilnehmerrechner in der Btx-Vermittlungsstelle. Aus diesem Ablauf ergibt sich, daß das Kennwort erst dann in dem Speicherbereich gespeichert wird, wenn die Anschlußkennung nicht mehr oder nicht mehr vollständig vorhanden ist.

(3) Nachdem beide Darstellungen in meiner Dienststelle eingehend gewürdigt worden waren, bat ich den BfD, eine Programmprüfung vorzunehmen mit dem Ziel, die Angaben der Post zu überprüfen und darüber hinaus zu untersuchen, ob nicht andere – von mir mangels Kenntnis der Btx-Programmlogik nicht hinterfragte – programmbedingte Ursachen für die unbeabsichtigte Anzeige der Kennungsdaten auf dem Bildschirm der Hacker infrage kommen können.

Die eingehende Prüfung des BfD hat ergeben, daß es zur Beurteilung der Frage, was aufgrund des bekannten Programmfehlers als „Ersatz" für beim Editieren eingegebene Inhalte möglicherweise auf dem Bildschirm erschienen ist, auf die

Bereiche des Hauptspeichers, in denen der Sessionsatz steht, nicht ankommmt. Denn diese Bereiche konnten auch unter den Bedingungen, die zum Fehler führten, nicht als zur editierten Seite zugehörig verarbeitet werden. Die fälschlich einer Seite zugeordneten Bereiche enthielten vielmehr je nach dynamisch wechselnden Zuständen

a) Angaben, die zur Weiterleitung zur Btx-Leitzentrale in Ulm vorgesehen waren,

b) Seiten oder Teile von Seiten, die für denselben oder einen anderen Teilnehmer abgesendet waren oder wurden, oder

c) Eingaben der Teilnehmer.

Zu a)

Diese Angaben sind nicht im CEPT-Code dargestellt, so daß auf dem Bildschirm des Benutzers kein inhaltsgleiches Bild erzeugt wird und deshalb diese Möglichkeit nicht weiter zu untersuchen ist.

Zu b)

Es läßt sich kaum abschätzen, was im einzelnen auf solchen Seiten gestanden haben kann, weil das überwiegend in der Verantwortung der Anbieter liegt.

Zu c)

Eingaben entstehen, wenn vom Teilnehmer im Rahmen eines Dialogs Daten einzutragen sind. Sie werden nach Abschluß der Eingabe zur weiteren Verarbeitung in Arbeitsbereichen zwischengespeichert. In dem Moment, in dem diese Arbeitsbereiche fälschlich einer gerade editierten Seite zugeordnet werden, stehen hier also möglicherweise auch die Angaben, die im Rahmen des Verbindungsaufbaues gemacht wurden. Weil aber im Rahmen eines Verbindungsaufbaues für alle notwendigen Eingaben derselbe Arbeitsbereich verwendet wird, konnten in einem Arbeitsbereich aus einem Verbindungsaufbau entweder die Anschlußkennung oder – neben anderen Daten – das Paßwort gespeichert werden; beide Daten konnten in einem Arbeitsbereich nicht gleichzeitig gespeichert sein, weil spätere Eingaben frühere, insbesondere die Anschlußkennung zerstören. In der damaligen Programmversion wurden nicht mehr benötigte und deshalb freigegebene Arbeitsbereiche aber nicht „gelöscht" und auch bei der evtl. folgenden Nutzung für andere Zwecke nur soweit überschrieben, wie es die neue Nutzung erforderte. Da insgesamt mehrere Arbeitsbereiche fälschlich einer Seite hätten zugeordnet und auf dem Bildschirm angezeigt werden können, kann nicht ausgeschlossen werden, daß aus einem früh abgebrochenen Verbindungsaufbau in einem Arbeitsbereich die Anschlußkennung und aus einem anderen Verbindungsaufbau in einem anderen Arbeitsbereich Eingaben, u.a. das Paßwort, noch ganz oder in wesentlichen Teilen gespeichert waren, gemeinsam fälschlich einer editierten Seite zugeordnet und auf dem Bildschirm angezeigt wurden. Ob aber eine solche „günstige" Konstellation vorgelegen hat, kann nicht rekonstruiert werden.

Nach allem kann nicht festgestellt werden, ob tatsächlich zum damaligen Zeitpunkt die Daten des Kreditinstituts auf dem Bildschirm der Hacker zu lesen waren. Absolut auszuschließen ist es – wie unter (3) dargestellt – nicht. Andere Möglichkeiten, an die Daten heranzukommen, haben immerhin auch bestanden. So konnten die Daten bei den Demonstrationen ausgespäht worden sein. Auch ein Abhören der Telefonleitung durch Aufschalten eines Gerätes zwischen Telefon und Hausanschluß war technisch möglich. Im Btx werden bekanntlich alle Daten unverschlüsselt über die Telefonleitung zur Btx-Vermittlungsstelle geschickt, und es ist allgemein bekannt, daß das Abhören einer Telefonleitung u.a. für Elektronik-Bastler kein Problem ist (wenn nur die Anschlußleitung ausfindig gemacht werden kann). Schließlich ist es nicht absolut unmöglich, daß ein unzuverlässiger Mitarbeiter die Daten verraten hat.

Welche Konzequenzen sind in datenschutzrechtlicher Hinsicht aus diesem Fall zu ziehen? Ganz sicher diese:

1. Jeder Benutzer von Btx muß sich vergegenwärtigen, daß als Übertragungsmedium die Telefonleitung dient, auf der Daten in unverschlüsselter Form übertragen werden. Die Telefonleitung kann abgehört werden.
2. Die Anschlußkennung und das Kennwort haben die Funktion eines „Tresorschlüssels". Wenn man diesen frei herumliegen läßt oder öffentlich aushängt, bedeutet dies eine Minderung der Sicherheit. Dagegen, daß durch einen vielleicht vorhandenen, bisher unentdeckten anderen Systemfehler (als den im Editierprogramm, der beseitigt wurde) die Kenndaten ohne Fahrlässigkeit des Teilnehmers Dritten zur Kenntnis gelangen, könnte die verschlüsselte Abspeicherung der Kenndaten Schutz bieten. Gegen das Abhören würde nur eine Verschlüsselung der Daten vor der Übertragung, also schon beim Teilnehmer, wirken. Durch eine solche Anforderung wäre das Btx-System als Massenkommunikationsmittel allerdings unattraktiv.

4.1.2 Landesmediengesetz

Ich habe in meinem 3. TB (S. 22) meine Vorschläge für Datenschutzregelungen skizziert, die ich in die Diskussion über das Landesmediengesetz eingebracht habe. Diese Vorschläge sind inhaltlich unverändert in den Entwurf übernommen worden, den der Senat der Bürgerschaft zur Beschlußfassung zugeleitet hat. Der wesentliche Inhalt soll hier noch einmal dargestellt werden:

- Soweit bei der Verteilung von Rundfunkprogrammen, Sendungen und Beiträgen (Angeboten) aufgrund der eingesetzten Technik Verbindungsdaten, d.h. Daten über die Vermittlung von Angeboten, und Abrechnungsdaten, d.h. Daten für die Abrechnung der erbrachten Leistungen, anfallen, dürfen

  Verbindungsdaten nur für die Dauer der Verbindung gespeichert und nicht übermittelt und

  Abrechnungsdaten nur so gespeichert werden, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit der Inanspruchnahme einzelner Angebote nicht erkennbar sind (es sei denn, der Teilnehmer wünscht eine detaillierte Speicherung), und nur an den Anbieter und nur dann übermittelt werden, wenn eine Forderung auch nach Mahnung nicht beglichen worden ist; im übrigen müssen sie nach Abrechnung bzw. Übermittlung gelöscht werden.
- Der Betreiber muß über § 6 BDSG hinaus technische und organisatorische Maßnahmen ergreifen.
- Umfangreiche Kontrollbefugnisse – voraussichtlich des HmbDSG – sollen gewährleisten, daß die Datenschutzvorschriften auch eingehalten werden.
- Entsprechend dem Stand der Diskussion über die Novellierung des BDSG sind in dem Gesetz auch Bestimmungen enthalten, die den Anbieter von Programmen verpflichten,

  veröffentlichte Gegendarstellungen zu den gespeicherten Daten zu nehmen und Auskunft über die einer Berichterstattung zugrundeliegenden Daten an den Betroffenen zu geben, wenn dieser durch die Berichterstattung in seinen schutzwürdigen Belangen beeinträchtigt wird, jedoch nur dann, wenn die Daten in Dateien gespeichert sind.

  Die Beschränkung des Auskunftsrechts auf Daten, die in Dateien gespeichert sind, ist im Interesse der Pressefreiheit notwendig, um das Auskunftsrecht auf die in Archiven gespeicherten Daten zu beschränken und persönliche Notizen der Redakteure auszunehmen.

4.1.3 TEMEX

Ich habe im 2. (S. 41) und im 3. TB (S. 22 f) über Fernwirkdienste allgemein berichtet und dabei die technische Wirkungsweise beschrieben sowie die damit verbundenen datenschutzrechtlichen Probleme dargestellt. Die Deutsche Bundespost betreibt z.Z. die Einführung von TEMEX, d.h. von Ferwirkdiensten unter Benutzung der Fernsprech-

netzes. Zu diesem Zweck werden System- und Betriebsversuche durchgeführt. In den Systemversuchen werden die Übertragungs- und Vermittlungstechnik, in den Betriebsversuchen unterschiedliche Anwendungen und die damit verbundenen Endgeräte erprobt.

Die Deutsche Bundespost hat einen Betriebsversuch in Hamburg genehmigt. Die Anwendungen in diesem Betriebsversuch sind noch nicht endgültig festgelegt. Es wird sich jedoch im wesentlichen um die Fernüberwachung von betriebstechnischen Einrichtungen in Behörden (z.B. Gewebekulturen in Einrichtungen der Gesundheitsbehörde, Pumpwerke, Rolltreppen u.a.m. im Zuständigkeitsbereich der Baubehörde) sowie von Brand-und Einbruchsmeldern und um das Messen des Energieverbrauchs (z.B. Heizung in Behördengebäuden) handeln. Auch die Fernüberwachung von betriebstechnischen Einrichtungen in der privaten Wirtschaft wird dazu gehören; bei letzteren werden Wach- und Sicherheitsdienste die Anbieter sein. Bei diesen Anwendungen fallen keine personenbezogenen Daten an. Als einzige Anwendung mit personenbezogenen Daten zeichnet sich die Fernüberwachung von Multiple-Sklerose-Kranken ab, bei der ebenfalls private Wachdienste als Anbieter auftreten.

Für diese Anwendung müssen in den Verträgen zwischen dem Anbieter und den Betroffenen und in der Definition der Anforderungen an die Endgeräte datenschutzrechtliche Vorkehrungen vorgesehen werden, die das Eindringen in die persönliche Sphäre des Betroffenen steuern und kontrollieren; dabei handelt es sich insbesondere um folgendes:

- Der Betroffene ist über Verwendungszweck sowie Art, Umfang und Zeitraum des Einsatzes des Dienstes aufzuklären;
- es muß eine schriftliche Einwilligung des Betroffenen vorliegen;
- die Einwilligung ist jederzeit widerrufbar;
- die Speicherung und Verarbeitung von personenbezogenen Daten darf nur im Rahmen der Einwilligung erfolgen;
- die gespeicherten personenbezogenen Daten sind nach Beendigung des Vertragsverhältnisses zu löschen.
- Das Endgerät muß erkennen lassen, daß der Dienst in Anspruch genommen wird, und es möglich machen, den Dienst jederzeit abzuschalten, wenn der Vertragszweck dem nicht entgegensteht.

Ich werde an der Begleitung des Betriebsversuches beteiligt. Dabei werde ich darauf achten, daß die oben beschriebenen datenschutzrechtlichen Vorkehrungen getroffen werden, soweit die Anwendungen es erfordern. Aufgrund der Erfahrungen aus dem Betriebsversuch sollen Vorschläge für Datenschutzvorschriften im Landesmediengesetz erarbeitet werden.

4.2 Personalwesen

4.2.1 Allgemeines

Ich habe mich im 3. TB (S. 23 ff.) ausführlich mit der Frage auseinandergesetzt, ob es in der Verwaltung der Freien und Hansestadt Hamburg ein intregriertes Personalinformationssystem gibt, und diese Frage verneint. Als nächstes werde ich das Personalaktenrecht überprüfen; eine Bestandsaufnahme aller relevanten Probleme habe ich eingeleitet.

Die in diesem Bericht angesprochenen Datenschutzprobleme im Personalwesen sind von außen an mich herangetragen worden.

4.2.2 Fragebogen für Bewerber und Einzustellende

In einer Schriftlichen Kleinen Anfrage (s. Drucksache 11/3558) ist u.a. gefragt worden, warum Bewerber – auch Bewerber für ABM-Stellen – Angaben über Ehrenämter,

Schulden, laufende Ermittlungs- und Strafverfahren sowie nicht getilgte Vorstrafen machen müssen. In seiner Antwort hat der Senat eingeräumt, daß detaillierte Fragen nach Schulden zu weitgehend sind und Fragen nach Vorstrafen sich nach den Durchführungshinweisen zum Bundeszentralregistergesetz zu richten haben.

Die Anfrage war Veranlassung für das Senatsamt für den Verwaltungsdienst, alle in den Behörden und Ämtern verwendeten Fragebogen für Bewerber und Einzustellende zu sammeln und auf dieser Grundlage einheitliche Fragebogen für Bewerber und Einzustellende in Abstimmung mit den Behörden und Ämtern zu entwerfen. Ich bin an diesem Vorhaben beteiligt worden.

Ziel der Gespräche war es, Fragebogen zu entwerfen, in denen nur Fragen gestellt werden, die für die Auswahl eines Bewerbers und – im Falle der Einstellung – für die Begründung und Fortführung eines Beschäftigungsverhältnisses erforderlich sind. Dabei stellte sich alsbald heraus, daß einheitlich nur ein gewisser Grundstock von Fragen vorgegeben werden kann und daß für besondere Gruppen von Beschäftigten – z.B. in sicherheitsempfindlichen Bereichen oder in pflegerischen Berufen – zusätzliche Fragen gestellt werden müssen.

Die beabsichtigte Vereinheitlichung kann ohnehin nur empfehlenden Charakter haben, weil die Gestaltung von Personalfragebogen der Mitbestimmung durch die Personalräte der Behörden und Ämter unterliegt (§ 87 Abs. 1 Nr. 23 HmbPersVG).

Als Ergebnis der Gespräche werden je ein Fragebogen für Bewerber und für Einzustellende vorgeschlagen, die auch aus meiner Sicht – mit einer Ausnahme, siehe 4.2.2.2 – nur Fragen enthalten, die für die Auswahl eines Bewerbes sowie die Begründung und Fortführung eines Beschäftigungsverhältnisses erforderlich sind. Die in der Schriftlichen Kleinen Anfrage kritisierten Fragen nach Schulden, Ehrenämtern und nicht getilgten Vorstrafen sind entfallen. Für besondere Gruppen von Beschäftigten wird zusätzlich danach zu fragen sein, ob die wirtschaftlichen Verhältnisse geordnet sind; ausnahmsweise kann es erforderlich sein, auch die Höhe der Schulden und der monatlichen Belastung zu erfragen.

4.2.2.2 In dem Fragebogen für Bewerber wird u.a. folgende Frage gestellt: „Ist gegen Sie ein gerichtliches Strafverfahren oder ein Disziplinarverfahren anhängig? Ja/Nein." Ich hatte in den Gesprächen gefordert, dieser Frage folgenden Zusatz anzufügen: „Die Beantwortung dieser Frage ist freiwillig; wir weisen Sie jedoch darauf hin, daß Sie unter Umständen gegebenenfalls auch dienstrechtliche Nachteile zu erwarten haben (Entlassung aus dem Beamtenverhältnis), wenn Sie rechtskräftig zu einer Strafe verurteilt werden, die in ein Führungszeugnis für Behörden nach dem Bundeszentralregistergesetz aufzunehmen ist." Diesen Zusatz halte ich aus folgenden Gründen für erforderlich:

§ 32 Abs. 2 Nr. 5 des Bundeszentralregistergesetzes (BZRG) schreibt vor, daß die Einstellungsbehörde keine Auskunft über eine rechtskräftige Verurteilung z.B. zu einer Geldstrafe von nicht mehr als 90 Tagessätzen oder zu einer Freiheitsstrafe von nicht mehr als drei Monaten erhält, sofern im Register keine weitere Strafe eingetragen ist. Das Bundeszentralregistergesetz räumt also bei einer rechtskräftigen Verurteilung in den Fällen des § 32 Abs. 2 den Interessen des Betroffenen am Verschweigen einer Bestrafung den Vorrang vor dem Informationsbedürfnis der Behörde ein, wenn keine Rückausnahme gem. § 32 Abs. 3 (bestimmte Eintragungen) oder Abs. 4 (Führungszeugnis für Entscheidungen nach § 149 Abs. 1 Nr. 1 GewO) vorliegt. Der Bewerber darf sich nach § 53 Abs. 1 BZRG auch gegenüber der Einstellungsbehörde als unbestraft bezeichnen. Für schwebende Straf- und Ermittlungsverfahren kann angesichts der Unschuldsvermutung nicht anderes gelten. Die geforderte unbeschränkte Auskunft würde daher die schutzwürdigen Belange des Bewerbers, nämlich das Nachteilsverbot vor der Verurteilung, beeinträchtigen.

Es kann daher keine unbeschränkte Auskunftspflicht bestehen. Ich verkenne keineswegs die Schwierigkeiten für den Bewerber; es wird ihm in den meisten Fällen unmöglich sein, die Höhe des ihm drohenden Strafmaßes verläßlich abzuschätzen. Einen

Ausweg sehe ich nur darin, daß die Beantwortung der Frage nach anhängigen Straf- und Ermittlungsverfahren generell freiwillig ist und der Bewerber auf die ihm bei einer Verurteilung u.U. drohenden Nachteile aufmerksam gemacht wird.

Unmittelbar vor Redaktionsschluß erhielt ich die Stellungnahme des Senatsamtes für den Verwaltungsdienst, die im wesentlichen zwei Argumente enthält: Art. 33 Abs. 2 GG verpflichtet die Verwaltung, u.a. die persönliche Eignung eines Bewerbers umfassend zu prüfen; ein gerichtliches Strafverfahren, ein Ermittlungsverfahren der Staatsanwaltschaft oder ein Disziplinarverfahren könnten je nach den Umständen des Einzelfalles nachhaltige Zweifel hervorrufen, ob der Bewerber die für den öffentlichen Dienst allgemein oder die für den vorgesehenen Verwendungsbereich speziell erforderliche Eignung besitze. Das Senatsamt hält es im übrigen nicht für vertretbar, daß die Verwaltung die Einstellung von persönlich ungeeigneten Bewerbern mit u.U. erheblichen Nachteilen für die Aufgabenerfüllung und das Ansehen der Verwaltung in der Öffentlichkeit in Kauf nimmt, und weist auf prozessuale Risiken und den Zeitbedarf bei der Beendigung eines eingegangenen Beschäftigungsverhältnisses hin. Abschließend bemerkt das Senatsamt, daß beabsichtigt sei, die Einschränkung der Fragestellung dann aufzugreifen, wenn die zum Personalaktenführungsrecht und zu den Mitteilungen in Strafsachen (MISTRA) angestellten Überlegungen für eine gesetzliche Regelung der jeweiligen Materie eine entsprechende Begrenzung nahelegen.

Ich werde diese Fragen in der nächsten Zeit mit dem Senatsamt erörtern.

4.2.3 Automatisiertes Verfahren zur Personaleinsatzplanung in den staatlichen Krankenhäusern

Der Landesbetrieb Krankenhäuser hat ein automatisiertes Verfahren entwickelt, mit dem eine bedarfsgerechte Personalbereitstellung nach den Anhaltszahlen der Deutschen Krankenhausgesellschaft in den Krankenhäusern des Landesbetriebs und damit die Finanzierung einer bedarfsgerechten Personalausstattung sichergestellt und zudem durch Ausweisung von Überschüssen oder Defiziten von Pflegekräften auf den Stationen eine Steuerung des Personaleinsatzes ermöglicht wird.

Zu diesem Zweck sollten

- der Bestand an Pflegekräften und
- ihre Zuordnung zu den Stationen personenbezogen auf Dauer gespeichert,
- die Erfassung der Einsatzzeiten für Zwecke der Personalabrechnung um Angaben über Ausfallzeiten, gegliedert nach Gründen, erweitert und diese Daten personenbezogen und auf Dauer

gespeichert werden.

Die Personalvertretungen sahen hierin eine Gefährdung der schutzwürdigen Belange der Arbeitnehmer. Landesbetrieb und Gesamtpersonalrat baten mich um eine Meinungsäußerung.

Die mit dem automatisierten Verfahren vorgesehene Speicherung von personenbezogenen Daten ist zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 23 BDSG i.V.m. § 2 Abs. 2 HmbDSG). Die berechtigten Interessen des Landesbetriebs als speichernde Stelle sind oben beschrieben. Die schutzwürdigen Belange der Betroffenen, nämlich der Pflegekräfte, können dann beeinträchtigt werden, wenn zusätzliche Daten oder vorhandene Daten so gespeichert werden, daß das Verhalten der Pflegekräfte überwacht werden kann. Ich habe empfohlen, die Daten über den tatsächlichen Einsatz der Pflegekräfte (Ist-Daten) nicht personenbezogen zu speichern, weil das für die Zwecke des Landesbetriebs nicht erforderlich ist. Auf dieser Basis gelang der Abschluß einer Dienstvereinbarung über die Einführung eines rechnergestützten Verfahrens der Personalbedarfsermittlung und Personaleinsatzplanung in den Krankenhäusern des Landesbetriebs, die Inhalt und Organisation des Verfahrens sowie die Rechte und Pflichten des Landesbetriebs und des Gesamtpersonalrats detailliert beschreibt. Darunter ist hervorzuheben:

Bei der Bedienung der erforderlichen Bildschirmarbeitsplätze anfallende Betriebsdaten dürfen nicht zu individueller Leistungskontrolle verwendet werden.

Die für Zahlungsanweisungen erforderlichen Daten werden auf anderen Vordrucken außerhalb dieses Verfahrens an die Besoldungs- und Versorgungsstelle geleitet. Darüber hinaus wird jegliche Verbindung mit dem Verfahren der Besoldungs- und Versorgungsstelle verboten.

4.2.4 Lehrerindividualdatei (LID) der Behörde für Schule und Berufsbildung

Die durch eine Eingabe veranlaßte Überprüfung der rechtlichen Grundlagen für das LID-Verfahren (s. 3. TB, 3.2.2.6) habe ich abgeschlossen. Zu beurteilen war folgender Sachverhalt:

Einmal jährlich im Herbst werden die Erhebungsunterlagen für das LID-Verfahren an die Schulen gesandt. Die Lehrer prüfen die im Erhebungsbogen (linker Teil) ausgedruckten Daten und tragen Änderungen im rechten Teil des Bogens ein. Außerdem müssen die Lehrer auf der Rückseite des Bogens ihre Ermäßigungs- und Entlastungsstunden sowie ihre Unterrichtsstundenverteilung signieren. Der Schulleiter prüft die mitgesandte Lehrerliste auf Vollständigkeit und trägt die Namen in der Liste fehlender Lehrer seiner Schule ein. Die Namen der Lehrer, die nicht mehr zu seinem Kollegium gehören, löscht er in der Liste. Außerdem trägt er den Grund für Zu- bzw. Abgänge ein.

Nach der Verarbeitung der korrigierten und aktualisierten Angaben der Lehrer aus den Erhebungsbogen im automatisierten LID-Verfahren erhält jede Schule Ergebnislisten mit den Daten aus der LID, die sie betreffen. Sie dienen im wesentlichen der Schulorganisation und als Abstimmungsunterlage gegenüber der Schulaufsicht. Aus der LID werden Auswertungen automatisiert erzeugt, die der Schulverwaltung für Planung und Organisation zur Verfügung gestellt werden. Darüber hinaus können mit zwei flexiblen Programmen (Selektieren von Fällen – z.B. Vollbeschäftigte – und Druck von Listen mit variablem Inhalt) Sonderauswertungen für verschiedene Fachabteilungen der BSB erstellt werden. Für die Personalverwaltung werden z.B. folgende Übersichten erstellt:

- Liste der zum nächsten Organisationstermin auslaufenden Beurlaubungen und Teilbeurlaubungen;
- alphabetische Listen für die einzelnen Schulzweige (z.B. Gymnasien) und für alle Schulbereiche;
- Liste der Sozialinspektoren;
- Liste der „mobilen Vertreter".

Von den in der Lehrerindividualdatei gespeicherten Daten sind insbesondere die schulbezogenen Unterrichtsentlastungen (z.B. für Betreuung des Sprachlabors oder der Bibliothek) und die Unterrichtsstundenverteilung in den Personalakten nicht enthalten. Insbesondere für diese Zwecke ist die LID für die BSB unverzichtbar (vor der Einführung der automatisierten Datenverarbeitung wurden die entsprechenden Daten mit großem Aufwand manuell erhoben).

Die Datenverarbeitung umfaßt solche personenbezogenen Daten der Lehrer, die

a) allgemein von den Bediensteten des öffentlichen Dienstes anzugeben sind und die – wie bei allen anderen Bediensteten – in den Personalakten geführt werden (allgemeine Personaldaten),

b) sich speziell auf die Tätigkeit als Lehrer beziehen, d.h. auf ihre Verwendungsmöglichkeit für bestimmte Unterrichtsveranstaltungen an bestimmten Schulen (schulbezogene Lehrerdaten).

Es werden keine Leistungs- und Verhaltensdaten erhoben und verarbeitet. Aus dem Datenbestand können keine Auswertungen zum Zweck der Überwachung von Leistung und Verhalten der Lehrer erfolgen. Die Daten über die Lehrer beziehen sich z.B. auf ihre Einsatzmöglichkeiten aufgrund ihrer Qualifikation und aufgrund ihrer persönlichen Pflichtstundenzahl, auf ihre nach Stundenplan vorgesehene Verwendung im laufenden Schulhalbjahr bzw. auf einen voraussichtlichen Abgang innerhalb der

nächsten zwölf Monate, d.h. es handelt sich um reine Planungsdaten (Soll-Daten). Es werden insbesondere keine Daten zur tatsächlichen Anwesenheit bzw. Fehlzeiten (Ist-Daten) erhoben und verarbeitet.

Das Verfahren bewerte ich wie folgt:

Auf das automatisierte Verfahren „Lehrerindividualkartei" der BSB findet gem. §§ 1 Abs. 2, 2 Abs. 1, 4 das HmbDSG Anwendung. Die Zulässigkeit der Datenverarbeitung im Rahmen der LID ist gem. §§ 5, 9 HmbDSG zu beurteilen.

Eine spezielle Rechtsvorschrift zur Regelung des LID-Verfahrens existiert bisher nicht.

Das Speichern und Verändern der Lehrerdaten ist gem. § 9 Abs. 1 HmbDSG zulässig, weil es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist:

Gem. §§ 1, 2 des Schulverfassungsgesetzes sowie Art. 66 der Hamburgischen Verfassung

- trägt die BSB die Verantwortung für das staatliche Schulwesen,
- hat sie die Funktionsfähigkeit der Schulen zu sichern und
- unterliegt sie dabei dem Gebot der Wirtschaftlichkeit und der Sparsamkeit (Kontrolle durch den Rechnungshof);
- sie hat insbesondere für rechtzeitige Korrekturen beim Stellenplan, d.h. in der jetzigen Situation (rückläufige Schülerzahlen, personalwirtschaftliche Erfordernisse aufgrund der Haushaltslage, geforderte Qualitätsverbesserungen) für die notwendigen Stellenveränderungen zu sorgen.

Zur Erfüllung dieser der BSB zugewiesenen Aufgaben ist die Verarbeitung der Lehrerdaten im Rahmen des LID-Verfahrens erforderlich (§ 9 Abs. 1 HmbDSG). Es bedarf daher auch keiner Einwilligung der Betroffenen (§ 5 Abs. 1 HmbDSG).

Ich habe auch untersucht, ob die BSB die Daten aufgrund einer Rechtsvorschrift (zwangsweise) von den Lehrern verlangen kann oder ob sie auf deren freiwillige Mitwirkung angewiesen ist. Zur Beurteilung dieser Frage ist auf die Vorschriften des Beamtenrechts zurückzugreifen und es ist zu prüfen, ob es hiernach für die Lehrer eine Dienstpflicht darstellt, die Erhebungsbogen auszufüllen.

Im Hamburgischen Beamtengesetz (HmbBG) sind – ebenso wie im Bundesbeamtengesetz (BBG) – die Dienstpflichten der Beamten in Form von Generalklauseln geregelt. Relevant sind hier insbesondere §§ 57-61 HmbBG, die wörtlich den §§ 52-57 BBG entsprechen. Zur Frage, ob diese beamtenrechtlichen Generalklauseln hinreichend bestimmt sind, so daß daraus konkrete Dienstpflichten abzuleiten sind, deren schuldhafte Verletzung als Dienstvergehen geahndet werden kann, führt das BVerfG in seinem Beschluß vom 17.9.1984 –2 BvR 1032/84– (in PersV 1985, 35) folgendes aus:

> Anders als das allgemeine Strafrecht, wo einzelne Straftatbestände mit entsprechenden Strafandrohungen zu versehen sind, ist das Disziplinarrecht seit jeher von Generalklauseln geprägt, wonach die schuldhafte Verletzung von Beamtenpflichten mit einer gesetzlich vorgesehenen Disziplinarstrafe geahndet wird (vgl. BVerfGE 26, 186 [204]). Die Verwendung von Generalklauseln findet ihre innere Rechtfertigung auch darin, daß eine vollständige Aufzählung aller Pflichten des Beamten im einzelnen in sachgerechter Weise kaum möglich ist. Sie ist auch nicht erforderlich. Denn die das Berufsbeamtentum regelnden Normen richten sich ausschließlich an den Personenkreis der Beamten. Sie konkretisieren ihre Pflichten, die sich unmittelbar aus den ihnen gestellten Aufgaben ergeben und die daher für sie als Betroffene aufgrund ihrer Vorbildung und ihres Status im allgemeinen ohne weiteres erkennbar sind (vgl. BVerfGE 48, 48 [57]). Generalklauseln, die diese Beziehung zwischen Berufspflicht und Berufsaufgaben zum Ausdruck bringen, sind daher eine hinreichend bestimmte Grundlage für eine disziplinarische Ahndung bei schuldhaften Verletzungen der Beamtenpflichten.

Das Beamtenverhältnis ist ausgestaltet als „Dienst- und Treueverhältnis". Die aus dieser Eigenart resultierenden Pflichten des Beamten im Verhältnis zu seinem Dienstherrn (daneben existieren Pflichten gegenüber dem Bürger) ergeben sich – soweit sie für das zu untersuchende Problem relevant sind – aus den §§ 57, 59, 60 HmbBG. Wesentlich ist hier die Pflicht zur wahrheitsgemäßen Auskunft oder sogar zur Offenbarung (ohne Befragung) über alle das Dienstverhältnis betreffenden Tatsachen. Auch für außerdienstliche Angelegenheiten bestehen Auskunftspflichten, wenn sie von dienstlicher Bedeutung sein können.

Die Wahrheitspflicht wird in den Beamtengesetzen nicht expressis verbis gefordert. Sie wird jedoch abgeleitet aus der Beratungs- und Unterstützungspflicht. Die Offenbarungspflicht ergibt sich auch aus der Pflicht zu achtungs- und vertrauenswürdigem Verhalten.

Die Pflicht zur Auskunft und zur Offenbarung hat jedoch Grenzen, sie besteht nicht,

- soweit Fragen gestellt werden oder Offenbarung verlangt wird über Angelegenheiten, denen jeder Bezug zum Amt oder zum Beamtenverhältnis fehlt,
- wenn der Beamte sich mit seiner Aussage selbst belasten müßte,
- soweit eine gesetzliche Geheimhaltungsvorschrift (z.B. das Wahlgeheimnis) entgegensteht.

Wegen dieser Begrenzung der Auskunfts- und Offenbarungspflicht ist diese an sich sehr weitgehende Beamtenpflicht, die mit dem aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG abgeleiteten Recht auf informationelle Selbstbestimmung konkurriert, auch verhältnismäßig.

Mit dem Verlangen, den LID-Fragebogen auszufüllen bzw. dort bereits vorgegebene Daten erforderlichenfalls zu korrigieren, wird die Grenze der Auskunftspflicht nicht überschritten:

- Durch die Erhebung werden vom Lehrer keine Daten zusätzlich zu den Daten erfragt, die dem Dienstherrn zulässigerweise schon bekannt sind bzw. die ihm schon aus anderen Gründen hätten mitgeteilt werden müssen. Der größte Teil der Daten ist nämlich in den Personalakten gespeichert und aufgrund von Gesetzen erhoben worden. Die restlichen Daten sind solche zum Beschäftigungsverhältnis im konkreten Fall (Stundenzahl, Mutterschutzfrist, Beurlaubung usw.), die in der Schule bei der Stundenplanerstellung und der sonstigen Organisation der Schule anfallen.
- Die Prüfung der einzelnen Daten der Lehrerindividualdatei hat ergeben, daß die Daten geeignet und erforderlich sind, um eine ordnungsgemäße Personalverwaltung und Personaleinsatzplanung in den Schulen zu gewährleisten. Gerade im Schulbereich liegt die Notwendigkeit der sorgfältigen Planung des Einsatzes der vorhandenen Lehrer in der gegenwärtigen Situation auf der Hand. Die vorgesehenen, durch das LID-Verfahren ermöglichten automatisierten Auswertungen sind ein Mittel zur Erfüllung der der BSB obliegenden Aufgaben und Pflichten.
- Die Daten werden bei den Betroffenen nur deshalb in dieser Form wiederholt abgefragt, weil der Dienstherr dies aus organisatorischen und verwaltungsökonomischen Gründen für das zweckmäßiste Verfahren hält.

Als Ergebnis ist festzustellen, daß die BSB die Daten zur LID aufgrund einer Rechtsvorschrift erhebt. Die Lehrer machen die Angaben nicht freiwillig, sondern in Erfüllung ihrer Beamtenpflichten. Wegen § 9 Abs. 2 HmbDSG ist auf den Erhebungsbogen darauf hinzuweisen, daß die Daten aufgrund der §§ 57, 59, 60 HmbBG erhoben werden.

4.2.5 Novellierung des Personalvertretungsgesetzes

Ich habe im 3. TB (3.2.4.1) über meine Vorschläge für eine Novellierung des Hamburgischen Personalvertretungsgesetzes berichtet. Inzwischen sind auch in Niedersachsen und Nordrhein-Westfalen die Personalvertretungsgesetze geändert worden. Die Änderungen gehen, soweit sie die Rechte der Personalvertretung beim Einsatz von

Technik betreffen, in dieselbe Richtung wie meine Vorschläge. Sie enthalten aber interessante Varianten:

- Das Niedersächsische Personalvertretungsgesetz gibt der Personalvertretung ein Recht auf Mitbestimmung bei der Festlegung der zu speichernden personenbezogenen Daten und der für sie geplanten Nutzungen, wenn zur Vorbereitung oder zum Vollzug personalrechtlicher Maßnahmen automatisierte Verfahren eingesetzt werden.

  Mit dieser Regelung wird die Mitbestimmung auf die Bestandteile eines automatisierten Verfahrens konzentriert, bei denen die schutzwürdigen Belange der Beschäftigten berührt sind, ohne daß die Personalvertretung das gesamte automatisierte Verfahren durcharbeiten und die für sie relevanten Bestandteile – es werden die in dem Niedersächsischen Personalvertretungsgesetz genannten sein – selbst herausfinden muß.

- Das Nordrhein-Westfälische Personalvertretungsgesetz geht in der Einräumung von Mitbestimmungsrechten am weitesten. Die Personalvertretung bestimmt danach unter der Überschrift „Mitbestimmung in Rationalisierungs-, Technologie- und Organisationsangelegenheiten" mit bei:

  Einführung, Anwendung, wesentlicher Änderung oder wesentlicher Erweiterung von automatisierter Verarbeitung personenbezogener Daten der Beschäftigten außerhalb von Besoldungs-, Gehalts-, Lohn- und Versorgungsleistungen;

  Einführung, Anwendung, wesentlicher Änderung oder Erweiterung von technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen;

  Einführung, wesentlicher Änderung oder wesentlicher Ausweitung neuer Arbeitsmethoden, insbesondere Maßnahmen der technischen Rationalisierung;

  Einführung, wesentlicher Änderung oder wesentlicher Ausweitung betrieblicher Informations- und Kommunikationsnetze.

  (Anmerkung: Dieser Mitbestimmungstatbestand zielt offensichtlich auf die Bürokommunikation.)

  Mit diesen Mitbestimmungstatbeständen wird praktisch die gesamte Informations- und Kommunikationstechnik abgedeckt; es ist schwer vorstellbar, daß ein Vorhaben nicht darunter fällt.

In Hamburg gibt es neben dem Ersuchen der Bürgerschaft an den Senat, ihr mitzuteilen, welche Notwendigkeiten zur Anpassung des Personalvertretungsgesetzes bestehen, damit noch in dieser Wahlperiode eine Novellierung erfolgen kann, einen Initiativantrag der GAL-Fraktion zur Novellierung des Hamburgischen Personalvertretungsgesetzes. Dieser Entwurf enthält für die Mitbestimmung der Personalvertretung beim Einsatz von Informations-und Kommunikationstechnik, insbesondere auch für die Verarbeitung personenbezogener Daten der Beschäftigten, brauchbare Ansätze, die jedoch im Lichte der Novellierungen in Hessen, Niedersachsen und Nordrhein-Westfalen präzisiert und ergänzt werden müssen. Die Hamburger Bürgerschaft hat in ihrer Sitzung am 5.9.1985 den Initiativantrag der GAL-Fraktion weder an einen Ausschuß überwiesen noch angenommen.

4.3 Statistik

4.3.1 Volkszählung

4.3.1.1 Volkszählungsgesetz 1987

Der Deutsche Bundestag hat in seiner Sitzung am 26.9.1985 das Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1987) gegen die Stimmen der GRÜNEN und einiger Abgeordneter der SPD

beschlossen. Der Bundesrat hat dem Volkszählungsgesetz 1987 in seiner Sitzung am 18.10.1985 zugestimmt. Das Volkszählungsgesetz 1987 ist am 14.11.1985 im Bundesgesetzblatt Teil I, S. 2078 verkündet worden und am 15.11.1985 in Kraft getreten.

Den Gesetzbeschlüssen ist eine ungewöhnlich intensive Beratung vorangegangen, in der alle Beteiligten sich bemüht haben, den Anforderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts zu entsprechen.

Die Datenschutzbeauftragten sind in beispielhafter Weise an der Erarbeitung des Gesetzes beteiligt worden, zuletzt in der Schlußphase der parlamentarischen Beratung bei der Suche nach einer Regelung, die sowohl den Informationsbedürfnissen der Kommunen als auch den Belangen des Datenschutzes Rechnung trägt (da Hamburg dieses Problem nicht betrifft, gehe ich nicht näher darauf ein).

In der Debatte des Deutschen Bundestages am 26.9.1985 haben die Sprecher der CDU/CSU, SPD und FDP übereinstimmend festgestellt, daß das Volkszählungsgesetz 1987 alle Anforderungen des Datenschutzes erfüllt. Dieser Feststellung schließe ich mich an.

In weiten Teilen der Bevölkerung bestehen – wenn man den Ergebnissen der Demoskopen trauen darf – auch weiterhin Reserve und Skepsis gegenüber der Volkszählung. Es wird sich in der von Bund und Ländern beabsichtigten Aufklärungskampagne herausstellen, in welchem Ausmaß die Reserve auf Unkenntnis beruht und durch entsprechende Informationen abgebaut werden kann. Man wird sich aber darauf einstellen müssen, daß ein Rest an grundsätzlichem Widerstand bleiben wird; wie groß dieses Verweigerunspotential sein wird, kann heute nicht einmal vermutet werden. Man kann aber heute schon sagen, daß Zwangs- und Bußgelder als Mittel der Durchsetzung versagen werden, wenn der Widerstand eine beträchtliche Größenordnung hat; denn Zwangs- und Bußgelder sind nur tauglich, eine kleine Minderheit an ihre Pflichten als Bürger zu erinnern.

4.3.1.2 Akzeptanz der Volkszählung

Die Anstrengungen von Bund und Ländern zur Vorbereitung der Volkszählung müssen sicher darauf gerichtet sein, über alle Maßnahmen zum Datenschutz zu informieren; für mindestens ebenso wichtig halte ich es, daß Bund und Länder auf folgende Fragen überzeugende Antworten geben:

(1) Ist eine Volkszählung überhaupt notwendig?

Nach meiner Auffassung genügt es hier nicht, auf die entsprechenden Ausführungen im Volkszählungsurteil des Bundesverfassungsgerichts hinzuweisen; diese sind zwar überzeugend, aber für weite Kreise der Bevölkerung zu allgemein und abstrakt. Die Verantwortlichen müssen die Notwendigkeit der Volkszählung an Beispielen veranschaulichen, die auch für Laien verständlich sind; ich denke dabei an die Zusammenhänge zwischen Bevölkerungsverteilung und Infrastrukturbedarf. Bund und Länder wären gut beraten, auf abgenutzte und schon daher wenig überzeugende Beispiele zu verzichten.

(2) Muß die Volkszählung eine Totalerhebung sein?

Hier scheint es mir möglich zu sein, auf der Grundlage der Anhörung im Bundestag jedermann, der bereit ist zuzuhören, zu überzeugen, daß die Volkszählung als Totalerhebung nicht durch Stichproben ersetzt werden kann. Auch hierbei wird es erforderlich sein, die abstrakten theoretischen Überlegungen durch lebensnahe und dadurch überzeugende Beispiele anschaulich zu machen.

An dieser Stelle halte ich es für notwendig, mich nochmals mit der Alternative auseinanderzusetzen, die Volkszählung durch eine Auswertung von Verwaltungsregistern zu ersetzen, wie es der Sprecher der GRÜNEN – für mich überraschend – in der 2. Lesung im Deutschen Bundestag wieder vorgeschlagen hat. Das Bundesverfassungsgericht hat zu Recht im Volkszählungsurteil diese Alternative als die datenschutzrechtlich weitaus bedenklichere verworfen: „Auch die Übernahme

sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung ist keine zulässige Alternative zu der vorgesehenen Totalzählung. Denn die Nutzung von Daten aus verschiedenen Registern und Dateien würde voraussetzen, daß technische, organisatorische und rechtliche Maßnahmen getroffen werden, die es erst erlauben, diese Daten, bezogen auf bestimmte Personen oder Institutionen, zusammenzuführen. Eine solche Maßnahme wäre z.B. die Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens oder dessen Substituts. Dies wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren. Die Verknüpfung vorhandener Dateien wäre danach auch nicht das mildere Mittel." (Urteil S. 60)

(3) Warum kann die Teilnahme an der Volkszählung nicht freiwillig sein?

Es wird nach meiner Auffassung schwer sein, die komplizierten fachlichen Überlegungen einer breiten Öffentlichkeit verständlich zu machen, die den gesetzlichen Auskunftszwang begründen; die notwendigen Anstrengungen müssen aber unternommen werden.

Ein wichtiges Argument ist dabei, daß der Deutsche Bundestag sich gerade auch mit der Freiwilligkeit auseinandergesetzt und im Rahmen der Volkszählung 1987 noch keine Möglichkeit gesehen hat, statistische Merkmale auf freiwilliger Grundlage zu erfragen. Er hat aber die Bundesregierung aufgefordert, im Zusammenhang mit der Volkszählung 1987 Untersuchungen über die Möglichkeit freiwilliger Erhebungen anzustellen.

In diesem Zusammenhang halte ich es für wichtig, darauf hinzuweisen, daß die Voraussetzungen in zwei Ländern, auf die als Beispiel für erfolgreiche freiwillige Erhebungen häufig hingewiesen wird, grundlegend anders sind als in der Bundesrepublik: In den USA wird die Teilnahme an solchen statistischen Erhebungen von der Bevölkerung als Bürgerpflicht angesehen, Verweigerungen sind so gut wie unbekannt. In Schweden werden Ausfälle infolge Nichtteilnahme durch Rückgriff auf Verwaltungsregister ausgeglichen.

(4) Sind die auf Dauer in den statistischen Landesämtern gespeicherten Volkszählungsdaten vor Mißbrauch sicher?

Ich bin sicher, daß Mißbrauch – soweit es durch technische und organisatorische Maßnahmen überhaupt möglich ist – ausgeschlossen ist. Für die Phase, in der die Daten noch nicht durch Entfernung der Ordnungsnummern und Ersetzung der Anschrift (Straße/Hausnummer) durch die entsprechende Blockseite hinreichend anonymisiert sind, werden besondere Vorkehrungen geplant, an denen ich frühzeitig beteiligt werde.

Danach ist ein Mißbrauch nicht lohnend, wenn nicht sogar unmöglich, weil die im Rechenzentrum gespeichertern Daten nicht mehr zugänglich sind und aus den Daten nicht mehr mit vertretbarem Aufwand und hinreichender Sicherheit auf eine bestimmte Person geschlossen werden kann.

In diesem Zusammenhang bekräftige ich meine an anderer Stelle in diesem Bericht (s. S. 19 f) ausführlich begründete Auffassung, daß die wiederholt aufgestellten Behauptungen haltlos sind, durch die Zusammenfassung der Statistikdaten mit anderen Daten in einem Rechenzentrum würde dem Mißbrauch Tür und Tor geöffnet und man könnte beweisen, daß trotz „Anonymisierung" auf die dahinter stehende Person geschlossen werden könne.

Die mißbräuchliche Nutzung der Statistikdaten wäre nur durch vorsätzlichen Gesetzesverstoß von Behörden möglich, die befugt sind, dem Rechenzentrum Aufträge zu erteilen; die entsprechende Verarbeitung wäre genau so auffällig, wie wenn die Daten in verschiedenen Rechenzentren gespeichert wären. Ich habe an anderer Stelle (S. 23 f) über die Ergebnisse meiner Prüfung im Rechenzentrum berichtet; daraus ergibt sich, daß ein Mißbrauch der Daten durch einzelne Bedienstete des Rechenzentrums so gut wie ausgeschlosssen ist.

Ich habe Zweiflern aus der Informatik angeboten, die Deanonymisierung in meinem Beisein praktisch zu demonstrieren. Sie haben das Angebot bis heute nicht angenommen.

Ich bin nicht sicher, ob ein noch späterer Zeitpunkt als der jetzt vorgesehene die Akzeptanz der Zählung erhöhen würde. Bei dieser Frage kommt es nicht so sehr auf die Auswirkungen für die staatliche Planung, sondern entscheidend darauf an, ob sich die Einstellung der Bevölkerung im Laufe der Zeit ändern wird. Wenn angenommen wird – und ich neige dieser Annahme zu –, daß die Skepsis und teilweise sogar Ablehnung der Volkszählung nicht so sehr die Volkszählung selbst betrifft, sondern eher Ausdruck eines allgemeinen Unbehagens und Mißtrauens ist, dann dürfte sich die Einstellung durch Zeitablauf kaum ändern; denn die Ursachen für diese Einstellung, vor allem die wegen der Komplexität der Lebensverhältnisse zwangsläufige Undurchschaubarkeit des staatlichen Handelns werden bleiben.

Der Deutsche Bundestag hat bei der Verabschiedung des Volkszählungsgesetzes festgestellt, daß es gegenwärtig keine andere Möglichkeit als die Volkszählung gibt, die notwendigen Grunddaten über die Bevölkerung zu erhalten, um eine sachgerechte und vorausschauende, im Interesse jedes einzelnen Bürgers liegende Politik zu betreiben, und alle Mitbürger gebeten, im Interesse der Allgemeinheit, aber auch jedes einzelnen, sich an der Zählung zu beteiligen und sie zu unterstützen.

Der Bundestag hat darüber hinaus die Bundesregierung ersucht, dafür Sorge zu tragen, daß der nach dem Mikrozensusgesetz vorgesehene wissenschaftliche Beirat auch an der Vorbereitung und Durchführung der Volkszählung mitwirkt, und er hat die Bundesregierung gebeten, bis 1.6.1986 über die bis dahin ergangenen landesrechtlichen Regelungen und den Stand der Vorbereitung der Zählung, bis 1.1.1988 über die Durchführung, den Stand der Auswertungen und die Einhaltung der datenschutzrechtlichen Sicherungen sowie den Stand der Methodendiskussion zu berichten. Der Bundestag hat damit demonstriert, daß er die Verantwortung für die Volkszählung auch weiterhin nicht allein der Regierung überlassen will.

Der Bundestag hat die Erwartung ausgesprochen, daß Länder und Gemeinden in zeitlicher und organisatorischer Verknüpfung mit der Volkszählung keine anderen, auch keine freiwilligen statistischen Erhebungen durchführen, weil dadurch die Akzeptanz und damit der Erfolg der Zählung gefährdet werden könnten. Mir sind z.Z. keine Absichten bekannt, in Hamburg zusätzliche Erhebungen durchzuführen; ich würde, wenn ich von derartigen Plänen hören sollte, entschieden davon abraten.

§ 9 des Volkszählungsgesetzes 1987 regelt die Einrichtung der Erhebungsstellen und die Pflichten des Personals in den Erhebungsstellen; § 9 Abs. 3 erlegt den Ländern auf, die Erhebungsstellen zu bestimmen und die Abschottung der Erhebungsstellen von der übrigen Verwaltung zu näher regeln; dies kann auch in Form einer Rechtsverordnung geschehen. Es gibt einen Musterentwurf für landesrechtliche Regelungen, den die Dienstaufsichtsbehörden der Statistischen Ämter erarbeitet haben. Ich erwarte, daß in Hamburg alsbald Schritte für eine landesrechtliche Regelung unternommen werden und daß ich frühzeitig daran beteiligt werde.

4.3.2 Mikrozensus und EG-Erhebung

4.3.2.1 Mikrozensusgesetz

Das Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensusgesetz) vom 10.6.1985 ist am 13.6.1985 verkündet worden und am 14.6.1985 in Kraft getreten. Die Erhebungsmerkmale werden durch die Verordnung zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensusverordnung) vom 14.6.1985 konkretisiert.

Damit sind die rechtlichen Voraussetzungen dafür geschaffen worden, den Mikrozensus 1985 wieder durchzuführen, nachdem er in den Jahren 1983 und 1984 ausgesetzt worden war.

Der Gesetzentwurf ist intensiv beraten worden; u.a. wurde eine umfangreiche öffentliche Anhörung von Sachverständigen durchgeführt. Die Beratungen haben zu zahlreichen Änderungen und insgesamt zu einem Gesetz geführt, das den Anforderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts entspricht. Meine Kritik im 3. TB (3.6.3.2) an dem damaligen Gesetzentwurf ist durch die endgültige Fassung erledigt. Ich habe daher keine datenschutzrechtlichen Bedenken mehr gegen das Mikrozensusgesetz.

4.3.2.2 Auskunftszwang oder Freiwilligkeit?

Neben dem Umfang der Erhebungsmerkmale und den Anforderungen an die Geheimhaltung stand die Frage, ob der Mikrozensus grundsätzlich unter Auskunftszwang oder auf freiwilliger Basis durchgeführt werden soll, im Vordergrund der Beratungen. Die Ansicht, daß aus dem Volkszählungsurteil des Bundesverfassungsgerichts abzuleiten sei, es sei verfassungsrechtlich geboten, statistische Erhebungen nur noch freiwillig durchzuführen, ist nach gründlicher verfassungsrechtlicher Prüfung verworfen worden. Der Deutsche Bundestag hat keinen anderen Weg gesehen, als den Mikrozensus einstweilen noch unter Auskunftszwang durchzuführen.

Er hat aber in einer Entschließung seinen Willen bekräftigt,

- den eingeschlagenen Weg, Bevölkerungsbefragungen als Bundesstatistiken auf freiwilliger Basis durchzuführen, konsequent mit dem Ziel fortzusetzen, die Freiwilligkeit der Beantwortung im Mikrozensus möglichst auf alle Sachverhalte zu erstrecken,
- die Bundesregierung ersucht, ihm vor und während der in § 13 Mikrozensusgesetz vorgeschriebenen Testerhebungen auf freiwilliger Basis darüber zu berichten,
- die Bundesregierung ferner ersucht, ihm umfassend über methodische Fragen beim Mikrozensus (Umfang der Erhebung, andere Methoden, Freiwilligkeit) zu berichten.

Diese Entscheidung spiegelt die Ergebnisse der fachlichen Diskussion über die Frage des Auskunftzwanges wider. Die überwiegende Mehrheit der in der öffentlichen Anhörung vertretenen Sachverständigen hat die Auffassung vertreten, daß jedenfalls zum gegenwärtigen Zeitpunkt auf eine Auskunftspflicht nicht verzichtet werden könne. Dies wurde vor allem damit begründet, daß die Antwortquote bei freiwilligen Erhebungen unvertretbar niedrig sei; sie betrage z.B. bei sozialwissenschaftlichen Instituten häufig nur 60 v.H., so daß die Befragung nur mit Hilfe der auf Auskunftszwang beruhenden Ergebnisse der amtlichen Statistik verwendbar gemacht werden könnten. Die positiven Erfahrungen des Instituts für Arbeitsmarkt- und Berufsforschung der Bundesanstalt für Arbeit mit freiwilligen Erhebungen könnten nicht verallgemeinert werden, weil sie in einem speziellen Bereich durchgeführt würden, in dem die Arbeitnehmer in besonderem Maße berührt seien und daher ein besonderes Engagement die Voraussetzung für hohe Antwortquoten bilde. Die Gefahr von niedrigen Antwortquoten liege bei einer fachlich sehr breiten, außerordentlich differenzierten Befragung wie dem Mikrozensus darin, daß die Ergebnisse nicht mehr repräsentativ und damit wertlos seien, weil die ausgefallenen Teilnehmer nicht genau so verteilt seien wie die insgesamt ausgewählten Teilnehmer (die Stichprobe).

Angesichts der Intensität der Beratungen und des erreichten Ergebnisses halte ich die Regelung im Mikrozensusgesetz (grundsätzlicher Auskunftszwang mit Freiwilligkeit bei bestimmten Fragen) für verfassungsrechtlich unbedenklich. Meine Auffassung ist inzwischen auch durch einen Beschluß des Verwaltungsgerichts Frankfurt bestätigt worden, mit dem ein Eilantrag auf Wiederherstellung der aufschiebenden Wirkung eines Widerspruchs gegen die Heranziehung zur Auskunftspflicht zurückgewiesen wurde.

4.3.2.3 Durchführung des Mikrozensus

Das Statistische Landesamt hat unmittelbar nach Inkrafttreten des Mikrozensusgesetzes begonnen, den schon vorher vorbereiteten Mikrozensus durchzuführen. Dies

führte u.a. dazu, daß mich Anfragen zum Mikrozensus erreichten, bevor ich den Gesetzestext in Händen hatte. Das Statistische Landesamt begründete diese Eile damit, daß der Mikrozensus 1985 – um die Vergleichbarkeit der Ergebnisse sicherzustellen – wie alle vorangegangenen Erhebungen in der ersten Jahreshälfte durchgeführt werden und im wesentlichen vor dem Beginn der Sommerferien abgeschlossen sein sollte. So verständlich diese Erwägungen aus der Sicht des Statistischen Landesamtes sein mögen, akzeptanzfördernd war das überfallartige Vorgehen m.E. nicht.

In den ersten Wochen haben sich viele Auskunftspflichtige an mich gewandt; ihre Fragen konzentrierten sich auf den Auskunftszwang und die Geheimhaltung. Ich habe den Petenten meinen oben wiedergegebenen Standpunkt dargelegt. Hinsichtlich der Geheimhaltung habe ich aufgrund früherer Prüfungen im Statistischen Landesamt versichert, daß ich die Gefahr eines Mißbrauchs für nahezu ausgeschlossen halte. Inzwischen habe ich mich im Statistischen Landesamt nochmals davon überzeugt, daß die Anforderungen an die Geheimhaltung im wesentlichen erfüllt werden. Ich halte es aber für notwendig, beim nächsten Mikrozensus das Verfahren für die Auswahl der Interviewer zu verbessern und den Nachbarschaftsbereich – in dem die Interviewer nicht eingesetzt werden dürfen – zu erweitern.

In der Presse hat es teilweise irreführende Berichte gegeben, die ich auch in diesem Bericht richtigstellen möchte:

(1) In einigen Zeitungen ist die Durchführung des Mikrozensus gerade in Hamburg als „hochgradig bedenklich" bezeichnet worden, weil aufgrund einer „im Bundesgebiet einmaligen und gefährlichen Kumulierung von Daten" die De-Anonymisierung leicht möglich sei. Mit diesen Vorwürfen setze ich mich an anderer Stelle (S. 19) ausführlich auseinander.

(2) Weiter wurde von einer „unzulässigen Nacherhebung" berichtet, weil im ersten Durchgang nicht genügend Auskunftspflichtige geantwortet hätten, – damit wurde der Eindruck erweckt, es würden weitere Personen in den Mikrozensus einbezogen. Das ist schlicht falsch; offenbar wurde die erneute Aufforderung an Auskunftspflichtige, die im ersten Durchgang ihrer Auskunftspflicht nicht nachgekommen waren, als erstmalige Heranziehung neuer Auskunftspflichtiger fehlinterpretiert.

4.3.2.4 Information der Bevölkerung

Auch beim Mikrozensus 1985 gab es Ansätze zu einer Boykottbewegung, die von einigen Presseerzeugnissen unterstützt wurde. Nach dem Stand vom 9.12.1985 haben von rd 8.000 auskunftspflichtigen Haushalten 128 ihre Auskunftspflicht noch nicht erfüllt.

Das Statistische Landesamt erzwingt die Beantwortung des Fragebogens mit der Androhung und Verhängung von Zwangsgeldern nach dem Hamburgischen Verwaltungsvollstreckungsgesetz vom 13.3.1961 in der Fassung vom 8.3.1982. Ich finde es sehr bedauerlich, daß die Auskunftspflichtigen hierüber nicht in der vor dem Mikrozensus verteilten Informationsbroschüre, sondern erst in dem sog. Heranziehungsbescheid informiert worden sind.

4.3.3 Handels- und Gaststättenzählung

4.3.3.1 Gesetz über die Statistik im Handel und Gastgewerbe

Aufgrund des § 1 Abs. 4 des Gesetzes über die Statistik im Handel und Gastgewerbe (HdlStatG) vom 10.11.1978 (BGBl. I S. 1733) wurde im Berichtszeitraum eine Zählung der Unternehmen und Arbeitsstätten im Handel und Gastgewerbe – Handels- und Gaststättenzählung 1985 – durchgeführt. Die Zählung erstreckte sich auf Unternehmen und Arbeitsstätten

des Groß- und Einzelhandels,
der Handelsvermittlung und
des Gastgewerbes.

4.3.3.2 Beschluß der Konferenz der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten hat sich mit der Handels- und Gaststättenzählung befaßt und dazu einen Beschluß gefaßt, der im wesentlichen folgende Punkte anspricht:

- Es wird gerügt, daß die Datenschutzbeauftragten nicht – wie vom Bundesverfassungsgericht gefordert – frühzeitig beteiligt worden sind.
- Es wird festgestellt, daß das Handelsstatistikgesetz in Teilen nicht den Anforderungen des Volkszählungsurteils entspricht und daher dringend einer Novellierung bedarf.
- Es wird bezweifelt, ob für einige Fragen im Erhebungsbogen (über gewerblichen Umsatz, unternehmensinterne Dienstleistungen, Zweigniederlassungen, Auszeichnung der Waren mit Brutto- oder Nettopreisen) eine gesetzliche Grundlage vorhanden ist.
- Es wird darauf hingewiesen, daß die Hilfsmerkmale in dem Gesetz überhaupt nicht bestimmt sind und daß präzise gesetzliche Regelungen über die Trennung der Hilfsmerkmale von den Erhebungsmerkmalen und ihre Löschung fehlen.
- Die Konferenz fordert die Abtrennung des Namens und der Anschrift sowie weiterer Hilfsmerkmale von den Erhebungsbogen unverzüglich nach Abschluß der maschinellen Plausibilitätskontrolle, spätestens bis zum Ablauf einer zu bestimmenden Frist, und ihre Vernichtung. Dies muß bis zu einer entsprechenden Änderung des Handelsstatistikgesetzes durch die zuständige oberste Landesbehörde festgelegt sein.
- Es wird gefordert, bis zu einer anderweitigen gesetzlichen Regelung die von den Finanzbehörden nach § 6 Abs. 2 HdlStatG für die Durchführung der Zählung gelieferten und mit den Angaben aus der Zählung korrigierten und ergänzten Adreßdateien nur für Zählungen nach dem HdlStatG, nicht aber für andere statistische Zwecke zu nutzen.

Die Beanstandungen der Datenschutzbeauftragten zum Verfahren werden durch das im Statistischen Landesamt Hamburg praktizierte Verfahren fast völlig ausgeräumt und ihre Forderungen weitgehend erfüllt. Insbesondere sollen Name und Anschrift sowie weitere Hilfsmerkmale in Hamburg nach Abschluß der maschinellen Plausibilitätskontrolle von den Erhebungsbogen abgetrennt und vernichtet werden; ich werde mich an Ort und Stelle davon überzeugen, daß das auch tatsächlich geschieht. Damit kann die im Erhebungsbogen benutzte Kenn-Nummer nicht mehr unmittelbar zur Identifizierung benutzt werden, weil der Teil des Fragebogens vernichtet worden ist, der den zur Kenn-Nummer gehörigen Namen und die Anschrift enthält.

Allerdings wird die Kenn-Nummer auch in der Adreßdatei gespeichert; dies geschieht aus folgendem Grund: Für künftige Befragungen nach dem Handelsstatistikgesetz und nach anderen Statistikgesetzen werden Unternehmen aufgrund einer Auswertung des Datenbestandes aus der Handels- und Gaststättenzählung 1985 ausgewählt. Von diesen Unternehmen sind zunächst nur die Kenn-Nummern bekannt. Anhand der Kenn-Nummer können dann Name und Anschrift des zu befragenden Betriebes festgestellt werden.

Durch die Speicherung der Kenn-Nummer im Datenbestand der Handels- und Gaststättenzählung und in der Adreßdatei ist ohne Zweifel die Möglichkeit der Reidentifizierung gegeben. Ich halte es jedoch wegen der im Statistischen Landesamt getroffenen Verfahrensregelungen für nahezu ausgeschlossen, daß diese Möglichkeit auch praktisch genutzt wird.

Das tatsächliche Verfahren der Handels- und Gaststättenzählung entspricht also weitgehend den Anforderungen des Bundesverfassungsgerichts. Das Handelsstatistikgesetz bleibt allerdings dahinter zurück. Daher zielt der Beschluß der Datenschutzbeauftragten hauptsächlich auf die Novellierung des Gesetzes.

4.3.3.3 Übermittlung von Daten durch die Finanzverwaltung

Gemäß § 6 Abs. 2 HdlStatG hat die Finanzverwaltung die Anschriften und Gewerbekennziffern aller Unternehmen des Handels- und Gastgewerbes an das Statistische Landesamt übermittelt, und darüber hinaus auch die Nummer des zuständigen Finanzamtes und die Steuernummer, ohne daß das Statistische Landesamt dies gefordert hat; das Statistische Landesamt benötigt diese Daten nicht und hat sie auch nicht genutzt. Es hat diese Daten inzwischen gelöscht. Die Übermittlung dieser Daten war durch die Rechtsvorschrift nicht gedeckt. Ich habe die Finanzbehörde aufgefordert, Stellung zu nehmen.

4.3.4 Hochschulstatistik

Ich habe im 3. TB ausführlich über die Probleme der Hochschulstatistik berichtet. In der Diskussion über die Novellierung des Hochschulstatistikgesetzes stand im Berichtszeitraum die Studentenverlaufsstatistik im Vordergrund.

4.3.4.1 Studentenverlaufsstatistik

Die Verlaufsstatistik erfordert, daß die von den Studenten semesterweise erhobenen Daten personenbezogen gespeichert werden. Zwar sind die Studenten nicht explizit bezeichnet, doch die zur Identifikation gespeicherten Daten bzw. Rudimente von Daten – z.B. Teile des Namens – erlauben die Reidentifizierung des Studenten. Insbesondere mit der Anonymisierung der Daten, die für statistische Zwecke erhoben und verarbeitet werden, hat das BVerfG aber datenschutzrechtliche Erleichterungen für die Statistik begründet.

4.3.4.2 Bewertung

Der Grundsatz der Verhältnismäßigkeit fordert, daß die Verlaufsstatistik zur Erreichung des angestrebten Zweckes geeignet und erforderlich sein muß und daß kein milderes Mittel zur Verfügung stehen darf.

An der Geeignetheit der Verlaufsstatistik bestehen schon deshalb Bedenken, weil nicht sicher ist, ob die Zusammenführung der Daten in ausreichendem Maße und mit vertretbarem Aufwand gelingt. Im Statistischen Landesamt ist bei dem jüngst unternommenen Versuch, die Daten aus nur zwei Semestern zusammenzuführen, eine hohe Zahl von Fehlern, darunter auch nicht zuzuordnende Fälle, aufgetreten.

Diese Erfahrung ist auch in einer Diskussion von Praktikern und Wissenschaftlern in einem „Fachgespräch zu Fragen der Studienverlaufsauswertungen" (im folgenden als „Fachgespräch" zitiert) 1982 bestätigt worden.

Es bestehen ferner gewichtige Zweifel daran, ob eine Verlaufsstatistik für hochschulpolitische Entscheidungen unverzichtbar ist. Von einigen Teilnehmern des„Fachgesprächs" sind Informationen über durchschnittliche Studienzeiten, Fachwechsel, Studienabbruch, Verlassen der Universität mit Examen (die sämtlich nur aus Verlaufsauswertungen gewonnen werden können) als unverzichtbar bezeichnet worden. Dem sind folgende Argumente entgegengehalten worden: Vorstellbare Verbesserungen bei den Prognosen der Studentenzahlen sind nicht so bedeutsam, daß allein dadurch die Einführung einer Verlaufsauswertung gerechtfertigt werden kann. Im allgemeinen lassen sich nämlich auch unter Verwendung der schon heute möglichen Verfahren auf der Basis der Stichtagserhebungen relativ zuverlässige Studentenzahlprognosen erstellen. Die zur Verbesserung der Prognose des Übergangsverhaltens in das Hochschulsystem wünschenswerte Differenzierung der Übergangsquote nach Jahr und Erwerb der Studienberechtigung sollte ebenfalls über die Bestandsstatistik möglich sein. Weiterhin ist zu bedenken, daß für die Analyse z.B. des Studienwechsels neben Zahlen auch Informationen über die Motive des Studienwechsels erforderlich sind. Diese kann aber auch die Studentenverlaufsstatistik nicht liefern.

Insgesamt sind ohne Zweifel Erhebungen über den Studienverlauf erforderlich. Es ist

jedoch fraglich, ob dies in der Form einer Totalerhebung geschehen muß. Zweifelsfrei ist das nur bei Mehrfachimmatrikulationen; in allen übrigen Fällen läßt sich der Informationsbedarf auch durch Stichprobenerhebungen und Hochrechnung auf der Grundlage der Bestandsstatistik decken.

Gegenüber einer Verlaufsstatistik als Totalerhebung mit Auskunftszwang ist eine Verlaufsstatistik auf Stichprobenbasis und auf der Grundlage der Freiwilligkeit das mildere Mittel. Dieses ist zu wählen, weil hiermit – wie das „Fachgespräch" ergeben hat – Ergebnisse in ausreichender Qualität erzielt werden können. So heißt es u.a., daß die höheren Ausfälle aufgrund der Freiwilligkeit methodisch bzw. verfahrenstechnisch nicht so schwerwiegend seien wie die Zusammenführungsverluste bei den Studienverlaufsauswertungen in der Amtlichen Statistik, daß ferner auch mit Hilfe von Daten aus der Bundesstatistik überprüft werden könne, ob die Zusammensetzung der bei einer Stichprobenbefragung Mitwirkenden in wesentlichen Merkmalen der Zusammensetzung der Grundgesamtheit entspricht.

Gegen eine Stichprobenerhebung kann auch nicht eingewendet werden, der zur Wahrung der Repräsentativität erforderliche Auswahlsatz von 200.000 Studenten sei organisatorisch nicht zu bewältigen. Die Erfahrungen aus dem Mikrozensus (600.000 Befragte) widerlegen diese Vermutungen.

Ein milderes Mittel gegenüber der Verlaufsstatistik als Totalerhebung und mit Auskunftszwang ist auch die Auswertung der Bestandsstatistik, wenn die Ergebnisse daraus ausreichend sind. Es dürfte unbestritten sein, daß durch die Auswertung der Bestandsstatistik – etwa mit dem Verfahren der auch in dem „Fachgespräch" mehrfach erwähnten Kohortenrechnung – die typischen Fälle erfaßt und nachgewiesen werden; es fehlen nur die „Exoten". Es ist nach meiner Ansicht aber sehr fraglich, ob diese wenigen Fälle den schwerwiegenden Eingriff, der alle Studenten trifft, rechtfertigen können, zumal in der gegenwärtigen Enge öffentlicher Haushalte kaum damit gerechnet werden kann, daß für ihre Probleme spezielle Maßnahmen ergriffen werden.

Ein zwischen den beteiligten Bundesministerien abgestimmter Entwurf für ein Hochschulstatistikgesetz liegt noch nicht vor.

4.3.5 Landesstatistikgesetz

Ich habe in meinem 3. TB (3.6.6) ausgeführt, es werde noch sorgfältig zu prüfen sein, ob angesichts der Tatsache, daß die Amtliche Statistik in Hamburg ausschließlich auf Bundesrecht beruht, Bedarf für ein Landesstatistikgesetz besteht. Folgende Gesichtpunkte sprechen für ein Landesstatistikgesetz:

- Durch ein Landesstatistikgesetz wird nicht nur die aufgrund von Rechtsvorschriften angeordnete, d.h. Amtliche Statistik zu regeln sein. Regelungsbedürftig sind alle Statistiken, also auch Geschäftsstatistiken, Statistiken für besondere Zwecke, z.B. Planungsvorhaben, Statistiken aufgrund Verwaltungsvereinbarung.
- Es gibt außerdem statistische Erhebungen von juristischen Personen des öffentlichen Rechts, die unter der Aufsicht der Freien und Hansestadt Hamburg stehen.
- Das Bundesstatistikgesetz ist als Rahmengesetz angelegt, das durch weitere Regelungen der Länder, die Bundesstatistiken als eigene Angelegenheit ausführen, ausgefüllt werden.

Ich beabsichtige, demnächst hierüber mit den beteiligten Behörden zu diskutieren.

4.4 Gewerbewesen

4.4.1 Übermittlungen aus dem Gewerberegister und durch die Handelskammer

Ich habe mehrere Eingaben erhalten, in denen die Petenten darüber klagten, daß sie nach Anzeige der Aufnahme eines Gewerbes Werbematerial zugesandt bekamen, obwohl sie die Erklärung abgegeben hatten, daß sie mit der Weitergabe ihrer Daten durch das Wirtschafts- und Ordnungsamt nicht einverstanden seien. Auf Nachfrage

erklärten die jeweiligen Wirtschafts- und Ordnungsämter, daß sie entsprechend der Weisung des Anzeigenden die Daten nicht weitergegeben hätten.

Durch Hinweise anderer Datenschutzbeauftragter und durch die Antwort des Senats auf eine Schriftliche Kleine Anfrage betr. Bekanntgabe von Anschriften aus dem Bereich der Gewerbeneuanmeldungen (Drucksache 11/3798) bin ich darauf gestoßen, daß die Handelskammer Hamburg – die von den Wirtschafts- und Ordnungsämtern Durchschriften der Gewerbeanzeigen erhält, wenn die Anzeigenden nach der Art ihres Gewerbes kammerzugehörig sind – die Daten aus Neuanmeldungen an Interessenten weitergibt. Bei der früheren Organisation des Verfahrens – die Erklärung des Anzeigenden befand sich nur auf der vom Wirtschafts- und Ordnungsamt angelegten Karteikarte, die die Handelskammer nicht erhielt, nicht aber auf der Gewerbeanzeige, die die Handelskammer erhielt – hatte die Handelskammer keine Kenntnis von der Entscheidung des Anzeigenden.

Die Verwaltung hat die Schriftliche Kleine Anfrage zum Anlaß genommen, die Übermittlung von Daten über neu aufgenommene Gewerbe aus dem Gewerberegister für Zwecke der Werbung und Meinungsforschung einzustellen. Maßgebend dafür war, daß nach den letzten Erhebungen über 90 v.H. derjenigen, die die Aufnahme eines Gewerbes anzeigen, nicht damit einverstanden waren, daß ihre Daten für Werbezwecke an Private übermittelt werden.

Die Handelskammer hat, nachdem sie erstmalig Kenntnis davon erhalten hatte, daß viele Kleingewerbetreibende mit der Übermittlung ihrer Daten nicht einverstanden sind, die Weitergabe eingestellt. Nach einer umfassenden Erörterung der datenschutzrechtlichen Problematik hat die Handelskammer folgendes Verfahren vorgesehen:

- Bei Neuzugängen wird sie den Gewerbetreibenden in einem Begrüßungsschreiben mitteilen, welche Daten über sie gespeichert werden, und ihnen auf diese Weise Gelegenheit zu Korrekturen geben. Gleichzeitig wird die Handelskammer die Betroffenen um Einwilligung bitten, daß ihre Daten (Name und Anschrift) „zur Anbahnung von Geschäftsbeziehungen und sonstigen der Wirtschaft dienenden Zwecken" weitergegeben werden.
- Gewerbetreibende, die ihr Gewerbe bereits ausüben, wird die Handelskammer gesondert anschreiben und ihnen Gelegenheit geben, der Weitergabe von Daten (Name und Anschrift) zu widersprechen.

Ich habe diesem Verfahren zugestimmt. Da der Zweck der Datenübermittlung nur sehr allgemein beschrieben wird (Anbahnung von Geschäftsbeziehungen und sonstige der Wirtschaft dienende Zwecke), habe ich der Handelskammer mitgeteilt, daß nach meiner Auffassung der Empfänger einen konkreten Zweck nennen muß und die Daten nur zu dem angegebenen Zweck verwenden darf. Dies ergibt sich daraus, daß § 12 Abs. 2 Satz 3 HmbDSG bei einer Übermittlung ohne Einwilligung des Betroffenen vorschreibt, daß der Empfänger die Daten nur für den angegebenen Zweck verwenden darf, und daß der Betroffene im Falle einer Einwilligung nicht schlechter gestellt werden darf.

4.4.2 Datenschutz bei der Durchführung der Taxenordnung

Am 1.1.1985 ist die neu erlassene Taxenordnung (TaxO) in Kraft getreten. § 7 Abs. 1 verpflichtet u.a. die Taxiunternehmer, die von ihnen im Fahrdienst beschäftigten Taxifahrer unverzüglich bei der zuständigen Behörde namentlich mittels Durchschreibeformblatt anzumelden, und die Taxifahrer, während des Fahrdienstes eine Durchschrift mitzuführen und den zuständigen Bediensteten der Behörde auf Verlangen zur Prüfung auszuhändigen. Mit diesem Verfahren sollen vor allem die Schwarzarbeit und die mehrfachen Beschäftigungsverhältnisse, die wegen Geringfügigkeit sozialversicherungs- und steuerfrei sind, im Taxengewerbe bekämpft werden.

Gegen diese Datenerhebung haben sich mehrere Betroffene mit der Begründung gewandt, die Meldepflicht entbehre einer verfassungsmäßigen Ermächtigungsgrundlage.

Auch nach meiner Auffassung bestehen Zweifel, ob die Ermächtigung zur Regelung der „Einzelheiten des Dienstbetriebes" die Befugnis umfaßt, personenbezogene Daten über die Fahrer zwangsweise zu erheben. Andererseits ist zu berücksichtigen, daß die Ermächtigungsgrundlage im Personenbeförderungsgesetz aus der Zeit vor dem VZ-Urteil stammt, die Meldepflicht sachlich notwendig ist (s. 4.4.2.1) und sich die Befugnis zur Erhebung personenbezogener Daten aus dem Normenkontext ergibt (s. 4.5.2.2), so daß der Mangel in der Ermächtigungsgrundlage für eine Übergangszeit hingenommen werden kann, bis das Personenbeförderungsgesetz bei nächster sich bietender Gelegenheit geändert werden kann.

4.4.2.1 Meldepflicht

Die Bekämpfung der Schwarzarbeit und der mehrfachen sozialversicherungs- und steuerfreien Beschäftigungsverhältnisse ist ein einleuchtender Grund für die Meldepflicht, weil mit ihr verhindert wird, daß einzelne unrechtmäßige Vorteile auf Kosten anderer (nämlich der Taxiunternehmer und -fahrer, die sich an die Gesetze halten) erlangen.

4.4.2.2 Zuständigkeit der Aufsichtsbehörde

Die Taxenordnung ist aufgrund der §§ 47 Abs. 3 und 51 Abs. 1 Personenbeförderungsgesetz (PBefG) vom Senat der Freien und Hansestadt Hamburg erlassen worden. Die durch § 47 Abs. 3 PBefG den Landesregierungen eingeräumte Ermächtigung umfaßt u.a. die Regelung der Einzelheiten des Dienstbetriebes und damit – so die Interpretation des Senats – auch der Verpflichtung der Taxiunternehmen, Angaben über ihre Taxifahrer zu machen.

Daß der Begriff Dienstbetrieb weit auszulegen ist, ergibt sich auch aus dem in § 54 Abs. 1 PBefG geregelten umfassenden Aufsichtsrecht der Genehmigungs- und Aufsichtsbehörde. Nach § 54 Abs. 2 Satz 1 PBefG kann sich die Aufsichtsbehörde über alle ihrer Zuständigkeit unterliegenden Einrichtungen und Maßnahmen des Unternehmens unterrichten; der Unternehmer ist nach § 54 a Abs. 1 Satz 1 Nr. 2 PBefG zur Auskunft verpflichtet.

Zur Zuständigkeit der Aufsichtsbehörde gehört auch, daß sie die Genehmigung für den Taxenbetrieb zurücknehmen kann, wenn bestimmte Voraussetzungen vorliegen; zur Prüfung dieser Voraussetzungen kann sie vom Unternehmer Nachweise verlangen (§ 25 PBefG). Nach § 25 Abs. 2 Nr. 3 PBefG kann die Genehmigung insbesondere auch dann zurückgenommen werden, wenn der Unternehmer die ihm gesetzlich obliegenden arbeitsrechtlichen, sozialrechtlichen oder steuerrechtlichen Verpflichtungen wiederholt nicht erfüllt. Nach § 25 Abs. 3 PBefG hat der Unternehmer auf Verlangen der Behörde den Nachweis der Erfüllung dieser Verpflichtungen zu führen. Darin ist auch das Recht der Aufsichtsbehörde enthalten, von dem Unternehmer Auskunft über alle Tatsachen zu verlangen, die für dessen arbeits-, sozialversicherungsrechtliche und steuerrechtliche Verpflichtungen von Bedeutung sein können.

Diese Ansicht ist inzwischen vom Kammergericht in Berlin bestätigt worden, das mehrere von der Verwaltungsbehörde verhängte Bußgeldbescheide wegen Verstoßes gegen die Meldepflicht nachgeprüft hat. In Hamburg hat bisher das Verwaltungsgericht nur den Erlaß einer einstweiligen Anordnung abgelehnt, mit der der Vollzug der Meldepflicht ausgesetzt werden sollte. Das Verwaltungsgericht stellt in seinem Beschluß ausdrücklich fest, daß ein Interesse, durch Aussetzung der Meldepflicht „einer Kontrolle in der Beachtung steuer-, sozial- und arbeitsrechtlicher Bestimmungen zu entgehen", nicht schützenswert ist und „als sozial schädlich rechtlich außer Betracht" bleiben muß.

4.4.3 Fachliche Weisungen

Die sachgerechte und einheitliche Erledigung der in den Bezirksämtern wahrgenommenen Aufgaben wird u.a. durch Fachliche Weisungen sichergestellt. Fachliche Wei-

sungen sind nach § 5 Abs. 2 des Bezirksverwaltungsgesetzes Richtlinien und allgemeine Grundsätze für die Wahrnehmung der den Bezirksämtern zugewiesenen fachlichen Aufgaben; sie werden von den jeweils zuständigen Fachbehörden erlassen und haben eine zeitlich begrenzte Gültigkeitsdauer von 5 Jahren (§ 5 Abs. 2 des Bezirksverwaltungsgesetzes).

Die Bezirksämter nehmen in den Wirtschafts- und Ordnungsämtern zahlreiche Aufgaben im Gewerbewesen wahr. Fachbehörde ist die Behörde für Wirtschaft, Verkehr und Landwirtschaft, die mithin auch die erforderlichen Fachlichen Weisungen zu erlassen hat. Im Berichtszeitraum hat die Behörde für Wirtschaft, Verkehr und Landwirtschaft mehrere Fachliche Weisungen erlassen, die auch datenschutzrelevante Vorschriften enthalten.

Es würde den Rahmen dieses Berichtes sprengen, wenn ich auf Details einginge. Die Behörde für Wirtschaft, Verkehr und Landwirtschaft stand meinen Anregungen stets aufgeschlossen gegenüber. Folgende grundsätzliche Ergebnisse der Abstimmung sind hervorzuheben:

(1) Das Gewerberecht weist ein erhebliches Defizit an Vorschriften über die Verarbeitung personenbezogener Daten auf; die Speicherung und insbesondere die Übermittlung sind auch nicht ansatzweise geregelt. Angesichts der Sensitivität der in Rede stehenden personenbezogenen Daten ist es nach den Grundsätzen des VZ-Urteils dringend notwendig, das Gewerberecht um bereichsspezifische und präzise Vorschriften über die Verarbeitung personenbezogener Daten zu ergänzen; nur für eine Übergangszeit kann noch auf die Generalklauseln des HmbDSG zurückgegriffen werden. Dieser Appell richtet sich an den Bundesgesetzgeber, der die Gesetzgebungskompetenz für das Gewerberecht hat.

(2) Das Gewerberecht regelt – wenn auch nach heutigem Verständnis nicht präzise genug – im allgemeinen die Erhebung der Daten beim Betroffenen oder bei anderen Stellen. Wenn die Vorschriften wegen mangelnder Präzision einen Spielraum lassen, müssen Umfang und Art der Erhebung den Grundsätzen des Bundesverfassungsgerichts entsprechen. Das bedeutet z.B. konkret, daß

- bei der Prüfung der Zuverlässigkeit die dafür u.a. erforderlichen Zeugnisse (Führungszeugnis und Auskunft aus dem Gewerbezentralregister) grundsätzlich vom Betroffenen beizubringen und nur dann von Amts wegen einzuholen sind, wenn es sich um sog. Vertrauensgewerbe handelt (§ 38 GewO). In diesen Fällen muß jedoch der Betroffene darüber informiert werden, daß diese Zeugnisse von Amts wegen eingeholt werden;
- bei der Prüfung der Zuverlässigkeit in gewerberechtlichen Erlaubnisverfahren der Umfang der Datenerhebung auf das für die Beurteilung der Zuverlässigkeit des Antragstellers notwendige Minimum beschränkt wird. So ist es z.B. nicht notwendig, bei der Prüfung des Antrages auf eine Erlaubnis nach dem Gaststättengesetz in allen Fällen auch ein Führungszeugnis und eine Auskunft aus dem Gewerbezentralregister für den Ehegatten des Antragstellers (bei juristischen Personen für die Ehegatten aller vertretungsberechtigten Personen) zu verlangen. Das muß auf die Fälle beschränkt werden, in denen Anhaltspunkte dafür bestehen, daß die Erlaubnis wegen Unzuverlässigkeit des Ehegatten versagt werden kann, weil nämlich der Ehegatte einen bestimmenden Einfluß auf den Betrieb der Gaststätte hat. Ebenso ist es nicht zulässig, bei ausländischen Antragstellern generell die bei der Ausländerbehörde geführte Akte beizuziehen.

(3) Das Wirtschafts- und Ordnungsamt übermittelt die in gewerberechtlichen Verfahren entstehenden Daten in erheblichem Umfang an andere Behörden, häufig abhängig von bestimmten Fallkonstellationen. Die Übermittlungen sind nach meinen Feststellungen auch zur Aufgabenwahrnehmung erforderlich; ich hätte jedenfalls keine Bedenken, ihrer Aufnahme in ergänzende gewerberechtliche Vorschriften zuzustimmen.

Gegenwärtig können diese Übermittlungen mangels spezieller Vorschriften im Gewerberecht häufig nur auf § 10 Abs. 1 HmbDSG gestützt werden. Daher ist § 10 Abs. 1 Satz 2 HmbDSG zu beachten, der vorschreibt, daß dem Betroffenen die Zulässigkeit mehrfacher Verwendung bekannt sein muß. Nach meiner Auffassung verpflichtet diese Vorschrift die speichernde Stelle – in diesem Fall das Wirtschafts-und Ordnungsamt –, dem Betroffenen bei der Erhebung personenbezogener Daten über alle Übermittlungen zu informieren, die der speichernden Stelle im Zeitpunkt der Erhebung bekannt sind. Das bedeutet nun allerdings nicht, daß der Betroffene mit einer Unmenge von Informationen überschüttet werden darf, aus der er die für ihn wesentlichen nur mit großer Mühe herausfinden kann. Vielmehr sollte der Betroffene bei der Erhebung personenbezogener Daten

- über die Übermittlungen informiert werden, die immer erfolgen,
- auf die Tatsache solcher Übermittlungen, die von bestimmten, nicht in jedem Falle vorhandenen Voraussetzungen abhängig sind, hingewiesen und darüber informiert werden, daß er auf Verlangen hierüber näher unterrichtet wird.

4.4.4 Gewerberechtliche Auskunft und Nachschau

§ 38 GewO ermächtigt die Landesregierungen, für die Gewerbezweige:

An- und Verkauf von Gebrauchtwaren,

An- und Verkauf von Edelmetallen und edelmetallhaltigen Legierungen sowie von Waren daraus,

An- und Verkauf von Altmetallen,

Auskunfteien und Detekteien,

Vermittlung von Eheschließungen,

Betrieb von Reisebüros und Vermittlung von Unterkünften,

Vermittlung der Beförderung von Personen mit Kraft- oder Luftfahrzeugen im nicht genehmigungspflichtigen Verkehr,

An- und Verkauf von Werken der bildenden Künste und der Bibliophilie

durch Rechtsverordnung Bestimmungen über die Buchführung, Auskunftserteilung und Nachschau zu treffen. Auskünfte sind hier solche, die der Gewerbetreibende an die für die Überwachung zuständigen Behörden erteilen muß; als Nachschau wird das Recht der für die Überwachung zuständigen Behörden bezeichnet, an Ort und Stelle Prüfungen und Besichtigungen vorzunehmen und in geschäftliche Unterlagen Einsicht zu nehmen. Entsprechende Verordnungsermächtigungen gibt es auch für erlaubnispflichtige Gewerbe, z.B. Pfandleiher, Bewacher.

Die in Hamburg erlassenen Rechtsverordnungen werden z.Z. überarbeitet, soweit es erforderlich ist.

Die für Auskunft und Nachschau nach den einzelnen Rechtsverordnungen zuständigen Behörden werden in Hamburg durch Zuständigkeitsanordnungen bestimmt; es sind das zuständige Bezirksamt (für die gewerberechtliche Überwachung) und die Behörde für Inneres (für die Erforschung von Straftaten).

Bei der Überarbeitung einer Rechtsverordnung sind die beteiligten Behörden darauf gestoßen, daß die im Gewerberecht normierte Pflicht zur Auskunft und Duldung der Nachschau nur gewerberechtlichen Zwecken dienen darf, nicht jedoch der im Strafprozeßrecht geregelten Strafverfolgung; dies hat auch das Bundesverwaltungsgericht festgestellt (Urteil vom 2.3.1971, GewArch 1971 S. 153 ff.).

Ich habe daraufhin die zuständigen Behörden gebeten, in den Zuständigkeitsanordnungen jeweils die Behörde für Inneres zu streichen, soweit es um die Auskunftspflicht und Duldung der Nachschau aufgrund der

Verordnung über den Geschäftsbetrieb der gewerblichen Pfandleiher,

Verordnung über das Bewachungsgewerbe,

Metallhandelsverordnung,

Auskunftei- und Detekteiverordnung,

Gebrauchtwaren- und Edelmetallverordnung

geht.

Um Irrtümer zu vermeiden: Damit wird der Polizei (sie ist mit Behörde für Inneres gemeint) nicht die Möglichkeit genommen, in solchen Gewerbebetrieben zum Zwecke der Strafverfolgung Auskünfte einzuholen und Nachschau zu halten. Dies kann sie jedoch nur auf § 163 StPO und nicht auf Gewerberecht stützen.

Bei der Überarbeitung der Rechtsverordnungen hatte ich mich auch mit dem Problem auseinanderzusetzen, ob die Rechtsgrundlage für die mit den Rechtsverordnungen angeordneten detaillierten Aufzeichnungspflichten im Geschäftsbetrieb ausreichend ist. Ich habe Bedenken zurückgestellt, weil es sich für jeden Gewerbezweig aus der Natur der Sache und aus einer jahrzehntelangen Praxis und Rechtsüberzeugung ergibt, um welche Bestimmungen der Buchführung, Auskunft und Nachschau es sich im einzelnen handelt. Ich halte es aber für notwendig, die Bedenken bei nächster Gelegenheit durch eine Novellierung der entsprechenden Vorschriften der Gewerbeordnung auszuräumen.

4.5 Bauwesen

4.5.1 Schlußbemerkung zur Befragung im Karolinenviertel

Wie in meinem 3. TB (3.4.1) angekündigt, habe ich die Behandlung der Fragebogen aus dem Karolinenviertel und die Verwendung der erhobenen Daten überprüft. Absprachegemäß wurden die Antworten auf die Fragen 1, 27 und 29 weder ausgewertet noch miterfaßt. Nach der Erfassung der übrigen Daten auf einem automatisierten Datenträger (Magnetband) wurden am 17.1.1985 sämtliche Erhebungsunterlagen (Zählerlisten, Vorblätter, Fragebogen) vernichtet. Anhand eines Ausdrucks aus der Banddatei mit den erfaßten Daten habe ich mich davon überzeugt, daß die Antworten zu den beanstandeten Fragen nicht miterfaßt worden sind. Der Personenbezug der auf dem Band gespeicherten Daten ist weitgehend aufgehoben. Die auf den Vorblättern zum Fragebogen erhobenen und auf die Banddatei mit übernommenen Merkmale „lfd. Nr." (der Wohnung im Baublock) und „Baublocknr." (in Hamburg die eindeutige Bezeichnung für eine bestimmte zusammenhängende Fläche, die auf allen Seiten durch einen Straßenabschnitt begrenzt ist) erlauben zwar die Wiederherstellung des Personenbezugs, wenn die Vergabe der „lfd. Nr." nach einem erkennbaren System erfolgt ist (z.B.: an einer Ecke des Baublocks beginnend in der Reihenfolge der Treppenhäuser, Stockwerke, rechte/linke Wohnung o.ä.) und wenn Zusatzwissen (Wer hat zur Zeit der Zählung in der betreffenden Wohnung gewohnt?) vorhanden ist. Die Reidentifizierung wäre aber mit so viel Aufwand verbunden, daß ich von einer faktischen Anonymisierung ausgehe. Gleichwohl ist die Datei gesichert aufzubewahren und – wenn die Daten zur Aufgabenerfüllung nicht mehr gebraucht werden – zu löschen.

Die Durchführung der Kontrolle war ausgesprochen mühsam. Die wesentliche Frage, ob die Baubehörde die Antworten zu den von mir beanstandeten Fragen miterfaßt hatte, konnten meine Mitarbeiter erst nach neunmonatigen Bemühungen klären. Dabei ging es im Grunde um eine ganz einfache Prüfung: Es mußte einerseits anhand einer Datensatzbeschreibung festgestellt werden, wie der Bandsatz aufgebaut ist, d.h. welche Datenfelder definiert sind, welche Ausprägungen als Feldinhalt zugelassen und in welcher Form die Daten in den Feldern gespeichert sind. Andererseits mußte anhand eines Bandausdrucks (mehrere Blöcke der Datei umfassend) festgestellt werden, welche Felder tatsächlich mit Inhalten gefüllt sind. Felder für Antworten auf die Fragen 1, 27 und 29 durften entweder im Bandsatz gar nicht (mehr) vorhanden sein oder sie durften – wenn an der ursprünglichen Definition des Bandsatzes nach den geäußerten Bedenken nichts verändert worden ist – nur den Inhalt „blank" (=leer) oder „0" haben.

Die Baubehörde war nicht in der Lage, eine Datensatzbeschreibung vorzulegen; es bedurfte sogar erheblicher Anstrengungen, der Baubehörde zu erläutern, daß entgegen ihrer Auffassung weder der Fragebogen noch der Ausdruck der Banddatei noch die mir übersandten Tabellen mit den statistischen Auswertungen eine Datensatzbeschreibung darstellen oder eine solche ersetzen können. Es gelang mir erst auf einem Umweg, die notwendigen Informationen zu beschaffen, die mich in die Lage versetzten, mir selbst eine Datensatzbeschreibung anzufertigen. Dazu mußte ich ermitteln, wer die automatisierte Datenverarbeitung im Falle Karolinenviertel technisch durchgeführt hatte. Dies war nicht die „Arbeitsgemeinschaft zur Durchführung vorbereitender Untersuchungen im Karolinenviertel", die als der vertragliche Auftragnehmer der Baubehörde die Datenverarbeitung nach deren Weisungen auszuführen hatte. Dies war auch nicht das von der Arbeitsgemeinschaft als Unter-Auftragnehmer herangezogene Institut für wohnungsbezogene Markt- und Sozialstudien. Ich erfuhr, daß der Unter-Auftragsnehmer seinerseits zur Erledigung der maschinellen Datenverarbeitung einen Unter-Auftragnehmer eingeschaltet hatte. Von diesem konnte ich schließlich in dessen Rechenzentrum mündlich eine Erläuterung zum Satzaufbau und zur Codierung der Daten erhalten. Eine Programmdokumentation war nicht vorhanden.

Diese Feststellungen veranlassen mich zu einigen grundsätzlichen Bemerkungen zur Datenverarbeitung im Auftrag. Öffentliche Stellen dürfen Datenverarbeitung durch Auftragnehmer ausführen lassen. Sobald die Datenverarbeitung jedoch personenbezogene Daten betrifft, hat die auftraggebende öffentliche Stelle gem. § 3 Abs. 1 HmbDSG den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen (§ 8 Abs. 1) sorgfältig auszuwählen. Ein öffentlicher Auftragnehmer hat gem. § 3 Abs. 2 HmbDSG und ein privater Auftragnehmer gem. § 37 BDSG zu beachten, daß er die Verarbeitung personenbezogener Daten nur im Rahmen der Weisungen des Auftraggebers vornehmen darf. (Für Sozialdaten gilt § 80 SGB X.)

Ich habe erhebliche Zweifel, ob ein Auftraggeber bei derartig geschachtelten Auftrags-, Unter-Auftrags-, Unter-unter-Auftragsverhältnissen noch die sorgfältige Auswahl aller Auftragnehmer „unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen (§ 8 Abs. 1 HmbDSG)" gewährleisten kann.

Ich habe auch Zweifel, ob bei derartig geschachtelten Verhältnissen noch sichergestellt werden kann, daß die von der öffentlichen Stelle erteilten Weisungen in allen Fällen vollständig weiterübermittelt und stets beachtet werden. Dies gilt insbesondere dann, wenn die Weisungen nicht vollen Umfangs schriftlich erteilt wurden. Schließlich bezweifele ich, daß der Auftraggeber unter solchen Verhältnissen kontrollieren kann, ob seine Weisungen strikt eingehalten werden.

Die Tatsache, daß im vorliegenden Fall die Baubehörde keine Dokumentation über die automatisierte Verarbeitung der Daten vorlegen konnte, zeigt mir, daß entweder ihre Weisungen unvollständig waren oder nicht befolgt wurden und letztlich auch der Auftragnehmer, der die technische Durchführung übernommen hatte, nicht sorgfältig ausgewählt war; denn die Erstellung einer Dokumentation über das anzuwendende automatisierte Verfahren hätte in diesem Fall zu den notwendigen organisatorischen Maßnahmen gehört, die gem. § 6 BDSG von dem Auftragnehmer zu treffen und gem. §§ 3 Abs. 1, 8 Abs. 1 HmbDSG von der auftraggebenden öffentlichen Stelle zu fordern sind.

4.5.2 Wohnraumdatei

In meinem 3. TB (3.4.2) hatte ich über die Wohnraumdatei und über meine Bedenken gegen die Speicherung bestimmter Daten in dieser Datei berichtet. Die Bedenken sind erst im November mit Vertretern der Baubehörde erörtert worden, nachdem ich anläßlich der Änderung der Meldedatenübermittlungsverordnung auf den Zusammenhang zwischen den rechtlichen Problemen bei der Speicherung bestimmter Daten in der

Wohnraumdatei und der Zulässigkeit der Datenübermittlung aus dem Melderegister gem. § 3 der Verordnung an die Bezirksämter für die Wohnraumdatei hingewiesen hatte.

Der Sachverhalt ist folgender: Ursprünglich war die Umstellung der alten, in den Bezirksämtern manuell geführten Wohnraumkartei auf ein automatisiertes Verfahren (Wohnraumdatei) zum Zweck der Erhebung von Ausgleichszahlungen nach dem Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen (Fehlbelegungsabgabe) geplant und begonnen werden. Die Datei sollte eine Doppelfunktion erfüllen. Zum einen sollte sie eine Überprüfung sämtlicher Sozialmieterhaushalte ermöglichen, um die Erhebung der Fehlbelegungsabgabe durchführen zu können; zum anderen sollte sie die durch § 2 Abs. 1 des Wohnungsbindungsgesetzes (WoBindG) vorgeschriebene Erfassung und laufende Überwachung des Sozialwohnungsbestandes sicherstellen. Der Umfang der in der Wohnraumdatei zu speichernden Daten war am Bedarf für den Zweck „Erhebung der Fehlbelegungsabgabe" ausgerichtet und durch das dafür vorhandene Gesetz rechtlich abgesichert.

Durch die Entscheidung des Senats, in Hamburg keine Fehlbelegungsabgabe zu erheben, war das Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen als Rechtsgrundlage für die Wohnraumdatei entfallen. Für die Beurteilung der Wohnraumdatei als Instrument zur Überwachung des Sozialwohnungsbestandes kann nun nur noch auf das WoBindG zurückgegriffen werden. Unstreitig entfiel mit der Entscheidung des Senats die Rechtsgrundlage für die Speicherung aller Daten, die zur Einkommensermittlung der Sozialwohnungsmieter vorgesehen waren. Solche Daten sind auch nicht erhoben und gespeichert worden. Die Baubehörde hat eingeräumt, daß eine entsprechende Anpasssung des Datensatzes der Datei und der Vordrucke im Verfahren Wohnraumdatei erforderlich ist, d.h. daß aus der Datei und den Vordrucken die Plätze (Felder) für Angaben über Einkommensverhältnisse – wie auch alle anderen nicht erforderlichen Angaben – zu eliminieren sind.

Unstreitig ist ferner die Zulässigkeit der Speicherung aller objektbezogenen Daten, d.h. der Daten, die die Sozialwohnungen beschreiben. Dies ergibt sich mit hinreichender Klarheit aus § 2 Abs. 1 WoBindG, der verlangt, daß zur Sicherung der Zweckbestimmung der öffentlich geförderten Wohnungen nach diesem Gesetz die zuständige Stelle alle öffentlich geförderten Wohnungen zu erfassen und die Unterlagen auf dem laufenden zu halten hat.

Zugestimmt habe ich schließlich auch der Speicherung des Namens des Wohnungsinhabers sowie eines Untermieters, der mehr als die Hälfte der Wohnfläche untermietweise bewohnt, weil der Wohnungsinhaber (bzw. Untermieter) gem. § 2 Abs. 3 WoBindG auch nach dem berechtigten Bezug der Sozialwohnung noch Mitwirkungspflichten hat.

Unterschiedliche Auffassungen bestehen dagegen hinsichtlich des Geburtsdatums des Wohnungsinhabers, seines Geschlechts, seiner Nationalität sowie der Zahl seiner Familienangehörigen, die mit ihm die Wohnung bewohnen. Die Baubehörde vertritt die Auffassung, die Erhebung, Speicherung und Fortschreibung dieser Daten sei ebenfalls durch § 2 Abs. 1 i.V.m. Abs. 3 WoBindG gesetzlich erlaubt, ja geboten. Sie beruft sich für ihre Auffassung auf die Kommentierung zu § 2 Abs. 3 WoBindG, z.B. in Fischer-Dieskau-Pergande-Schwender, und erklärt, in anderen Bundesländern werde ihre Ansicht geteilt und entsprechend verfahren.

Ich habe dem WoBindG nicht entnehmen können, daß die Verarbeitung der umstrittenen Daten zulässig ist. Ich begrüße daher, daß die Baubehörde mit Schreiben vom 19.11.1985 an die Mitglieder der Fachkommission Wohnungsbindungs- und Berechnungsrecht und an den Bundesminister für Raumordnung, Bauwesen und Städtebau die Frage der Normenklarheit des § 2 Abs. 1 WoBindG zur Diskussion gestellt hat. Über die Verfahrensweise in anderen Bundesländern ist mir nichts näheres bekannt. Ich beabsichtige, eine Umfrage unter den Datenschutzbeauftragten durchzuführen. Außerdem habe ich nach wie vor Zweifel, ob die Speicherung der einzelnen Daten erforderlich ist. Die Baubehörde räumt zwar ein, daß sich im WoBindG kein Instrument findet, mit dem zwangsweise gegen Wohnungsinhaber vorgegangen werden kann, um

sie – beispielsweise – zur Räumung einer unterbelegten Sozialwohnung zu veranlassen. Sie meint aber, die Übermittlung der Daten sei Voraussetzung dafür, daß die zuständige Stelle von nicht im Sinne des WoBindG belegten Wohnungen Kenntnis erlange, wodurch sie in die Lage versetzt werde, Anstrengungen zur besseren Belegung auf freiwilliger Basis zu unternehmen. Die zweckentsprechende Verwendung des Sozialwohnungsbestandes sicherzustellen, sei oberstes Gebot des WoBindG. Zu den einzelnen umstrittenen Daten führt die Baubehörde Gründe zur Erforderlichkeit an, die nur zum Teil einleuchten.

Das Geburtsdatum des Wohnungsinhabers hat keine Auswirkungen auf die Frage, ob eine Sozialwohnung zweckentsprechend genutzt wird. Immerhin kann das Alter eines alleinstehenden Wohnungsinhabers insofern relevant sein, als für Planungsaufgaben Erkenntnisse über die Struktur der Sozialwohnungsmieter benötigt werden. Dafür reicht die Angabe des Geburtsjahres.

Inwiefern das Geschlecht des Wohnungsinhabers relevant sein soll im Sinne des WoBindG, ist nicht erkennbar. Zur korrekten Anrede („Herr" oder „Frau") beim Erhebungsverfahren wird es jedenfalls nicht gebraucht. Z.Z. wird gar keine Erhebung von Daten beim Betroffenen durchgeführt, sondern die Daten werden durch Übermittlung aus dem Einwohnermeldeverfahren gewonnen. Falls die Betroffenen einmal an Erhebungen mitwirken sollen, werden sie durch automatisiert erstellte Formschreiben angesprochen, in denen die Anrede – wie weit verbreitet – mit „Herr / Frau" erfolgen kann. Wenn die Baubehörde vorträgt, die Speicherung des Geschlechtes sei bei Alleinstehenden auch wegen der unterschiedlichen Lebenserwartung von Frauen und Männern erforderlich, so scheint mir dieses Argument recht weit hergeholt. Ich vermag nicht zu erkennen, welche steuernden oder planerischen Maßnahmen hieran anknüpfen sollten.

Die Speicherung der Zahl der Familienmitglieder wäre dann gerechtfertigt, wenn auf das Erkennen von – nach Bezug eingetretener – Unterbelegung hin tatsächlich Maßnahmen der zuständigen Stelle erfolgen würden, deren Erfolg allerdings von der Bereitschaft der Mieter abhängt, den Vorschlägen zu folgen. Bisher wird dies noch nicht so gehandhabt.

Es fällt mir auch schwer, die Speicherung der Nationalität auf das WoBindG zurückzuführen. Dieses Datum könnte zur Steuerung der Ansiedlung von Ausländern im Stadtgebiet erforderlich sein, um Ghettobildung und andere Mißstände zu vermeiden. Der Senat plant z.Z. jedoch keine besondere Steuerung der Wohnungsvergabe an Ausländer. Von der Einrichtung der dafür vorgesehenen Clearingstelle hat er Abstand genommen. Stattdessen hat er vor, mit den großen Wohnungsunternehmen einen Vertrag zu schließen, dessen Zweck es ist, die Problemgruppe der vordringlich Wohnungssuchenden besser unter den Vermietern aufzuteilen. Hiervon wären auch Ausländer betroffen, soweit sie dieser Gruppe zuzurechnen sind.

Die Baubehörde macht geltend, alle strittigen Daten würden – losgelöst von den Aufgaben der Bezirksämter nach dem WoBindG – für die Planung auf dem Gebiet des Sozialwohnungsbaues benötigt. Um die Struktur der Sozialwohnungsmieter zu erkennen und um dem Senat eine adäquate Planung und Steuerung zu ermöglichen, hält sie sogar noch ein weiteres Datum, nämlich das Mietereinkommen (pauschaliert) nach Minderverdiener, Mehrverdiener, für wünschenswert. Dazu vertrete ich folgende Auffassung:

Die Speicherung des Mietereinkommens kann mangels Rechtsgrundlage ohne Einwilligung der Mieter nicht erfolgen. Die Wahrscheinlichkeit, daß Mieter freiwillig ihr Einkommen angeben und die Angabe immer wieder aktualisieren, halte ich für gering. Ob ein unvollständiger Datenbestand noch zu gebrauchen ist, ist fraglich.

Für Planungs- und Steuerungsaufgaben werden keine Daten mit Personenbezug gebraucht. In aller Regel genügen aggregierte Daten. Für Planungs- und Steuerungsaufgaben und auch als Kontrollinstrument für die Vergabepraxis der großen Wohnungsunternehmen genügen gezielte Auswertungen der Wohnraumdatei, bei denen als kleinste Einheit die Summen aus einem Baublock aussagekräftig genug sein müßten. Eine Übermittlung nichtanonymisierter und -aggregierter Daten aus der Wohn-

raumdatei an die Baubehörde oder andere Stellen für Zwecke außerhalb des WoBindG halte ich deshalb für unzulässig.

4.5.3 Katastergesetz

Hamburg hat als einziges Bundesland kein Katastergesetz. Anders als der Senat in seiner Stellungnahme zu meinem 3. TB (Drs 11/3876 Nr. 4.3) kann ich nicht feststellen, daß § 2 Abs. 2 Grundbuchordnung, § 43 Grundbuchverfügung und das Bodenschätzungsgesetz als Rechtsgrundlage für das Liegenschaftskataster ausreichen. In den angeführten Bestimmungen wird zwar auf ein „amtliches Verzeichnis der Grundstücke" bezug genommen, es wird die Existenz eines solchen Verzeichnisses vorausgesetzt. Darin erschöpft sich der Regelungsgehalt dieser Vorschriften für das Liegenschaftskataster auch schon. Sie definieren weder die Aufgaben des Liegenschaftskatasters noch enthalten sie eine abschließende Aufzählung der Daten, die im Liegenschaftskataster nachzuweisen sind. Es fehlen auch Regelungen darüber, wie und bei wem die Daten für das Liegenschaftskataster zu erheben sind und wem das Liegenschaftskataster zur Verfügung stehen soll. Welche Auskunftspflichten hat z.B. der Grundstückseigentümer, welche Duldungspflicht hat etwa ein Nachbar bei einer Vermessung, gibt es ein Einsichtsrecht für jeden oder nur für denjenigen, der ein berechtigtes Interesse geltend macht oder ein solches nachweist?

Durch das VZ- Urteil des Bundesverfassungsgerichts ist ausdrücklich bestätigt worden, daß über die Voraussetzungen und den Umfang der – nicht auf freiwilliger Basis erfolgenden – Verarbeitung personenbezogener Daten gesetzliche Grundlagen vorhanden sein müssen. Dabei wird die Regelungsdichte entsprechender Normierungen bestimmt von Art, Umfang und erkennbarer Verwendung der Daten sowie den Mißbrauchsmöglichkeiten. Die übrigen Bundesländer haben durch Vermessungs-und Katastergesetze diesen Anforderungen Rechnung getragen. Hamburg sollte ihrem Beispiel folgen.

4.5.4 Entwurf einer Hamburgischen Bauordnung

Am Abstimmungsverfahren über den Entwurf einer Hamburgischen Bauordnung bin ich nicht beteiligt worden. Ich bedauere sehr, daß ich deshalb keine Gelegenheit hatte, die aus der Sicht des Datenschutzes gebotenen Anforderungen an das neue Gesetz darzustellen.

So vermisse ich in dem Entwurf Regelungen für die Übermittlung von Daten aus dem Bauantragsverfahren an andere Stellen. Im Baugenehmigungsverfahren hat der Bauherr detaillierte Auskünfte zu geben, die u.U. einen Einblick in seine Lebensverhältnisse und in seine wirtschaftlichen Verhältnisse gestatten (Ausstattung, sanitäre Einrichtungen, Anzahl der Räume, Garagen, Schwimmbad usw.). In diesem Zusammenhang ist von Bedeutung, welche Übermittlungen im Rahmen des Baugenehmigungsverfahrens zum Zweck der Erteilung der Baugenehmigung erfolgen und welche Übermittlungen auf welcher gesetzlichen Grundlage zu anderen Zwecken durchgeführt werden und in welchem Umfang Daten aus dem Baugenehmigungsverfahren im einzelnen übermittelt werden dürfen. Der Bürger, der Daten zur Erlangung einer Baugenehmigung angibt, sollte übersehen können, welchen Stellen diese Daten bekannt werden.

4.6 **Umweltschutz**

Auf Probleme im Verhältnis zwischen Umweltschutz und Datenschutz hatte ich in meinem 3. TB (3.15) hingewiesen und betont, daß es mir wichtig ist zu vermeiden, daß Datenschutz zum Vertuschen von Umweltverstößen mißbraucht wird. Ich habe festgestellt, daß – mehr noch als die Gesetze zum Schutz personenbezogener Daten – das gewerberechtliche Verbot der Offenbarung von Betriebs- und Geschäftsgeheimnissen Konfliktstoff bietet. Ich habe inzwischen mit Vertretern der Umweltbehörde erörtert, wo Datenschutzprobleme auftreten und wie diese lösbar sein könnten. Das Emissionskataster – z.B. – wäre rechtlich wesentlich besser abgesichert, wenn es nicht nur

auf einen Senatsbeschluß, sondern auf eine der gesetzlichen Alternativen des Bundes-Immissionsschutzgesetzes gestützt werden könnte. (§ 46 Abs. 1 BImSchG schreibt die Aufstellung eines Emissionskatasters vor für Gebiete, die als „Belastungsgebiete" ausgewiesen sind. Abs. 2 läßt die Aufstellung eines Emissionskatasters in anderen Gebieten zu, wenn dies durch Landesgesetz beschlossen wird. Beide Voraussetzungen liegen in Hamburg nicht vor.)

Das Altlastkataster ist ein weiteres Beispiel: Das Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung kann schon deshalb für das Altlastkataster keine zureichende Rechtsgrundlage abgeben, weil das SOG nur Regelungen für den Bereich der Gefahrenabwehr trifft. Das Altlastkataster hat aber erhebliche Bedeutung auch für die Bauplanung, die Landschaftsplanung, das Baugenehmigungsverfahren, für Mieter und Nachbarn der betreffenden Grundstücke u.a., also für Bereiche, die nicht unter den Begriff der Gefahrenabwehr zu subsumieren sind.

4.7 Schulwesen

4.7.1 Bereichspezifische Datenschutzregelungen im Schulgesetz

In meinem 3. TB (3.5.1) hatte ich über Bestrebungen berichtet, bereichsspezifische Datenschutzregelungen für den Schulbereich zu formulieren und im Zuge der aus anderen Gründen vorbereiteten Novellierung des Schulgesetzes in das Gesetz mit einzuarbeiten. Am 18.6.1985 ist eine Änderung des Schulgesetzes verkündet worden (GVBl I Seite 143 ff.), jedoch ohne eine bereichsspezifische Datenschutzregelung. Der Senatsentwurf (Drs 24/85 vom 10.1.1985) sah mit einem § 41 a zwar eine solche vor, diese ist bei den bürgerschaftlichen Beratungen aber ausgeklammert worden, um die Verabschiedung der Novelle angesichts des für die datenschutzrechtliche Problematik erwarteten Erörterungsbedarfs nicht zu verzögern. Die Forderung nach einer Datenschutzregelung besteht also nach wie vor.

Ich hatte im Abstimmungsverfahren gegen den Entwurf des § 41 a SchulG Vorbehalte geäußert, weil die Regelung den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit noch nicht hinreichend entsprach. So war z.B. der Umfang der zu erhebenden und zu speichernden Daten nicht in einem abschließenden Katalog festgelegt, sondern er wurde allgemein umschrieben (..., soweit es zur Durchführung des Erziehungs- und Bildungsauftrages der Schule ... erforderlich ist ...) und nur zum Teil konkretisiert (... Zu diesen Daten gehören ...), so daß die Erhebung und Verarbeitung weiterer Daten nicht ausgeschlossen war.

Erlaubt sein sollte auch die Erhebung und Verarbeitung von „Daten über das Arbeits- und Sozialverhalten" der Schüler. Eine so weitgefaßte Befugnis schließt nicht aus, daß auch Daten gespeichert werden über das Verhalten der Schüler außerhalb der Schule, z.B. Aktivitäten in Sportvereinen, Clubs, Discos, in der Kirche, in Gruppen usw. Die Einschränkung der Speicherungsbefugnis durch die Formulierung „... soweit es zur Durchführung des Erziehungs- und Bildungsauftrages der Schule erforderlich ist" ändert daran wenig, da diese Formulierung ihrerseits unscharf und auslegungsbedürftig ist.

Die vorgesehene Regelung ließ in keiner Weise erkennen, aus welchem Anlaß und zu welchem Zweck die Daten jeweils erhoben werden durften. Dasselbe gilt für die Übermittlungsregelung, die ebenfalls weder Anlaß noch Zweck von Übermittlungen festlegte, sondern nur die Stellen nannte, zwischen denen eine Übermittlung von Daten aus dem Schulbereich erlaubt sein sollte. Maßstab für die Zulässigkeit von Übermittlungen sollte lediglich sein, daß die Daten „zur sachgerechten Wahrnehmung der Aufgaben benötigt werden".

Auch für die Datenerhebung und -verarbeitung durch schulärztliche und schulpsychologische Dienststellen enthielt der Entwurf lediglich eine Generalklausel, die als Zulässigkeitsvoraussetzung ausschließlich auf die Erforderlichkeit abstellt. Für statistische Auswertungen und Forschungsvorhaben fehlte jegliche Regelung.

Noch während des Abstimmungsverfahrens über die Schulgesetznovelle hat die BSB eine konkretere Regelung des Datenschutzes im Schulbereich sowie Vorstellungen über eine ergänzende Rechtsverordnung entwickelt. Es besteht inzwischen Einigkeit über folgende Punkte:

- Die bereichsspezifische Datenschutzregelung im Schulbereich soll auf jede Art von Datenverarbeitung Anwendung finden; auf die Form der Verarbeitung (in Dateien) soll es nicht ankommen.
- Entsprechend den unterschiedlichen Aufgaben, die im Schulbereich wahrgenommen werden, ist eine differenziertere Regelung des Datenschutzes erforderlich. Ich empfehle folgende Gliederung:

  (1) Eine datenschutzrechtliche Grundnorm;

  (2) eine Vorschrift für die Datenverarbeitung im Zusammenhang mit Begutachtungen, Tests, Untersuchungen (d.h. Datenschutz bei der Vorbereitung schulischer Maßnahmen, z.B. Übergang auf eine Sonderschule, bei der Schulgesundheitspflege und beim schulpsychologischen Dienst);

  (3) eine weitere Bestimmung für die Datenverarbeitung im Rahmen wissenschaftlicher Forschung an Schulen;

  (4) schließlich Regelungen über die Voraussetzungen und den Umfang der Datenverarbeitung zum Zweck statistischer Auswertungen.

- Die Regelung muß dem Gebot der Normenklarheit entsprechen. Dies kann durch eine umfassende Regelung im Schulgesetz erfüllt werden. Denkbar ist aber auch, im Gesetz nicht alle Einzelheiten zu regeln, sondern dies einer Rechtsverordnung vorzubehalten, für die im Gesetz eine Rechtsgrundlage zu schaffen ist. An den Bestimmtheitsgrad der Ermächtigungsnorm sind indessen hohe Anforderungen zu stellen. Die wesentlichen Elemente einer Einschränkung des Rechts auf informationelle Selbstbestimmung sind durch formelles Gesetz festzulegen. In der Rechtsverordnung können in erster Linie ergänzende verfahrensrechtliche Vorkehrungen für die Durchführung und Organisation der Datenerhebung sowie die notwendigen Sicherheitsmaßnahmen geregelt werden.

4.7.2 Einsatz von Computern in Schulen

Über den Einsatz von Computern an Schulen findet in Hamburg eine öffentliche Auseinandersetzung statt, wobei eine Polarisierung der Standpunkte zu beobachten ist: Auf der einen Seite wird die Forderung erhoben, der zunehmenden Verbreitung der „Neuen Technologien" im Produktions-, Dienstleistungs- und Verwaltungsbereich Rechnung zu tragen, indem den jungen Menschen frühzeitig der Umgang mit solchen neuen Techniken ermöglicht und ihnen schon in der Schule das nötige Rüstzeug für den Eintritt in entsprechende Berufsbildungsgänge vermittelt wird. Es müßten mehr Computer für die Schulen angeschafft und mehr und besserer Informatikunterricht erteilt werden. Auf der Gegenseite wird vor einer „Computerisierung" der Schule gewarnt. Neben gesellschaftspolitischen Vorbehalten gegen die fortschreitende Automatisierung im allgemeinen befürchten die Gegner des Computereinsatzes an Schulen, daß bestimmte Hersteller und Wirtschaftsverbände ihren Einfluß bis in die Schulen ausdehnen könnten. Sie äußern auch die Befürchtung, daß die BSB noch gar kein bildungspolitisches Konzept für die Ausbildungsinhalte, insbesondere die Auseinandersetzung mit den Begleitumständen der neuen Technologien entwickelt hat und daher Fragen nach den sozialen Voraussetzungen und Auswirkungen, z.B. auf Arbeitsplätze und Freizeitgestaltung, nicht angemessen berücksichtigt werden.

Parallel zu dieser Auseinandersetzung wird darüber gestritten, ob und ggf. in welchem Umfang die für den Informatikunterricht an Schulen angeschafften Computer auch für schulische Verwaltungsaufgaben genutzt werden dürfen. Besonders solchen Lehrern, die Informatikunterricht erteilen, die also die Bedienung der Geräte beherrschen und Programme erstellen können, erscheint es nur natürlich, die Computer auch zur komfortableren Erledigung von Verwaltungsaufgaben einzusetzen: warum sollen die

Geräte, die nur vormittags im Unterricht gebraucht werden, nicht nachmittags zur Stundenplanerstellung, Aufstellung der Kurspläne für die reformierte Oberstufe, Vorbereitung von Zeugniskonferenzen usw. genutzt werden?

Ich vertrete dazu folgenden Standpunkt: Sobald auf den Rechnern der Schulen Verwaltungsaufgaben mit personenbezogenen Daten erledigt werden sollen, findet das Hamburgische Datenschutzgesetz Anwendung. Dieses verbietet die Verarbeitung personenbezogener Daten auf den im Informatikunterricht benutzten Rechnern nicht. Zulässig ist die Verarbeitung aber nur dann, wenn die Vorschriften des HmbDSG eingehalten werden. Die Beachtung der Anforderungen des § 8 und der Anlage dazu stößt im Schulbereich allerdings auf Schwierigkeiten. In den Schulen sind ausschließlich Personal-Computer vorhanden. Auf diesen werden Betriebssysteme eingesetzt, die (noch) keine ausreichenden Vorkehrungen gegen unbefugte Benutzung (Zugriffskontrolle, Speicherkontrolle, Eingabekontrolle) enthalten.

Inzwischen werden auf dem Markt Betriebssysteme mit entsprechenden Sicherungskomponenten angeboten. Ich halte es auch für denkbar, daß im Schulbereich eigene Sicherungssoftware als Ergänzung zu vorhandenen Betriebssystemen entwickelt wird. Daneben müßten – ebenfalls in § 8 HmbDSG geforderte – organisatorische Maßnahmen getroffen werden, um den unberechtigten Zugriff auf Datenträger mit personenbezogenen Verwaltungsdaten (z.B. durch Schüler) zu verhindern. Auf die beim Einsatz von PCs für Verwaltungsaufgaben ganz allgemein gesehenen Risiken bin ich unter 3.3 näher eingegangen.

Wenn die BSB die Situation an den Schulen heute so beurteilt, daß sie die datenschutzrechtlich geforderte Datensicherheit bei einer gemischten Verwendung der Rechner noch nicht für gewährleistet hält und wenn sie deshalb in ihrer Verwaltungsvorschrift (Datenschutz-Info, MittBlSchul 1985, S. 36) den Einsatz von Schulcomputern für Verwaltungsaufgaben nur sehr restriktiv, nämlich nicht auf den im Unterricht eingesetzten Geräten und nicht auf privaten Rechnern der Lehrer außerhalb der Schule zuläßt, so habe ich dagegen nichts einzuwenden, wenngleich ich selbst eine solche Entscheidung nicht gefordert habe. Ich halte eine gemeinsame Nutzung der Computer für Unterricht und Verwaltungsaufgaben erst für möglich, wenn im Schulbereich ein angemessenes Sicherungskonzept entwickelt und verbindlich vorgeschrieben wird.

4.8 Einwohnerwesen

4.8.1 Automation im Einwohnerwesen

Ich habe in meinem 3. TB (3.7.1.1, S. 48) ausführlich über das geplante Verfahren berichtet. Seitdem ist die Konzeption nochmals geändert worden; nunmehr soll im Einwohnerwesen von vornherein ein Volldialogverfahren eingeführt werden, das auf einer Einwohnerdatenbank aufbaut. In dieses Verfahren sind alle Aufgaben der Einwohnerdienststellen integriert. Über Bildschirme, die dezentral in allen Dienststellen eingerichtet werden, sollen Veränderungen in vorhandenen Einwohnerdatensätzen oder die Daten neu zugezogener Einwohner on-line eingegeben werden.

Die Verwaltung meint, daß die Absicherung gegen Anlaufrisiken auch bei zügiger Einführung eines volldialogisierten Verfahrens mit einem mikroverfilmten Datenbestand als Rückfallstufe gewährleistet werden kann. Darum soll jeder Sachbearbeiter sofort ein Dialoggerät an seinem Arbeitsplatz erhalten.

Da diese Änderung der Konzeption nicht zu einer Verstärkung der datenschutzrechtlichen Risiken führt, habe ich keine Bedenken geäußert.

4.8.2 Gesetzentwurf zur Änderung des Hamburgischen Meldegesetzes (HmbMG)

Über die automationsbedingte Novellierung des HmbMG habe ich ebenfalls bereits in meinem 3. TB berichtet (vgl. Nr. 3.7.1.2, S. 50 ff.). Inzwischen hat die Bürgerschaft über das Änderungsgesetz beraten. Bis zum Redaktionsschluß waren die Ausschußbera-

tungen zwar abgeschlossen, eine Verabschiedung durch die Bürgerschaft stand jedoch noch aus.

4.8.2.1 On-line-Zugriff der Polizei

Meine anfänglichen Bedenken gegen den automatisierten Abruf von Meldedaten durch die Polizei (vgl. 3. TB, Nr. 3.7.1.3, S. 50) sind nunmehr aus folgenden Gründen ausgeräumt worden:

- Für dieses Verfahren wird es eine gesetzliche Regelung im HmbMG geben.
- Der Teil des Datenbestandes, der nur die Identifizierungsdaten enthält und der allein dem Zugriff der Polizei unterliegt, wird physisch aus dem Melderegister abgesplittet.
- Die Suchmöglichkeiten werden eng eingegrenzt sein, so daß Rasterfahndungen ausgeschlossen sind.
- Die Datensicherungsmaßnahmen werden durch Rechtsverordnung geregelt werden. Insbesondere sind Vorkehrungen vorgesehen, die es ermöglichen sollen, die Zulässigkeit der Abrufe zu kontrollieren.

4.8.2.2 Hotelmeldepflicht

Durch das Änderungsgesetz ist auch die Regelung des Hotelmeldeverfahrens geändert worden. Danach sind die Meldescheine von der Beherbergungsstätte künftig drei Monate aufzubewahren und anschließend zu vernichten. Außerdem werden künftig die Hotelmeldescheine nicht mehr generell der Polizei übergeben, sondern nur noch auf Verlangen und nur solche, die nicht älter als eine Woche sind. Auf Durchschriften wird ganz verzichtet.

Mit dieser Änderung ist eine Regelung des HmbMG, die von mir (Nr. 3.7.15, S. 53 meines 3. TB) als vordringlich änderungsbedürftig bezeichnet wurde,den Bestimmungen in anderen Landesmeldegesetzen angepaßt worden. Die Zweifel an der Verfassungsmäßigkeit der Krankenhaus- und Hotelmeldepflicht, die vom ehemaligen Präsidenten des Bundesverfassungsgerichts Ernst Benda bei den Beratungen zur Novellierung des Berliner Meldegesetzes geäußert wurden und die von mir geteilt werden, bleiben jedoch bestehen. Wegen der Rahmenkompetenz des Bundes muß zunächst das MRRG geändert werden.

4.8.3 Auskunftssperre nach dem Hamburgischen Meldegesetz

Nach § 34 Abs. 5 HmbMG ist jede Melderegisterauskunft unzulässig, wenn der Betroffene der Meldebehörde hat glaubhaft machen können, daß ihm oder einer anderen Person aus einer solchen Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann. Selbst bei Nachweis eines berechtigten Interesses dürfen an Private dann keine Auskünfte erteilt werden. Datenübermittlungen an öffentliche Stellen richten sich nach einer anderen Vorschrift und sind weiterhin zulässig.

Wird bei der Meldebehörde ein Auskunftsersuchen bezüglich einer Person gestellt, für die eine Auskunftssperre vermerkt ist, so wird dem Anfragenden mitgeteilt, daß aus Rechtsgründen keine Auskunft erteilt werden könne. Gleichzeitig unterrichtet die Meldebehörde den betroffenen Einwohner über die Anfrage, damit er seinerseits mit dem Auskunftssuchenden Verbindung aufnehmen kann. Hiervon wird wiederum der Anfragende unterrichtet. Weitere Maßnahmen zugunsten des Anfragenden sind der Meldebehörde nach der Rechtslage nicht möglich.

Die Behörde für Inneres hat mir nun mitgeteilt, daß aufgrund dieser melderechtlichen Regelung wiederholt Schuldner sich dem Zugriff ihrer Gläubiger haben entziehen können. Deshalb wird erwogen, in einem solchen Fall die erbetene Auskunft nicht dem Gläubiger, sondern unmittelbar dem örtlich zuständigen Gerichtsvollzieher zuzuleiten, um so eine Vollstreckung aus dem auf frühere Anschriften des Schuldners lautenden Vollstreckungsbescheid zu ermöglichen.

Ich habe Bedenken gegen eine solche Auslegung des § 34 Abs. 5 HmbMG. Zum einen sollen nach Sinn und Zweck dieser Vorschrift Auskunftssperren –ohne Einwilligung des Betroffenen– ein unüberwindbares Hindernis für das Informationsinteresse eines jeden Auskunftssuchenden sein; zum anderen dürfte es in der Praxis zu erheblichen Problemen führen, wenn die Meldebehörde die Voraussetzungen der Auskunftssperre bei jedem Auskunftsersuchen erneut prüfen müßte. Im übrigen meine ich, die Meldebehörde kann nicht mit hinreichender Sicherheit ausschließen, daß eine Gefahr für Leben, Freiheit, Gesundheit und ähnliche schutzwürdige Belange eines Betroffenen bei einer bestimmten einzelnen Auskunft doch eintritt. Dies gilt vor allem deshalb, weil der Meldebehörde die rechtliche Handhabe fehlt, um eine eingeschränkte Verwendung der Meldedaten durchzusetzen.

Wenn meine strikte Auslegung des § 34 Abs. 5 HmbMG in der Praxis zu unerträglichen, vom Gesetzgeber nicht vorgesehenen Ergebnissen führen sollte – was ich aber für unwahrscheinlich halte, zumal ein Anspruch von Gläubigern auf Auskunftserteilung ohnehin nur im Rahmen des Gleichbehandlungsgrundsatzes besteht – , kommt nur eine Änderung des HmbMG in Betracht.

4.8.4 Paß- und Personalausweiswesen

In meinen beiden letzten TBen (2. TB, 3.8.2, S. 66 f.; 3. TB, 3.7.2, S. 54 f.) habe ich ausführlich die Probleme erörtert, die sich im Zusammenhang mit der Einführung eines maschinenlesbaren Personalausweises ergeben. Im Berichtszeitraum ist die Diskussion u.a. auf einer Sachverständigen-Anhörung des Bundestag-Innenausschusses im Mai 1985 fortgeführt worden, an der ich teilgenommen habe. Auf dieser Anhörung zeigte sich, daß die von vielen Seiten vorgetragenen Zweifel am Sicherheitsgewinn und befürchteten Gefahren für das Recht auf informationelle Selbstbestimmung unvermindert fortbestehen. Gleichwohl hält die Bundesregierung an ihren Absichten zur baldigen Einführung des neuen Personalausweises fest. Dies ist vor allem deshalb außerordentlich bedenklich, weil es mir ausgeschlossen erscheint, daß Bundestag und Bundesrat die mit dem maschinenlesbaren Ausweis verbundenen Risiken für die Persönlichkeitsrechte der Bürger angemessen bewerten können, ohne sicher zu wissen, wann und unter welchen Voraussetzungen die Polizei mit Hilfe des Personalausweises Informationen erheben und verwenden darf. Die Verabschiedung von bereichsspezifischen Regelungen für die Informationsverarbeitung durch die Polizei ist jedoch noch nicht in Sicht (vgl. 4.9).

Nach den mir bislang bekannt gewordenen Vorstellungen der Bundesregierung bzw. der Regierungsparteien, soll zwar die Strafprozeßordnung um einen § 163 d ergänzt werden, der die Speicherung von Personalausweisdaten im einzelnen regelt. Danach sollen Protokollierungen bei der Verfolgung von Straftaten i.S. des § 100 a StPO zulässig sein und einer richterlichen Bestätigung bedürfen. Auch nach dieser Regelung bleibt jedoch offen, in welchen Fällen die Polizei mit Hilfe des Ausweises Daten erheben, also Personen kontrollieren darf.

Insgesamt halte ich meine Bedenken gegen den neuen Personalausweis in vollem Umfang aufrecht: Vor der Einführung derartiger Technologien müssen ihre Folgen absehbar und ggf. durch klare normative Regelungen eingegrenzt sein.

4.8.5 Prüfung der Verwarnungs- und Bußgeldstelle

Ich habe in diesem Jahr die Datenverarbeitung durch die Verwarnungs- und Bußgeldstelle der Behörde für Inneres geprüft, die zuständig ist für die Verfolgung und Ahndung von Ordnungswidrigkeiten im Straßenverkehr. Der überwiegende Teil der Datenerhebungen erfolgt durch die Polizei, die die Aufnahmebelege der Verwarnungs- und Bußgeldstelle übermittelt. Dann werden die Daten bei der DVZ erfaßt und in der Ordnungswidrigkeiten-Datei gespeichert. Mit der Speicherung der Daten aus den Aufnahmebelegen bei der DVZ wird ein automatischer Verfahrensablauf in Gang gesetzt, in dessen Verlauf im Wege des Bandaustausches die Halterdaten vom Kraftfahrtbundesamt (KBA) erfragt sowie Verwarnungsgeldangebote ausgedruckt und versendet werden. Die DVZ übernimmt im weiteren Verlauf des Verfahrens folgende Arbeiten:

- Ausdrucken und Versenden des Bußgeldbescheides;
- Ausdrucken und Versenden einer Mahnung;
- Ausdrucken eines Vollstreckungsersuchens;
- Buchung von Zahlungseingängen;
- Auslagerung von erledigten Verfahren.

Sowohl das Programm als auch das Verfahren bei der DVZ habe ich in meine Überprüfung der Verwarnungs- und Bußgeldstelle nicht mit einbezogen.

Bei Unfällen im Straßenverkehr wird je nach Schwere der Schäden von den Beteiligten die Polizei benachrichtigt, die dann ihre Ermittlungen aufnimmt und eine Verkehrsunfallanzeige fertigt. Diese Verkehrsunfallanzeige wird ggf. mit weiteren Unterlagen (Vernehmungsprotokolle, Beweismittel) von der Polizei an die Staatsanwaltschaft übersandt, sofern Anhaltspunkte für die Verfolgung einer Straftat vorliegen, sonst an die Verwarnungs- und Bußgeldstelle, sofern nur die Verfolgung als Ordnungswidrigkeit in Betracht kommt. Stellt die Staatsanwaltschaft das Verfahren ein, so gibt sie die Sache an die Verwarnungs- und Bußgeldstelle ab und übersendet die Akten.

Meine Gespräche mit der Behörde für Inneres über die Prüfung sind noch nicht abgeschlossen. An dieser Stelle beschränke ich mich darauf, auf folgende Punkte hinzuweisen:

Die Polizei erhebt die Daten aufgrund der Bestimmung des § 53 OWiG. Es handelt sich hierbei um eine Generalklausel, die dem Gebot der Normenklarheit, wie es vom Bundesverfassungsgericht in seinem VZ-Urteil formuliert worden ist, nicht genügt. Eine Präzisierung dieser Vorschrift ist deshalb erforderlich. Gegen den Umfang der Datenerhebung habe ich dagegen keine Einwände erhoben. Als Maßstab hierfür ist die Bestimmung des § 66 OWiG heranzuziehen, die den Inhalt des Bußgeldbescheides hinreichend konkretisiert.

Die Aufnahme des Geburtsdatums des Betroffenen in das Aktenzeichen bei der Bearbeitung von Verkehrsunfallangelegenheiten in der Verwarnungs- und Bußgeldstelle – wie es zur Zeit geschieht – halte ich nicht für erforderlich. Die interne Geschäftsverteilung läßt sich ebenso gut durch fortlaufende numerische Aktenzeichen regeln.

Ist gegen den Betroffenen ein Fahrverbot nach § 25 StVG rechtskräftig festgesetzt, macht die Verwarnungs- und Bußgeldstelle hiervon Mitteilung an die zuständige Führerscheinstelle. Für diese Praxis gibt es bislang keine Rechtsgrundlage. Über die Notwendigkeit dieser Mitteilungen wird diskutiert.

Soweit Daten beim Betroffenen in Anhörbogen erhoben werden, ist inzwischen die Anzahl der erhobenen Daten auf den erforderlichen Umfang eingeschränkt worden. So wird z.B. bei Verwarnungsgeldangeboten auf die Erhebung von Führerscheindaten generell verzichtet, auch sind die Hinweise klarer gefaßt worden. Ich habe i.ü. gefordert, ausdrücklich auf die Freiwilligkeit der nicht von § 111 OWiG umfaßten Angaben hinzuweisen, wie es § 9 Abs. 2 HmbDSG vorsieht. Ein solcher Hinweis ist auch für die Datenerhebungen bei Zeugen in das entsprechende Formblatt aufzunehmen.

Über den Ausgang meiner Gespräche mit der Behörde für Inneres sowie meine abschließende datenschutzrechtliche Bewertung der Informationsverarbeitung bei der Verwarnungs- und Bußgeldstelle werde ich im nächsten Jahr berichten.

4.9 Polizei

Im Sicherheitsbereich lag im Berichtszeitraum erneut einer der Schwerpunkte meiner Tätigkeit. Nachdem im Juni 1985 die Hamburgischen Dateienrichtlinien (vgl. Amtl. Anzeiger, S. 1085)erlassen worden waren, sind mir eine ganze Reihe von Feststellungsanordnungen für bereits bestehende Dateien sowie Errichtungsanordnungen für neue Dateien – insbesondere Spurendokumentationssysteme – vorgelegt worden, mit denen ich mich auseinanderzusetzen hatte. Daneben war wiederum eine erhebliche Anzahl von Eingaben zu bearbeiten, in denen es vornehmlich um die Löschung

von Daten ging, die von der Polizei gespeichert wurden. Schließlich habe ich die Überprüfung einiger Dienststellen in Angriff genommen. Die Aktivitäten im einzelnen zu beschreiben, würde den Rahmen des Berichts sprengen. Ich habe mich daher nur auf wenige beschränkt (Errichtungsanordnung APIS, Speicherung personengebundener Hinweise, ZEVIS) und mich im übrigen vornehmlich dem Problemkreis zugewendet, in den die Auseinandersetzung bei fast allen praktischen Fragen immer wieder einmündete: die Frage nach den Rechtsgrundlagen der polizeilichen Informationstätigkeit. Ständig werde ich mit dem Problem konfrontiert, an welchen konkreten Kontrollmaßstäben ich z.B. die Einrichtung neuer Dateien messen soll. Immer wieder muß ich feststellen, daß das schlichte Kriterium der „Erforderlichkeit zur Aufgabenerfüllung" bei meiner praktischen Tätigkeit wenig hilfreich, sondern viel zu unbestimmt ist. Als Beispiel verweise ich nur auf die ermüdende, über drei Jahre andauernde Auseinandersetzung über die Zulässigkeit von Hinweisen auf Freitodversuche.

Auch wegen dieser Erfahrungen habe ich mich im Berichtszeitraum besonders intensiv an der Diskussion um die Schaffung präziserer Rechtsgrundlagen für die polizeiliche Informationstätigkeit (SOG-Novellierung) beteiligt, die ich auch in diesem Berichtsteil in den Vordergrund gerückt habe. Gesetzgeberische Maßnahmen sind mithin nicht nur dringend geboten, um den Betroffenen deutlich zu machen, mit welchen Beschränkungen ihres Rechts auf informationelle Selbstbestimmung sie zu rechnen haben, und den Polizeibeamten einen klaren normativen Handlungsrahmen zu weisen, sondern auch, um dem Datenschutzbeauftragten die Möglichkeit einer effektiven Kontrolltätigkeit zu eröffnen. Wie ich schon im 3. TB (3.10., S. 89) betont habe, nützt die Einrichtung von Kontrollinstanzen relativ wenig, wenn die Maßstäbe der Kontrolle unklar sind.

4.9.1 Allgemeine Bemerkungen zur Novellierung des Polizeirechts

Die Bemühungen um die gebotene Novellierung des Polizeirechts (vgl. 3. TB, 3.8.5 S. 76 ff.) sind im Berichtszeitraum weitergegangen und haben zu ersten Gesetz-Entwürfen geführt. Im Januar 1985 hat die Konferenz der Datenschutzbeauftragten einen Beschluß über „Anforderungen an Datenschutzregelungen im Polizeirecht" gefaßt und den Innenministern zugeleitet. Gleichzeitig wurde ein Formulierungs-Vorschlag für Datenschutzregelungen übergeben, den ein Arbeitskreis der DSB-Konferenz erarbeitet hatte. Die Innenminister-Konferenz legte ihrerseits einen „Vorentwurf zur Änderung des Musterentwurfes für ein einheitliches Polizeigesetz" (nachfolgend „ME-VE") zur Stellungnahme vor.

Die bisherige Diskussion läuft allerdings im wesentlichen verwaltungsintern. Lediglich in Hessen gibt es bereits Entwürfe von Regierung und Opposition, die der Öffentlichkeit vorgelegt worden sind. Nachfolgend habe ich mich zunächst – anknüpfend an meine Ausführungen im 3. TB (3.8.5) – darauf konzentriert, meine Position in Auseinandersetzung mit den Regelungen des ME-VE weiter zu präzisieren, die mir bislang besonders kritikbedürftig erscheinen. Anschließend habe ich noch einmal kurz – soweit es mir bis zum Redaktionsschluß möglich war – die Punkte hervorgehoben, die mir im neuesten Entwurf zur Novellierung des SOG besonders problematisch erscheinen.

Ein Hauptproblem der bisherigen Novellierungsdiskussion liegt darin, daß die Polizei von einer ganz anderen Ausgangsposition ausgeht als die Datenschutzbeauftragten. Die Polizei geht davon aus – und so kommt es auch in der Begründung des ME-VE, den ein Arbeitskreis der IMK vorgelegt hat, zum Ausdruck – daß eine Novellierung lediglich aus Gründen der Klarstellung erforderlich ist und daß alle Regelungen daher auf eine Fixierung des „Ist-Zustandes" hinauslaufen, da die bisherige Praxis auch in Zukunft zulässig sein müsse.

Dieser Ansatzpunkt ist nach der Auffassung aller Datenschutzbeauftragten völlig verfehlt:

a) Es geht nicht nur um klarere Formulierungen bereits vorhandener Rechtsgrundlagen, sondern auch um die erstmalige Schaffung von Eingriffsermächtigungen für

polizeiliche Maßnahmen, die bislang ohne gesetzliche Eingriffsermächtigung vorgenommen worden sind. Wie ich in meinen Tätigkeitsberichten bereits mehrfach deutlich gemacht habe (vgl. 2. TB, 5.1.3, S. 143 ff.; 3. TB, 3.8.5, S. 70 ff.) fehlt es z.Z. insbesondere an Rechtsgrundlagen für alle Formen der Datenverarbeitung, bei denen in das informationelle Selbstbestimmungsrecht von Nichtstörern und Nichtverdächtigen eingegriffen wird. Das betrifft z.B. Maßnahmen wie die polizeiliche Beobachtung, die Rasterfahndung, die Speicherung „anderer Personen" i.S. von Ziff. 2.2.11 der KpS-Richtlinien und das Festhalten friedlicher Demonstrationsteilnehmer auf Bild- und Tonträgern.

In der neueren Rechtssprechung ist auch anerkannt, daß z.B. die Führung von Kriminalakten mangels Vorliegens einer konkreten Gefahr nicht auf die polizeiliche Generalklausel gestützt werden kann (vgl. BayVerfGH, Entscheidung vom 9.7.1985 – AZ 44-VI-84, die mit eindrucksvollen Argumenten einige frühere Entscheidungen unterer Instanzen widerlegt; VG Frankfurt, Urteil vom 19.3.1985 – IV/1 E 3524/83). Hier gibt es also keine Befugnisse, die sich durch Auslegung unklarer Rechtsvorschriften absichern lassen, sondern hier gibt es – wie der bayerische Verfassungsgerichtshof eindeutig festgestellt hat – schlicht Regelungslücken. Das offene Problem, das aber nicht pauschal gelöst werden kann, besteht allein darin, ob und nach welcher Maßgabe solche Regelungslücken für eine Übergangszeit hingenommen werden können, um dem Gesetzgeber ausreichend Zeit für die Beratung und den Erlaß der erforderlichen Vorschriften zu lassen.

b) Auch die weitere Ausgangsposition der Polizei, wonach die polizeiliche Informationsverarbeitung im gegenwärtigen Ausmaß auch künftig zulässig sein müsse, ist bereits im Ansatz verfehlt.

Diese These ist mit den vom Bundesverfassungsgericht aufgezeigten Grenzen einer gesetzlichen Regelung nicht vereinbar: Das Recht auf informationelle Selbstbestimmung darf nur eingeschränkt werden, soweit ein überwiegendes Allgemeininteresse dies gestattet. Der damit gebotenen Interessenabwägung kommt überall dort besondere Bedeutung zu, wo es sich um Maßnahmen mit besonders hoher Eingriffsqualität oder um solche handelt, bei denen eine Vielzahl von Unbeteiligten einbezogen werden. Bei der Abwägung ist auch dem allgemein gültigen polizeirechtlichen Grundsatz Rechnung zu tragen, daß Eingriffe allein zur Erleichterung polizeilicher Aufsicht unzulässig sind. Eine ungeprüfte Übernahme und Festschreibung der gegenwärtigen Praxis ist schon deshalb bedenklich, weil diese Praxis sich in einer Zeit entwickelt hat, in der der polizeiliche Umgang mit personenbezogenen Daten noch als nicht regelungsbedürftiger, weil „schlichthoheitlicher Vorgang" angesehen wurde. Hinzu kommt, daß die Erhebung und Verarbeitung von Daten im Sicherheitsbereich durch die ständige Verfeinerung eine neue Qualität mit neuen Gefahrenquellen für das Persönlichkeitsrecht erhalten hat, was eine Überprüfung der gegenwärtigen Verfahrensweisen unverzichtbar macht: Großräumige Verbundsysteme, völlig neue Formen der Massendatenverarbeitung, hochleistungsfähige Verknüpfungsverfahren und eine ständig zunehmende Zahl von on-line-Verbindungen bringen ebenso wie etwa der neue maschinenlesbare Ausweis, der Ausbau von ZEVIS und der Einsatz selbsttätiger Aufzeichnungsgeräte neuartige Gefährdungen des Rechts auf informationelle Selbstbestimmung mit sich, denen nur mit präzisen, den polizeilichen Handlungsspielraum eingrenzenden Bestimmungen wirksam begegnet werden kann.

Solange die Polizei die kritisierten Ausgangspositionen nicht aufgibt und die Zielrichtung des VZ-Urteils nicht akzeptiert, ist die Entwicklung konsensfähiger Vorschläge zur Novellierung des Polizeirechts sehr schwierig.

4.9.2 Zur Kritik des Musterentwurfs

4.9.2.1 Neubestimmung der polizeilichen Aufgaben

Nach dem aktuellen Stand der Diskussion sollen die Befugnisse der Polizei nicht mehr auf die traditionellen Aufgabenbereiche der Gefahrenabwehr sowie der Verfolgung

von Straftaten und Ordnungswidrigkeiten begrenzt bleiben; vielmehr sollen die Entwicklungen der polizeilichen Praxis nachvollzogen und auch Befugnisse zur „vorbeugenden Bekämpfung von Straftaten" und zur „Gefahrenvorsorge" begründet werden (vgl. dazu auch 3. TB 3.8.5.1, S. 76).

Um dem rechtsstaatlichen Gebot der Normenklarheit gerecht werden zu können, sind für die geplante Ausweitung polizeilicher Befugnisse sehr differenzierte gesetzliche Regelungen notwendig. Grundvoraussetzung ist zunächst, daß die Aufgaben der Polizei neu bestimmt werden. Es ist zu klären, in welchem Verhältnis die „Gefahrenvorsorge" und die vorbeugende Bekämpfung von Straftaten zur klassischen Gefahrenabwehr stehen sollen. Da die neuen Aufgaben gerade nicht mehr an das Vorliegen einer konkreten Gefahr anknüpfen, droht sonst eine Vermischung der Begriffe der konkreten und abstrakten Gefahr.

Darüber hinaus ist es erforderlich, jede neue Aufgabe – nach Möglichkeit nicht erst bei der Begründung neuer Befugnisse – genauer zu definieren und einzugrenzen. Während die traditionelle Aufgabe der Gefahrenabwehr durch jahrzehntelange Lehre und Rechtssprechung deutlich umrissen ist, bleiben die Konturen des neuen Aufgabenbereichs „vorbeugende Bekämpfung von Straftaten" noch recht unklar. Dabei sollte wenigstens in der Begründung klargestellt werden, daß es vornehmlich um den Umgang mit personenbezogenen Informationen geht; und zwar in erster Linie um die Sicherstellung einer Verwertungsmöglichkeit für Informationen, die im Rahmen von Strafermittlungsverfahren gewonnen wurden, sowie die Schaffung einer Möglichkeit zur Inanspruchnahme heimlicher Informationseingriffe für die Bekämpfung bestimmter Deliktsarten.

Problematisch ist es darüber hinaus, die sog. „Gefahrenvorsorge" als besondere Aufgabe anzuerkennen und der Polizei auch zu diesem Zweck zusätzliche Befugnisse einzuräumen. Selbstverständlich muß sich die Polizei auf die Bekämpfung von künftigen Gefahren vorbereiten und einstellen; selbstverständlich kann sie nur Gefahren abwehren, wenn sie über die jeweils erforderlichen Informationen verfügt. Fraglich ist allerdings, ob aus diesen Selbstverständlichkeiten schon die Gefahrenvorsorge als eigenständige polizeiliche Aufgabe abzuleiten ist.

Ich gehe davon aus, daß die Polizei die zur Vorbereitung auf künftige Gefahrensituationen vorzuhaltenden Informationen mit dem Einverständnis der Betroffenen erheben und speichern kann. Sollte sich dieses bei genauerer Analyse als unpraktikabel erweisen, erscheint es mir aus Gründen der Normenklarheit zumindest erforderlich, genauer festzulegen, welche Daten welches Personenkreises zu Zwecken der Gefahrenvorsorge gespeichert und in aktuellen Gefahrenabwehrsituationen genutzt werden dürfen. Dabei dürfte es sich nach in der Begründung zum ME-VE genannten Beispielen vornehmlich um Angaben über die Erreichbarkeit solcher Personen handeln, deren Fachkenntnisse bzw. technische Geräte zur Abwehr von Gefahren benötigt werden. Auf keinen Fall kann eine generelle Befugnis zur Verarbeitung personenbezogener Daten zu Zwecken der Gefahrenvorsorge akzeptiert werden, die nur durch den Erforderlichkeitmaßstab begrenzt wird. Dies wäre verfassungswidrig.

4.9.2.2 Neubestimmung polizeipflichtiger Personen

Eine Neubestimmung der Aufgaben macht auch präzisere Bestimmungen des Personenkreises erforderlich, der Beschränkungen seines Rechts auf informationelle Selbstbestimmung akzeptieren soll. Die bisherige Inanspruchnahme von Störern, also Verursachern einer konkreten Gefahr, reicht nicht mehr. Bedenklich ist allerdings die allgemeine Ausweitung des Adressatenkreises polizeilicher Informationseingriffe auf „andere Personen", wie im ME-VE vorgesehen.

Es mag zwar anzuerkennen sein, daß die Polizei unter bestimmten Voraussetzungen Daten von Personen erhebt, die nicht polizeipflichtig im herkömmlichen Sinne sind, etwa von Auskunftspersonen. Dies rechtfertigt jedoch nicht eine Ausdehnung des Adressatenkreises auf jedermann, wenn die Inanspruchnahme nur durch das Erforderlichkeitsprinzip eingegrenzt wird.

Es ist daher zunächst erforderlich, den Kreis der sog. „anderen Personen" – und zwar differenziert nach den unterschiedlichen polizeilichen Aufgabengebieten – näher einzugrenzen. Zu denken wäre etwa – im Bereich der Gefahrenabwehr – an Zeugen, Hinweisgeber u.ä. sowie an Opfer und Geschädigte. Im Bereich der vorbeugenden Bekämpfung von Straftaten an „Vorverdächtige", also an Personen, bei denen aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, daß deren Speicherung zur Aufklärung schwerwiegender Straftaten angemessen ist.

Ferner sind neben dem schlichten Erforderlichkeitsmaßstab zusätzliche Eingriffsvoraussetzungen zu formulieren; denn aus dem Verhältnismäßigkeitsprinzip folgt, daß Nicht-Störer nur als ultima ratio in Anspruch genommen werden dürfen. Um diesem Grundsatz Rechnung zu tragen, dürfen polizeiliche Vorbeugungsmaßnahmen mit Eingriffscharakter nur zugelassen werden, soweit es um die Verhütung von Straftaten mit erheblicher Bedeutung für die Allgemeinheit geht. Welche Straftaten aufgrund ihrer Schwere eine solche Bedeutung haben, ist näher zu definieren, nach Möglichkeit durch einen abschließenden Katalog bestimmter Straftatbestände.

Schließlich ist nicht nur klarzustellen, inwieweit sich aus dem Gesetz Erhebungsrechte der Polizei ergeben; sondern die Betroffenen müssen ihm auch klar entnehmen können, ob und unter welchen Voraussetzungen sie zur Mitwirkung bei der Erhebung verpflichtet sind (Auskunftspflicht). Bisher wurde die polizeiliche Generalklausel auch als Rechtsgrundlage für die Auskunftspflicht des Bürgers anerkannt. Diese Auffassung ist nach dem VZ-Urteil nicht mehr haltbar. Wenn die Begründung einer Auskunftspflicht zu Zwecken der Gefahrenabwehr für notwendig erachtet wird, muß eine spezielle, den Geboten der Normenklarheit gerecht werdende Befugnis formuliert werden.

4.9.2.3 Verdeckte Datenerhebung

In einem demokratischen Gemeinwesen sollen staatliche Informationserhebungen grundsätzlich offen und beim Bürger selbst erfolgen. Nur wenn der Staat ihm „mit offenem Visier" gegenübertritt, kann der Bürger wissen, wer was wann bei welcher Gelegenheit über ihn weiß, und sein Recht auf informationelle Selbstbestimmung wahrnehmen.

Es liegt allerdings auf der Hand, daß es Fälle gibt, in denen ein Rückgriff auf heimliche Informationsbeschaffungsmaßnahmen unverzichtbar ist. Dieses Privileg war nach der bisherigen Gesetzeslage allerdings dem nur beobachtenden, nicht mit exekutiven Befugnissen ausgestatteten Verfassungsschutz vorbehalten. Eine Übertragung heimlicher Erhebungsbefugnisse auf die Polizei kommt wegen des besonders schwerwiegenden Eingriffs in das Recht auf informationelle Selbstbestimmung nur für die Bekämpfung besonders gravierender Straftaten in Betracht. Keinesfalls gerechtfertigt ist es, heimliche Maßnahmen gleichsam in das routinemäßige Arsenal polizeilicher Eingriffsmittel zu übernehmen, über deren Einsatz – selbst bei Fehlen einer Gefahr im Verzuge – nur ein Dienststellenleiter entscheidet und die fast immer – mit Ausnahme von Bagatellfällen – zur Anwendung kommen könnten. Genau dies wäre aber die Folge, wenn der ME-VE geltendes Recht würde.

4.9.2.3.1 §§ 32, 34 StGB als Rechtsgrundlage

Die Schaffung von Rechtsgrundlagen für die heimliche Datenerhebung ist zwar im ME-VE vorgesehen. Deren Notwendigkeit wird jedoch in der öffentlichen Diskussion immer wieder in Zweifel gezogen. Insbesondere wird damit argumentiert, daß eine Schaffung besonderer Befugnisse für Ausnahme-Maßnahmen wie den Einsatz von verdeckten Ermittlern (und Lauschangriffen) nicht geboten sei, da die Polizei für diese hoheitlichen Maßnahmen auf die strafrechtlichen Rechtfertigungsgründe der §§ 32, 34 StGB zurückgreifen könne.

Diese Auffassung ist nicht haltbar:

Der Staat kann seine Eingriffsmaßnahmen nur auf gesetzliche Befugnisse stützen, die speziell hoheitliches Handeln regeln und damit gleichzeitig dessen Voraussetzung

und Grenzen für den Bürger transparent machen. Das BVerfG hat hierzu im VZ-Urteil ausgeführt, daß jedenfalls Informationseingriffe, die zwangsweise durchgesetzt werden können, einer gesetzlichen Grundlage bedürfen, die „bereichsspezifisch und präzise" regelt, was mit diesen Daten geschieht. Diese Anforderung gilt auch, ja erst recht, für heimliche Maßnahmen, denn hier ist der Informationseingriff noch intensiver, weil er dem Bürger unbekannt ist und dieser zunächst keine Möglichkeit hat, sich mit rechtlichen Gegenmaßnahmen zu wehren.

Die §§ 32 und 34 StGB sind gewiß nicht als bereichsspezifische und präzise Regelungen im vorstehend genannten Sinne anzusehen. Der Bürger kann ihnen weder die Voraussetzungen für Beschränkungen seines Rechts auf informationelle Selbstbestimmung noch deren Umfang entnehmen. Die §§ 32 und 34 regeln nur, wann ein an sich tatbestandsmäßiges Verhalten ausnahmsweise gerechtfertigt ist. Das Handeln selbst wird durch die genannten Vorschriften nicht geregelt. Davon abgesehen erscheint es ohnehin nicht zulässig, das regelmäßige Handeln von Behörden auf Befugnisse zu stützen, die im absoluten Ausnahmefall jedermann zugestanden werden.

Die §§ 32, 34 enthalten deshalb auch keine Hinweise auf einschränkbare Grundrechte mit Gesetzesvorbehalt, wie es z.B. Eingriffe in das Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG) und das Recht auf Unverletzlichkeit der Wohnung (Art. 13) erfordern. Eine Berufung auf die §§ 32 und 34 StGB kommt nach allem nicht als Grundlage für polizeiliches Handeln in Betracht. Allenfalls können sich einzelne Beamte in einem gegen sie gerichteten Strafverfahren darauf berufen. Neue Eingriffsbefugnisse der Polizei – wie der Einsatz verdeckter Ermittler – erfordern neue Rechtsgrundlagen.

4.9.2.3.2 Definition heimlicher Erhebungsmaßnahmen

Nach dem ME-VE sind folgende Methoden heimlicher Datenerhebung vorgesehen, die auch in der bisherigen Praxis schon eingesetzt wurden:

- Observation
- Einsatz von Vertrauenspersonen („V-Leute")
- verdeckter Einsatz von technischen Mitteln
- Einsatz von Polizeivollzugsbeamten unter einer Legende (verdeckte Ermittler).

Die Notwendigkeit dieser Maßnahmen bedarf zuallererst einer tragfähigen Begründung, um genau prüfen zu können, ob derart weitgehende Eingriffe im überwiegenden Allgemeininteresse zu rechtfertigen sind.

Ferner müssen die genannten Maßnahmen im Gesetz jeweils präzise definiert werden. So ist z.B. klarzustellen, was unter dem verdeckten Einsatz von technischen Mitteln zu verstehen ist und was verdeckte Ermittler tun bzw. nicht tun dürfen.

Schließlich sind die Voraussetzungen für die jeweiligen heimlichen Erhebungsmaßnahmen (Zwecke, betroffener Personenkreis, Anordnungskompetenz, Kontrollmaßnahmen) differenziert, je nach der Intensität des Eingriffs zu regeln. Besonders einengender Regelungen bedürfen dabei der verdeckte Einsatz von technischen Mitteln in und an Wohnungen (sog. „Lauschangriff") und der Einsatz verdeckter Ermittler.

4.9.2.3.3 Zugelassene Zwecke

Nicht jeder polizeiliche Zweck kann heimliche Datenerhebungen rechtfertigen. Zweifelhaft erscheint insbesondere, ob die Abwehr von Gefahren als Zweck in Betracht kommt. Stichhaltige Begründungen dafür gibt es bislang nicht. In den bislang diskutierten Fallbeispielen geht es in aller Regel gleichzeitig – neben der Gefahrenabwehr – um die Verfolgung von Straftaten, also z.B. die Befreiung eines Opfers aus den Händen eines Entführers.

Sollten heimliche Formen der Datenerhebung sich jedoch auch für Gefahrenabwehrzwecke als unverzichtbar erweisen, so sind zumindest an die Qualität der Gefahr höhere Anforderungen zu stellen. Das alleinige Abstellen auf erhebliche Gefahren – wie es im ME-VE vorgesehen ist – reicht nicht aus. „Erheblich" sind nach allgemeiner

Ansicht alle Gefahren für ein bedeutsames Rechtsgut, d.h. nach der Legaldefinition des NdsSOG „für den Bestand des Staates, Leben, Gesundheit, Freiheit, nicht unwesentliche Vermögenswerte sowie andere strafrechtlich geschützte Güter". Daß schon bei einer Gefahr z.B. für nicht unwesentliche Vermögenswerte verdeckte technische Mittel eingesetzt werden dürfen, halte ich für unverhältnismäßig. Der Einsatz heimlicher Datenerhebung muß daher – wenn er im Rahmen der Gefahrenabwehr überhaupt in Betracht kommt – auf die Abwehr von gegenwärtigen Gefahren für Leib und Leben beschränkt werden und darf sich nur gegen polizeilich verantwortliche Personen – also Störer und Notstandspflichtige – richten. Die Inanspruchnahme anderer Personen verstieße gegen das Übermaßverbot.

Ein Einsatz heimlicher Datenerhebungsmaßnahmen zu Zwecken der vorbeugenden Verbrechensbekämpfung muß ebenfalls eng begrenzt werden. Er kommt nur bei besonders schwerwiegenden und anderweitig schwer aufklärbaren Delikten in Betracht. Die Regelungen des ME-VE gehen hier viel zu weit.

§ 8 ME-VE sieht zwar eine Begrenzung auf katalogmäßig genannte Straftaten vor, dieser Katalog umfaßt jedoch mehr als zwei Drittel der Verbrechen und Vergehen des Strafgesetzbuches: Danach dürfen die besonderen Formen der Datenerhebung eingesetzt werden für

- alle Delikte, bei denen eine Telefonüberwachung gem. § 100a StPO zulässig ist (insgesamt ca. 70 Delikte),

ferner für

- eine Reihe von Sexualdelikten (§§ 176-181a StGB),
- besonders schwere Diebstahlsfälle (§§ 243, 244 StGB),
- gewerbsmäßige Hehlerei (§ 260 StGB),
- Betrug und Untreue (§§ 263, 264, 265, 266 StGB),
- alle Umweltdelikte (§§ 324-330 StGB),

sowie für

- alle Straftaten, die gewerbsmäßig, gewohnheitsmäßig oder von Banden begangen werden.

In diesem Umfang geht ein Einsatz heimlicher Mittel zur Informationserhebung entschieden zu weit und ich bezweifele, daß selbst aus polizeilicher Sicht derart umfassende Eingriffsbefugnisse gewollt sind.

Nach meinen Erfahrungen kommt der Einsatz dieser Mittel im Rahmen der vorbeugenden Bekämpfung von Straftaten nur in Kriminalitätsbereichen in Betracht, die mit anderen weniger intensiven Informationseingriffen nicht mehr aufklärbar und beherrschbar sind. Dabei handelt es sich

- um den Bereich der organisierten Gewaltkriminalität (Terrorismus, Katalog des § 129a StGB),
- um die Rauschgiftkriminalität sowie
- um näher zu definierende Erscheinungsformen der modernen organisierten Kriminalität.

Dies sind Bereiche, die sich dadurch auszeichnen, daß die Polizei kaum Informationen von Hinweisgebern und Zeugen erhält, auf die sie üblicherweise bei ihrer Aufgabenerfüllung zurückgreifen kann. In diesen Bereichen ist sie also darauf angewiesen, sich selbst Informationen zu verschaffen, um überhaupt Straftaten aufklären zu können, und diese erhält sie nicht, wenn sie offen danach fragt. Es ist aber zwingend erforderlich, daß die heimlichen Eingriffe auf diese drei Bereiche beschränkt werden, und es ist nicht vertretbar, diese Beschränkungen im Hinblick auf zukünftige, heute noch nicht absehbare Entwicklungen der Kriminalität zu verwässern.

4.9.2.3.4 Materielle Voraussetzungen

Allein die Tatsache, daß die Polizei aufgrund von tatsächlichen Anhaltspunkten heimliche Erhebungsmaßnahmen zur vorbeugenden Bekämpfung einer Straftat aus den vorstehend genannten Kriminalitätsbereichen für erforderlich hält, vermag diese noch nicht zu rechtfertigen. Es muß vielmehr feststehen, daß eine Informationsbeschaffung mit herkömmlichen (offenen) Mitteln die Erfüllung der polizeilichen Aufgabe erheblich erschweren, wenn nicht gar vereiteln würde.

Darüber hinaus ist es notwendig, den in Betracht kommenden Personenkreis genauer einzugrenzen. Die Bezugnahme auf Störer bzw. Tatverdächtige paßt jedenfalls bei der vorbeugenden Verbrechensbekämpfung nicht. In Betracht kommt hier eine Eingrenzung auf Personen, bei denen Anhaltspunkte bestehen, daß sie (erneut) Straftaten des Kataloges begehen werden (Vorverdächtige).

4.9.2.3.5 Anordnungskompetenz

Weiter ist es erforderlich, den Einsatz der heimlichen Formen der Datenerhebung auch durch besondere Verfahren abzusichern.

Nach dem ME-VE ist als einzige Sicherung vorgesehen, daß der „Behördenleiter/Leiter der Dienststelle oder von ihm besonders bestimmte Beamte" über die Anordnung der Maßnahme entscheiden. Selbst diese Beschränkung entfällt bei Gefahr im Verzuge. Dies hat zur Folge, daß faktisch jeder Polizeibeamte, wenn er eine Gefahr im Verzuge annimmt, über den Einsatz nachrichtendienstlicher Mittel und den Einsatz verdeckter Ermittler entscheiden kann. Dies darf nicht sein, und ich kann mir auch nicht vorstellen, daß dies von der Polizei gewollt ist.

Es ist daher dringend notwendig, zusätzliche verfahrensrechtliche Sicherungen vorzunehmen. Dabei kann allerdings nach Maßnahmen unterschiedlicher Eingriffsintensität differenziert werden. Über Maßnahmen der Observation oder des Einsatzes von V-Leuten kann m.E. ein Polizeibeamter des höheren Dienstes (Inspektionsleiter) entscheiden, die Entscheidung über den Einsatz verdeckter Ermittler muß hingegen einer politisch verantwortlichen Ebene vorbehalten werden. Der Lauschangriff (s. 4.9.2.5) bedarf eines Richtervorbehalts wie Maßnahmen zur Überwachung des Fernmeldeverkehrs bei der Strafverfolgung gem. § 100 a StPO.

4.9.2.3.6 Zusätzliche verfahrensrechtliche Sicherungen

Neben der gestuften Anordnungskompetenz bzw. neben dem Richtervorbehalt sind zusätzliche verfahrensrechtliche Sicherungen vorzusehen. Insbesondere ist festzuschreiben, daß die Betroffenen über die durchgeführten Maßnahmen und die dabei gespeicherten Daten – sobald der Zweck der Maßnahme dies zuläßt – benachrichtigt werden. Eine derartige Unterrichtung ist unverzichtbar, um dem Betroffenen zumindest die Möglichkeit einer nachgehenden gerichtlichen Überprüfung des Informationseingriffs zu geben. Eine besondere Mitteilung mag entbehrlich sein, wenn sich ein Strafverfahren an die Maßnahme anschließt, jedenfalls in diesem Verfahren muß die Unterrichtung jedoch nachgeholt werden.

4.9.2.4 Datenerhebungen in Versammlungen

Sorgfältiger Eingrenzungen bedarf auch die Datenerhebung in Versammlungen (vgl. dazu schon 3. TB, 3.8.5.3, S. 79). Auch hier lassen die bisherigen Regelungsvorschläge zu wünschen übrig.

Der ME-VE räumt der Polizei Erhebungsbefugnisse in Versammlungen schon dann ein, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß Gefahren für die öffentliche Sicherheit und Ordnung entstehen. Diese weitgehende Befugnis, die nicht einmal das Vorhandensein einer konkreten Gefahr voraussetzt, ist mit dem Schutz der Versammlungsfreiheit nach Art. 8 GG nicht zu vereinbaren.

Das BVerfG hat im Volkszählungsurteil betont, daß ein Bürger grundsätzlich unbeobachtet von staatlichen Stellen an Versammlungen muß teilnehmen können. Es hat ausgeführt:

„Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf die Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Diesen Standpunkt hat das BVerfG in seinem, am 14.5.1985 ergangenen „Brokdorf-Beschluß" – (NJW 1985, 2395) nochmals unterstrichen. Es hat das besondere Gewicht des Art. 8 GG erläutert und ausgeführt, daß die Versammlungsfreiheit nur zum Schutz gleichgewichtiger anderer Rechtsgüter unter strikter Wahrung des Grundsatzes der Verhältnismäßigkeit begrenzt werden darf. Das BVerfG hat ausdrücklich betont, daß es mit diesen Grundsätzen nicht vereinbar ist, den staatsfreien, unreglementierten Charakter einer Versammlung durch exzessive Oberservationen und Registrierungen zu verändern.

Aus diesen Grundsätzen folgt, daß Maßnahmen der polizeilichen Informationserhebung in Versammlungen i.S.d.Art. 8 GG nur in sehr engen Grenzen zulässig sind. Zur Gefahrenabwehr (und zur Strafverfolgung) kommen Informationseingriffe nur in Betracht, wenn bestimmte Tatsachen die Annahme rechtfertigen, daß gegenwärtige erhebliche Gefahren für die öffentliche Sicherheit bestehen (bzw. bestimmte Straftaten begangen werden). Daten von Nicht-Störern dürfen dabei nur erhoben werden, soweit dies unvermeidlich ist (wenn sie also von Störerdaten nicht getrennt werden können).

Technische Mittel wie Bild- und Tonaufnahmegeräte darf die Polizei ebenfalls nur einsetzen, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr erforderlich ist. Tritt ein schädigendes Ereignis nicht ein, so sind die technischen Aufnahmen und anderweitige Unterlagen unverzüglich zu vernichten, soweit sie zur Identifizierung von Personen geeignet sind.

Bildaufzeichnungen, die die Polizei nicht zum Zweck personenbezogener Auswertung angefertigt hat (z.B. zur Verkehrsleitung oder Gebäudeüberwachung) dürfen nur dann personenbezogen verwertet werden, wenn dies zur Abwehr einer gegenwärtigen erheblichen Gefahr oder zur vorbeugenden Bekämpfung einer Straftat der in § 138 StGB genannten Art erforderlich ist.

4.9.2.5 Datenerhebung aus Wohnungen

Für die Datenerhebung aus Wohnungen, die dem besonderen Schutz des Art. 13 GG unterliegen, sieht der ME-VE eine Reihe von Beschränkungen vor, allerdings nur für den Einsatz technischer Mittel (also die Anfertigung von Bildaufnahmen sowie das Abhören und Aufnehmen des gesprochenen Wortes auf Tonträger). Dieser soll nur zulässig sein, wenn die erhebliche Gefahr „gegenwärtig" ist und wenn – außer bei Gefahr im Verzuge – der zuständige Amtsrichter die Maßnahme angeordnet hat.

Diese Regelung wird dem grundrechtlich verbürgten Schutz der Wohnung nicht gerecht:

Zunächst einmal fehlen zusätzlich einschränkende Bedingungen völlig für den Einsatz von verdeckten Ermittlern in Wohnungen. Dieser soll offenbar ohne zusätzliche Einschränkungen möglich sein.

Dies ist von der Regelung des Gesetzesvorbehalts in Art. 13 Abs. 3 GG nicht gedeckt. Hiernach dürfen Eingriffe und Beschränkungen nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, aufgrund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung vorgenommen werden. Der Ausdruck „dringende Gefahr" verbindet Elemente der Gefahrenlage und des gefährdeten Schutzgutes in einem qualitativen Sinne. Die zu verhütende Gefahr muß also einerseits mit großer Wahrscheinlichkeit eintreten und

andererseits ein bedeutendes Gemeinwohlgut betreffen. Nur unter diesen engeren Voraussetzungen dürfen noch Datenerhebungen durch verdeckte Ermittler in Wohnungen zugelassen werden, nicht aber zur Abwehr jeder – noch nicht gegenwärtigen – erheblichen Gefahr und nicht zur vorbeugenden Bekämpfung der in § 100a StPO genannten Straftaten und vieler anderer mehr.

Auch die vorgesehene Regelung zum Einsatz technischer Mittel bei der Datenerhebung in Wohnungen kann nicht befriedigen. Sie ist zwar wie die Durchsuchung unter den Vorbehalt einer richterlichen Anordnung gestellt. Dies gilt jedoch nicht bei Gefahr im Verzug. Gefahr im Verzug liegt immer dann vor, wenn mit der Anrufung des Richters der Zweck der beabsichtigten Maßnahme gefährdet ist. Ein Verzicht auf richterliche Entscheidung stellt nach dem Gesetz zwar die Ausnahme dar; Erfahrungen mit polizeilichen Durchsuchungen belegen aber, daß die Praxis das Regel-Ausnahme-Verhältnis umkehrt, sehr häufig also eine gerichtliche Entscheidung unterbleibt.

Diese Entwicklung ist auch beim Einsatz technischer Mittel nicht ausgeschlossen, so daß grundsätzliche Wertentscheidungen der Verfassung geradezu auf den Kopf gestellt wären. Während jede Art von Überwachung des Brief- und Fernmeldeverkehrs ausnahmslos einer Anordnung oder Bestätigung durch den Richter (oder aber – bei den Geheimdiensten – durch die G-10 Kommission) bedarf, gibt es für den mindestens ebenso weitgehenden Eingriff in die private Kommunikation, die aus einer Wohnung nicht herausdringt, keine solchen Verfahrenssicherungen. Sie können vielmehr in das polizeitaktische Ermessen gestellt werden. Dies ist nach meiner Auffassung nicht hinnehmbar.

4.9.2.6 Polizeiliche Beobachtung

Die polizeiliche Beobachtung (PB) ergänzt die vorstehend beschriebenen Maßnahmen der heimlichen Datenerhebung. Sie erfolgt ebenfalls heimlich, hat allerdings im Gegensatz zu diesen Maßnahmen keinen aktiven, sondern einen reaktiven Charakter; die Polizei geht nicht gezielt auf die Betroffenen zu, um sich Informationen zu verschaffen, sondern registriert lediglich das Auftreten der Personen an bestimmten Orten anläßlich von Maßnahmen zur Identitätsfeststellung. Anhalte- und Kontrollbefugnisse können auf die Befugnis zur polizeilichen Beobachtung nicht gestützt werden.

Aus diesem reaktiven Charakter folgt, daß eine polizeiliche Beobachtung zur Abwehr konkreter Gefahren nicht geeignet ist. Auf diesen Erhebungszweck ist daher zu verzichten. Für den Erhebungszweck „vorbeugende Verbrechensbekämpfung" gilt wie bei den sonstigen heimlichen Erhebungsmaßnahmen, daß die in Betracht kommenden Straftatbestände weiter einzuschränken sind. Auf die obigen Ausführungen wird verwiesen.

Die Erhebung von Daten etwaiger Begleitpersonen kommt nur in Betracht, soweit diese zur Verhütung und Aufklärung weiterer Straftaten des – zu formulierenden – Katalogs unerläßlich ist. Dies ist klarzustellen.

Weiterhin wird der Gesetzgeber organisatorische und verfahrensrechtliche Vorkehrungen treffen müssen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken, nämlich:

- Die polizeiliche Beobachtung muß von einem Beamten des höheren Dienstes schriftlich angeordnet werden.
- Die Anordnung muß den Betroffenen bezeichnen, gegen den sie sich richtet, sowie Art, Umfang und Dauer der Maßnahme bestimmen.
- Die Anordnung ist auf maximal ein Jahr zu befristen.
- Nach Ablauf von jeweils drei Monaten ist zu prüfen, ob die Voraussetzungen für den Erlaß der Anordnung fortbestehen.
- Die Gründe für die erstmalige Anordnung und für die Weiterführung sind jeweils aktenkundig zu machen.
- Über eine polizeiliche Beobachtung von mehr als einem Jahr Dauer entscheidet der Richter.

- Liegen die Voraussetzungen für den Erlaß der Anordnungen nicht mehr vor oder ist der Zweck der Maßnahme erreicht, ist die polizeiliche Beobachtung unverzüglich einzustellen.
- Unterlagen, die im Zusammenhang mit der Beobachtung angefallen sind und zur Erfüllung polizeilicher Aufgaben nicht mehr benötigt werden, sind unverzüglich zu vernichten.
- Unerläßlich ist schließlich auch bei der PB eine Pflicht zur nachträglichen Unterrichtung der Betroffenen.

4.9.2.7 Weitergabe von Daten durch die Polizei

Um die Einhaltung des Zweckbindungsgebotes zu sichern, ist auch die Weitergabe von Daten differenziert zu regeln. Zum einen bedarf es für jeden Erhebungszweck („Gefahrenabwehr", „Gefahrenvorsorge", „vorbeugende Verbrechensbekämpfung") spezieller Weitergaberegelungen. Desweiteren ist nach unterschiedlichen Empfängergruppen zu differenzieren. Zu denken ist hierbei zunächst an andere Polizeidienststellen. Hier kann aufgrund der gleichen Aufgabenstellungen grundsätzlich an die Erforderlichkeit zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben angeknüpft werden, soweit es nicht besondere Weitergabeverbote gibt.

Desweiteren sind spezielle Regelungen für die Weitergabe an den Verfassungsschutz (vgl. dazu 4.10.6.3) sowie an andere öffentliche Stellen erforderlich. Für den letztgenannten Empfängerkreis sieht der ME-VE Generalklauseln vor, die noch sehr viel stärker konkretisiert werden müssen.

In der vorliegenden Form sind sie mit den Grundsätzen des Volkszählungsurteils nicht vereinbar, da dem Prinzip der Zweckbindung nicht hinreichend Rechnung getragen worden ist. Es muß gesetzlich klargestellt werden, daß Übermittlungen an andere öffentliche Stellen als Polizeibehörden, soweit in Spezialgesetzen nichts anderes bestimmt ist, nur in Betracht kommen, soweit dies im Einzelfall erforderlich ist

- zur Abwendung einer konkreten Gefahr,
- zur Abwendung einer erheblichen sozialen Notlage oder
- zur Verfolgung von öffentlich-rechtlichen und zivilrechtlichen Ansprüchen.

Der Bedarf nach einer Übermittlung zu anderen Zwecken ist bislang nicht dargelegt worden. Nicht akzeptabel ist es – wie im ME-VE auch vorgesehen –, eine Übermittlung schon unter der Voraussetzung zuzulassen, daß sie mit dem Erhebungs- und Speicherungszweck vereinbar ist.

Für den Bereich der Polizei sollte überdies ein Weitergabeverbot für personenbezogene Daten, die zur vorbeugenden Bekämpfung von Straftaten erhoben wurden, festgelegt werden. Solche Daten dürfen nur an andere Polizeibehörden weitergegeben werden. Daten, die zur vorbeugenden Straftatenbekämpfung erhoben und gespeichert werden, sind besonders sensibel. Bei einer Nutzung außerhalb der Polizei besteht in besonderem Maße die Gefahr, daß die Resozialisierung verurteilter Straftäter beeinträchtigt wird bzw. daß polizeibekannten Personen ungerechtfertigte Nachteile entstehen, obwohl sie mangels Verurteilung durch die rechtsstaatliche Unschuldsvermutung geschützt werden sollen.

Schließlich ist auch das Verfahren bei den Datenübermittlungen zu regeln. Erhebliche Bedenken bestehen gegen den im ME-VE vorgesehenen Wegfall der Prüfung der Voraussetzungen der Datenübermittlung durch die übermittelnde Stelle. Es ist nicht sachdienlich, die Verantwortlichkeit für die Übermittlung im Bereich der Polizei abweichend von Datenschutz-und Amtshilferecht zu regeln.

Ferner fehlen bislang Bestimmungen zur Übermittlung bestrittener Tatsachen und Bewertungen, ein Verbot der Übermittlung zu löschender Daten sowie Protokollierungspflichten.

Nach Auffassung der Datenschutzbeauftragten müssen schließlich folgende Regelungen getroffen werden:

- Die übermittelnde Stelle muß vorab prüfen, ob die Informationen zu löschen sind. Bei Fremderkenntnissen hat sie grundsätzlich Rückfrage bei den datenanliefernden Stellen zu halten. Ergibt die Überprüfung, daß die Informationen zu löschen sind, so dürfen sie nicht übermittelt werden, soweit dies nicht im Interesse des Betroffenen liegt.
- Die anfragenden Stellen haben der übermittelnden Stelle den Zweck, für den die Informationen benötigt werden, und die übrigen für die Prüfung der Zulässigkeit der Übermittlung erforderlichen Angaben mitzuteilen. Die empfangenen Stellen dürfen die übermittelten Informationen nur zu dem angegebenen Zweck, im übrigen nur mit Zustimmung der übermittelnden Stelle verwenden.
- Bestrittene Tatsachen und Bewertungen dürfen grundsätzlich nur mit entsprechender Kennzeichnung und unter Hinzufügung der Beweismittel und Beurteilungsgrundlagen übermittelt werden.
- Tatsache und Inhalt der Übermittlung sind in der Akte festzuhalten. Bei Veränderungen wesentlicher Gesichtspunkte, insbesondere späterer Löschung der Erkenntnisse, hat die auskunftgebende Stelle die Änderung nachzuberichten.

4.9.2.8 Datenabgleich

Wie schon im 3. TB (3.8.5.6) dargestellt, bedarf auch der Datenabgleich als sonstige Verwendung personenbezogener Daten einengender gesetzlicher Regelungen: Ein Abgleich neu erhobener Daten mit bereits vorhandenen Datenbeständen darf nur zugelassen werden, wenn er sowohl vom Zweck der Erhebung als auch vom Zweck der Speicherung erfaßt wird. Demgegenüber geht die Polizei davon aus, daß ein Abgleich fast beliebig zulässig ist.

So soll die Polizei nach dem ME-VE personenbezogene Daten von Handlungsstörern und Zustandsstörern ohne jegliche Beschränkung mit dem Inhalt polizeilicher Dateien abgleichen dürfen. Dies ist zu weitgehend. Störer dürfen nur insoweit in Anspruch genommen werden, als dies zur Abwehr der Gefahr, die sie verursacht haben, erforderlich ist. Nur in diesem Rahmen ist auch ein Datenabgleich zulässig.

Ferner soll die Polizei Daten anderer Personen mit ihren Dateien abgleichen dürfen, wenn dies aufgrund tatsächlicher Anhaltspunkte zur Erfüllung polizeilicher Aufgaben erforderlich erscheint. Auch dies geht zu weit. Es muß klargestellt werden, daß dieser Datenabgleich auf die Fälle beschränkt ist, in denen Notstandspflichtige und andere Personen polizeilich auf gesetzlicher Grundlage in Anspruch genommen werden dürfen.

Schließlich soll die Polizei alle sonstigen im Rahmen ihrer Aufgabenerfüllung erlangten Daten mit ihrem Fahndungsbestand abgleichen können. Diese Vorschrift, die offenbar den Beschluß der IMK vom September 1977 über die fahndungsmäßige Überprüfung im Zusammenhang mit der Terrorismusfahndung (vgl. 3. TB, 3.8.1.2) absichern soll, ist zu streichen. Nach geltendem Recht ist ein Abgleich personenbezogener Daten mit dem Fahndungsbestand nur dann zulässig, wenn die Voraussetzungen für eine Personenkontrolle gegenüber dieser Person nach dem jeweiligen Polizeigesetz bzw. spezialgesetzlichen Regelungen vorliegen. Eine Erweiterung dieser Befugnisse mit der Folge, daß beliebige Personen – ohne konkreten Anlaß – mit den Fahndungsdateien abgeglichen werden dürfen, halte ich für unverhältnismäßig.

Völlig offen geblieben – im ME-VE nicht geregelt – ist bislang die Frage, ob und unter welchen Voraussetzungen die Polizei – über Einzelfallanfragen hinaus – ihren Fahndungsbestand mit öffentlichen Registern – wie etwa dem Melde- und dem Kraftfahrzeugregister – abgleichen darf. Auch diese Frage muß im Polizeirecht geregelt werden, allerdings wesentlich restriktiver als es der heutigen Praxis entspricht.

4.9.2.9 Rasterfahndung

Schließlich bleibt das Problem der sog. Rasterfahndung, das ich ebenfalls im 3. TB (a.a.O.) ausführlich behandelt habe. Im Gegensatz zu den o.g. Formen des Datenab-

gleichs, die darauf abzielen, namentlich bekannte gesuchte Personen festzustellen, geht es bei der Rasterfahndung darum, namentlich unbekannte Störer (oder Straftäter) anhand unterschiedlicher Merkmale zu identifizieren.

Nach dem jetzigen Stand meiner Erkenntnisse besteht für Befugnisse zur Rasterfahndung im präventiven Bereich kein Bedarf. Mir ist kein Fall bekanntgeworden, in dem die Polizei Maßnahmen der Rasterfahndung lediglich zur Gefahrenabwehr für erforderlich gehalten hätte. Solche Maßnahmen zielen vielmehr typischerweise auf unbekannte Straftäter. Ich habe zwar bisher den Standpunkt vertreten, daß – nach dem Vorbild des novellierten bremPolG – auch für den präventiven Aufgabenbereich vorsorglich eine einengende Befugnisregelung geschaffen werden sollte. Zwischenzeitlich hat sich die Diskussion aber insofern weiter entwickelt, als ein anzuerkennender Bedarf der Polizei ausgeschlossen werden kann. Eine Befugnis zur Rasterfahndung zu Zwecken der Gefahrenabwehr sollte der Polizei daher nicht eingeräumt werden.

4.9.3 Kritik am SOG-Entwurf

Der SOG-Entwurf (SOG-E), den die Behörde für Inneres Ende November in die Behördenabstimmung geben wollte, ist bis zum Redaktionsschluß dieses TB noch nicht bei mir eingegangen. An dieser Stelle werde ich auf der Grundlage der mir bekannten Vorentwürfe einige kritische Punkte ansprechen, die in der kommenden –nunmehr hoffentlich öffentlichen– Diskussion ein besonderes Gewicht erhalten werden. Im übrigen verweise ich auf meine Position, wie ich sie in den letzten Tätigkeitsberichten sowie oben (4.9.2) in Auseinandersetzung mit dem ME-VE der IMK entwickelt habe. Hieran werde ich auch den SOG-E messen.

4.9.3.1 Allgemeine Einschätzung

Einen positiven Eindruck vermittelt der SOG-E –etwa im Vergleich mit dem ME-VE, aber auch zum Novellierungsentwurf für das Hess SOG– insoweit, als er Voraussetzungen und Umfang polizeilicher Informationseingriffe außerordentlich differenziert regelt. Es wurden sichtbare Anstrengungen unternommen, um den Ansprüchen des Bundesverfassungsgerichts nach normenklaren Regelungen gerecht zu werden. Wieweit das in jeder einzelnen Vorschrift auch gelungen ist, wird allerdings noch zu prüfen sein.

Weit weniger gelungen ist es der Behörde für Inneres, auch der zweiten zentralen Forderung des BVerfG im VZ-Urteil zu entsprechen: also dem Grundsatz der Verhältnismäßigkeit, nach dem Informationseingriffe auf das Maß zu beschränken sind, das im überwiegenden Allgemeininteresse erforderlich ist. In zentralen Punkten unterscheidet sich der SOG-E –wie ich zeigen werde– nicht nennenswert vom ME-VE. Einschränkungen der derzeitigen Informationspraxis durch strengere gesetzliche Vorgaben werden nicht für notwendig gehalten, da die Hamburger Polizei angeblich seit jeher besonders liberal und restriktiv verfahre.

Richtig ist zwar, daß die Hamburger Polizei an einer Reihe von Aktivitäten im Rahmen des INPOL nicht teilgenommen hat (z.B. Meldedienst Landfriedensbruch, SPUDOK „Heißer Herbst"). Zu erinnern ist aber auch daran, daß sie bei anderen INPOL-Verbund-Anwendungen datenschutzrechtliche Bedenken weitgehend ignoriert hat: z.B. beim KAN (vgl. 3.TB, 3.8.1.3, S.68), bei der Haftdatei (3.TB, 3.8.1.4, S.69 f), bei APIS (4.9.5), bei der Speicherung personengebundener Hinweise (4.9.4).

Richtig ist ferner, daß die Polizei den POLAS-Datenbestand –nach Inkrafttreten des HmbDSG–stark reduziert hat und eine Reihe von Übermittlungen an andere Behörden –auch um sich selbst zu entlasten– eingestellt hat. Nach wie vor werden jedoch in erheblichem Umfang Daten über nicht-polizeipflichtige Personen im POLAS gespeichert (z.B. Suizidenten) und routinemäßig Daten an andere Stellen übermittelt (z.B. Verfassungsschutz, Ausländerbehörden, Jugendämter), obwohl keine konkreten Anhaltspunkte dafür vorliegen, daß die jeweilige Information für die Aufgabenerfüllung der Empfängerbehörde erforderlich sein kann.

Ich sehe daher keine Veranlassung für die Bfl, sich für ihre Liberalität auf die Schulter zu klopfen. Auch bei der Hamburger Polizei gibt es nach wie vor genügend Gründe für eine selbstkritische Überprüfung ihrer Praxis.

4.9.3.2 Wichtige Kritikpunkte

Ein zentrales Problem, das sich durch den gesamten SOG-E zieht, besteht in folgendem:

Die Bfl nennt polizeiliche Aufgabenstellungen, die jedermann einleuchten, und trägt viele Informationsbedürfnisse vor, die erforderlich erscheinen, gleichzeitig aber formuliert sie die vorgehenden Befugnisse so, daß sie auch alle möglichen anderen Informationseingriffe abdecken. Ich will dies an Beispielen verdeutlichen.

4.9.3.2.1 Gefahrenvorsorge

Der SOG-E führt als neue Aufgabe die sog. „Gefahrenvorsorge" ein und begründet zu diesem Zweck Befugnisse zur Erhebung und Speicherung von

- erheblich gefährdeten Personen,
- Verantwortlichen für erheblich gefährdete Anlagen und Einrichtungen,
- Verantwortlichen für Anlagen und Einrichtungen, von denen eine erhebliche Gefahr ausgehen kann und
- Personen, deren Fachkenntnisse zur Gefahrenabwehr benötigt werden.

Nun wird zwar niemand bestreiten wollen, daß die Polizei sich auf eine effektive Bekämpfung künftiger Gefahren vorbereiten und einstellen muß; außerordentlich zweifelhaft ist, ob diese Aufgabe schon Eingriffe in das informationelle Selbstbestimmungsrecht nicht polizeipflichtiger Bürger rechtfertigt. Es ist bisher für mich nicht nachvollziehbar, warum die Polizei erforderliche Gefahrenvorsorgemaßnahmen nicht mit dem Einverständnis der betroffenen Bürger organisieren kann. Insbesondere eine Befugnis zur Speicherung erheblich gefährdeter Personen (welche sind das?) ohne deren Kenntnis und Einwilligung geht erheblich zu weit.

4.9.3.2.2 Vorbeugende Bekämpfung von Straftaten

Als weitere neue Aufgabe führt der SOG-E -wie der ME-VE- die „vorbeugende Bekämpfung von Straftaten" ein und begründet u.a. allgemeine Befugnisse zur Erhebung und Speicherung von

- Personen, bei denen Anhaltspunkte bestehen, daß sie Straftaten begehen werden,
- Kontakt- oder Begleitpersonen einer der o.g. Personen,
- erheblich gefährdeten Personen sowie
- Zeugen, Hinweisgebern und sonstigen Auskunftspersonen.

Diese Maßnahmen sollen lediglich dadurch begrenzt werden, daß sie aufgrund tatsächlicher Anhaltspunkte erfahrungsgemäß zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich sind.

Enger als der ME-VE sieht der SOG-E vorbeugende Informationseingriffe zwar nur bei Straftaten mit erheblicher Bedeutung vor; diese Formulierung ist jedoch immer noch zu unbestimmt, um die Informationstätigkeit der Polizei in dem Maß einzugrenzen, wie es der Grundsatz der Verhältnismäßigkeit erfordert. Eine polizeiliche Ermittlungstätigkeit (Erheben und Speichern von Daten), die sich gezielt gegen Personen richtet, bei denen weder ein konkreter Tatverdacht vorliegt noch die konkrete Gefahr besteht, daß sie Straftaten begehen, ist allenfalls in präzise zu benennenden Kriminalitätsbereichen zu rechtfertigen, die durch andere Maßnahmen nicht mehr beherrschbar sind. Es kann dabei an den Straftatenkatalog des § 100 a StPO angeknüpft werden, der allerdings auch Straftaten von geringerer Bedeutung umfaßt. Eine großzügigere Regelung kommt nur für Personen in Betracht, die Beschuldigte in früheren Ermittlungsverfahren waren. Wenn bei diesen nach Art und Ausführung der Tat sowie nach der Persön-

lichkeit des Täters die Gefahr der Begehung weiterer erheblicher Straftaten besteht, erscheint eine weitere Verwendung der Unterlagen aus den Ermittlungsverfahren (in Kriminalakten, Sammlungen, erkennungsdienstlichen Unterlagen, deliktsspezifischen Täterkarteien) zur vorbeugenden Bekämpfung von Straftaten unbedenklich.

4.9.3.2.3 Datenerhebung in Versammlungen

Der SOG-E enthält für die Datenerhebung bei öffentlichen Veranstaltungen, Ansammlungen und Versammlungen zwar etwas präzisere Regelungen als der ME-VE, dem gem. Art. 8 GG gebotenen besonderen Schutz der Versammlungsfreiheit (vgl. 3.9.1.5) wird er jedoch ebenfalls nicht gerecht:

- Zwischen Versammlungen i.S.d. Art. 8 und sonstigen Ansammlungen (z.B. Besucher des Volksparkstadions) wird kein Unterschied gemacht.
- Da ein Bürger grundsätzlich verlangen kann, daß er bei der Ausübung seines Grundrechts nicht registriert wird, dürfen nicht zum bloßen Zweck der Gefahrenermittlung („Erfassung der Geschehensabläufe und Beurteilung der Gefahrenlage") Bild-und Tonaufnahmegeräte eingesetzt werden.
- Der Einsatz solcher Instrumente kann vielmehr nur zu Zwecken der Beweiserleichterung in Betracht kommen, wenn Anhaltspunkte dafür vorliegen, daß die Begehung einer Straftat unmittelbar bevorsteht. Wenn bzw. insoweit keine Straftaten begangen werden, sind die Unterlagen umgehend zu vernichten.
- Eine Ermächtigung zum Einsatz von Bild- und Tonaufnahmegeräten bei Versammlungen zum Zweck der vorbeugenden Bekämpfung von Straftaten –wie es der SOG-E, insoweit sogar über den ME-VE hinausgehend, vorsieht– ist mit Art. 8 GG nicht vereinbar.

4.9.3.2.4 Verdeckte Datenerhebungen

Die Regelungen des SOG-E über die sog. besonderen Formen der Datenerhebung unterscheiden sich nur unwesentlich von denen des ME-VE. Ich verweise daher auf meine oben ausgeführte grundsätzliche Kritik (4.9.2.4) und unterstreiche noch einmal:

- Die zum Einsatz kommenden heimlichen Erhebungsmethoden dürfen nicht über einen Kamm geschoren werden, sondern müssen entsprechend ihrer unterschiedlichen Eingriffsintensität wesentlich differenzierter geregelt werden;
- insbesondere Datenerhebungen durch verdeckte Ermittler dürfen nur dann zugelassen werden, wenn der Gesetzgeber klar entschieden hat, was diese Beamte dürfen bzw. welche Vorschriften des StGB und der StPO für sie ggf. nicht gelten;
- der Einsatz optischer und akustischer Hilfsmittel in Wohnungen, die bekanntlich dem besonderen Schutz des Art. 13 unterliegen, kann nur akzeptiert werden zur Abwehr einer Gefahr für Leib und Leben einer Person. Ein Richtervorbehalt ist unverzichtbar.

4.9.3.2.5 Datenabgleich

Die Regelungen des SOG-E zu Datenabgleich und Rasterfahndung entsprechen dem ME-VE. Ich verweise daher auf 4.9.2.8 und 4.9.2.9.

4.9.4 Speicherung von personenbezogenen Hinweisen insbesondere auf Freitodversuche

Schon seit Jahren habe ich von der Behörde für Inneres den Verzicht auf die Speicherung von Hinweisen auf Suizidversuche verlangt (vgl. 1. TB, 6.7.2.3; 2. TB, 3.10.5.2, S. 84 f.). 1985 hat die Polizei nun eine Erhebung durchgeführt, um den Sinn und Zweck der Hinweise besser belegen zu können. Auch dadurch konnten meine Bedenken nicht ausgeräumt werden.

Nach wie vor bin ich aus drei Gründen der Auffassung, daß die polizeiliche Generalklausel des § 3 SOG keine tragfähige Rechtsgrundlage für die Speicherung polizeilich bekannter freitodgefährdeter Personen bildet.

- Außerordentlich zweifelhaft ist zunächst, ob unmittelbar nach einem gescheiterten Selbstmordversuch (Zeitpunkt der Einspeicherung) die konkrete Gefahr besteht, daß der Betroffene einen erneuten Selbstmordversuch begehen wird. Konkret ist eine Gefahr bekanntlich dann, „wenn in dem zu beurteilenden Einzelfall irgendwann, freilich in überschaubarer Zukunft mit dem Schadenseintritt gerechnet werden muß." Die hinreichende Wahrscheinlichkeit eines erneuten Selbstmordversuches muß also im konkreten Einzelfall tatsächlich bestehen, und zwar in dem Zeitpunkt, in dem die polizeiliche Maßnahme (hier: Einspeicherung) vorgenommen wird.

  Nach der Behörde für Inneres beruht die Einschätzung der konkreten Gefahr eines erneuten Selbstmordversuches auf der wissenschaftlichen (statistischen) Erkenntnis, daß ein Selbsttötungsversuch keine einmalige Handlung ist, sondern in vielen Fällen wiederholt wird. Diese – von mir nicht bestrittenen– Erkenntnisse reichen jedoch nicht zur Annahme einer im Einzelfall bestehenden Gefahr aus. Allein aus dieser Erkenntnis läßt sich nicht mit hinreichender Sicherheit ableiten, daß eine bestimmte Einzelperson erneut einen Selbstmordversuch begehen wird. Wo es um den Schutz besonders hochwertiger Rechtsgüter - etwa des Lebens – geht, kann zwar auch schon die entfernte Möglichkeit eines Schadens eine begründete Befürchtung auslösen. Ich meine aber nicht, daß eine bloße aus statistischen Erkenntnissen abgeleitete Wahrscheinlichkeit bereits eine Gefahr im Einzelfall begründen kann.

- Weitere Zweifel an der Rechtmäßigkeit der Speicherung der suizidgefährdeten Personen ergeben sich daraus, daß die Speicherung als solche nicht geeignet ist, die Gefahr (den erneuten Selbstmordversuch) abzuwehren. Die Tatsache, daß ein Suizidgefährdeter im Polizeicomputer gespeichert ist, verhindert keinen erneuten Selbstmordversuch, sondern führt nach der Stellungnahme der Gesundheitsbehörde (vgl. meinen 2. TB S. 84) sogar eher dazu, daß die Suizidgefahr erhöht wird, da die therapeutisch gebotene Entlastung und Stabilisierung von Patienten nach Freitodversuchen gefährdet wird.

  Für wenig überzeugend halte ich das Argument, daß es auf die Gefahr therapeutischer Erschwernisse nicht ankommt, weil ein höherwertiges Rechtsgut, nämlich das Leben, geschützt werden muß. Die Bfl meint zu Unrecht, daß zwei Rechtsgüter unterschiedlichen Wertes, offenbar das Leben auf der einen und die Gesundheit auf der anderen Seite, gegeneinander abzuwägen seien. Es geht vielmehr darum, für ein und dasselbe Rechtsgut, nämlich Leben und Gesundheit des Patienten, zu prüfen, ob die Risiken, die sich aus medizinischer Sicht durch eine polizeiliche Speicherung ergeben, die Risiken überwiegen, die sich aus polizeilicher Sicht durch den Verzicht auf eine Speicherung ergeben. Nach den Erkenntnissen, die mir bislang zugänglich geworden sind, ist es aber wahrscheinlicher, daß eine polizeiliche Speicherung dem Betroffenen schadet als daß sie ihm nützt.

  Selbstmordversuche verhindern kann die Polizei nur dann, wenn ein Suizidgefährdeter in ihren Einflußbereich gelangt ist. Dies ist regelmäßig erst dann der Fall, wenn er sich (nach der Verhaftung) in polizeilichem Gewahrsam befindet. In diesen Fällen kann die Polizei aufgrund des Hinweises besondere zusätzliche Schutzmaßnahmen ergreifen. Es ist allerdings – entgegen den Behauptungen der Bfl – nicht so, daß besondere Schutzmaßnahmen nur zugunsten polizeilich gespeicherter Personen möglich sind; denn auch ohne spezielle Hinweise sind die für die Bewachung Verantwortlichen verpflichtet, alle erforderlichen Maßnahmen zu treffen, um eine Selbsttötung zu verhindern. Dazu können gehören häufige Zellenkontrollen oder sogar sorgfältige Beobachtung. Diese Pflichten bestehen unabhängig davon, ob POLAS einen Hinweis auf die Suizidgefahr enthält oder nicht.

  Im mittelbaren Einflußbereich der Polizei befinden sich ferner solche Personen, die vermißt gemeldet werden. In diesen Fällen kann die Polizei sich aufgrund des POLAS-Hinweises auf eine Suizidgefährdung veranlaßt fühlen, intensivere Such- und Ermittlungsmaßnahmen vorzunehmen als in sonstigen Vermißtenfällen. Diese

zusätzlichen Maßnahmen wiederum können u.U. dazu beitragen, einen Selbstmordversuch zu verhindern. Selbst wenn ich unterstelle, daß etwa die den Vermißtenfall anzeigenden Personen häufig keine Kenntnis von einer Suizidgefahr haben, ist die Eignung des POLAS-Hinweises dennoch stark begrenzt.

Nach den Ergebnissen der von der Polizei durchgeführten Erhebung lagen bei fast 2/3 der Fälle (98 von 165) neben dem POLAS-Hinweis weitere Hinweise auf die Suizidgefährdung vor. Bei den verbleibenden 67 Fällen sind zwar wegen des POLAS-Hinweises besondere Aufklärungs- oder Schutzmaßnahmen getroffen worden; niemand weiß jedoch, ob dadurch tatsächlich Selbstmorde verhindert worden sind bzw. was passiert wäre, wenn die Polizei keinen entsprechenden Hinweis gehabt hätte.

- Bei dieser Sachlage liegt die Vermutung nahe, daß die Speicherung gar nicht in erster Linie der Abwehr von Gefahren, sondern vornehmlich der Erleichterung polizeilicher Aufsicht dient: Für den Fall, daß ein Suizidgefährdeter in den Einflußbereich der Polizei kommt, wird das Ergreifen besonderer, gefahrenverringernder Maßnahmen gefördert.

  Es ist aber ein klassischer, allgemein anerkannter Rechtssatz, daß Polizeimaßnahmen nicht lediglich der Erleichterung polizeilicher Aufsicht dienen dürfen. Dieser Rechtssatz gilt auch dort, wo die Gesetze nicht ausdrücklich eine entsprechende Bestimmung enthalten. Genausowenig wie die Polizei Handlungen oder Konstellationen, aus denen sich nach ihrer Ansicht Gefahren entwickeln können (die aber z.Z. noch nicht bestehen), verbieten darf, weil sie die Vorgänge schlecht überwachen kann, darf sie alle in bestimmten Gefahrensituationen befindlichen Personen speichern, um geeignete Abwehrmaßnahmen zu veranlassen, wenn die Gefahr sich im Einflußbereich der Polizei realisieren sollte.

  Es ist zwar notwendig, daß die Polizei Anstrengungen unternimmt, um Selbstmorde zu verhindern, wenn es in ihren Möglichkeiten (s.o.) liegt, und es ist verständlich, daß die Polizei sich diese Aufgabe dadurch zu erleichtern versucht, daß sie alle besonders gefährdeten Personen speichert; dies Motiv rechtfertigt nach herkömmlichem Polizeirecht jedoch keine Informationseingriffe, die ansonsten nicht zur Gefahrenabwehr geeignet sind.

Bei Redaktionsschluß dieses Berichts war noch offen, ob der Senat meinen Bedenken Rechnung trägt und die Behörde für Inneres veranlaßt, die Hinweise auf freitodgefährdete Personen zu streichen, oder ob die Behörde für Inneres die Beibehaltung des derzeitigen Zustands durchsetzt.

Rein vorsorglich möchte ich hier jedoch folgendes klarstellen:

Die Speicherung der Hinweise auf Freitodversuche ist nicht nur generell rechtswidrig, weil die polizeiliche Generalklausel des § 3 Abs. 1 SOG keine ausreichende Rechtsgrundlage bietet; sie ist darüber hinaus auch materiell nicht mit dem Grundsatz der Verhältnismäßigkeit in Einklang zu bringen. Die von der Behörde für Inneres vorgebrachten Gründe reichen nicht aus, um ein überwiegendes Allgemeininteresse an der Speicherung zu rechtfertigen.

Einer mit der Novellierung des SOG auch beabsichtigten gesetzlichen Absicherung der Suizid-Speicherungen (vgl. § 12 a Abs. 6 des SOG-Entwurfs) stehen daher gravierende verfassungsrechtliche Bedenken entgegen.

4.9.5 Arbeitsdatei PIOS (APIS)

Ende 1984 hat die Behörde für Inneres mir die Errichtungsanordnung für die neue „Arbeitsdatei PIOS Innere Sicherheit" (APIS) zur Stellungnahme übersandt. Der Sinn dieser neuen Datei für die Polizei besteht zum einen in der Zusammenfassung bisher getrennt gehaltener Datenbestände im Staatsschutzbereich, zum anderen in der Einführung des Verfahrens „PIOS-neu", das der Polizei erheblich erweiterte Verknüpfungs- und Auswertungsmöglichkeiten liefern sollte (zu den PIOS-Dateien allgemein vgl. 3. TB, 3.8.2.1, S. 72).

Zu der Errichtungsanordnung habe ich im Mai 1985 eine Reihe von Bedenken formuliert, die sich – kurz zusammengefaßt – auf folgende Punkte bezogen:

- den Umfang des aufzunehmenden Sachverhaltes,
- die Einspeicherung von geschädigten und gefährdeten Personen,
- die Einspeicherung und Übermittlung von Daten sog. „anderer Personen",
- das Verhältnis von APIS zum kriminalpolizeilichen Meldedienst in Staatsschutzsachen sowie zu den Arbeitsdateien PIOS Landfriedensbruch (APLF) und PIOS Landesverrat (APLV),
- die Festlegung des Zeitpunktes der Einspeicherung,
- die Festlegung von Überprüfungspflichten,
- die Sicherstellung der Zweckbindung.

Bis zum Redaktionsschluß dieses Berichtes hat die Behörde für Inneres es nicht für erforderlich gehalten, zu meinen Bedenken inhaltlich Stellung zu nehmen. Sie teilte mir nur mit, daß der Arbeitskreis II der IMK schon im März eine ad-hoc-Arbeitsgruppe eingesetzt hatte, um die Errichtungsanordnung nochmals zu überprüfen. Im Anschluß an dessen Ergebnis wollte sie auf mein Schreiben zurückkommen. Auch auf meine Anfang November erfolgte Bitte um Sachstandsmitteilung kam jedoch keine Reaktion der Behörde für Inneres.

Dieser Fall ist leider nicht untypisch für die Art und Weise, wie die Behörde für Inneres mich über manche datenschutzrechtlichen Vorhaben unterrichtet. Wenn ich einmal von der nach den Hamburgischen Dateienrichtlinien vorgeschriebenen Beteiligung an Feststellungs- und Errichtungsanordnungen absehe, die regelmäßig gut funktioniert, werde ich über andere datenschutzrechtliche Vorhaben (z.B. die Neufassung von Richtlinien über kriminalpolizeiliche Meldedienste) häufig gar nicht oder erst dann unterrichtet, wenn ich von anderer Seite Kenntnis von dem Vorhaben erhalten und gezielt nachgefragt habe.

4.9.6 ZEVIS

Auch mit der Einführung des Zentralen Verkehrsinformationssystems (ZEVIS) beim Kraftfahrtbundesamt in Flensburg habe ich mich schon in meinen beiden letzten TBen (2. TB, 3.10.6.3; 3. TB, 3.9.2, S. 85 ff.) ausführlich auseinandergesetzt. Obwohl datenschutzrechtliche Bedenken unvermindert fortbestehen, hält die Bundesregierung in kaum verändertem Umfang an ZEVIS fest. Auch der neueste mir bekannte Entwurf zur Änderung des StVG läßt es zu, das Zentrale Kfz-Register mit Hilfe der sog. P-Anfrage auch zu Zwecken zu nutzen, die mit der Eigenschaft der betroffenen Person als Kfz-Halter nichts zu tun haben (vgl. 3. TB 3.9.2.1, S. 87).

Solche Zweckdurchbrechungen sollen etwa zulässig sein für die Polizei (zu Zwecken der Strafverfolgung, Strafvollstreckung und Gefahrenabwehr), für die Geheimdienste (zur Erfüllung ihrer Aufgaben) sowie für die Finanzverwaltung (zur Erfüllung gesetzlicher Mitteilungspflichten). Die Übermittlung von Halterdaten und Fahrzeugdaten muß nach dem StVG-Änderungs-Entwurf zwar „unerläßlich" sein und die gewünschten Daten dürfen auf andere Weise als aus dem zentralen Fahrzeugregister „nicht oder nicht rechtzeitig oder nur mit unverhältnismäßig hohem Aufwand zu erlangen" sein. Diese Einschränkungen bilden aber nur scheinbar eine Hürde: Da es – aus wohlerwogenen Gründen – kein Bundes- und keine Landesadreßregister gibt und die Polizei die kommunalen Melderegister zumeist noch nicht in direktem Zugriff abfragen kann, werden unbekannte Anschriften schnell und mit relativ geringem Aufwand nur aus dem Zentralen Fahrzeugregister zu erlangen sein. Diesem wird damit zwangsläufig die Funktion eines Ersatz-Bundesadreßregisters für den größten Teil der erwachsenen Bevölkerung zuwachsen.

Desweiteren soll der Polizei (und anderen Stellen) nach wie vor die Möglichkeit einer Halteranfrage im automatisierten Abrufverfahren eingeräumt werden, ohne daß vorher der Umfang ihrer Befugnisse zur Halterfeststellung einwandfrei und für jedermann

überschaubar geregelt ist (vgl. auch hierzu 3. TB, 3.8.2.1, S. 86 f.). Ich kann nur erneut betonen, daß ich es für außerordentlich bedenklich halte, der Polizei erheblich erweiterte technische Kontrollmöglichkeiten zu geben, ohne daß der Gesetzgeber vorher eindeutig festgelegt hat, welches Ausmaß an Kontrollen er der Bevölkerung zumuten will.

4.10 Verfassungsschutz

Wie ich bereits in meinem 3. TB (3.10, S. 88 ff.) ausführlich dargelegt habe, halte ich die Schaffung präziserer Rechtsgrundlagen für die Informationstätigkeit des Verfassungsschutzes für vordringlich. Aktivitäten zur Novellierung des HmbVerfSchG haben meine Vorschläge allerdings nicht in Gang gesetzt: während des ganzen Berichtsjahres ist mir keinerlei inhaltliche Reaktion des Landesamtes für Verfassungsschutz zugegangen. Die Feststellung in meinem 3. TB, daß ich zu Beanstandungen in Einzelfällen keine Veranlassung hatte, darf nicht darüber hinwegtäuschen, daß es insbesondere bei der Praxis der informationellen Zusammenarbeit des Verfassungsschutzes mit der Polizei datenschutzrechtliche Probleme gibt, die dringend zu lösen sind (vgl. 3. TB, 3.10.2, S. 90 f.; 3.8.4, S. 75).

Auf Bundesebene sind die Diskussionen – bedingt durch das Vorhaben der Regierungskoalition in Bonn, die Einführung des maschinenlesbaren Personalausweises durch die Verabschiedung eines Paketes von Begleitgesetzen zu fördern (vgl. dazu 1.1) – im Berichtszeitraum vorangekommen. Ich hatte Gelegenheit, zu einem AK IV der Innenminister-Konferenz erarbeiteten „Vorentwurf für die Novellierung des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes (BVerfSchG-VE)" sowie einem „Vorentwurf eines Gesetzes über die informationelle Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Staats-und Verfassungsschutzes (ZAG-VE)" Stellung zu nehmen. Da diese Gesetzesvorhaben erhebliche Signal-, wenn nicht gar Bindungswirkungen für die Novellierung des HmbVerfSchG entfalten werden, habe ich – in Ergänzung meiner Ausführungen im 3. TB – meine wesentlichen Kritikpunkte hier einmal zusammengefaßt.

4.10.1 Grundsätzliche Defizite des BVerfSchG-VE

Die im Vorentwurf vorgesehenen Regelungen weisen, unbeschadet der weiter unten darzustellenden Einzelkritik drei grundsätzliche Defizite auf:

a) Nach dem VZ-Urteil kommt es darauf an, die jetzige Praxis der Verfassungsschutzämter im Lichte der dort formulierten Grundsätze kritisch zu überprüfen. Es hieße dieses Urteil mißverstehen, wenn die Novellierung nur zum Anlaß genommen wird, die bisherige Datenverarbeitungspraxis gesetzlich abzusichern. Nichts anderes wird aber in wesentlichen Teilen des Vorentwurfs getan.

b) Das VZ-Urteil betont, daß das Recht auf informationelle Selbstbestimmung unabhängig von den dabei angewandten Verfahren gilt. Hiermit ist es nicht vereinbar, wenn Befugnisse zu Informationseingriffen (Speicherung, Veränderung, Nutzung) nur für eine Verarbeitung in Dateien geregelt werden (so aber §§ 7, 12, 13 des BVerfSchG-VE).

   Diese künstliche Beschränkung der Regelung auf einen Aspekt der Datenverarbeitung ist nicht akzeptabel. Sie verhindert einen angemessenen Datenschutz, denn die verschiedenen Formen der Informationsverarbeitung (Akten und Dateien) bilden ein integriertes Ganzes, dessen einzelne Teile – jeweils für sich betrachtet – kaum einer adäquaten Beurteilung zugänglich sind.

   Dies bedeutet nicht, daß an alle Formen der Datenverarbeitung unterschiedslos die gleichen Anforderungen zu stellen sind. Aus dem VZ-Urteil ergeben sich durchaus Ansätze zu differenzierten Betrachtungsweisen, je nachdem ob es sich um Akten, manuelle Karteien, automatisierte Dateien oder Datenbanken handelt.

c) Der BVerfSchG-VE wird schließlich dem im VZ-Urteil formulierten Grundsatz der Zweckbindung nicht gerecht. Aus diesem Grundsatz folgt, daß die Verwendung

von personenbezogenen Daten grundsätzlich – Ausnahmen sind gesondert zu regeln – auf den Zweck beschränkt ist, für den sie erhoben worden ist. Da der Verfassungsschutz ganz unterschiedliche Aufgaben (Extremismusbeobachtung, Spionageabwehr etc.) zu erfüllen hat, ist es nicht sachgerecht, bei der Regelung der Befugnisse nur an den allgemeinen Zweck „Aufgabenerfüllung des Verfassungsschutzes" anzuknüpfen.

Die unterschiedlichen Aufgaben erfordern vielmehr entsprechend differenzierte Befugnisse. Was beispielsweise für die Abwehr von Spionen einer fremden Macht vertretbar ist, ist nicht unbedingt angemessen für die Beobachtung extremistischer Bestrebungen: Bei der Datenspeicherung für Zwecke der Spionageabwehr etwa wird in anderen Zeiträumen zu denken sein als bei der – nicht selten junge Menschen betreffenden – Extremismusbeobachtung. Ein Spion, der Strafrechtsnormen verletzt, wird sich auch weit weniger auf Grundrechtsnormen berufen können als ein – wenn auch extremistischer – Teilnehmer am politischen Willenbildungsprozeß.

4.10.2 Präzisierung der Aufgabenstellung

Wie ich bereits im 3. TB (Tz. 3.10.1, S. 89) ausgeführt habe, ist es dringend erforderlich, die Aufgaben der Verfassungsschutzämter (vgl. § 3 BVerfSchG; § 3 HmbVerfSchG) präziser zu beschreiben.

4.10.2.1 Beobachtung extremistischer Bestrebungen

Da an anderer Stelle Forderungen mit Eingriffscharakter an die Aufgabenzuweisungen des § 3 geknüpft werden, ist bereits in dieser Vorschrift die nötige Normenklarheit zu gewährleisten.

Diese Feststellung gilt insbesondere für die Beobachtung extremistischer Bestrebungen. Es bleibt bislang völlig offen, ob und in welchem Umfang diese Aufgabe personenbezogene Beobachtungen rechtfertigen kann. Die Verwendung des Begriffs „Bestrebung" signalisiert zwar, daß nicht politische Eigenbrötelei, Einzelgängertum und vereinzelte Außenseiterpositionen Beobachtungsobjekte des Verfassungsschutzes sind, sondern nur extremistische Aktivitäten mit einem gewissen Gras organisatorischer Verfestigung. Unklar bleibt aber, wo die Schwelle zwischen verfassungsfeindlichen Aktivitäten und schlicht regierungskritischer Gesinnung liegt. Diese Schwelle ist jedenfalls für den betroffenen Bürger nicht hinreichend deutlich erkennbar.

Aus der Anknüpfung an „Bestrebungen" ergibt sich zwar, daß nicht Einzelpersonen im Zentrum der Extremismusbeobachtung stehen. Sie kann der Beobachtung und Registrierung von Personen andererseits auch nicht von vornherein entgegenstehen, da extremistische Bestrebungen letztlich von natürlichen Personen getragen werden. Eine denkbare Lösung des Problems könnte darin gesehen werden, daß die Verfassungsschutzbehörden verpflichtet werden, eine Liste der Beobachtungsobjekte, d.h. der Organisationen, die als verfassungsfeindliche Bestrebungen verdächtig sind, nicht nur intern abzusprechen, sondern zu Beginn eines jeden Jahres publik zu machen. Eine gewisse Publizität der beobachteten Organisationen ergibt sich bereits jetzt aus den jährlichen Tätigkeitsberichten der Verfassungsschutzbehörden. Was allerdings nicht für die – vertraulich behandelten – Tätigkeitsberichte des Hamburgischen Verfassungsschutzes gilt.

Eine Regelung, die den verfassungsrechtlichen Anforderungen der Normenklarheit gerecht wird, muß klarstellen, daß die Beobachtung und Registrierung von Personen stets der primären Aufgabe „Beobachtung von Bestrebungen" untergeordnet ist. Lediglich in diesem Rahmen dürfen personenbezogene Daten verarbeitet werden. Eine personenbezogene Speicherung darf mithin nur dann erfolgen, wenn ein Bezug zu einer extremistischen Bestrebung in der Person des Betroffenen konkret erfüllt ist.

Auch die im Bundesverfassungsschutzgesetz genannten Schutzgüter (wie „freiheitliche demokratische Grundordnung" und „auswärtige Belange") sollten im Interesse der Normenklarheit weiter konkretisiert werden (vgl. meinen 3. TB Tz. 3.10.2.).

Schließlich sollte klargestellt werden, inwieweit die Informationstätigkeit des Verfassungsschutzes nur „passiv" erfolgt, was die Formulierung „Sammlung und Auswertung" nahelegen könnte, oder inwieweit ihm auch die – aktive – Beschaffung von Informationen obliegt.

4.10.2.2 Mitwirkung an Sicherheitsüberprüfungen

Auch die in § 3 Abs. 2 unverändert vorgesehene Aufgabe des Verfassungsschutzes zur Mitwirkung an Sicherheitsüberprüfungen ist in doppelter Hinsicht ergänzungsbedürftig: Zum einen ist der Umfang der Mitwirkungspflichten des Verfassungsschutzes zu präzisieren, des weiteren sind aber auch für die Sicherheitsüberprüfungen selbst gesetzliche Grundlagen erforderlich.

Bei einer gesetzlichen Regelung der Sicherheitsüberprüfungen selbst sind folgende Prinzipien zu beachten:

- Die Sicherheitsüberprüfungen sind auf das erforderliche Maß zu beschränken. Dies gilt insbesondere für die Intensität der Prüfung, die von der Gefährdung im Einzelfall abhängen muß.
- Die Sicherheitsüberprüfung soll erst durchgeführt werden, wenn die sonstigen Voraussetzungen zur Befassung mit sicherheitsrelevanten Vorgängen oder zum Einsatz im sicherheitsrelevanten Bereich gegeben sind. Für den personellen Sabotageschutz ist zudem die exakte Beschreibung der sicherheitsempfindlichen Bereiche und die Begrenzung der Überprüfung auf tatsächlich in diesem Bereich eingesetzte Personen zu fordern.
- Es muß klargestellt werden, welche Stelle die Aufgabe hat, im Rahmen der Sicherheitsüberprüfung die Auskünfte aller beteiligten Stellen zu koordinieren. Dies muß nicht zwangsläufig die Aufgabe des Verfassungsschutzes sein.
- Das Verfahren muß für den Betroffenen transparent sein. Er ist über die Tatsache, den Ablauf, die beteiligten Stellen und das Ergebnis der Sicherheitsüberprüfung zu unterrichten. Ihm ist im Fall von Sicherheitsbedenken Gelegenheit zur Stellungnahme zu geben, insbesondere zu den Auskünften sog. „Auskunftspersonen". Die Ausnahmen von der Unterrichtungspflicht sind eng zu fassen. Auch Auskunftspersonen sind über den Zweck der Befragung zu unterrichten, um Fehlschlüsse zu Lasten des Betroffenen zu vermeiden, und auf die Freiwilligkeit ihrer Anfgaben hinzuweisen.
- Die speziell für die Sicherheitüberprüfungen beim Betroffenen oder anderen Stellen erhobenen Daten dürfen i.d.R. nur für diesen Zweck verwendet werden. Die Trennung von Sicherheits- und Personalakten ist streng zu wahren.

Bei der Regelung der Mitwirkungsaufgabe des Verfassungsschutzes ist folgendes zu berücksichtigen:

- Zunächst einmal soll hier klargestellt werden, daß die Verfassungsschutzbehörden nur „auf Antrag" der betroffenen Stellen bei der Personalüberprüfung mitwirken. Dies ist in § 3 Abs. 2 zum Ausdruck zu bringen.
- Einer klaren gesetzlichen Regelung bedürfen weiterhin insbesondere die Fragen des Umfangs der vom Verfassungsschutz auszuwertenden Datenbestände, der einzuholenden Auskünfte, der Einbeziehung dritter Personen sowie schließlich der weiteren Verarbeitung der personenbezogenen Daten.

4.10.3 Regelungen zum Einsatz nachrichtendienstlicher Mittel

4.10.3.1 Definition nachrichtendienstlicher Mittel

Der Begriff „nachrichtendienstliche Mittel" ist in den Verfassungsschutzgesetzen bislang nicht näher definiert worden.Die Einschätzung, daß eine Präzisierung dieses Begriffes „untunlich" sei, dürfte sich nach dem VZ-Urteil kaum noch halten lassen (vgl. a. schon 3. TB, 3.10.2, S. 90). Auch die vorgebrachten Argumente gegen eine nähere

Beschreibung der nachrichtendienstlichen Mittel sind nicht überzeugend: Warum eine genaue Regelung der Voraussetzungen und Modalitäten bestimmter Eingriffe in das informationelle Selbstbestimmungsrecht die durch den Parlaments-Vorbehalt gezogene Grenze des Regelungsbedarfs übersteigen soll, ist völlig unerfindlich. Auch die Feststellung, daß eine gesetzliche Festschreibung und damit Aufdeckung der nachrichtendienstlichen Mittel ihre schnelle und unbemerkte Anwendung bei Terroristen, Extremisten und Spionen unmöglich machen würde, ist wenig plausibel. Eine typisierte Auflistung der zulässigen nachrichtendienstlichen Mittel dürfte konspirativ arbeitenden Organisationen kaum Neues sagen.

Nach Möglichkeit sollten die zulässigen nachrichtendienstlichen Mittel im Gesetz abschließend genannt werden. Zu denken ist dabei etwa an eine Definition, wie sie die Verfasser des Entwurfs in der Begründung selbst angedeutet haben.

Danach könnten etwa folgende Mittel aufgelistet werden:

Die Erhebung personenbezogener Daten

- durch systematische Observation verdächtiger Personen,
- durch verdeckten Einsatz von technischen Mitteln zum Anfertigen von Bildaufnahmen sowie zum Abhören und Aufnehmen des gesprochenen Wortes auf Tonträger,
- durch Einsatz von Beamten unter einer Legende,
- durch das Einschleusen oder Anwerben und Führen von V-Leuten in extremistische und terroristische Organisationen oder
- durch Überwachungsmaßnahmen nach dem G-10.

Sollte eine abschließende Regelung im Hinblick auf die Tätigkeit des Verfassungsschutzes nicht möglich sein – was ich nach den in der Begründung genannten Beispielen bezweifele –, müßten die zulässigen Mittel im Gesetz zumindest beispielhaft aufgezählt werden. Daneben müßten die Verfassungsschutzbehörden verpflichtet werden, alle in Frage kommenden Mittel intern zu beschreiben und ihren Einsatz zu dokumentieren. Den Datenschutzbeauftragten sollte ggf. Gelegenheit zur Stellungnahme – zu diesen internen Beschreibungen – gegeben werden.

4.10.3.2 Begrenzungen des Einsatzes

Auch die Voraussetzungen für die Anwendung nachrichtendienstlicher Mittel müssen noch näher konkretisiert werden. Unklar ist bislang insbesondere, wann nachrichtendienstliche Mittel keinesfalls eingesetzt werden dürfen, welche absoluten Grenzen hier also zu ziehen sind. Klargestellt werden sollte ferner, daß die Anwendung nachrichtendienstlicher Mittel nicht von der Beachtung der allgemeinen Rechtsordnung entbindet (vgl. bereits § 4 Abs. 1 Satz 2 des niedersächsischen Verfassungsschutzgesetzes). Das heißt in erster Linie, daß der Einsatz nachrichtendienstlicher Mittel keine Verstöße gegen Strafrechtsnormen rechtfertigt.

Ferner sollten beim Einsatz nachrichtendienstlicher Mittel zum Schutze des Betroffenen – wie bei § 5 Abs. 5 G-10 – zusätzliche Verfahrenssicherungen eingebaut werden. Um dem Betroffenen die Möglichkeit zu geben, sich gegen eine mögliche Verletzung seiner Rechte zur Wehr zu setzen, ist er vom Einsatz der nachrichtendienstlichen Mittel zu unterrichten, sobald eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann.

Schließlich fehlt bislang die Klarstellung, daß sich der Einsatz nachrichtendienstlicher Mittel nur gegen denjenigen richten darf, der selbst in Verdacht steht, die vom Verfassungsschutz beobachteten Bestrebungen oder Tätigkeiten ausüben. Soweit beim Einsatz nachrichtendienstlicher Mittel Informationen über Personen anfallen, bei denen die o.g. Voraussetzungen nicht vorliegen, sollte entsprechend § 7 Abs. 3 G-10 ein Verwertungsverbot statuiert werden.

4.10.4 Verfassungsschutz und Grundrechtsausübung

Auch außerhalb des Einsatzbereiches nachrichtendienstlicher Mittel müssen die Befugnisse des Verfassungsschutzes eingegrenzt werden. Die Tätigkeit des Verfas-

sungsschutzes kann insbesondere mit den für unser demokratisches Gemeinwesen besonders wichtigen Grundrechten der Meinungs- und Versammlungsfreiheit kollidieren.

Das BVerfG hat dazu in seinem „Brokdorf-Beschluß" vom 14.5.1985 (NJW 1985, 2395) insbesondere deutlich gemacht, daß der staatsfreie, unreglementierte Charakter der politischen Meinungsbildung nicht durch exzessive Observationen und Registrierungen verändert werden darf. Diesen Anforderungen ist in den vorliegenden Gesetzentwürfen nicht hinreichend Rechnung getragen worden. Es muß klargestellt werden, daß die Erhebung (und Speicherung) personenbezogener Daten wegen der Ausübung der genannten Grundrechte nur dann gerechtfertigt sein kann, wenn in der Ausübung selbst die extremistische Betätigung liegt.

Insbesondere sollte deutlich werden, daß Informationen nur über solche Personen erhoben werden dürfen, die selbst den Verdacht von Bestrebungen und Tätigkeiten nach § 3 Abs. 1 begründet haben. Es muß vermieden werden, daß auch Daten von Mitgliedern demokratischer Organisationen erhoben werden, nur weil der Verfassungsschutz davon ausgeht, daß eine solche Organisation von Extremisten unterwandert wird.

4.10.5 Speicherung und Löschung von Daten

Völlig unzureichend sind die im BVerfSchG-VE enthaltenen Regelungen zu der zentralen Frage des Umfangs der Speicherbefugnis.

Bereits erwähnt habe ich, daß eine Regelung nach den bisherigen Vorstellungen nur für die Speicherung und Löschung in Dateien vorgesehen ist (s. 4.10.1). Dadurch entstehen bedenkliche Regelungslücken: weder ist eine Ausklammerung der Informationsverarbeitung in Akten akzeptabel, noch erscheint eine Fixierung auf den Dateibegriff im Hinblick auf moderne Formen der Textverarbeitung und Datenbankstrukturen sachgerecht.

4.10.5.1 Eingrenzung des betroffenen Personenkreises

Für wesentlich halte ich eine klare Eingrenzung des von Speicherungen betroffenen Personenkreises. Eine schlichte Bezugnahme auf die Erforderlichkeit zur Aufgabenerfüllung des Verfassungsschutzes reicht hier nicht aus. Vielmehr ist klarzustellen, daß Speicherungen nur gerechtfertigt sind, wenn in der Person des Betroffenen selbst tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG vorliegen (vgl. a. 4.10.2. und 4.10.4).

Nicht akzeptabel ist auch eine Speicherregelung, die lediglich daran anknüpft, daß eine Speicherung für die „Erforschung und Bewertung von Bestrebungen und Tätigkeiten nach § 3 Abs. 1" erforderlich ist. Eine solche Formulierung würde eine generalklauselartige Erlaubnis zur Speicherung von Daten über demokratische, sog. „beeinflußte" Organisationen bieten. Dies wäre unverhältnismäßig.

4.10.5.2 Speicherung bei Sicherheitsüberprüfungen

Völlig unklar ist bislang der Umfang der vorgesehenen Speicherung von Daten aus der Sicherheitsüberprüfung. Vorgesehen ist eine Speicherung „für Zwecke des Verfassungsschutzes". Diese Regelung läßt völlig offen, welche Personen im Rahmen einer Sicherheitsüberprüfung in Dateien bzw. sonstwie personenbezogen abrufbar gespeichert werden dürfen, insbesondere ob außer der überprüften Person auch z.B. Daten über Auskunftspersonen, Verwandte etc. erfaßt werden dürfen.

Offen bleibt ferner, welche Daten in welcher Form gespeichert werden dürfen. Bei einer Sicherheitsüberprüfung werden besonders viele und besonders sensible Daten erfaßt, um eine möglichst zuverlässige Beurteilung der Persönlichkeit des Betroffenen erreichen zu können. Würden alle diese Daten in automatisierter Form gespeichert, könnten hieraus, ohne daß eine wertende Analyse im Einzelfall stattfindet, automatisierte Persönlichkeitsprofile errichtet werden, was ich für verfassungsrechtlich außer-

ordentlich bedenklich hielte. Deshalb darf die Einrichtung automatisierter Datensammlungen nicht ins Belieben der Verfassungsschutzbehörden gestellt werden.

Schließlich fehlt eine Regelung, die den Zweck der Datenspeicherung im Rahmen der Sicherheitsüberprüfung begrenzt. Die vorgesehene Zustimmung des Betroffenen dürfte sich kaum auf eine beliebige Verwertung der Daten „für (alle) Zwecke des Verfassungsschutzes" erstrecken.

Auch die bei Dritten eingeholten Auskünfte dürften in aller Regel ausschließlich für die Sicherheitsüberprüfung bestimmt sein. Schon aus diesen Gründen sind einengende Regelungen dringend geboten. Von einer Zweckbindung noch gedeckt sein dürfte die Verwertung der Daten zur Spionageabwehr, da diese gleichgelagerte Zielrichtungen wie die Sicherheitsüberprüfung verfolgt.

4.10.5.3. Rechtsgrundlage für NADIS

Der BVerfSchG-VE enthält weiter einen Vorschlag zur Schaffung einer Rechtsgrundlage für das nachrichtendienstliche Informationssystem (NADIS). Diese Vorschrift soll offenbar die gegenwärtige Praxis absichern, ohne sie an irgendwelche einengende Voraussetzungen zu knüpfen. Dies erscheint mit zu weitgehend. Die Zulässigkeit eines Verbundsystems, wie es gegenwärtig im NADIS realisiert ist, dürfte zwar im überwiegenden Allgemeininteresse zu bejahen sein. Gleichwohl sollte festgestellt werden, daß on-line-Anschlüsse und Verbundsysteme nicht nach Belieben eingerichtet werden dürfen.

Zur Zeit hat NADIS im wesentlichen den Charakter eines Aktennachweissystems. Im BfV sowie in einzelnen Landesämtern werden jedoch bereits ADV-Anwendungen betrieben, die darüber weit hinausgehen. Planungen für die Ausweitung der Verbundanwendungen liegen vor. Diese technischen Entwicklungen werden unweigerlich Quantität und Qualität der Informationstätigkeit bei den Verfassungsschutzbehörden beeinflussen. Dies gilt insbesondere für den Umfang der Datenspeicherung sowie die Ausweitung von Verknüpfungs- und Recherchemöglichkeiten. Dementsprechend wird das Potential für mögliche Gefährdungen des Rechts auf informationelle Selbstbestimmung ansteigen.

Aus diesen Gründen sollten wesentliche Schritte der Automatisierung nur zugelassen werden, wenn sie für die Erfüllung der jeweiligen, zu benennenden Aufgaben nötig sind und schutzwürdige Belange des Betroffenen dadurch nicht unverhältnismäßig beeinträchtigt werden. Anders formuliert: Für den jeweiligen Automatisierungsschritt muß eine Notwendigkeit bestehen, die stärker wiegt als die in dieser besonderen Form der Datenverarbeitung liegenden Gefahren für das Grundrecht auf informationelle Selbstbestimmung.

Ferner muß sichergestellt sein, daß durch die Automation keine Verkürzung und Verzerrung von Sachverhalten entsteht.

4.10.5.4 Löschungsregelungen

Ein weiterer Mangel der bisherigen Entwürfe liegt darin, daß nur generalklauselartige Löschungsregelungen vorgesehen sind, die den Anforderungen der Normenklarheit nicht gerecht werden.

Notwendig erscheint es, gesetzliche Regelfristen für die Überprüfung und Löschung der gespeicherten Daten festzulegen. Dabei sollte zwischen den einzelnen Aufgabenbereichen (Extremistenbeobachtung / Spionageabwehr / Sicherheitsüberprüfung) unterschieden werden. Es liegt auf der Hand, daß Überlegungen, die unter dem Aspekt der Spionageabwehr relevant sein mögen, wie man sich z.B. am besten vor Perspektivagenten schützen kann, nicht unverändert auf die Extremismusbeobachtung übertragen werden können.

Die bisher in Verwaltungsvorschriften festgelegten Löschungsvorschriften dürfen allerdings nicht pauschal übernommen, sondern müssen überprüft werden. Insbe-

sondere die bislang vorgesehene Regelfrist von 15 Jahren im Extremismusbereich muß als zu lang erachtet werden. Es verwundert, daß bei der Polizei, wo es um die Registrierung strafbarer Handlungen geht, eine Regelfrist von 10 Jahren – und in Fällen von geringerer Bedeutung von 5 Jahren – für ausreichend erachtert wird, während beim Verfassungsschutz, wo es um extremistische Aktivitäten geht, die häufig nicht die Qualität einer Straftat haben, 15 Jahre für erforderlich angesehen werden.

Sicherzustellen ist ferner, daß Löschungen nicht nur bei der speichernden Stelle erfolgen, sondern daß die Tatsache der Löschung an andere Stellen nachberichtet wird. Diese Pflicht zum Nachbericht muß nicht nur gegenüber Dritten gelten, die Kenntnis von der gespeicherten Information erhalten haben, sondern auch und gerade gegenüber den Verbundteilnehmern. In der Regel bestehen in einem Verbundsystem wie NADIS zum Datensatz einer Person mehrere Notierungen (insbesondere Hinweise auf Aktenfundstellen) von verschiedenen Verbundteilnehmern. Da aber diese verschiedenen Hinweise oft auf ein und demselben sachlichen Vorgang beruhen, ist die Löschung einer Information den Verbundteilnehmern, die ebenfalls Daten zu dieser Person gespeichert haben, bekanntzugeben, um dort ebenfalls eine Überprüfung und ggf. Löschung zu veranlassen.

4.10.6. Zusammenarbeit zwischen Verfassungsschutz und Polizei

Die informationelle Zusammenarbeit zwischen Verfassungsschutz- und Polizeibehörden wirft wegen des Trennungsgebots besondere Probleme auf und bedarf sorgfältiger Regelungen und Abgrenzungen.

4.10.6.1 Zum sog. Trennungsgebot

Nach dem Zusammenbruch des NS-Regimes wurden Macht und Willkür der Gestapo u.a. auf die Zusammenballung polizeilicher und nachrichtendienstlicher Befugnisse zurückgeführt. Im sog. „Frankfurter Polizeibrief", auf den im alliierten Genehmigungsschreiben zum Grundgesetz ausdrücklich Bezug genommen wurde, haben die Alliierten deswegen die Trennung von Polizei und Verfassungsschutz verlangt.

Ziel dieses – verfassungskräftigen – Trennungsgebotes ist nicht nur die – rein organisatorische – Schaffung zweier unterschiedlicher Behörden. Seine materiell-inhaltliche Bedeutung besteht vielmehr darin, daß durch die Verteilung polizeilicher Befugnisse auf die eine und nachrichtendienstlicher Befugnisse auf die andere der beiden Behörden auch eine Zusammenballung nachrichtendienstlicher und polizeilicher Befugnisse verhindert werden sollte. (Vgl. z.B. § 4 Abs. 2 HmbVerfSchG.)

Es wäre wünschenswert, das Trennungsgebot – in Anlehnung an § 4 Abs. 4 des neuen bremischen VerfSchG – dadurch zu verdeutlichen, daß der Verfassungsschutz die Polizei auch nicht um Amtshilfe zu einer Maßnahme ersuchen darf, zu der er selber nicht befugt ist. Über diesen Grundsatz bin ich mir mit dem Hamburger Landesamt einig (vgl. a. 2. TB., Tz 3.11, S. 90).

Das Trennungsgebot kann auch nicht ohne Auswirkungen auf die informationelle Zusammenarbeit zwischen Polizei und Verfassungsschutz bleiben. Wenn die unter Anwendung der je spezifischen Befugnisnormen gewonnenen Informationen frei ausgetauscht werden könnten – was einer insbesondere in den Sicherheitsbehörden weit verbreiteten Ansicht entspräche – entstünde aus einem Prinzip der Machthemmung ein Instrument möglichst effektiver Arbeitsteilung. Zur Erreichung der mit dem Trennungsgebot verfolgten Ziele bedarf es andererseits auch keiner totalen informationellen Abkapselung zwischen Polizei und Verfassungsschutz, wie ich schon im 3. TB (Tz. 3.10.2, S. 91) dargelegt habe.

Aufgabe der zu schaffenden gesetzlichen Regelungen ist es aber, die Grenzen des Informationsaustausches zwischen Polizei und Verfassungsschutz im einzelnen festzulegen. Dem werden die bisherigen Entwürfe allerdings längst nicht gerecht.

4.10.6.2 Grundsätzliche Kritik des ZAG

Für weitgehend mißlungen halte ich vornehmlich das von der Bundesregierung in die Diskussion gebrachte ZAG. Ich habe bereits Zweifel, ob das ZAG als Querschnittsgesetz überhaupt notwendig ist. Bereichsspezifische und präzise Regelungen der Weitergabe von Informationen sollten grundsätzlich dort erfolgen, wo der Zweck der jeweiligen Datenverarbeitung festgelegt ist, also in dem Gesetz, das für die abgebende Behörde gilt. Es sollte daher erwogen werden, die Regelungen des ZAG in die jeweils geltenden Verfassungsschutz- oder Polizeigesetze zu übernehmen. Die ursprünglich vorgesehene Funktion des ZAG als Auffangnorm, die weitere bereichsspezifische Regelungen für den BND entbehrlich machen soll, ist ohnehin absolet geworden, da der BND im ZAG bislang ausgespart wird.

Unter diesen Umständen liegt die Vermutung nahe, daß die Querschnittsregelungen des ZAG in erster Linie einen Appell zur Zusammenarbeit ausdrücken und Verpflichtungen zur Datenweitergabe begründen sollen, um die bisher nach den „Zusammenarbeitsrichtlinien" geforderte Zusammenarbeit von Polizei und Nachrichtendiensten ohne Abstriche in der Praxis weiterführen zu können.

Diese Befürchtung wird dadurch bestätigt, daß der Zweck des ZAG in dessen § 1 nur relativ verschwommen formuliert wird: Es bleibt unklar, was „Angelegenheiten des Verfassungsschutzes" sind und wie sie von „Angelegenheiten des Staatsschutzes" abzugrenzen sind. Ein Verweis auf das BVerfSchG wäre nur akzeptabel, wenn dieses selbst präzise Definitionen enthielte (s. aber meine Kritik dazu 4.10.2). „Staatsschutz" soll sowohl die Verhinderung (Gefahrenabwehr?) als auch die Verfolgung von Straftaten umfassen. Relevant sollen hier alle Straftaten sein, bei denen Anhaltspunkte vorliegen, daß sie wegen

- ihrer Angriffsrichtung,
- des Motivs des Täters oder
- seiner Verbindung zu einer Organisation

gegen die im VerfSchG vage umschriebenen Schutzgüter gerichtet sind.

Diese Definition des (polizeilichen) Staatsschutzes ist zu ungenau. Sie ermöglicht es, fast jedes Delikt bei einer bestimmten Fallgestaltung zu einer Staatsschutzangelegenheit zu erklären. Delikte, die sich gegen Schutzgüter des Staatsschutzes richten, sollten in einem Katalog abschließend aufgezählt werden; als Muster kommt etwa § 2 G-10 in Betracht.

In § 1 werden ferner das Trennungsgebot sowie der Grundsatz der Zweckbindung nicht hinreichend berücksichtigt. Bei der Anordnung von Zusammenarbeitspflichten, wie sie das ZAG regeln soll, muß der Gesetzgeber von den unterschiedlichen Aufgaben der verschiedenen Polizei- und Verfassungschutzbehörden ausgehen und auf dieser Grundlage festlegen, wann Zweckdurchbrechungen im überwiegenden Allgemeininteresse zugelassen werden können.

Ich habe schließlich Zweifel, ob alle im ZAG vorgesehenen Regelungen überhaupt von der Gesetzgebungskompetenz des Bundes (Art. 73 Nr. 10 GG) erfaßt werden. Problematisch erscheinen mir vor allem Regelungen zu Übermittlungen von Polizeibehörden eines Landes an Verfassungsschutzbehörden des Bundes oder eines anderen Landes sowie von Verfassungsschutzbehörden eines Landes an Polizeibehörden des Bundes oder eines anderen Landes.

Ich rege daher an, auf ein ZAG als Querschnittsgesetz ganz zu verzichten und die gebotenen Regelungen in die jeweiligen Spezialgesetze für Polizei und Verfassungsschutz zu übernehmen.

4.10.6.3 Anlieferung von Daten durch Polizeibehörden ohne Ersuchen

Die vorliegenden Gesetzentwürfe sehen für die Polizei- und Strafverfolgungsbehörden weitgehende Verpflichtungen zu sog. „Spontan-Übermittlungen" von personen-

bezogenen Daten an den Verfassungsschutz vor. Derartige Pflichten sind zwar im Grundsatz anzuerkennen, sollten aber an präzise Voraussetzungen gebunden werden. Gesetzgebungstechnisch sind sie meiner Auffassung nach am sachgerechtesten in den einschlägigen Polizeigesetzen (Länderpolizeigesetze, BKAG, BGSG) bzw. in der StPO zu regeln.

Bei der Regelung sollten folgende Grundsätze berücksichtigt werden:

Zunächst sollte festgelegt werden, daß die übermittelnde Stelle im Einzelfall konkrete Anhaltspunkte dafür haben muß, daß die zu übermittelnde Information für die Aufgabenerfüllung des Verfassungsschutzes erforderlich ist, um eine routinemäßige Weitergabe nahezu aller Informationen aus dem polizeilichen Staatschutzbereich zu unterbinden. Solche Anhaltspunkte können sich z.B. aus der Kenntnis einer Liste der vom Verfassungsschutz beobachteten Bestrebungen ergeben. Es sollte ausgeschlossen werden, daß Daten über Betroffene nur aufgrund ihrer Zugehörigkeit zu einer bestimmten Personengruppe (z.B. Hausbesetzer) ohne Ersuchen listenmäßig an die Nachrichtendienste geliefert werden.

Eine Pflicht des Verfassungsschutzes zur Überprüfung muß daneben bestehen bleiben.

Weiter muß – nach dem Vorbild des bremVerfSchG – sichergestellt werden, daß die Sicherheitsbehörden nur solche Informationen weitergeben dürfen, die sie ihrerseits rechtmäßig erhoben und gespeichert haben. Die Weitergabe sog. „Zufallsfunde" – also solcher Informationen, die lediglich bei Gelegenheit polizeilicher Aufgabenerfüllung anfallen, ohne für die Polizei selbst erforderlich zu sein – ist mit dem Trennungsgebot nicht vereinbar, denn dadurch würde die Polizei quasi zum „verlängerten Arm" des Verfassungsschutzes werden.

Es sollte ferner sichergestellt werden, daß von der Polizei nur Angaben weitergegeben werden, die einen solchen Reifegrad erreicht haben, daß sie an die Staatsanwaltschaft weiterzugeben sind. Es wäre bedenklich, wenn der Verfassungsschutz ohne größere Einschränkungen an den polizeilichen Vorfeldermittlungen partizipieren könnte, die nicht zu strafrechtlichen Ermittlungsverfahren führen. Besondere Einschränkungen müssen insbesondere für die Informationen gelten, die mit Methoden der verdeckten Datenerhebung gewonnen wurden.

Darüber hinaus muß es ergänzende Regelungen für die Weitergabe solcher Informationen geben, die die Polizei unter Einsatz spezieller strafprozessualer Befugnisse gewonnen hat und für die besondere Zweckbindungen zu berücksichtigen sind. Dies gilt insbesondere für Informationen, die aus der Post- und Telefonkontrolle (gem. § 100 a StPO) oder aus Durchsuchungen von Wohnungen (gem. § 108 StPO) stammen. Die bislang vorgeschlagenen Regelungen reichen noch nicht aus.

Nach dem ZAG soll die Übermittlung von Informationen, die Sicherheitsbehörden durch Maßnahmen nach § 100 a StPO gewonnen haben, insoweit eingeschränkt werden, als Anhaltspunkte für den Verdacht bestehen müssen, daß eine der in § 2 G-10 genannten Handlungen geplant oder begangen wird oder begangen worden ist. Diese Regelung geht also davon aus, daß der Verfassungsschutz alle Informationen, die er selbst durch eine Überwachung des Post- und Fernsprechverkehrs erhalten könnte, ebensogut von der Polizei erlangen können muß. Dies halte ich für bedenklich, denn es kann dazu führen, daß das G-10 mit seinen speziellen Verfahrensvoraussetzungen und Schutzbestimmungen unterlaufen wird. Vertretbar erscheint mir eine Weitergabae allenfalls dann, wenn es sich um Handlungen aus dem Terrorismus- und Spionagebereich handelt.

Nicht geeignet erscheint mir eine Bezugnahme auf die Regelung des § 7 Abs. 3 G 10, da die dort vorgesehenen Verwertungsbeschränkungen für die Nachrichtendienste, die sich insbesondere als Übermittlungsbeschränkungen gegenüber der Polizei auswirken, in umgekehrter Richtung schlecht passen. Sinnvoll und erforderlich erscheint es mir allerdings, die Informationen, die der Verfassungsschutz aus polizeilichen Post- und Telefonüberwachungsmaßnahmen – nach Maßgabe der hier vorgeschlagenen

Regelung – erhalten hat, ebenfalls den Verwertungsbeschränkungen des § 7 Abs. 3 G 10 zu unterwerfen. Das heißt, solche Informationen dürfen – innerhalb es Verfassungsschutzes – nur zu dem der Übermittlung zugrundeliegenden Zweck genutzt werden, es sei denn, daß es Anhaltspunkte für eine in § 138 StGB genannte Straftat gibt.

Informationen, die bei der Durchsuchung einer Wohnung gewonnen worden sind, sollen nach dem ZAG-VE übermittelt werden dürfen, „wenn eine Abwägung mit den schutzwürdigen Belangen des Betroffenen ergibt, daß das Allgemeininteresse überwiegt". Diese Regelung stößt ins Leere. Sie enthält keine besondere Einschränkung, denn nach dem VZ-Urteil gilt für alle Informationseingriffe – wie die Weitergabe von Informationen – schlechthin, daß sie im überwiegenden Allgemeininteresse erforderlich sein müssen. Für gerade noch vertretbar halte ich eine Regelung, die allein daran anknüpft, ob Anhaltspunkte vorliegen für

„1. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder

2. Bestrebungen im Sinne des § 3 Abs. 1 BVerfSchG, die darauf gerichtet sind, Gewalt anzuwenden."

Für eine noch darüber hinaus gehende Einbeziehung von Bestrebungen, die darauf gerichtet sind, „Gewaltanwendung vorzubereiten" sehe ich kein Bedürfnis. Damit könnte die Eingriffsschwelle zu weit abgesenkt werden.

4.10.6.4 Anlieferung von Daten durch Polizeibehörden auf Ersuchen

Auch Übermittlungen auf Ersuchen müssen auf solche Daten begrenzt werden, die die Polizei zur eigenen Aufgabenerfüllung rechtmäßig erhoben und gespeichert hat und die eine strafrechtliche Relevanz haben (vgl. o. 4.10.5.3). Dies gilt auch für den Bundesgrenzschutz. Wenn schon pauschalierte Amtshilfeersuchen des Verfassungsschutzes für unverzichtbar gehalten werden, so sind sie auf Zwecke der Spionageabwehr zu begrenzen. Die Erfassung von Trägern extremistischer Bestrebungen bei Grenzübertritten dürfte nicht mehr verhältnismäßig sein.

Der völlige Verzicht auf eine Begründungspflicht ist auch hier abzulehnen: Soweit nicht besondere Gründe entgegenstehen (z.B. schutzwürdige Belange des Betroffenen oder Sicherheitsinteressen des Staates) sind die Auskunftsersuchen vom Verfassungsschutz zu begründen. Insbesondere bei Ersuchen im Rahmen von Sicherheitsüberprüfungen sind entgegenstehende Gründe nicht erkennbar (vgl. a. 4.10.4.3).

4.10.6.5 Weitergabe von Daten des Verfassungsschutzes an Polizeibehörden

Auch die Weitergabe von Daten durch den Verfassungsschutz an die Polizei muß restriktiv geregelt werden. Sie sollte grundsätzlich nur zulässig sein, wenn die Erfüllung spezieller Aufgaben des Verfassungsschutzes dies erfordert, oder wenn konkrete Anhaltspunkte dafür bestehen, daß die Übermittlung für die Verfolgung bzw. Verhinderung von Straftaten nötig ist.

Zu berücksichtigen ist, daß Informationen, die der Verfassungsschutz durch den Einsatz nachrichtendienstlicher Mittel gewonnen hat, einer besonders strengen Zweckbindung unterliegen. Für Kenntnisse und Unterlagen, die aus der Überwachung des Post- und Fernmeldeverkehrs stammen, ist bereits in § 7 Abs. 3 G-10 geregelt, daß sie nur dann zweckentfremdet verwendet werden dürfen, wenn jemand eine der in § 138 StGB genannten Straftaten zu begehen vorhat, begeht oder begangen hat (§ 138 StGB zählt diejenigen Straftaten auf, zu deren Anzeige jedermann verpflichtet ist, wenn er von ihrer Planung oder Vorbereitung erfährt). Nach diesem Vorbild sollte auch die Verwendung von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen werden, eingeschränkt werden.

Für die Polizei ist schließlich festzulegen, daß sie zu prüfen hat, ob die Voraussetzungen für die Einleitung eines Strafverfahrens vorliegen. Bei negativem Ergebnis sind die Daten zu löschen.

4.10.7 Zusammenarbeit des Verfassungsschutzes mit anderen Stellen

Die informationelle Zusammenarbeit des Verfassungsschutzes mit anderen Stellen unterliegt zwar nicht den besonderen Restriktionen des Trennungsgebotes. Auch hier sind jedoch präzise Regelungen nötig, die die Einhaltung der Verhältnismäßigkeit gewährleisten und Zweckbindungen sicherstellen.

4.10.7.1 Anlieferung von Daten durch andere Behörden ohne Ersuchen

Zunächst ist zu regeln, zu welchen Zwecken und unter welchen Voraussetzungen Behörden verpflichtet sind, von sich aus den Verfassungsschutz zu unterrichten. Es dürfte mittlerweile unstreitig sein, daß die (in § 5 BVerfSchG statuierte) Pflicht zur gegenseitigen Rechts- und Amtshilfe keinen hinreichend eingegrenzten Erlaubnistatbestand schafft (vgl. 3. TB Tz 3.10.4, S. 91). Der BVerfSchG-VE trägt dem insoweit Rechnung, als er Informationenspflichten für andere Behörden (als Sicherheitsbehörden) nur begründet, wenn Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des Verfassungsschutzes im Bereich der Terrorismus-Beobachtung und der Spionageabwehr erforderlich ist.

Bedenklich ist allerdings, daß es nicht bei diesen Informationspflichten bleiben soll. Darüber hinaus sind andere Behörden berechtigt, dem Verfassungsschutz sonstige Informationen jeglicher Art mitzuteilen, „wenn Anhaltspunkte dafür bestehen, daß die Übermittlung für die Aufgabenerfüllung des Verfassungsschutzes erforderlich ist."

Diese Regelung halte ich für unverhältnismäßig, weil die berechtigten Informationsinteressen des Verfassungsschutzes durch seine sonstigen Befugnisse hinreichend abgesichert sind. Desweiteren entspricht die Regelung auch nicht den Anforderungen der Normenklarheit, denn bei dieser Regelung kann kein Bürger, der in Kontakt mit irgendeiner beliebigen Verwaltungsbehörde tritt, mehr wissen, was diese wann und bei welcher Gelegenheit über ihn an den Verfassungsschutz übermittelt hat.

Übermittlungen, die auf vagen Verdachtsmomenten beruhen, können sich generell schädlich auf das Verhältnis der Bürger zu den Behörden auswirken. Es muß vermieden werden, daß ein allgemeines Klima des Denunziantentums entsteht.

4.10.7.2 Erteilung von Auskünften auf Ersuchen

Auch die Frage, wann Behörden verpflichtet sind, dem Verfassungsschutz auf Ersuchen Auskunft zu erteilen, bedarf einer klaren Regelung. Der BVerfSchG-VE sieht bislang vor, daß der Verfassungsschutz Auskünfte verlangen darf, wenn die Erforschung eines Sachverhaltes im Rahmen seiner Aufgabenerfüllung nicht, nur mit unverhältnismäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erfolgen kann und wenn besondere gesetzliche Übermittlungsregelungen nicht entgegenstehen. Diese Einschränkungen, die die Anforderungen des Verhältmäßigkeitsgrundsatzes verdeutlichen, stellen zwar schon einen Fortschritt dar, sie reichen jedoch noch nicht aus.

Ferner muß deutlich werden, daß der Verfassungsschutz von den zur Übermittlung verpflichteten Behörden nur die Weitergabe solcher Daten verlangen kann, die bei diesen zur rechtmäßigen eigenen Aufgabenerfüllung gespeichert sind. Der Verfassungsschutz kann die anderen Behörden nicht um spezielle Ermittlungen ersuchen, zu denen er selbst u.U. gar nicht befugt ist.

Nicht akzeptabel ist schließlich, daß der Verfassungsschutz – nach dem bisherigen Diskussionsstand – seine Übermittlungsersuchen generell nicht begründen, sondern nur intern dokumentieren muß. Eine derartige generelle Befreiung von der Begründungspflicht erscheint mir nicht zwingend geboten. Bei Ermittlungen im Rahmen einer Sicherheitsüberprüfung kann der Verfassungsschutz ohne weiteres seine Informationsersuchen begründen.

4.10.7.3 Einsichtnahme in öffentliche Register

Regelungsbedürftig ist ferner die Frage, ob und unter welchen Voraussetzngen der Verfassungsschutz nicht nur Auskünfte verlangen, sondern selbst Einsicht in öffentliche Register nehmen kann. Dabei sollten nach Auffassung der Datenschutzbeauftragten folgende Gesichtspunkte berücksichtigt werden:

Zunächst einmal ist zu berücksichtigen, daß eine Einsichtnahme des Verfassungsschutzes in öffentliche Register – wie das Melde-, Personalausweis und Paßregister – nach geltendem Recht unzulässig ist und jede Regelung somit zu einer Ausweitung der Befugnisse des Verfassungsschutzes führt.

Grundsätzlich ist zwar ein Bedürfnis des Verfassungsschutzes nach über einzelfallbezogene Auskünfte hinausgehenden Übermittlungen aus öffentlichen Registern anzuerkennen. Nach den Meldegesetzen ist dies auch nach geltendem Recht unter bestimmten Voraussetzungen bereits zulässig. Die Befriedung der Informationsbedürfnisse des Verfassungsschutzes sollte – je nach Erforderlichkeit – in einem abgestuften Verfahren erfolgen:

- bei Sicherheitsüberprüfungen z.B. reichen im Regelfall einzelfallbezogene Auskünfte;
- im Rahmen der Spionageabwehr können (nach dem Vorbild der Gruppenauskünfte nach den Meldegesetzen), auch Auskünfte über eine Vielzahl nicht namentlich genannter Betroffener, bei denen bestimmte Merkmale vorliegen, vorgesehen werden;
- eine – unbeaufsichtigte – Einsichtnahme in öffentliche Register sollte nur ausnahmsweise in Betracht kommen, wenn etwa die Bekanntgabe des zu überprüfenden Personenkreises bzw. der für eine Gruppenauskunft maßgeblichen Merkmale gegenüber den registerführenden Stellen die Aufgabenerfüllung des Verfassungsschutzes erheblich beeinträchtigen würde. Eine Einsichtnahme ist zu dokumentieren;
- Gruppenauskünfte und Einsichtnahmen in Register sollten auf den Zweck der Spionageabwehr beschränkt werden. Ein Bedarf für eine Ausweitung dieser Befugnisse auf den Bereich der Terrorismusbekämpfung ist nicht erkennbar. Nach der bestehenden Arbeitsteilung mit der Polizei hat der Verfassungsschutz nur das legale Umfeld des Terrorismus abzuklären.
- Dem Verfassungsschutz sollte nicht pauschal die Einsicht in alle öffentlichen Register (vom Gewerbe- über das Melde- bis zum Bundeszentralregister) gestattet werden. Um den Besonderheiten der einzelnen Register (insbesondere Zweckbindungen) besser Rechnung zu tragen, sollten die Regelungen – nach Maßgabe der o.g. Grundsätze – vielmehr in den jeweils einschlägigen Registergesetzen getroffen werden.

  Ein Bedürfnis für eine Einsichtnahme durch den Verfassungsschutz ist z.Z. nur bei einigen im Melde- und im Personalausweisregister gespeicherten Daten zu erkennen.

4.10.7.4 Weitergabe von Daten des Verfassungsschutzes an andere Stellen

Auch die Weitergabe von Daten durch den Verfassungsschutz bedarf differenzierter Regelungen.

Der BVerfSchG-VE sieht bisher nicht näher ausdifferenzierte Regelungen für Übermittlungen des Verfassungsschutzes an Behörden bzw. öffentliche Stellen des Bundes jeglicher Art vor. Die einzige Einschränkung soll darin bestehen, daß der Empfänger die Daten für Aufgaben benötigt, die mit dem Zweck des Verfassungsschutzes nicht vereinbar sind.

Diese Regelung wird dem vom BVerfG postulierten Grundsatz der Zweckbindung nicht gerecht. Die Einführung des Grundsatzes der Zweckvereinbarkeit führt zu einer generellen Aufweichung des Zweckbindungsprinzips, die einer Aufhebung gleichkommt.

Denn in der Praxis dürften kaum Fälle denkbar sein, in denen eine Datenübermittlung an eine Verwaltungsbehörde an fehlender Zweckvereinbarkeit scheitern könnte (s. dazu auch 3.3).

Übermittlungen an andere als Sicherheitsbehörden kommen nur zur Erfüllung von eigenen Aufgaben des Verfassungsschutzes in Betracht sowie dann, wenn eine Sicherheitsüberprüfung von der Empfängerbehörde beantragt worden ist. Aus anderen Gründen erscheint mir eine Durchbrechung des Zweckbindungsprinzips nicht gerechtfertigt.

4.10.8 Bürgerrechte gegenüber dem Verfassungsschutz

Im 3. TB (Tz. 3.10.5, S. 92) habe ich bereits die Notwendigkeit einer Verstärkung der Bürgerrechte gegenüber dem Verfassungsschutz begründet. Es muß sichergestellt werden, daß die Verfassungsschutzbehörden Auskunftsersuchen von Bürgern nicht – wie dies derzeit die meisten Ämter handhaben – schematisch ablehnen. (vgl. dazu meine Ausführungen zur BDSG-Novellierung, 6.2.1)

4.11. Justizwesen

Auch im Bereich der Justiz kommt die Diskussion über die Schaffung bereichsspezifischer Rechtsgrundlagen für die Informationsverarbeitung –wenn auch langsam– voran. Der Schwerpunkt der Diskussion liegt z.Z. bei der Novellierung der StPO sowie beim Schuldnerverzeichnis. Nachfolgend möchte ich einen Überblick über den derzeitigen Sachstand geben.

4.11.1 Zur Novellierung der StPO

Der Schaffung präziser Rechtsgrundlagen für Informationseingriffe im Rahmen der strafverfahrensrechtlichen Ermittlungstätigkeit kommt eine ebenso große Bedeutung zu, wie der Novellierung des Polizeirechts (vgl. 4.9.1).

Nachdem die Innenminister-Konferenz erste Entwürfe für Regelungen im Bereich der präventiven Verbrechensbekämpfung vorgelegt hat, beginnen die Justizverwaltungen nunmehr damit, über entsprechende Regelungen für den Bereich der (repressiven) Strafverfolgung, insbesondere über Rechtsgrundlagen für moderne Fahndungsmethoden nachzudenken. Erste Ergebnisse liegen vor: Weitgehende Einigkeit besteht inzwischen darüber, daß spezifische Eingriffsermächtigungen erforderlich sind. Für bestimmte Fahndungsmaßnahmen wie Rasterfahndung und polizeiliche Beobachtung liegen Formulierungsvorschläge vor. Wichtige Fragen sind allerdings noch offen.

Auch in den Justizverwaltungen scheint sich nach dem VZ-Urteil langsam die Einsicht durchgesetzt zu haben, daß mit der sog. Schwellentheorie keine strafprozessualen Eingriffsmaßnahmen zu rechtfertigen sind (vgl. schon 2.TB, 5.2.1, S. 146). Diese "Theorie" läuft darauf hinaus, die §§ 160, 163, 161 StPO, wonach Polizei und Staatsanwaltschaft beim Verdacht einer Straftat den Sachverhalt zu erforschen haben, als Befugnisnormen in Form von Generalklauseln zu interpretieren. Diese Klauseln sollen –nach der Schwellentheorie– alle Eingriffsmaßnahmen abdecken, die unterhalb der Schwelle der besonderen Eingriffsermächtigungen –namentlich solcher mit Zwangscharakter (wie Verhaftung, Durchsuchung, erkennungsdienstliche Behandlung etc.)– liegen.

Eine solche Betrachtungsweise widerspricht jedoch der Grundstruktur unseres Strafverfahrensrechts und wird i.ü. den Anforderungen des Bundesverfassungsgerichts an normenklare gesetzliche Grundlagen für Eingriffe in das informationelle Selbstbestimmungsrecht nicht gerecht.

Das Strafverfahrensrecht enthält anders als das Polizeirecht keine Generalermächtigung zum Eingriff in Individualrechtsgüter. Das Gesetz stellt den Strafverfolgungsorganen die umfassende Aufgabe zur Aufklärung und Verfolgung strafbarer Handlungen (§§ 152 Abs.2, 160, 163 Abs. 1 StPO) und folgt im übrigen der Methode der erschöpfenden Aufzählung einzelner Eingriffsermächtigungen, die in ihren Voraussetzungen

und Rechtsfolgen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes unterschiedlich ausgestaltet sind.

Die §§ 160, 163 StPO sind also bloße Aufgabenzuweisungsnormen, aus denen sich keine Eingriffsbefugnisse ableiten lassen. Auch § 161 StPO, wonach die Staatsanwaltschaft Ermittlungen jeder Art entweder selbst vornehmen oder durch Polizeibehörden vornehmen lassen kann, rechtfertigt nach mittlerweile allgemeiner Meinung keine Grundrechtseingriffe, sondern statuiert lediglich den "Grundsatz der freien Gestaltung des Ermittlungsverfahrens."

Spätestens nachdem im VZ-Urteil klargestellt worden ist, daß die –zwangsweise– Erhebung und Verarbeitung von Daten einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt, der einer normenklaren gesetzlichen Grundlage bedarf, ist die "Schwellentheorie" nicht mehr vertretbar.

Erste ausformulierte Vorschläge zu gesetzlichen Regelungen gibt es bislang vornehmlich für Rasterfahndung und polizeiliche Beobachtung. Die Tendenz geht dabei dahin, diese Maßnahmen in neuen §§ 100 c und 100 d zu regeln und sie materiell an dieselben Voraussetzungen wie die Überwachung des Post- und Fernmeldeverkehrs (§ 100 a StPO) zu knüpfen. Rasterfahndung und polizeiliche Beobachtung sollen also zulässig werden, wenn bestimmte Tatsachen den Verdacht begründen, daß eine in § 100 a StPO bezeichnete Straftat begangen oder ihre Begehung in strafbarer Weise versucht worden ist. Ob diese Eingriffsvoraussetzung dem Grundsatz der Verhältnismäßigkeit hinreichend Rechnung trägt oder ob der in Bezug zu nehmende Straftatenkatalog enger gefaßt werden muß, wird noch zu klären sein. Neben diesen materiellen Voraussetzungen sollen die genannten Fahndungsmethoden näher definiert und zusätzlichen organisatorischen und verfahrensrechtlichen Absicherungen unterworfen werden. Vorgesehen sind Regelungen über Anordnungskompetenz (Richtervorbehalt für die Rasterfahndung), Form und Verfahren der Anordnung, Löschungsregelungen, Verwertungsverbote, Benachrichtigung von Betroffenen (sobald eine Gefährdung des Untersuchungszwecks nicht mehr zu besorgen ist) sowie – bei der Rasterfahndung – eine Unterrichtung der zuständigen Datenschutzbeauftragten.

Ferner wird erörtert, ob der bisherige § 161 StPO durch einen neuen Absatz zu ergänzen ist, der eine ausdrückliche Ermächtigung zu bestimmten Informationserhebungen, wie z.B. einfache Observation vorsieht. Außerdem wurden Vorschläge für die Regelung von Akteneinsichtsrechten im Strafverfahren sowie für die Verbesserung der rechtlichen Grundlagen von Fahndungsmaßnahmen vorgelegt.
Alles in allem bilden die Vorschläge bereits eine geeignete Diskussionsgrundlage. Eine Arbeitsgruppe der DSB-Konferenz ist dabei, sie zu prüfen und ggf. alternative Vorstellungen zu entwickeln. Viele regelungsbedürftige Probleme im strafverfahrensrechtlichen Bereich sind allerdings noch ungeklärt. Zu nennen sind hier insbesondere:

- bei den Erhebungsmaßnahmen: Die Anwendung von verdeckten Methoden, Einsatz von V-Leuten, verdeckten Ermittlern und verdeckten technischen Überwachungsmaßnahmen (vgl. dazu – für den Bereich der vorbeugenden Verbrechensbekämpfung – 4.9.1.4);
- bei der Speicherung: Der Einsatz automatisierter Systeme wie SPUDOKs (vgl. dazu 3. TB, 3.8.2.2, S. 72 f.) sowie zentraler Namensdateien und Nachweissysteme. Offen ist in diesem Zusammenhang auch das Problem des Zugriffs der Staatsanwaltschaft auf Datenbestände der Polizei, die der Strafverfolgung dienen.

Einer präziseren gesetzlichen Regelung bedürfen ferner Akteneinsichts- und Auskunftsrechte. Nicht unerwähnt bleiben soll auch die Schaffung von gesetzlichen Grundlagen für die Mitteilungen in Strafsachen (vgl. 4.11.2). Hier ist noch offen, ob eine Regelung in der StPO oder aber in einem besonderen Bundesmitteilungsgesetz erfolgt.

Ich möchte in diesem Zusammenhang an meine Anregung aus dem 3. TB (3.12.1, S. 94) erinnern: Es sollte geprüft werden, ob es nicht den Anforderungen der Normenklarheit eher gerecht wird, für die Daten, die von unterschiedlichen Stellen für letztlich ein und denselben Zweck verarbeitet werden – nämlich Verfolgung einer bestimmten

Straftat – eine einheitliche und zusammenhängende Querschnittsregelung zu schaffen statt an bestehende Regelungen jeweils Vorschriften über Datenverarbeitung anzuflicken.

4.11.2 Rechtsgrundlage für Mitteilungen in Strafsachen

In der Diskussion um die Schaffung gesetzlicher Grundlagen für die sog. Anordnung über Mitteilungen in Strafsachen (MiStra) –vgl. dazu die Anl. 2 zu meinem 2. TB, S. 153– haben die Justizverwaltungen sich mittlerweile darauf verständigt, die erforderlichen Rechtsgrundlagen in einem Bundesgesetz zusammenzufassen. Ein entsprechender Gesetzentwurf des Bundesjustizministers wird für die erste Hälfte des Jahres 1986 erwartet.

Dieses Gesetz sollte die zulässigen Mitteilungstatbestände und -pflichten abschließend regeln und dabei folgende Grundsätze berücksichtigen:

- Die Beachtung des Grundsatzes der Zweckbindung ist durch die ausdrückliche Bestimmung sicherzustellen, daß die Empfängerbehörden die mitgeteilten Daten nur für den Zweck verwenden dürfen, zu dessen Erfüllung sie zulässigerweise übermittelt worden sind.
- Der aus dem Prinzip der Verhältnismäßigkeit abgeleitete Grundsatz der Erforderlichkeit gebietet, die Mitteilungen und ihren Inhalt auf das im Einzelfall erforderliche Mindestmaß zu beschränken. Es sollte daher sichergestellt werden, daß Mitteilungen tatsächlich nur dann gemacht werden, wenn sie für die empfangende Stelle entscheidungserheblich sind. Grundsätzlich ist die Mitteilung auf den Anklagesatz bzw. den Tenor der Entscheidung zu beschränken; die Übermittlung von Entscheidungsgründen kommt nur in absoluten Ausnahmefällen in Betracht.
- Bei der Festlegung des Zeitpunktes der jeweils ersten Mitteilung ist zu berücksichtigen, daß sich strafrechtlich relevante Sachverhalte erst nach rechtskräftigem Abschluß eines Strafverfahrens abschließend beurteilen lassen. Vorzeitige Mitteilungen müssen daher die Ausnahme bilden. Sie erscheinen nur dann erforderlich, wenn wegen der Bedeutung des möglicherweise verletzten Rechtsgutes vorzeitige Maßnahmen der empfangenden Stelle notwendig sind.
- Mitteilungen, die nicht vom Richter oder Staatsanwalt veranlaßt werden, dürfen nur zugelassen werden, wenn Anlaß, Inhalt und Zeitpunkt dieser Mitteilungen abschließend und eindeutig festgelegt sind. Setzt der sachgerechte Vollzug einzelner Mitteilungspflichten eine Abwägung im Einzelfall voraus, ist diese Entscheidung stets dem Richter oder Staatsanwalt vorzubehalten.
- Für alle Mitteilungsfälle muß festgelegt werden, wie lange die empfangende Stelle die Mitteilungen aufbewahren und verwerten darf. Die entsprechenden Bestimmungen des BZRG könnten hierfür Anhaltspunkte geben. Überhaupt ist es geboten, die einschlägigen Regelungen des BZRG mit denen des neuen Gesetzes abzustimmen (vgl. dazu 3. TB, 3.12.1, S. 94).
- In Anbetracht der Bedeutung die das Bundesverfassungsgericht der Unterrichtung des Betroffenen eingeräumt hat –sie ist vielfach Voraussetzung für die Ausübung des Rechts auf informationelle Selbsbestimmung–, müssen die Betroffenen künftig grundsätzlich von Tatsache und Inhalt einer Mitteilung unterrichtet werden. Ausnahmen sollten nur zulässig sein, wenn andernfalls der Zweck des Strafverfahrens gefährdet wäre oder in der Person des Betroffenen besondere Gründe vorliegen. Meines Erachtens dürften der generellen Unterrichtung auch keine unüberwindlichen organisatorischen Schwierigkeiten entgegenstehen.

Als Übergangslösung bis zur Verabschiedung des neuen Gesetzes haben die Justizverwaltungen am 1.4.1985 eine leicht veränderte Fassung der MiStra in Kraft gesetzt. Wesentliche Grundsätze des Beschlusses des DSB-Konferenz vom 28.11.1983 (vgl. Anl. 2 zum 2. TB) sind dabei allerdings noch nicht berücksichtigt worden. Für eine relativ kurze Übergangszeit erscheint mir diese Regelung jedoch hinnehmbar.

4.11.3 Rechtsgrundlagen für die Mitteilungen in Zivilsachen

Die Überarbeitung der Anordnung über Mitteilungen in Zivilsachen (MiZi) (vgl. dazu schon meinem 2. TB, 3.13.1.2, S. 94) kommt nur langsam voran. Die Justizverwaltungen haben zwar eine umfassende Überprüfung der MiZi eingeleitet, Ergebnisse liegen jedoch noch nicht vor. Insbesondere zur Schaffung bereichsspezifischer Rechtsgrundlagen für die Mitteilungen nach der MiZi hat die Verwaltung noch keine Vorstellungen erarbeitet.

Die von der DSB-Konferenz eingeleitete Überprüfung der MiZi konnte im Berichtszeitraum abgeschlossen werden. Ein Arbeitskreis hat die verschiedenen Abschnitte der MiZi untersucht. Das Ergebnis ist den Justizverwaltungen im Spätsommer zugeleitet worden, Reaktionen stehen allerdings noch aus.

Die Datenschutzbeauftragten gehen bei der Beurteilung der MiZi und der Schaffung der gebotenen Rechtsgrundlagen von folgenden Grundsätzen aus:

- Ausgangspunkt der Überprüfung muß die Frage der Erforderlichkeit der Mitteilungen sein, denn viele bislang praktizierte Mitteilungen haben angesichts eines veränderten gesellschaftlichen Umfeldes und eines Wandels der Verwaltungsaufgaben ihren Sinn verloren. Soweit Mitteilungen weiterhin erforderlich bleiben, müssen sie nach Voraussetzungen, Inhalt, Umfang und Form in einer Rechtsvorschrift geregelt werden. Generalklauseln, nach denen Mitteilungen im Einzelfall auch dann zu machen sind, wenn sie zwar nicht ausdrücklich vorgeschrieben, aber durch ein besonderes öffentliches Interesse geboten sind, verstoßen gegen den Grundsatz der Normenklarheit und müssen entfallen.
- Grundsätzlich sollte sich die Übermittlung auf den Tenor der Entscheidung beschränken. Die Übermittlung von Entscheidungsgründen ist nur zuzulassen, wenn deren Kenntnis für die Aufgabenerfüllung der zu benachrichtigenden Behörde erforderlich ist.
- Wo eine Abwägung im Einzelfall zu erfolgen hat, ist sie durch den Richter oder im Rahmen der ihm nach dem RPflG übertragenen Aufgaben durch den Rechtspfleger wahrzunehmen.
- Die Übermittlungsvorgänge müssen transparenter gestaltet werden. Das Unbehagen vieler Bürger beim Umgang mit der öffentlichen Verwaltung rührt oftmals daher, daß diese über Kenntnisse verfügt, deren Herkunft den Betroffenen unbekannt ist. Wo es ohne unzumutbaren Aufwand möglich ist, sollte daher grundsätzlich vorgesehen werden, die von den Mitteilungen Betroffenen in geeigneter Weise über Inhalt, Adressat und zugrundeliegende Rechtsnorm zu unterrichten.
- Bei der Bestimmung der Empfängerbehörde ist auf einen funktionalen Behördenbegriff abzustellen. Eine genaue Bezeichnung des Empfängers (z.B. Jugendamt, Straßenverkehrsamt) dient Anforderungen, die das Bundesverfassungsgericht an die präzise Bestimmung des Verwendungszwecks geknüpft hat.
- Übermittelte Daten dürfen nur im Rahmen des Zwecks, zu dem sie übermittelt wurden, genutzt werden (Zweckbindung). Die Aufbewahrungsdauer ist, unter Berücksichtigung auch der Belange der Betroffenen, auf das erforderliche Maß zu beschränken.

4.11.4 Schuldnerverzeichnis

4.11.4.1 Novellierung des § 915 ZPO

In die bei den Amtsgerichten geführten Schuldnerverzeichnisse sind nach § 915 Abs. 1 ZPO die Personen einzutragen, die eine eidesstattliche Versicherung abgegeben haben oder gegen die zur Erzwingung einer eidesstattlichen Versicherung Haft angeordnet ist oder bei denen diese Haft sechs Monate lang vollstreckt wurde. Die Eintragungen werden nach Ablauf bestimmter, im Gesetz festgelegter Fristen – zum Teil, etwa bei Nachweis der Befriedigung des Gläubigers, auch vorzeitig - gelöscht. In die Schuldnerverzeichnisse kann jedermann Einsicht nehmen. Auch können Abschriften erteilt werden, wenn die Einhaltung der Löschungsfristen gewährleistet erscheint.

Das Verfahren ist bisher in § 915 ZPO und in den vom Bundesminister der Justiz erlassenen "Allgemeinen Vorschriften über die Erteilung und die Entnahme von Abschriften oder Auszügen aus den Schuldnerverzeichnissen" vom 1.8.1955 (Bundesanzeiger Nr. 156 vom 16.8.1955) geregelt.

Die bisherige Praxis insbesondere des weiten Streuens der in den Schuldnerverzeichnissen enthaltenen Informationen wird bereits seit Jahren unter Datenschutzgesichtspunkten kritisiert (vgl. 1 TB, Nr. 6.8.3, S. 47 f.). Nach dem Volkszählungsurteil des Bundesverfassungsgerichts steht nun endgültig fest, daß das bisherige Verfahren nicht aufrechterhalten bleiben kann. Der Bundesminister der Justiz plant deshalb eine Neufassung des § 915 ZPO, in die auch die jetzt in den "Allgemeinen Vorschriften" enthaltenen Regelungen übernommen werden sollen. Die bislang vorgelegten Entwürfe zur Änderung der Vorschriften über das Schuldnerverzeichnis und für eine Verordnung über die Erteilung von Abdrucken aus den Schuldnerverzeichnissen (Stand: jeweils 1.8.1985) können noch nicht als eine datenschutzrechtlich akzeptable Lösung angesehen werden.

Die jetzt vorliegenden Entwürfe enthalten zwar einige kleinere Verbesserungen der Position der Schuldner, die aus datenschutzrechtlicher Sicht zu begrüßen sind. Im Prinzip wird aber an dem gegenwärtig praktizierten Verfahren festgehalten, es soll lediglich auf eine formell einwandfreie Grundlage gestellt werden. Dem ist entschieden entgegenzutreten, da das heutige Verfahren des praktisch unkontrollierten Verteilens des Inhalts des Schuldnerverzeichnisses aus Datenschutzgesichtspunkten nicht länger hinnehmbar ist. § 915 ZPO muß mit dem Ziel geändert werden, dem Anspruch des Bundesverfassunggerichts gerecht zu werden, eine Rechtsordnung zu erreichen, in der der Bürger wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß.

Im einzelnen ist eine Regelung anzustreben, die folgende Grundsätze beachtet: Es ist akzeptabel, daß Industrie- und Handelskammern und andere Körperschaften des öffentlichen Rechts, in denen Angehörige eines Berufes kraft Gesetzes zusammengeschlossen sind, Abschriften aus dem Schuldnerverzeichnis erhalten können. Hier sollte die Verbreitung von Abschriften bzw. Vervielfältigungen jedoch enden, da eine breitere Streuung nicht mehr zu kontrollieren ist. Der Vorschlag des Entwurfs führt dieses Ergebnis jedoch nicht herbei; er ändert praktisch nichts an dem gegenwärtigen Zustand.

Zur Zeit gibt das Amtsgericht Hamburg zentral für alle Hamburger Amtsgerichte einmal monatlich Abschriften aus dem Schuldnerverzeichnis an einen Verlag, der diese "im Auftrag der Handelskammer Hamburg" vertreibt. Jedes Mitglied der Handelskammer, also jeder Gewerbetreibende, kann diese Mitteilungen abonnieren. Dabei kann meiner Auffassung nach nicht sichergestellt werden, daß die Empfänger dieser Mitteilungen – entsprechend ihren vertraglichen Verpflichtungen – die Löschungsfristen einhalten und sie nicht unberechtigterweise weitergeben.

Die vom Bundesminister der Justiz vorgelegten Entwürfe wollen zulassen, daß die Körperschaften, die die Abschriften aus dem Schuldnerverzeichnis erhalten, diese durch Dritte vervielfältigen und an die von den Körperschaften bestimmten Personen versenden lassen dürfen. Auch bei dieser Art des Vertriebs der Listen wäre nicht kontrollierbar, ob die Empfänger die Löschungsfristen einhalten und an wen sie die Listen möglicherweise weitergeben. Nach meiner Auffassung muß in die Neufassung des § 915 ZPO eine Regelung aufgenommen werden, nach der die Empfänger der Abschriften diese nicht vervielfältigen oder vervielfältigen lassen dürfen und sie auch nicht Dritten in anderer Form listenmäßig zur Verfügung stellen oder zur Verfügung stellen lassen dürfen. Auskünfte aus den Abschriften dürfen nur im Einzelfall erteilt werden und nur dann, wenn ein berechtigtes Interesse nachgewiesen wird.

Meinem Vorschlag, die Körperschaften Auskünfte nur im Einzelfall erteilen zu lassen, und dies auch nur dann, wenn ein berechtigtes Interesse nachgewiesen wird, wird entgegengehalten, mit diesem Auskunftsdienst der einzelnen Körperschaften für ihre Mitglieder sei ein unverhältnismäßiger Aufwand verbunden. Dieses Argument kann ich nicht akzeptieren: Ein Verfahren, das keine Gewähr für effektiven Datenschutz bietet,

kann nicht für rechtlich unbedenklich erklärt werden, weil das datenschutzrechtlich einwandfreie Verfahren mit einem gewissen Aufwand verbunden ist.

Auch ich halte es im übrigen für vertretbar, daß neben den genannten Körperschaften andere Stellen (ich denke dabei in erster Linie an Wirtschaftsauskunfteien und die Schufa) Abschriften aus dem Schuldnerverzeichnis sollen erhalten können, wenn sie sie für ihre gewerbliche Tätigkeit als Auskunftei benötigen und wenn sie ihrerseits Einzelauskünfte nur bei Nachweis eines berechtigten Interesses erteilen. Weiter sollen diese Stellen Abschriften nur erhalten können, wenn sie der regelmäßigen Kontrolle von Datenschutz-Aufsichtbehörden (4. Abschnitt des BDSG) unterliegen. Nur so kann eine wirksame Kontrolle gewährleistet werden.

Neben dieser zentralen Forderung müßten bei der Änderung des § 915 ZPO folgende Grundsätze beachtet werden:

Betroffene müssen ausführlicher und deutlicher als bisher über Inhalt und Verfahren des Schuldnerverzeichnisses unterrichtet werden. Die derzeit verteilten Hinweise verlieren sich im "Kleingedruckten" auf der Rückseite der Ladung zur Abgabe einer eidesstattlichen Versicherung und werden sicher nur von einem Bruchteil der Betroffenen inhaltlich zur Kenntnis genommen.

Eine Auskunftserteilung des Amtsgerichts aus dem Schuldnerverzeichnis an jedermann, wie sie in den Entwürfen des Bundesministers der Justiz vorgesehen ist, geht m.E. zu weit. Zumindest die Darlegung eines berechtigten Interesses durch den Anfragenden muß verlangt werden.

Der Betroffene muß über jede Auskunftserteilung aus dem Schuldnerverzeichnis (sei es im Einzelfall oder in Form von Abschriften) und über jede Auskunftserteilung aus den Abschriften unter Angabe des Empfängers der Auskunft benachrichtigt werden.

Es ist sicherzustellen, daß vorzeitige Löschungen an alle Empfänger von Auskünften weitergemeldet werden, um diese zu veranlassen, ebenfalls eine (vorzeitige) Löschung vorzunehmen.

Jede Weitergabe von Informationen aus dem Schuldnerverzeichnis (egal auf welcher Stufe) muß zwingend von einem Hinweis begleitet sein, wann genau die betreffende konkrete Information zu löschen ist.

Als Sanktion bei Verstößen gegen Schutzvorschriften sind neben dem Ausschluß von weiteren Auskünften bzw. Abschriften Ordnungsgelder und Geldbußen vorzusehen.

Zur genaueren Identifikation des Betroffenen sollte das Geburtsdatum –soweit möglich– mit in alle Eintragungen im Schuldnerverzeichnis aufgenommen werden.

Mit diesen Grundsätzen wird sichergestellt, daß weiterhin die Personen Informationen aus dem Schuldnerverzeichnis erhalten können, die diese aus wirtschaftlichen Gründen benötigen. Gleichzeitig wird aber auch erreicht, daß diese Informationen nicht – wie derzeit– unkontrolliert und unkontrollierbar breit gestreut und sogar von zweifelhaften Finanzierungsfirmen zur Werbung genutzt werden.

Dieser Mittelweg zwischen dem gegenwärtigen Zustand und einer radikalen Reduzierung des Zugangs zum Schuldnerverzeichnis auf Einsichtsrechte im Einzelfall erscheint als datenschutzrechtlich vertretbarer Weg zur Anpassung des § 915 ZPO an die vom Bundesverfassungsgericht postulierten Grundsätze, der gleichzeitig die Interessen des Wirtschaftsverkehrs angemessen berücksichtigt.

4.11.4.2 Werbung mit Angaben aus dem Schuldnerverzeichnis

In den letzten Monaten erreichten mich mehrere Beschwerden von Bürgern, die Werbung von Finanzvermittlern erhalten haben, welche die Anschriften offensichtlich aus den von dem o.g. Verlag vertriebenen Listen mit Angaben aus dem Schuldnerverzeichnis entnommen haben. In einzelnen Fällen wurde in den Werbeschreiben sogar indirekt auf die schlechte finanzielle Lage der Umworbenen Bezug genommen. Ich habe den Verlag über diese Entwicklung informiert. Da die Benutzung der Listen aus dem Schuldnerverzeichnis für Werbezwecke ein Mißbrauch ist, den auch dieser Ver-

lag nicht duldet, hat er in einigen Fällen den Beziehervertrag gekündigt. Darüber hinaus hat er alle Bezieher außerhalb von Hamburg eine Erklärung abgeben lassen, daß sie die Listen nicht für Werbezwecke nutzen.

Ich halte die Verwertung der Abschriften aus dem Schuldnerverzeichnis für Werbezwecke für eine zweckwidrige und unzulässige Nutzung. Daß derartige Fälle vorkommen, unterstreicht die Notwendigkeit, den Kreis der Bezieher der Abschriften aus dem Schuldnerverzeichnis bzw. deren Vervielfältigungen möglichst klein zu halten. Anders wird man Mißbräuche der Listen nicht ausschließen oder zumindest eindämmen können.

4.11.4.3 Löschung von Eintragungen im Schuldnerverzeichnis nur auf Antrag

Nach dem geltenden § 915 Abs. 2 ZPO werden Eintragungen im Schuldnerverzeichnis nur auf Antrag des Schuldners gelöscht, und zwar normalerweise nach drei Jahren, bei Nachweis der Tilgung der Schuld auch vor Ablauf dieser Frist. Es bedarf jedoch eines Antrags des Schuldners, was offenbar viele Schuldner nicht wissen, die – fälschlicherweise – erwarten, der Gläubiger werde bei Tilgung der Schuld automatisch das Amtsgericht informieren.

Für die Neufassung des § 915 ZPO ist es notwendig, zumindest nach Ablauf von drei Jahren die Eintragung automatisch zu löschen. Doch für vorzeitige Löschungen bei Tilgung der Schuld wird man auch in Zukunft nicht auf den Antrag des Schuldners verzichten können, da nicht sicherzustellen ist, daß der Gläubiger das Amtsgericht darüber informiert.

Bei der derzeit geltenden Rechtslage ist es für die Schuldner wichtig zu wissen, daß eine Löschung in jedem Fall nur auf ihren Antrag hin vorgenommen wird.

4.11.4.4 Automation des Schuldnerverzeichnisses bei dem Amtsgericht Hamburg

Die Justizbehörde plant, das Schuldnerverzeichnis beim Amtsgericht Hamburg zu automatisieren. Die Arbeiten im Zusammenhang mit der Schuldnerkartei, die derzeit etwa 180.000–200.000 Eintragungen umfaßt, können z.Z. nur noch unter großen Anstrengungen oder gar nicht mehr ordnungsgemäß durchgeführt werden. Die Zahl der Auskunftsersuchen hat in den letzten Jahren erheblich zugenommen (auf grob geschätzt 70.000 im Jahr 1985).

Die Konzeption zur Lösung dieser Probleme mit Hilfe der Automation wird z.Z. geprüft. Ich habe mir noch keine abschließende Meinung dazu gebildet.

4.11.5 Notare und Datenschutz

Hamburgische Notare sind bislang die einzigen öffentlichen Stellen (i.S. des § 2 Abs. 1 HmbDSG), die der Verpflichtung, die von ihnen geführten Dateien (Massekarteien, Erbvertragsverzeichnisse u.ä.) zum Datenschutzregister zu melden, nicht nachkommen. Um diesem Defizit abzuhelfen, habe ich im September 1984 die Notarkammer auf die Meldepflicht aufmerksam gemacht und um eine Stellungnahme gebeten.

Eine inhaltliche Antwort der Notarkammer steht noch immer aus.

4.12 Strafvollzug

Im Berichtszeitraum hatte ich mich – vornehmlich durch Eingaben einzelner Strafgefangener veranlaßt – erneut mit einer Reihe von Problemen aus dem Bereich des Strafvollzuges zu befassen. In den meisten Fällen konnte ich dabei einvernehmliche Lösungen mit dem Strafvollzugsamt erzielen. Beanstandungen waren nicht auszusprechen.

Auch in diesem Bereich gibt es jedoch diverse Informationseingriffe, die nicht auf – den Anforderungen des VZ-Urteils nach normenklaren und verhältnismäßigen Regelungen entsprechenden – Rechtsgrundlagen beruhen. Die Datenschutzbeauftragten sind daher daran gegangen, die Regelungsdefizite im Strafvollzugsgesetz zu analysieren und Novellierungsvorschläge zu entwickeln. Diese Arbeit ist jedoch nicht abgeschlossen.

Auch der Strafvollzugsausschuß der Länder hat jetzt Aktivitäten eingeleitet, um das StVollzG den präzisierten verfassungsrechtlichen Anforderungen anzupassen. Eine erste „Entwurfsskizze" für datenschutzrechtliche Ergänzungen des StVollzG liegt bereits vor. In dieser sind u.a. Regelungen vorgesehen über

- die Erhebung von Daten,
- Aktenführung und Aufbewahrungsfristen,
- besondere Geheimhaltungspflichten,
- Weitergabe personenbezogener Daten,
- Datenschutz für andere Personen als Gefangene.

Weitere Erörterungen und Überprüfungen sind erforderlich, auf der Grundlage der Entwurfsskizze jedoch auch gut möglich. Die Verfasser dieses Papiers haben offenbar nicht versucht, lediglich den Ist-Zustand festzuschreiben, sondern etwa zur Lösung der nachstehend dargestellten Probleme (4.12.1, 4.12.2) Vorschläge gemacht, die die – in den einzelnen Ländern allerdings unterschiedliche – Informationspraxis erheblich ändern würden.

4.12.1 Überprüfung von Besuchern

Ein Problembereich betrifft die Überprüfung der Besucher von Gefangenen. Nach § 25 StVollzG kann der Leiter einer Justizvollzugsanstalt Besuche untersagen, wenn die Sicherheit oder Ordnung der Anstalt gefährdet würde oder wenn zu befürchten ist, daß Besucher einen schädlichen Einfluß auf den Gefangenen haben oder seine Eingliederung behindern würden. Um hier sachgerechte Entscheidungen treffen zu können, ist der Anstaltsleiter auf Informationen angewiesen. Solche Informationen über Besucher, die aus dem Umfeld des Gefangenen stammen, sind in der Regel etwa aus Erzählungen des Gefangenen, aus der Überwachung früheren Besuchs- oder Schriftverkehrs (§§ 27, 29 StVollzG) sowie aus persönlichen Gesprächen mit den Besuchern bekannt. Ausnahmsweise besteht allerdings das Bedürfnis, zusätzliche Informationen einzuholen, etwa durch Auskünfte der Polizei oder anderer öffentlicher Stellen.

Für solche Maßnahmen gibt es z.Z. keine gesetzliche Grundlage, die den Anforderungen des VZ-Urteils entspricht: Ein Besucher kann dem StVollzG derzeit nicht entnehmen, ob und unter welchen Voraussetzungen er mit derartigen Überprüfungen zu rechnen hat. Die Justizbehörde hat diese Regelungslücke anerkannt, und die oben erwähnte Entwurfsskizze für datenschutzrechtliche Ergänzungen des StVollzG sieht auch für diesen Bereich Regelungen vor.

Für eine Übergangszeit bis zum Inkrafttreten der erforderlichen Rechtsgrundlagen können Regelungslücken nach der ständigen Rechtssprechung des BVerfG (E 33, 1; 41, 251; 51,268) gleichwohl unter bestimmten Voraussetzungen hingenommen werden. Es soll vermieden werden, daß eine Funktionsunfähigkeit staatlicher Einrichtungen entsteht, die der verfassungsmäßigen Ordnung noch ferner stünde als Eingriffsmaßnahmen auf unzureichender gesetzlicher Grundlage. Diese könnte entstehen, wenn das Strafvollzugsamt den Besucherverkehr wegen fehlender Überprüfungsbefugnisse einschränken müßte; denn die Beteiligung von Bezugspersonen eines Gefangenen bei den Bemühungen um seine Eingliederung ist ein wesentliches Element der Vollzugsplanung.

Die Überprüfungsmaßnahmen müssen während der Übergangszeit allerdings auf das Maß reduziert werden, das zur Vermeidung der Funktionsunfähigkeit unerläßlich ist, d.h. daß Auskünfte von anderen Stellen dürfen wirklich nur in absoluten Ausnahmefällen eingeholt werden.

4.12.2 Überprüfung von Bezugspersonen bei der Gewährung von Urlaub

Eine ähnliche Problematik wie bei der Überprüfung von Besuchern ergibt sich bei der Überprüfung von Bezugspersonen, bei denen Gefangene einen Hafturlaub verbringen wollen. Auch hier gibt es einen Informationsbedarf der Anstaltsleitung, denn sie hat

gem. § 11 Abs. 2 StVollzG zu prüfen, ob im Einzelfall die Gefahr einer Flucht oder eines Mißbrauchs der Vollzugslockerung zur Begehung neuer Straftaten besteht. Dies setzt Kenntnisse über Bezugspersonen voraus, die die Anstalt sich früher regelmäßig auch durch Anfragen bei anderen staatlichen Stellen verschaffte.

Auch in diesem Fall gibt es für die Überprüfung der Bezugspersonen keine Rechtsgrundlage, die den Anforderungen des VZ-Urteils gerecht wird. Im Unterschied zur Überprüfung der Besucher ist jedoch eine Überprüfung der Bezugspersonen ohne deren Einwilligung nicht unerläßlich zur Wahrung der Funktionsfähigkeit der Anstalt. Ein Gefangener ist ohnehin verpflichtet, an der Entscheidung über eine Vollzugslockerung mitzuwirken. So muß er u.a. den Nachweis führen, daß Unterkunft und Lebensunterhalt für die Dauer des Urlaubs sichergestellt sind. Es liegt daher nahe, den Gefangenen zu veranlassen, eine Einwilligungserklärung der Bezugsperson beizubringen, falls Nachforschungen für unumgänglich gehalten werden.

Ein entsprechendes Verfahren habe ich dem Strafvollzugsamt empfohlen. Es hat meiner Empfehlung entsprechend seine Praxis geändert.

4.12.3 Erteilung von Auskünften über Gefangene an Gläubiger

Mehrfach wurde ich um Auskunft gebeten, ob es rechtlich zulässig ist, daß eine Justizvollzugsanstalt Gläubigern eines Gefangenen mitteilt, ob dieser (noch) inhaftiert ist bzw. welches seine Entlassungsanschrift ist. Ich vertrete hierzu folgenden Standpunkt:

Rechtsgrundlage für die Beurteilung dieser Frage ist § 12 Abs. 2 Satz 1 HmbDSG. Danach ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und die Übermittlung wegen der Art der Daten oder wegen des Verwendungszwecks schutzwürdige Belange des Betroffenen nicht beeinträchtigt. Es ist also jeweils eine Abwägung vorzunehmen: Besteht ein über das normale Maß hinausgehendes berechtigtes Interesse an der Übermittlung, so müssen auch qualifizierte Belange der Betroffenen auf dem Spiel stehen, wenn sie überwiegen sollen.

Wenn nun ein anfragender Gläubiger – unter Hinweis etwa auf einen einzuklagenden Zahlungsanspruch oder eine schon titulierte Forderung – in schlüssiger Form sein berechtigtes Interesse darlegt, so führt die Abwägung mit den schutzwürdigen Belangen des Betroffenen im Regelfall zu folgenden Ergebnissen:

- Der Nachweis von Anschriften bestimmter Einwohner ist grundsätzlich Aufgabe der Meldebehörden (vgl. § 1 Abs. 2 MRRG, § 1 Abs. 1 HmbMG). Dementsprechend hat jedermann ohne nähere Begründung einen Anspruch auf einfache Melderegisterauskünfte (§ 34 Abs. 1 HmbMG). Der Anspruch läßt sich bei Gefangenen allerdings nur in beschränktem Umfang realisieren, da Freiheitsentziehungen nur in Ausnahmefällen meldepflichtig sind (§ 25 Abs. 1 Satz 2 HmbMG) und auch der Auskunftsanspruch nach Maßgabe des § 25 Abs. 2 HmbMG eingeschränkt ist. Sicher auskunftsfähig sind bei inhaftierten Personen also nur die jeweiligen Vollzugsanstalten.

  Deshalb werden schutzwürdigen Belange der Gefangenen in der Regel zurücktreten müssen, da etwaigen Gläubigern mangels anderer auskunftsfähiger Stellen eine Geltendmachung ihrer Ansprüche sonst unmöglich gemacht werden würde.

- Wenn Anfragen die Zustellungen von Mahnbescheiden o.ä. vorbereiten sollen, ist die JVA darüber hinaus auch befugt, den Anfragenden ggf. davon zu unterrichten, daß der Gefangene bereits in naher Zukunft entlassen werden wird, weil sonst Maßnahmen, die der Anfragende im Vertrauen auf die Richtigkeit der Auskunft ergreift, ins Leere gehen könnten. Der Gefangene wird eine solche zusätzliche Auskunft hinnehmen müssen, wenn seine Entlassung binnen eines Monats – des für Zustellungen normalerweise ausreichenden Zeitraums – bevorsteht (OLG Celle, Beschluß vom 21.9.1984, NStZ 1985, 44).

- Abzulehnen ist allerdings die Mitteilung von Entlassungsanschriften nicht mehr inhaftierter Gefangener. Hier greift wiederum die Zuständigkeit der Meldebehörde Platz. Es kann zwar unter Umständen schwierig sein, eine Anschrift auf diesem Wege zu ermitteln, weil zuständige Meldebehörden (Gemeinden) schwer zu ermitteln sind oder weil der Betroffene seinen Meldepflichten nicht nachgekommen ist. Diese Problematik gilt jedoch allgemein und ist vom Gesetzgeber (Verzicht auf ein Bundesadreßregister) in Kauf genommen worden. Sie kann nicht zu einer Erweiterung der Auskunftspflichten von Strafvollzugsanstalten führen.

  Eine Beeinträchtigung schutzwürdiger Belange des Betroffenen bei der Mitteilung von Entlassungsanschriften ergibt sich ferner aus folgenden Erwägungen: Die Verwendung von Daten eines Betroffenen ist – nach dem VZ-Urteil – grundsätzlich auf den gesetzlich bestimmten Zweck begrenzt. Eine zweckfremde Nutzung braucht der Betroffene also nicht zu dulden. Die Erhebung und Speicherung von Entlassungsanschriften hat nur den Zweck, die Abwicklung bestimmter Aufgaben des Vollzugs sicherzustellen. Ihr Zweck ist es nicht, Dritten – in Konkurrenz zu den Meldebehörden – Auskünfte über den Verbleib ehemaliger Gefangener zu geben.

4.13 Gesundheitswesen

4.13.1 Datenschutz im Krankenhaus

Der Datenschutz im Krankenhaus wirft nach wie vor erhebliche Probleme auf. Bereits vor Jahren hatte ich Gespräche mit den hamburgischen Krankenhausträgern geführt (vgl. dazu meinen 2. TB, 3.14.2, S. 96), die zur Einrichtung von Arbeitskreisen führten, welche federführend vom UKE sowie vom Landesbetrieb Krankenhäuser betreut wurden. Definitive, in Regelungen umgesetzte Ergebnisse haben diese Arbeitskreise jedoch nicht erbracht. Das UKE hat mir im Berichtszeitraum allerdings einen Entwurf für eine Dienstanweisung vorgelegt, die nur noch in unwesentlichen Punkten überarbeitet werden muß. Keine greifbaren Ergebnisse hat der Arbeitskreis erbracht, der sich mit dem Problem befassen sollte, ob und unter welchen Voraussetzungen Patientendaten zu Forschungszwecken übermittelt bzw. verwendet werden dürfen.

Vorangeschritten ist inzwischen die Diskussion im Kreise der Datenschutzkontrollinstanzen (Düsseldorfer Kreis, AK Sozialwesen der DSB-Konferenz). Die bisherigen Diskussionsergebnisse sowie die Erfahrungen, die ich zwischenzeitlich bei der Prüfung der Abrechnungsabteilung eines Allgemeinen Krankenhauses sammeln konnte (vgl. 4.13.1.1), haben mich in die Lage versetzt, der Gesundheitsbehörde und der Behörde für Wissenschaft und Forschung Ende des Jahres Vorschläge für normative Datenschutzregelungen vorzulegen (vgl. 4.13.1.2). Die weitere Beratung dieser Vorschläge (unter Einbeziehung der Ergebnisse des Düsseldorfer Kreises und der DSB-Konferenz) wird einer der Schwerpunkte meiner Tätigkeit im kommenden Jahr sein. Dabei setze ich meine Hoffnung darauf, durch die personelle Verstärkung meiner Dienststelle zusätzliche Kapazitäten für diesen wichtigen Bereich freimachen zu können.

4.13.1.1 Prüfung des AK Altona

Im Berichtszeitraum habe ich die Abrechnungsabteilung des AK Altona überprüft. Gegenstand der Prüfung war die Einhaltung datenschutzrechtlicher Vorschriften bei der Verarbeitung von Informationen zum Zwecke der Patientenverwaltung. Den Prüfvermerk habe ich dem Landesbetrieb Krankenhäuser im Dezember zugeleitet. Eine Stellungnahme kann daher noch nicht vorliegen, so daß die nachfolgende Darstellung als Zwischenbericht anzusehen ist.

Die Prüfung hat neben Verstößen gegen datenschutzrechtliche Vorschriften eine Reihe von grundsätzlichen Mängeln und Problemen deutlich gemacht, die ich nachfolgend kurz wiedergeben will.

4.13.1.1.1 Nicht erforderliche Erhebung von Daten

Bei der Aufnahme eines Patienten in ein allgemeines Krankenhaus werden mit dem

sog. Aufnahmesatz routinemäßig Daten in erheblich weiterem Umfang erhoben, als es zur Abwicklung des Behandlungsvertrages einschließlich der Abrechnung der erbrachten Leistungen mit den Kostenträgern sowie zur Durchführung sonstiger gesetzlicher Vorschriften (z.B. Melderecht, Personenstandsrecht) erforderlich ist.

Beim Aufnahmesatz handelt es sich um einen Durchschreibe-Schnelltrennsatz, der aus fünf Blättern besteht:

- dem Erfassungsbeleg: dieser wird für Abrechnungszwecke an die DVZ weitergeleitet, dort optisch gelesen und anschließend in der Rechnungsabteilung des Krankenhauses verwahrt;
- der Krankengeschichte: diese wandert als 1. Blatt der Krankenakte zur Station und wird nach der Behandlung im Krankengeschichtenarchiv verwahrt;
- dem 1. und 2. Kostenverpflichtungsschein: diese werden, soweit erforderlich, an die Krankenkasse weitergegeben;
- dem Aufnahmebeleg: bei diesem handelt es sich um eine Tasche, die den Rahmen der in der Forderungsabteilung geführten Aufnahmeakte abgibt. In der Aufnahmeakte werden alle für die Abrechnung relevanten Vorgänge gesammelt.

Mit dem Aufnahmesatz sollen die Daten erhoben werden, die die Krankenhaus-Verwaltung regelmäßig für ihre Aufgaben benötigt. Dazu gehören etwa Angaben von Identifikationsdaten (Name, Geburtsname, Anschrift), Patienten- und Krankenhaus-Identitäts-Nr., Aufnahmezeitpunkt, Abrechnungsschlüssel, Angaben zum Kostenträger, Hinweise auf frühere Behandlungen im Krankenhaus.

Neben diesen Daten werden jedoch routinemäßig einige weitere Daten erhoben und anschließend gespeichert, die nicht regelmäßig für Verwaltungszwecke benötigt werden, sondern allenfalls in besonders gelagerten Einzelfällen von Bedeutung sein können. Dazu gehören:

- Familienstand: diese Angabe ist regelmäßig überflüssig. Sie kann allenfalls in seltenen Einzelfällen aus vollstreckungsrechtlichen Gründen relevant werden, wenn Ehegatten – etwa bei Selbstzahlern und Wahlleistungen – mithaften;
- Geburtsort und Geburtsname: diese Angaben sind zu Identifikationszwecken nicht erforderlich. Sonstige Gründe sind nicht ersichtlich;
- Ausweis- oder Paßnummer: ebenfalls zur Identifizierung nicht erforderlich. Bei Zweifeln über Angaben des Patienten kann das Krankenhaus sich durch Vorlage der Ausweispapiere Gewißheit verschaffen;
- (bei Ausländern) Datum und Ort des Grenzübertritts: Gründe für die Notwendigkeit sind nicht erkennbar;
- Beruf/Arbeitgeber: diese Angaben können lediglich in den seltenen Fällen ungeklärter Kostentragungspflicht Hinweise auf etwaige Kostenträger geben;
- Name und Anschrift des einweisenden Arztes: diese Angaben können nur erforderlich werden, wenn der einweisende gleichzeitig nachbehandelnder Arzt sein soll, dem Befundbriefe, Arztbriefe o.ä. übersandt werden sollen. Diese Unterrichtung erfolgt jedoch nicht durch die Krankenhausverwaltung, sondern wird durch den stationär behandelnden Arzt ausgelöst. Es reicht daher aus, wenn die auf einweisende nachbehandelnde Ärzte bezogenen Daten in der Krankenakte notiert werden.
- Name und Anschrift von Angehörigen, die im Notfall zu unterrichten sind: diese Angabe ist zwar sinnvoll, aber freiwillig, worauf der Patient bei der Aufnahme hinzuweisen ist. Er ist ferner darüber zu unterrichten, daß der Angehörige von der Speicherung zu benachrichtigen ist. Es sollte erwogen werden, auch diese Daten nicht bei der Aufnahme, sondern auf der Station in der Krankenakte zu notieren.
- Religionszugehörigkeit: dieses Datenfeld ist zwar auf dem Aufnahmesatz noch enthalten. Entsprechende Angaben werden jedoch nicht mehr erfragt (vgl. hierzu auch 2. TB, 3.14.4, S. 98).

Da die vorstehend genannten Angaben zur Abwicklung des Behandlungsvertrages nicht regelmäßig und unmittelbar erforderlich sind, müssen die entsprechenden Datenfelder aus dem Aufnahmesatz gestrichen werden.

4.13.1.1.2 Unterlassene Verpflichtung auf das Datengeheimnis

Gem. § 5 Abs. 1 BDSG sind Personen, die bei der Datenverarbeitung beschäftigt sind, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis des § 5 Abs. 1 BDSG zu verpflichten. Diese Vorschrift gilt ohne Zweifel auch für die Mitarbeiter der Rechnungsabteilung und der Aufnahme. Dieser Personenkreis war im AK Altona noch nicht verpflichtet worden. Ich habe verlangt, dies umgehend nachzuholen.

4.13.1.1.3 Unterlassene Benachrichtigung gem. § 26 BDSG

Gem. § 26 BDSG sind Betroffene von der speichernden Stelle über die erstmalige Speicherung ihrer Daten zu unterrichten, soweit sie nicht auf andere Weise Kenntnis von der Speicherung erlangt haben. Solche Benachrichtigungen werden vom AK Altona nicht versandt. Bei der Bewertung ist nach mehreren Personengruppen zu differenzieren:

- Bei Patienten, die dem Krankenhaus als Vertragspartner – etwa bei der Aufnahme – selbst Angaben machen (z.B. den Aufnahmesatz ausfüllen) kann in aller Regel davon ausgegangen werden, daß sie von der Speicherung Kenntnis haben.
- Bei der Speicherung von Daten über dritte Personen: z.B. Angehörige, deren Name, Anschrift und Telefonnummer zwecks Benachrichtigung im Notfall gespeichert werden kann, regelmäßig unterstellt werden, daß die Patienten die von ihnen angegebenen Kontaktpersonen über die Speicherung unterrichten.
- Beim einweisenden Arzt wird ohne weiteres davon auszugehen sein, daß er von der Speicherung seiner Daten auf andere Weise Kenntnis erlangt hat. Soweit der weiterbehandelnde nicht mit dem einweisenden Arzt identisch ist, erscheint es vertretbar, darauf abzustellen, daß er mit dem Erhalt des Arztbriefes anderweitig Kenntnis von der Speicherung erlangt.

4.13.1.1.4 Weitergabe von medizinischen Daten an Kostenträger

Die Übermittlung medizinischer Daten (wie z.B. Diagnosen) an Kostenträger unterliegt unzweifelhaft der ärztlichen Schweigepflicht. Sie ist also nur zulässig, wenn eine entsprechende Offenbarungsbefugnis vorliegt.

Ich habe zunächst geprüft, ob sozialrechtliche Vorschriften eine Offenbarung zulassen. In Betracht kommt vornehmlich § 184 Abs. 1 RVO. Danach wird Krankenhauspflege nur dann gewährt, wenn die Aufnahme in ein Krankenhaus erforderlich ist, um die Krankheit zu erkennen oder zu behandeln oder Krankheitsbeschwerden zu lindern.

Man könnte argumentieren, die Prüfung der Anspruchsvoraussetzungen des § 184 Abs. 1 RVO durch den Kostenträger setzte die Kenntnis der Diagnose voraus. Ähnlich hat etwa das BSG für den Bereich des Kassenarztrechts in § 368 Abs. 2 Satz 2 RVO (wonach die kassenärztliche Versorgung die Ausstellung von Bescheinigungen und die Erstellung von Berichten umfaßt, die die Krankenkasse und der vertrauensärztliche Dienst zur Durchführung ihrer gesetzlichen Aufgaben benötigen) eine Offenbarungsermächtigung gesehen (vgl. BSGE 55, 150 ff.). Gegenüber einer solchen Argumentation ist jedoch insbesondere vor dem Hintergrund des VZ-Urteils des Bundesverfassungsgerichts erhebliche Skepsis anzumelden. Der Bürger, der i.d.R. von der Übermittlung der Diagnose nicht einmal Kenntnis haben dürfte, kann auf der Basis von § 184 Abs. 1 RVO in zumutbarer Weise nicht feststellen, welche Einschränkungen seines Rechts auf informationelle Selbstbestimmung er zu gewärtigen hat.

Sonstige Rechtsvorschriften der RVO, die eine Offenbarungsbefugnis enthalten, sind nicht ersichtlich.

Auch auf die traditionellen strafrechtlichen Rechtfertigungsgründe läßt sich die Verletzung der ärztlichen Schweigepflicht, die in der Weitergabe medizinischer Daten an den Kostenträger liegt, nicht stützen. Problematisch erscheint insbesondere die Berufung auf das Vorliegen einer konkludenten Einwilligung. Es wird die Ansicht vertreten, daß eine Person, die ärztliche Leistungen in Anspruch nimmt, dadurch gleichzeitig zu erkennen gibt, daß sie mit einer Offenbarung abrechnungsrelevanter Diagnosedaten einverstanden ist. Diese Annahme kann nicht überzeugen: Die Situation in der ärztlichen Sprechstunde und erst recht im Krankenhaus ist entscheidend durch die Hilfsbedürftigkeit des Patienten geprägt. Wenn dieser es geschehen läßt, daß der Arzt der Kassenärztlichen Vereinigung bzw. der zuständigen Krankenkasse Angaben über ihn offenbart, so liegt darin noch lange keine Einwilligung. Es ist schon sehr fraglich, ob wirklich alle Patienten wissen, wohin welche Informationen gehen; daß sie dies auch wollen, dürfte eine unbegründete Unterstellung sein.

Dieser Fall ist ein Beispiel dafür, daß das Instrument der (konkludenten) Einwilligung in der Praxis häufig überstrapaziert wird (vgl. auch 4.13.1.2.2). Ich verkenne zwar nicht, daß die Kostenträger in gewissem Umfang auch medizinische Daten benötigen, um die Voraussetzungen ihrer Leistungspflicht prüfen zu können. Es ist jedoch unumgänglich, hierfür rasch präzise gesetzliche Grundlagen zu schaffen. Für eine Übergangszeit — bis zur Schließung dieser Regelungslücken — halte ich eine Fortsetzung der Praxis nur mit der Maßgabe für akzeptabel, daß die Weitergabe von Daten auf das unerläßliche Mindestmaß reduziert wird. Auf die Vorlage vollständiger ärztlicher Aufzeichnungen, z.B. Arztbriefe und Entlassungsberichte, an Kostenträger muß also verzichtet werden.

4.13.1.1.5 Weitergabe von Todesbescheinigungen

Wenn ein Patient im Krankenhaus verstirbt, wird von dem Arzt, der die Leichenschau vorgenommen hat, die Todesbescheinigung ausgefüllt. Das Formular besteht aus 4 Blättern, Blatt 2 und 4 verbleiben bei dem die Todesbescheinigung ausstellenden Arzt. Das 1. Blatt ist als verschließbarer Umschlag ausgestaltet, auf dessen Innenseite sich der vertrauliche Teil der Todesbescheinigung (medizinische Daten, Todesursache) befindet. Der Umschlag wird zusammen mit dem 3. Teil dem Amtsarzt übergeben.

Da das BDSG auf die Daten Verstorbener keine Anwendung findet, ist dieser Vorgang allein unter dem Gesichtspunkt der ärztlichen Schweigepflicht zu würdigen. Diese gilt auch über den Tod hinaus.
Bedenken gegen das Verfahren beständen dann nicht, wenn die formularmäßig vorgesehene Vorgehensweise (Verschließung des vertraulichen Teils) tatsächlich eingehalten würde.

Dies ist indes in der Praxis regelmäßig nicht der Fall. Vor Verschließung des vertraulichen Teils werden die darin vorgenommenen Eintragungen durch die Rechnungsabteilung auf ihre Vollständigkeit überprüft. Dieses Verfahren wird mit der Erwägung begründet, daß eine fehlerhafte Ausfüllung der Bescheinigung von den Empfängern häufig beanstandet werde und deshalb schon im Vorfeld eine richtige Ausfüllung der Todesbescheinigung gewährleistet sein müsse. Auch im Interesse der Angehörigen, die erst nach korrekter Anzeige des Sterbefalles den Verstorbenen bestatten dürfen, werde diese Vorgehensweise praktiziert.

Diese Erwägungen vermögen die Durchbrechung der ärztlichen Schweigepflicht indessen nicht zu rechtfertigen. Im übrigen kann es doch nicht schwerfallen, durch eine präzise Aufklärung der die Todesbescheinigungen ausstellenden Ärzte eine korrekte Ausfüllung der Formulare sicherzustellen.

4.13.1.2 Notwendigkeit bereichsspezifischer Regelungen

Bislang gibt es nur in wenigen Bundesländern (Bayern, Berlin) Ansätze für bereichsspezifische Regelungen der Verarbeitung von Patientendaten in Krankenhäusern. In den meisten Ländern — so auch in Hamburg — ist die Zulässigkeit dieser Maßnahmen daher nach den allgemeinen Datenschutzgesetzen zu beurteilen. Dabei ergeben sich

jedoch zahlreiche Defizite, die – spätestens seit dem VZ-Urteil – nur durch präzisere gesetzliche Regelungen beseitigt werden können.

Die Befugnisse und Pflichten der Hamburger Krankenhäuser im Rahmen der Datenverarbeitung sind derzeit nach den Vorschriften des BDSG zu beurteilen, die die Datenverarbeitung nicht-öffentlicher Stellen für eigene Zwecke betreffen. Dies ergibt sich für die staatlichen Krankenhäuser aus § 2 Abs. 2 HmbDSG, denn es wird allgemein davon ausgegangen, daß auch Krankenhäuser am Wettbewerb teilnehmen. Gewisse Besonderheiten für das UKE, die daraus folgen, daß es in den Bereichen Ausbildung und Forschung besondere gesetzliche Aufgaben wahrzunehmen hat, muß ich hier vernachlässigen.

4.13.1.2.1 Defizite der BDSG-Regelung

Als generelles Defizit des geltenden BDSG ist zunächst festzuhalten, daß es die Erhebung von Daten nicht regelt. Im übrigen knüpft es die Zulässigkeit von Datenverarbeitungsmaßnahmen im wesentlichen an zwei Voraussetzungen: zum einen an die Zweckbestimmung eines Vertragsverhältnisses zwischen dem Betroffenen und der speichernden Stelle – also im hier interessierenden Zusammenhang an den Behandlungsvertrag; darüber hinaus läßt es jedoch auch Speicherungen und Übermittlungen zur Wahrung nicht näher definierter berechtigter Interessen der speichernden Stelle nach Abwägung mit den schutzwürdigen Belangen des Betroffenen zu (§§ 23 Satz 1, 2. Alt; 24 Abs. 1 Satz 1 letzte Alt.). Diese Regelung wird im Hinblick auf die besondere Eingriffsintensität der Verarbeitung medizinischer Daten der gebotenen Normenklarheit und dem notwendigen Schutz der Zweckbindung nicht annähernd gerecht.

Eine Verarbeitungsbefugnis aufgrund „berechtigter Interessen" des Krankenhauses ist mit dem Recht auf informationelle Selbstbestimmung nicht mehr vereinbar. Diese oben erwähnten Erlaubnistatbestände sollten daher bei verfassungskonformer einschränkender Auslegung des BDSG – jedenfalls im Krankenhausbereich – nicht angewandt werden. Vom Behandlungszweck nicht gedeckte Datenverarbeitungsmaßnahmen, etwa zu Zwecken der Planung, Statistik und Forschung, bedürfen einer speziellen gesetzlichen Ermächtigung, es sei denn, daß eine Einwilligung des Patienten – unter Berücksichtigung der unten (4.13.1.2.2) dargestellten Einschränkungen – als spezielle Rechtsgrundlage in Betracht kommt.

Ein weiteres Defizit des geltenden Datenschutzrechts besteht darin, daß es keine Regelungen für die im Krankenhausbereich noch relativ weit verbreitete nicht-dateimäßige Datenverarbeitung (z.B. Krankenakten) vorsieht. Auch diese Lücke muß durch eine bereichsspezifische Regelung geschlossen werden.

Schließlich gilt es, die Unsicherheiten zu beseitigen, die sich in der Praxis immer wieder daraus ergeben, daß neben dem allgemeinen Datenschutzrecht auch die Wahrung der ärztlichen Schweigepflicht zu berücksichtigen ist. Die z.T. konkurrierenden Vorschriften des Arztrechts und des Datenschutzrechts sind durch eine bereichsspezifische Regelung in Übereinstimmung zu bringen.

4.13.1.2.2 Zur Problematik von Einwilligungserklärungen

Die – im Strafrecht im Gegensatz zum allgemeinen Datenschutzrecht – bestehende Möglichkeit, die Weitergabe medizinischer Daten an Dritte auch durch eine konkludente Einwilligung des Patienten zu rechtfertigen, verführt in der Praxis häufig dazu, für notwendig gehaltene Maßnahmen mit dem Vorliegen angeblicher Einwilligungen zu begründen. Dementsprechend gibt es Bestrebungen, die Datenverarbeitungsmaßnahmen der Krankenhäuser mit Allgemeinen Geschäftsbedingungen oder Vertragsklauseln abzusichern, die der Patient dann bei der Aufnahme zu unterzeichnen hätte. Diesen Lösungsansatz halte ich für außerordentlich problematisch.

Vielfältige soziale Zwänge, denen der behandlungsbedürftige Patient unterliegt, stützen die Zweifel, daß es sich bei der Datenverarbeitung auf der Grundlage der Einwilligung nur um eine „Scheinfreiwilligkeit" handelt. Bei der Notaufnahme Schwerverletzter oder gar Bewußtloser ist die freie Entscheidung des Patienten jedenfalls aus-

zuschließen. Selbst die der freien Arztwahl vergleichbare Entscheidung für die Behandlung in einem bestimmten Krankenhaus wird durch die regional unterschiedliche Krankenhausdichte und die in bestimmten medizinischen Fachbereichen bestehenden Engpässe relativiert.

Der Patient kann regelmäßig im Krankenhaus nicht behandelt werden, wenn er nicht zu einem Mindestmaß an Mitwirkung bei der Datenerhebung bereit ist (vgl. die Parallele zur Obliegenheit des Sozialleistungsberechtigten; § 60 SGB I). Da er Angaben im Zusammenhang mit Krankenhausleistungen zu machen hat, von denen er abhängig ist, sind, wie in Fällen gesetzlichen Auskunftszwangs, bereichsspezifische Regelungen erforderlich. Hinzu kommt noch, daß der Umfang der Datenerhebung und die Verwendungszusammenhänge angesichts der komplizierten Organisation von Krankenhäusern sowie ihrer komplexen internen und externen Kommunikation selten hinreichend verdeutlicht werden können. Die Aufklärung des Betroffenen ist jedoch unabdingbare Voraussetzung einer rechtswirksamen Einwilligung. Angesichts der Unsicherheiten in der Beurteilung der Zulässigkeit der Informationsverarbeitung im Krankenhaus muß deshalb Tendenzen entgegengewirkt werden, die Befugnisse zur Datenerhebung und -speicherung nicht auf den Zweck der Behandlung zu begrenzen, sondern durch Einwilligung zu erweitern. Es verbietet sich deshalb auch, die Allgemeinen Geschäftsbedingungen immer detaillierter auszugestalten und damit das informationelle Selbstbestimmungsrecht des Patienten auszuhöhlen. Nicht zuletzt steht die nicht seltene Berufung auf das therapeutische Privileg und die daraus resultierende Informationszurückhaltung gegenüber dem Patienten einer Einwilligungslösung entgegen. Die Einwilligung kann daher nur als Rechtsgrundlage für die Datenerhebung und -speicherung in Betracht kommen, wenn dem Patienten eine echte Entscheidungs-und Wahlfreiheit offensteht. Der Datenschutz will den eigenverantwortlichen Handlungsspielraum des Betroffenen erhalten und nach Möglichkeit erweitern. Dies kann jedoch bei der Verarbeitung von Patientendaten nicht bedeuten, daß auf eine normenklare, notwendige Beschränkungen des informationellen Selbstbestimmungsrechts verdeutlichende gesetzliche Regelung verzichtet und stattdessen auf eine regelmäßig nur scheinbar mögliche eigenständige Entscheidung des Patienten abgestellt wird.

4.13.1.2.3 Zweckbindung und Patientengeheimnis

Eine weitere Frage, auf die bislang weder das ärztliche Standesrecht noch das allgemeine Datenschutzrecht eine eindeutige Antwort geben, betrifft die interne Nutzung der Patientendaten in einem Krankenhaus. Mit der ärztlichen Schweigepflicht kann das Problem schon deshalb nicht gelöst werden, weil diese in ihrer überkommenen Form an ein personales Vertrauensverhältnis zwischen dem Patienten und seinem Arzt anknüpft. Diese Betrachtungsweise wird jedoch der besonderen Lage eines Patienten, der die Dienstleistung eines komplexen, arbeitsteilig organisierten Betriebes wie eines Krankenhauses in Anspruch nimmt, nicht gerecht. Persönliche Vertrauensbeziehungen kommen hier nur selten zum Tragen; an der Wiederherstellung der Gesundheit des Patienten sind vielmehr zahlreiche Fachkräfte beteiligt, die er z.T. gar nicht mehr persönlich kennenlernt.

Die Zweckbindung der Daten und das aus dem konkreten Arzt-Patientenverhältnis abzuleitende Arztgeheimnis gestatten es nicht, das Krankenhaus insgesamt als eine Einheit anzusehen, die alle zu krankenpflegerisch-ärztlichen, diagnostischen Zwekken einerseits und zur verwaltungsmäßigen Abwicklung andererseits erforderlichen Daten zentral an einer Stelle erheben und verarbeiten darf. Der funktionsbezogene, organisatorische Einsatz des Personals muß generell berücksichtigt werden.

Zwar ist der Arztgehilfe zur Mitkenntnis von Patientendaten berechtigt, soweit er sie zur Erfüllung seiner jeweiligen Aufgabe benötigt. Der Umfang seiner Kenntnis ist jedoch grundsätzlich durch das Erforderlichkeitsprinzip begrenzt. Deshalb dürfen Verwaltungsbedienstete in Krankenhäusern Daten lediglich erheben und verarbeiten, soweit sie sie zu Verwaltungszwecken, insbesondere zur Abrechnung, benötigen. Es ist nicht gerechtfertigt, den Umfang der durch die Verwaltung zu erhebenden Daten mit

der Begründung zu erweitern, daß die Daten zu medizinischen Zwecken benötigt werden (z.B. Anzahl der Kinder). Auch im Interesse der Aufgabenerleichterung kann die Befugnis der Krankenhausverwaltung nicht erweitert werden, weil sonst die Grenzen der zulässigen Datenerhebung durch die Verwaltung nicht mehr eindeutig festgestellt werden können. Der Arzt soll lediglich von solchen Tätigkeiten befreit sein, die nicht typisch medizinischer Natur und deshalb auch weniger eingriffsintensiv sind. Da Verwaltungsdaten der Krankenhausbehandlung zu dienen bestimmt sind, dürfen sie indessen auch zu krankenpflegerischen und ärztlichen Zwecken genutzt werden. Die grundsätzliche Abschottung zwischen den verwaltungs- und der ärztlich-krankenpflegerischen Funktion führt zwar nicht zu einer Vorenthaltung von Verwaltungsdaten gegenüber dem Arzt. Die Funktionsbezogenheit zulässiger Informationsverarbeitung im Krankenhaus sowie das persönliche Vertrauensverhältnis zwischen Arzt und Patient erfordern jedoch, daß nur der jeweils behandelnde Arzt auf Verwaltungsdaten zugreifen und Behandlungsdaten erheben und speichern darf. Organisatorisch-technische Maßnahmen haben die funktionsbezogene Verwendung sicherzustellen. Alle den Krankenhausbediensteten bekannt gewordenen Daten (einschließlich der Tatsache des Krankenhausaufenthaltes) unterliegen jedoch dem Patientengeheimnis.

4.13.1.2.4 Resümee und Konsequenzen

Die vorstehenden Überlegungen machen deutlich, daß die baldige Schaffung bereichsspezifischer Grundlagen der Datenverarbeitung im Krankenhaus unverzichtbar ist. Um den Diskussionsprozeß zu beschleunigen, habe ich der Gesundheitsbehörde Ende 1985 nicht nur die Notwendigkeiten begründet, sondern zugleich einen ausformulierten Gesetzesvorschlag zugeleitet, den ich gemeinsam mit anderen Datenschutzbeauftragten erarbeitet habe. Dieser Gesetzentwurf enthält Regelungen für folgende Sachverhalte:

- Anwendungsbereich eines solchen Gesetzes;
- Erhebung und Speicherung von Patientendaten;
- Weitergabe von Patientendaten mit besonderen Vorschriften zur Weitergabe an Kostenträger sowie zu Forschungszwecken;
- Auskunfts- und Akteneinsichtsrechte der Patienten;
- Löschung von Daten;
- interne Verarbeitung und Verwendung;
- Datensicherung;
- Datenschutzbeauftragte für jedes Krankenhaus;
- Datenverarbeitung von Patientendaten im Auftrag (insbesondere Mikroverfilmung).

4.13.2 Gesundheitsämter

Wie im 3. TB (3.13.1, S. 95 f.) bereits erwähnt, habe ich im Jahr 1984 ein Bezirksgesundheitsamt geprüft. Die Auswertung dieser Prüfung bereitete meiner Dienststelle besondere Schwierigkeiten und zog sich daher bis Ende des Jahres 1985 hin. Dies hatte mehrere Gründe: Zunächst einmal handelte es sich um die erste breiter angelegte Querschnittsprüfung, die meine Mitarbeiter durchführten. Wir konnten daher noch nicht auf die Prüferfahrungen und -routinen zurückgreifen, die sich mittlerweile angesammelt haben. Bei dieser Prüfung stießen wir überdies auf eine Dienststelle, die ganz unterschiedliche Aufgaben zu erfüllen hat und zu den unterschiedlichsten Zwekken außerordentlich große Mengen an personenbezogenen Daten verarbeitet (vgl. 3. TB a.a.O.). Es erforderte schon einen beträchlichen Aufwand, die diversen Informationsverarbeitungsvorgänge überhaupt zu erfassen. Überdies mußten wir feststellen, daß es so gut wie keine normativen Regelungen für die Informationsverarbeitung gibt, so daß uns keine konkreten Kontrollmaßstäbe zur Verfügung standen. Wir mußten Kontrollmaßstäbe, so gut es ging, also selbst entwickeln. Gegen Ende des Berichtszeitraumes habe ich die Auswertung einstweilen abschließen und dem Bezirksge-

sundheitsamt sowie der Gesundheitsbehörde zur Stellungnahme zuleiten können. An dieser Stelle möchte ich meine wichtigsten Feststellungen referieren und deutlich machen, wo ich rechtspolitischen Handlungsbedarf sehe.

4.13.2.1 Zweckkollisionen bei der Zentralkartei

Das Gesundheitsamt erhebt und verarbeitet –wie erwähnt– personenbezogene Daten zur Erfüllung einer Vielzahl von Aufgaben. Dabei tritt es dem Bürger in völlig unterschiedlicher Weise gegenüber:
Zum einen nimmt es Aufgaben der Gefahrenabwehr wahr, erfüllt also die Funktionen der Gesundheitspolizei im klassischen Sinne. Dazu gehört etwa der Vollzug des Bundesseuchengesetzes, aber auch die Überwachung der Medizinalpersonen. Es tritt den betroffenen Bürgern dabei hoheitlich gegenüber, erhebt und verarbeitet personenbezogene Daten also zwangsweise.

Zum zweiten erfüllt es Aufgaben der Gesundheitshilfe, bietet also unterschiedlichen Personengruppen Beratung und Betreuung an. Dazu gehören etwa der sozialpsychiatrische Dienst, die Fürsorge für Körperbehinderte sowie die Säuglings- und Kleinkinderfürsorge. Zur Inanspruchnahme dieser Dienstleistungen ist niemand verpflichtet. Sie beruhen auf der absolut freien Mitwirkung der Betroffenen (eine gewisse Sonderrolle, die ich hier allerdings vernachlässigen muß, kommt dabei nur der Schulgesundheitspflege zu, die ebenfalls den Gesundheitsämtern obliegt).
Schließlich ist das Gesundheitsamt die zuständige Stelle für die Ausstellung von amtlichen Gutachten und Gesundheitszeugnissen, die den unterschiedlichsten Zwecken dienen können. Die Begutachtung erfolgt teils zwangsweise, teils auf Antrag der Betroffenen.

Aus dieser völlig unterschiedlichen Zielrichtung der verschiedenen Aufgabenbereiche ergaben sich besondere Anforderungen für die Wahrung des Rechts auf informationelle Selbstbestimmung. Um sicherzustellen, daß die bei den verschiedenen Aufgaben anfallenden Daten nur zu dem jeweiligen Erhebungszweck verwendet werden, ist vor allem eine klare Trennung der einzelnen Datenbestände voneinander geboten. Es liegt auf der Hand, daß z.B. die Tatsache, daß ein Bürger Beratungsdienste des Gesundheitsamtes in Anspruch genommen hat (oder gar Tatsachen, die er dem Beratungspersonal dabei anvertraut) nicht ohne weiteres etwa zur Erfüllung seuchenpolizeilicher Zwecke gegen ihn verwendet werden dürfen.

Nach meinen Feststellungen wird den unterschiedlichen Funktionen im Gesundheitsamt nicht hinreichend Rechnung getragen. Vielmehr wird das Gesundheitsamt generell als Einheit betrachtet. Dies kommt vor allem darin zum Ausdruck, daß eine gemeinsame Zentralkartei geführt wird, die zur Auffindung der meisten im Gesundheitsamt vorhandenen personenbezogenen Vorgänge genutzt wird. Die Führung einer solchen gemeinsamen Nachweiskartei ist nach meiner Auffassung mit dem verfassungsrechtlichen Grundsatz der Zweckbindung nicht vereinbar. Ich habe daher ihre Auflösung gefordert. Welche Alternativ-Lösungen in Betracht kommen, muß noch im einzelnen geklärt werden.

Aufgabe des Gesetzgebers wird es sein, die unterschiedlichen Zwecke bei der Verarbeitung personenbezogener Daten präzise festzulegen und voneinander abzugrenzen.

4.13.2.2 Gutachterwesen

Nach § 1 Nr.5 der 2. Durchführungsverordnung (2.DVO) zum Gesetz über die Vereinheitlichung des Gesundheitswesens vom 22.2.1935 hat das Gesundheitsamt amtliche Zeugnisse in allen Fällen auszustellen, in denen die Beibringung eines amtsärztlichen Zeugnisses vorgeschrieben ist. § 20 der 2. DVO bestimmt ferner, daß das Gesundheitsamt Privatpersonen amtliche Zeugnisse ausstellen darf, soweit ihm eine amts- oder vertrauensärztliche Tätigkeit übertragen worden ist. Nähere –allgemeine– Bestimmungen zum Verfahren bei der Erstellung der Gutachten fehlen. Ob und –wenn ja–welche Daten an den Veranlasser der Begutachtung bzw. an Dritte weitergegeben

werden dürfen und in welcher Weise der Betroffene dabei zu beteiligen ist, ist völlig ungeregelt. Dementsprechend uneinheitlich und für den Betroffenen wenig transparent wird in der Praxis verfahren.

Anlässe für Gutachten ergeben sich aus diversen Gesetzen und Verordnungen sowie z.T. auch nur aus Verwaltungsvorschriften. Zu nennen sind hier beispielsweise Führerscheintauglichkeit, Unterbringung in Kinderheimen oder psychiatrischen Einrichtungen, Bewilligung bestimmter Leistungen nach dem BSHG und dem Lastenausgleichsgesetz (LAG), Bewilligung von Steuerermäßigungen, Zeugnisse nach dem Bundesseuchengesetz, Aufenthaltsgenehmigungen für Ausländer etc., also alle Anlässe zu amtsärztlicher Überprüfung, die in Hamburg nicht speziellen ärztlichen Diensten (wie dem Personalärztlichen Dienst, dem Ärztlichen Dienst der Behörde für Inneres oder dem Versorgungsärztlichen Dienst) zugewiesen sind.

Die Verarbeitung der bei der Anfertigung der Gutachten und Zeugnisse gewonnenen Daten erfolgt in unterschiedlicher Weise: Es gibt zum einen spezielle Sammlungen von Vorgängen über Ausländer sowie über Personen, die mit Lebensmitteln in Berührung kommen sollen. Die amtsärztlichen Untersuchungen dieser Personenkreise werden ständig in erheblichem Umfang durchgeführt.

Die amtsärztliche Untersuchung von Ausländern ist nicht gesetzlich vorgeschrieben, sondern wird lediglich in der Verwaltungsvorschrift zum Ausländergesetz gefordert. Hier besteht also ein Regelungsbedarf. Die Ergebnisse der Untersuchungen werden der Behörde für Inneres (Ausländerbehörde) mitgeteilt. Dies verstößt mangels gesetzlicher Offenbarungsbefugnisse gegen die ärztliche Schweigepflicht, soweit der Patient den Amtsarzt nicht hiervon entbunden hat (vgl. dazu schon 3. TB, 3.7.3.2, S. 59 f.).

Personen, die berufsmäßig mit Lebensmitteln in Berührung kommen, müssen sich gem. § 18 BSeuchG regelmäßig amtsärztlich untersuchen lassen und diese Untersuchung ihrem Dienstherrn gegenüber nachweisen. Die detaillierten medizinischen Ergebnisse der genannten Untersuchungen verbleiben beim Gesundheitsamt und werden drei Jahre lang aufbewahrt. Sie sind dort z.T. alphabetisch, z.T. chronologisch geordnet. Materielle Bedenken gegen diese Speicherung, die lediglich Dokumentationszwecken dient, bestehen nicht.

Von allen amtsärztlichen Gutachten, die aus anderen Anlässen als den vorstehend beschriebenen erstellt werden, verbleibt ebenfalls eine Durchschrift im Gesundheitsamt und wird dort in Stehordnern – nach lfd. Nummern sortiert – aufbewahrt. Die Auffindung bestimmter Gutachten namentlich bekannter Personen geschieht mit Hilfe der Zentralkartei (so. 3. TB 2.1). Die Aufbewahrungsfrist beträgt 10 Jahre. Ich habe erhebliche Zweifel, ob die Aufbewahrung der Gutachtendoppel im Gesundheitsamt überhaupt erforderlich ist. Hier könnte es sich um unzulässige Vorratsdatenhaltung zu unbestimmten oder noch nicht bestimmbaren Zwecken handeln. Vor einer abschließenden Bewertung dieser Frage sind allerdings noch weitere Erörterungen erforderlich. Dabei wird ggf. auch die Frage der Speicherungsdauer zu klären sein (10 Jahre im Gegensatz zu drei Jahren bei den eingangs genannten amtsärztlichen Untersuchungen).

4.13.2.3 Überwachung des Medizinalwesens

Das Gesundheitsamt nimmt die Aufgabe der Aufsicht über die staatlich geregelten Berufe des Medizinalwesens wahr. Gemäß § 1 der 3. DVO zum Gesetz über die Vereinheitlichung des Gesundheitswesens vom 30.3.1935 hat es Listen über die in seinem Bezirk selbständig oder in abhängiger Stellung arbeitenden Medizinalpersonen zu führen. Nach § 1 Abs. 2 ist für jede Berufsart (also Ärzte, Krankenpflegepersonal, Heilpraktiker) eine besondere Liste zu führen; die Führung als Kartei ist statthaft.
Die Anlieferung der Daten erfolgt in der Weise, daß die verschiedenen Kliniken die Zu- und Abgänge der verschiedenen Gruppen von Medizinalpersonen monatlich in Listenform melden. Diese Listen werden in chronologischer Reihenfolge abgeheftet und nach Kliniken sortiert in Stehordnern aufbewahrt. Zusätzlich wird eine Karteikarte

für jede gemeldete Person angelegt und – nach Klinik, Beruf und Alphabet sortiert– gespeichert. Die Aufbewahrungsdauer für diese Speicherung ist unklar: Karteikarten von abgemeldeten Personen werden nicht vernichtet, sondern in einer besonderen, "toten" Kartei gesammelt. Dies wird damit begründet, daß ein Betroffener im Falle einer Wiederanmeldung nicht erneut seine Berechtigung zur Ausübung des Berufes nachweisen muß. Das reicht nach meiner Auffassung nicht aus, um das überwiegende Allgemeininteresse an der weiteren Speicherung der Daten zu begründen.

Neben den Medizinalpersonen überwacht das Gesundheitsamt nach § 3 der 3. DVO den Geschäftsbetrieb der Apotheken. Zu diesem Zweck erfaßt es Apotheker, Apothekenverwalter und –personal in Stehordnern, die nach den Apotheken des Bezirks sortiert sind. An– und Abmeldungen erfolgen durch die Apothekenkammer. Die Unterlagen werden nach derzeitiger Praxis aufbewahrt, solange eine Apotheke existiert. Präzise Regelungen über die Verarbeitung der Daten gibt es nicht.

Zur Überwachung des Medizinalwesens gehört schließlich die Überwachung des Verkehrs mit Betäubungsmitteln (BTM). Zu diesem Zweck sammelt das Gesundheitsamt vorsorglich alle BTM-Rezepte, die in den Apotheken des Bezirks eingelöst werden. Das Verfahren läuft so, daß die Apotheken per Post eingelöste BTM-Rezepte einsenden. Von diesen werden zwei Kopien gemacht. Die Originale der Rezepte werden nach Kontrolle durch die zuständige Ärztin in Umschlägen nach Apotheken sortiert aufbewahrt. Eine Kopie wird unter dem Namen des verschreibenden Arztes einsortiert, die zweite geht an den Sozial-Psychiatrischen Dienst des Gesundheitsamtes. Dieses Verfahren erscheint mir in mehrfacher Hinsicht bedenklich. Die vollständige Anforderung und Aufbewahrung aller Rezepte dürfte schon über die einschlägigen Verwaltungsvorschriften hinausgehen. Die Grundlage für die Vorlage der Rezepte findet sich in den §§ 5 Abs. 5 und 7 Abs. 3 der BTM-Verwaltungsvorschrift. Danach hat der Apothekenleiter Teil I und der verschreibende Arzt Teil II der dreiteiligen BTM-Rezepte chronologisch geordnet drei Jahre lang aufzubewahren und "auf Verlangen" des Bundesgesundheitsamtes oder der nach § 19 Abs. 1 BTM-G zuständigen Behörde einzureichen. Von einer vollständigen Registrierung der Abgabepraxis aller Apotheken sowie der Verschreibungspraxis von Ärzten bei den Gesundheitsämtern ist nicht die Rede, und dies dürfte auch kaum im überwiegenden Allgemeininteresse erforderlich sein.

Große Bedenken habe ich auch gegen die routinemäßige Weiterleitung einer Kopie der Rezepte an den Sozialpsychiatrischen Dienst, die diesem ermöglichen soll, Suchtkranken vorsorgend zu helfen. Hier dürfte es sich um eine zweckwidrige Verwendung der erlangten Informationen handeln. Der Zweck der Ablieferung von Rezepten nach der BTM-VV besteht ausschließlich in der Kontrolle des Betäubungsmittelverkehrs.

Die gleichzeitige Registrierung der Rezeptempfänger, also der behandelten Patienten könnte zwar im Einzelfall die Feststellung ermöglichen, ob z.B. jemand unter ständigem Wechsel des Arztes eine Vielzahl von Betäubungsmittelrezepten sammelt und gebraucht. Sie hätte damit z.B. wegen § 29 Abs. 1 Nr. 9 BTM-G (Erschleichen von Verschreibungen aufgrund unrichtiger Angaben) überwiegend strafverfolgenden Charakter. Das breit angelegte Sammeln von Hinweisen auf einen möglichen strafbaren Betäubungsmittel-Mißbrauch durch die Registrierung aller BTM-Patienten ist jedoch nicht Aufgabe des Gesundheitsamtes nach der BTM-VV.

Nach § 6 HmbPsychKG sollen die Gesundheitsämter zwar durch vorsorgende Hilfe dazu beitragen, daß der Betroffene (Suchtkranke) schon bei Anzeichen einer Störung behandelt werden kann. Diese Aufgabe besteht aber vor allem darin, adäquate Einrichtungen zur Verfügung zu halten. Sie begründet keinesfalls eine Befugnis zur Speicherung personenbezogener Daten. Nach allem ist eine gründliche Überprüfung bei der Praxis der Überwachung des BTM-Verkehrs dringend geboten.

4.13.2.4 Sammlung von Geburts- und Todesbescheinigungen

Die Gesundheitsämter erhalten von den Krankenhäusern (über die Standesämter) ein Exemplar der von den Ärzten oder Hebammen auszustellenden Geburtsbescheinigungen. (Zum Inhalt dieser Unterlagen vgl. bereits 3.TB, 3.13.2, S.96). Der Zweck die-

ser Bescheinigungen besteht für das Gesundheitsamt darin, zu prüfen, ob der Mutter ein Angebot zur Unterstützung im Rahmen der Mütterberatung unterbreitet werden kann.

Die Rechtsgrundlage für die Aufbewahrung der Geburtsbescheinigungen durch das Gesundheitsamt ergibt sich aus Nr. III, B. 6 der Ausführungsbestimmungen zum Gesetz über das Gesundheitswesen vom 15.3.1920. Die Aufbewahrungsfrist beträgt z.Z. 15 Jahre. Dies erscheint mir jedoch für die Zwecke des Gesundheitsamtes auf keinen Fall gerechtfertigt.

Ferner erhält das Standesamt nach Nr. III, C.6 der o.g. Ausführungsbestimmungen jeweils ein Exemplar der Todesbescheinigungen und bewahrt diese für einen Zeitraum von 30 Jahren auf. Der Zweck dieser Datensammlung besteht in der Überwachung der sorgfältigen Ausstellung von Todesscheinen durch die Ärzte und der in gesundheitlich in einwandfreier Weise zu erfolgenden Leichenbeförderung. Ob dies allerdings bei zeitgemäßer Betrachtungsweise die Übermittlung und Speicherung aller Todesbescheinigungen rechtfertigt, halte ich für sehr zweifelhaft. Ebenfalls nicht erforderlich erscheint mir eine 30-jährige Aufbewahrungsfrist.

Sowohl die Registerierung der Geburts- als auch die der Todesbescheinigungen muß gründlich überprüft und ggf. auf einwandfreie Rechtsgrundlagen gestellt werden.

4.13.2.5 Beratung durch Psychiatrischen Dienst

Nach § 6 HmbPsychKG haben die Gesundheitsämter die Aufgabe, psychisch Kranken vorsorgende Hilfe anzubieten. Zur Durchführung dieser vorsorgenden Hilfe halten sie – gemäß § 7 HmbPsychKG – regelmäßig Sprechstunden ab, um im Einzelfall festzustellen, ob und in welcher Weise geholfen werden kann. Erforderlichenfalls werden auch Hausbesuche gemacht.

Das Gesundheitsamt wartet allerdings nicht nur ab, daß psychisch Kranke sich bei ihm melden, sondern es geht auch gezielt auf solche Personen zu und bietet ihnen Hilfe an. Datenschutzrechtliche Probleme ergeben sich in diesem Zusammenhang aus folgendem: Um gezielt psychisch Kranke ansprechen zu können, werden die Gesundheitsämter von einer Vielzahl staatlicher Einrichtungen über Vorgänge unterrichtet, die als Anlaß für eine psychiatrische Beratung in Betracht kommmen könnten. Zu nennen sind hier beispielsweise:

- Mitteilungen aus der Überwachung des BTM-Verkehrs (vgl. 4.13.2.3);
- Mitteilungen von der Polizei über Suizidversuche (vgl. 2. TB, 3.10.5.2, S. 84);
- Mitteilungen von den Gerichten über vorläufige Vormundschaften und Entmündigungen.

Ich habe erhebliche Zweifel, ob routinemäßige Mitteilungen im derzeitigen Umfang für die Aufgabenstellung des Gesundheitsamtes erforderlich sind. Speziell nachgegangen bin ich dieser Frage am Beispiel der gerichtlichen Mitteilungen über vorläufige Vormundschaften und Entmündigungen, die auf der Grundlage von Ziff. III 3 Abs. 2 c der Anordnung über Mitteilungen in Zivilsachen (MiZi) erfolgen. Ich habe zu diesem Zweck stichprobenartig ca. 60 derartige Vorgänge beim Gesundheitsamt überprüft. Eine Erforderlichkeit der Mitteilungen habe ich dann als gegeben angenommen, wenn aufgrund der Mitteilung Tätigkeiten des Gesundheitsamtes veranlaßt wurden.

Im Ergebnis habe ich folgendes festgestellt:

- In keinem einzigen der von mir überprüften Vorgänge sind durch die Mitteilung Aktivitäten des Gesundheitsamtes gegenüber den Entmündigten oder unter vorläufige Vormundschaft gestellten Person veranlaßt worden.
- In über 90% der von mir geprüften Fälle bestand der Vorgang lediglich aus einer Durchschrift des amtsgerichtlichen Beschlusses, z.T. sind sogar lediglich Aufhebungsbeschlüsse vorhanden.

Unter Berücksichtigung dieses Ergebnisses haben die Datenschutzbeauftragten die Streichung dieser Mitteilungspflicht in der MiZi gefordert. Dem sind die zuständigen

Stellen jedoch bislang nicht nachgekommen (vgl. 4.11.3). Es besteht nach diesen Feststellungen auch Veranlassung, die Erforderlichkeit anderer Routine-Mitteilungen einmal gründlich zu überprüfen.

Ein weiteres Problem der Informationsverarbeitung beim sozialpsychiatrischen Dienst besteht darin, daß einmal erlangte Informationen erst nach sehr langer Zeit wieder gelöscht werden.

Es gibt zwar eine Dienstanweisung des Gesundheitsamtes zu „Aufbewahrungsfristen ärztlicher Vorgänge/Akten" vom 15.6.1971. Die dort vorgesehenen Fristen erscheinen mir – jedenfalls für den sozialpsychiatrischen Dienst – zu lang und werden in der Praxis häufig auch noch überschritten. So bin ich bei meinen Überprüfungen auf Vorgänge (z.B. Suizidmeldungen) gestoßen, die länger als 20 Jahre zurücklagen. Ich bin generell der Auffassung, daß Informationen über Betroffene, die die Beratungsangebote des Gesundheitsamtes nicht annehmen wollen, alsbald – längstens nach etwa einem halben Jahr – zu löschen sind.

4.13.2.6 Sonstige Feststellungen

Neben den von mir dargestellten Informationssammlungen gibt es noch zahlreiche andere, die jedoch nach meinen Feststellungen keine besonderen materiellen Probleme aufwerfen. Es handelt sich in erster Linie um Unterlagen über Klienten, die vom Gesundheitsamt überwacht werden (z.B. Geschlechtskranke, Dauerausscheider und sonstige – nach dem BSeuchG – meldepflichtige Personen) oder betreut werden (z.B. im Rahmen der Fürsorge für Schwangere, für Säuglinge und Kleinkinder, Körperbehinderte).

Gewisse Besonderheiten gibt es im Schulärztlichen und Schulzahnärztlichen Dienst. Diesen Bereich habe ich jedoch noch nicht in eine gründliche Prüfung einbezogen. Hier bietet sich eine Prüfung im Zusammenhang mit der Informationsverarbeitung an den Schulen an.

Festzustellen waren ferner diverse Verstöße gegen Gebote der Datensicherheit, die hier jedoch nicht im einzelnen dargestellt werden können. Häufig besteht keine Klarheit darüber, daß auch ein Unterlassen den Tatbestand einer Schweigepflichtverletzung erfüllen kann: Es sind auch technische, organisatorische, bauliche und personelle Vorkehrungen zu treffen, die geeignet sind, eine Offenbarung medizinischer Daten an Unbefugte zu verhindern.

In anderen Fällen waren Bediensteten diese Pflichten durchaus bewußt, die gebotenen Maßnahmen scheiterten jedoch an finanziellen Engpässen.

Abschließend gestatte ich mir den Hinweis, daß es für – möglicherweise für notwendig zu erachtende – Auswertungen von Unterlagen der Gesundheitsämter zu Zwecken epidemiologischer Forschung nur sehr unvollkommene Rechtsgrundlagen gibt. Ich verweise hierzu auf meine Ausführungen zum Forschungsprojekt „Dioxin und frühkindliche Mißbildungen" im 3. TB (3.14.1, S. 97).

4.13.2.7 Resümee

Insgesamt hat die Prüfung mir gezeigt, daß es dringend notwendig ist, für die Informationsverarbeitung in den Gesundheitämtern ein den heutigen Anforderungen entsprechendes Fundament zu schaffen. In den letzten 60 Jahren – seit Inkrafttreten des Gesetzes über die Vereinheitlichung des Gesundheitswesens (GVGw) – hat sich eine Informationspraxis entwickelt, die mit dem gewandelten Grundrechtsverständnis nicht mehr in Einklang zu bringen und möglicherweise auch aus anderen Gründen nicht mehr zeitgemäß ist. Aus diesen Gründen gehört eine kritische Überprüfung des öffentlichen Gesundheitsdienstes und eine darauf aufbauende Formulierung präziser, bereichspezifischer Grundlagen für die Informationsverarbeitung zu den Aufgaben, die besonders vordringlich sind. Andere Länder (Berlin, Schleswig-Holstein) haben schon Schritte in die richtige Richtung genommen, das GVGw aufgehoben und neue Gesetze über den öffentlichen Gesundheitsdienst verabschiedet. Hamburg darf hier nicht länger zurückstehen.

4.14 Sozialwesen

Nach wie vor hat die Verwaltung mit der Handhabung des Sozialdatenschutzes Schwierigkeiten.

Seit meinen Ausführungen hierzu im 2. TB (3.15, S. 98 ff.) sind zwar erfreulicherweise die Probleme des Datenschutzes sehr viel deutlicher in das Blickfeld und auch in das Bewußtsein der Mitarbeiter in der Sozialverwaltung und den sozialen Diensten gerückt; jedoch habe ich festgestellt, daß die Sensitivität hierfür in den einzelnen Trägerbereichen und bei den einzelnen Mitarbeitern teilweise recht unterschiedlich ist. Der Lernprozeß, der mit dem Inkrafttreten des SGB X eingesetzt hat, ist noch in vollem Gange.

Erhebliche Bedeutung auch für die Datenverarbeitung in der Sozialverwaltung hat das VZ-Urteil des Bundesverfassungsgerichts, dessen Anforderungen auch in dem spezifischen Bereich des Sozialrechts zu berücksichtigen sind. Spätestens nach dieser Entscheidung können Hinweise auf die Gefährdung des Verwaltungsablaufs und auf die unbeschränkte Amtshilfepflicht der Behörden nicht mehr gleichrangig dem Recht des Bürgers auf Schutz seiner Sozialdaten gegenübergestellt werden. So darf auch die Sozialverwaltung nur ausnahmsweise dann Amtshilfe leisten, wenn die zuständige Behörde selbst nicht in der Lage ist, die notwendigen Angaben – vor allem durch Einschaltung des Bürgers – auf andere Weise zu beschaffen.

Nach meinen Feststellungen neigt die Sozialverwaltung weiterhin dazu, Daten auf Vorrat zu sammeln, was nicht erst seit dem VZ-Urteil des Bundesverfassungsgerichts ohne Zweifel unzulässig ist. Dies gilt auch für Daten, die einem Mitarbeiter der Sozialverwaltung zwar bei Wahrnehmung einer bestimmten Aufgabe vom Bürger mitgeteilt worden sind, die aber zur Erfüllung dieser Aufgabe nicht benötigt werden.

Daraus folgt, daß nicht alle Daten, die von den Mitarbeitern der Sozialverwaltung und der sozialen Dienste in Erfahrung gebracht werden, auch aufbewahrt werden dürfen.

Schließlich ein paar Worte zu der vielfach noch anzutreffenden Praxis, Datenerhebungen mit der Einwilligung der Betroffenen zu rechtfertigen. Bei meinen Prüfungen von Teilen der Sozialverwaltung, über die ich weiter unten berichte, habe ich festgestellt, daß des öfteren pauschale Einwilligungen formularmäßig verlangt werden. Dabei versucht die Sozialverwaltung, in den Vordrucken möglichst viele denkbare Fallkonstellationen in einem vorformulierten Text zu berücksichtigen. Es liegt auf der Hand, daß eine solche Erklärung dem Betroffenen nicht hinreichend verdeutlicht, welche Tragweite die Einwilligung hat; insbesondere wird ihm nicht klar, welche Offenbarungen möglich oder beabsichtigt sind. Deshalb sind pauschale Einwilligungen nicht zulässig.

4.14.1 Prüfung der Ämter für Ausbildungsförderung

In Hamburg werden die Aufgaben nach dem Bundesausbildungsförderungsgesetz (BAföG) von verschiedenen Behörden wahrgenommen. So sind die Bezirksämter als Amt für Ausbildungsförderung zuständig für Auszubildende an

- weiterführenden allgemeinbildenden Schulen und Fachoberschulen;
- Abendhauptschulen, Berufsaufbau- und Abendrealschulen, Abendgymnasien, Kollegs und vergleichbaren Einrichtungen;
- Berufsfachschulen einschl. der Klassen aller Formen der beruflichen Grundbildung und Fachschulen;
- höheren Fachschulen und Akademien;
- Ergänzungsschulen;
- Ausbildungsstätten nach § 2 Abs. 3 BAföG.

Das Studentenwerk ist Amt für Ausbildungsförderung für Auszubildende der Hochschulen in Hamburg, während die Behörde für Wissenschaft und Forschung – Landesamt für Ausbildungsförderung – diese Aufgaben wahrnimmt, soweit es zu fördernde Ausbildung im Ausland und Fernunterrichtslehrgänge von Auszubildenden,

die ihren ständigen Wohnsitz in Hamburg haben und Auszubildenden an einer Hochschule gleichgestellt sind, betrifft.

Ich habe bei meiner datenschutzrechtlichen Überprüfung der Ämter für Ausbildungsförderung keine gravierenden Verstöße gegen die gesetzlichen Vorschriften festgestellt.

So sind auch die umfangreichen Informationen von dem Auszubildenden, seinen Eltern, seinem Ehegatten u.a. notwendig, damit die Ämter für Ausbildungsförderung den Bedarf des Auszubildenden berechnen können.

Ich habe allerdings festgestellt, daß mit Hilfe des bundeseinheitlich vorgeschriebenen Formblattes 3/83 Daten von den Eltern, dem Ehegatten und den Kindern des Ehegatten des Auszubildenden erfragt werden, die für die Bestimmung der Höhe der Ausbildungsförderung nicht erforderlich sind. So habe ich Zweifel, ob z.B. die Frage nach den Wohnverhältnissen der Kinder (bei den Eltern/nicht bei den Eltern) für die Berechnung der Ausbildungsförderung erforderlich ist. Ich werde deshalb darauf hinwirken, daß eine bundeseinheitliche Überarbeitung des Vordrucks erfolgt.

Bedenklich erscheint mir auch, daß der Auszubildende seinen Vermieter von seinem Antrag auf Ausbildungsförderung zu unterrichten hat bzw. dieser indirekt darüber informiert wird, sofern der Auszubildende Zusatzleistungen über den Regelbedarf hinaus, wie die Kosten der Unterkunft, geltend macht. Gem. § 9 Abs. 3 der Härteverordnung zum BAföG hat der Auszubildende durch Vorlage einer schriftlichen, von ihm selbst und dem Vermieter unterschriebenen Vereinbarung die Höhe der Kosten für die Unterkunft nachzuweisen. Da der Nachweis auch anderweitig, und zwar ohne die Einbeziehung des Vermieters, möglich wäre, sollte nach meiner Meinung § 9 Abs. 3 der Härteverordnung entsprechend geändert werden.

Beim Bezirksamt Hamburg-Mitte, das auch zuständig ist für die Gewährung von Ausbildungsbeihilfe nach dem Gesetz über Ausbildungsbeihilfen für Schüler, habe ich festgestellt, daß in die BAföG-Akte auch die Ausbildungsbeihilfe-Akten übernommen wurden, sofern der Antragsteller eine entsprechende Leistung erhalten hat. Eine Berechtigung für diese Verfahrensweise vermag ich nicht zu erkennen, weil die Ausbildungsbeihilfe nach einer völlig anderen gesetzlichen Regelung bewilligt wird. Die Ausbildungsbeihilfe-Akten sind daher nach bestimmten Fristen zu vernichten und dürfen nicht wie bisher der BAföG-Akte vorgeheftet werden.

Ich habe im übrigen durch Stichproben ermitteln können, daß die bestehenden Vernichtungsfristen für die BAföG-Akten weitgehend eingehalten worden sind. In 2 Fällen habe ich eine Fristüberziehung festgestellt.

Eine Besonderheit beim Studentenwerk ist die Micro-Verfilmung bereits abgeschlossener Förderungsakten, die bis zur endgültigen Rückzahlung der als Darlehen gewährten Ausbildungsförderung aufbewahrt werden müssen. Da der Bundesminister für Bildung und Wissenschaft erst seit dem 1.7.85 die Vernichtungsfristen von Förderungsakten geregelt hat, sind bis zu diesem Zeitpunkt beim Studentenwerk weder Akten noch micro-fiches vernichtet worden. Es ist deshalb erforderlich, daß dort der Aktenbestand durchgesehen und die nicht mehr benötigten Förderungsakten und micro-fiches vernichtet werden.

4.14.2 Prüfung der Wohngelddienststelle des Bezirksamtes Eimsbüttel

Bei der Überprüfung der Informationsverarbeitung in der Wohngelddienststelle des Bezirksamtes Eimsbüttel habe ich keine nennenswerten datenschutzrechtlichen Mißstände in der Verwaltungspraxis feststellen können. Die gewichtigsten Kritikpunkte ergaben sich im Vordruckwesen. Sie lassen sich weitgehend unter dem Stichwort „mangelnde Tansparenz" zusammenfassen. Sei es, daß in dem Wohngeldantragsformular ein Hinweis auf die Rechtsgrundlagen für die Fragen fehlt (z.B. Auskunftspflicht des Antragstellers gem. § 60 SGB I i.V.m. den Vorschriften des Wohngeldgesetzes) oder daß dem Antragsteller die Freiwilligkeit einzelner Fragen nicht deutlich gemacht wird. Ich habe im übrigen festgestellt, daß einige Fragen offensichtlich für die Gewäh-

rung von Wohngeld nicht erforderlich sind, so daß ich eine Überarbeitung der Fragebogen gefordert habe.

Ich habe außerdem festgestellt, daß eine Reihe von Daten aus der Bearbeitung von Wohngeldanträgen an das Statistische Landesamt übermittelt wird. Dort werden auf Hamburg bezogene aus aggregierten Daten bestehende Übersichten erstellt, aus denen allein kein Personenbezug herzustellen ist. Dennoch ist die Wohngeldnummer, die einen Personenbezug ermöglicht, weiterhin auf den Magnetbändern gespeichert, von denen eine Kopie an das Statistische Bundesamt übersandt und ein Exemplar 10 Jahre lang aufbewahrt wird. Dieser statistischen Verarbeitung der Daten des Antragstellers steht eine irreführende Aufklärung in den Wohngeldanträgen gegenüber, in denen es heißt, daß die erbetenen Daten auch anonym, d.h. ohne Namen, Anschrift und Wohngeldnummer für statistische Zwecke verwendet werden können.

Die Übermittlung der Daten mit der Wohngeldnummer an das Statistische Bundesamt ist an § 11 Abs. 2 Bundesstatistikgesetz zu messen. Danach ist der Datenaustausch von Einzelangaben zwischen den an der Bundesstatistik beteiligten Stellen zulässig, soweit dies für die Erstellung der Bundesstatistik erforderlich ist. Da eine Plausibilitätskontrolle nach meinen Informationen aber bereits auf Landesebene stattfindet, ist für eine Übermittlung der Wohngeldnummer keine Notwendigkeit mehr erkennbar. Deshalb ist zukünftig darauf zu verzichten.

4.14.3 Prüfung der Informationsverarbeitung im Bereich der Jugendbehörden Hamburgs

Im Berichtszeitraum habe ich die Informationsverarbeitung im Amt für Jugend der BAJS und – stellvertretend für die Bezirksverwaltung – im Jugendamt des Bezirksamtes Bergedorf geprüft. Die Bezirksverwaltung und die BAJS haben das Ergebnis meiner Prüfung in einem Arbeitskreis diskutiert und inzwischen zu meinen Feststellungen und Hinweisen Stellung genommen.

Da meine Gespräche mit der Verwaltung darüber noch nicht abgeschlossen sind, gebe ich hiermit in Form eines Zwischenberichtes meine ersten Eindrücke wieder.

Auch die Jugendbehörden sind verpflichtet, personenbezogene Daten nur in dem Umfang zu erheben, wie dies zur Erfüllung ihrer Aufgaben unbedingt erforderlich ist. Dies ergibt sich schon aus dem verfassungsrechtlich verankerten Grundsatz der Verhältnismäßigkeit, der durch die Sozialgesetze näher konkretisiert wird. Über diesen Maßstab geht die derzeitige Praxis der Jugendbehörden nach meinen Feststellungen vielfach hinaus.

Desweiteren wird der Bürger häufig darüber im unklaren gelassen, welche Daten er nach welchen gesetzlichen Bestimmungen offenbaren muß und welche Angaben freiwillig erfolgen können. Einen entsprechenden Hinweis nach § 9 Abs. 2 BDSG habe ich oft in den verwendeten Formularen nicht gefunden. Auch wird nicht auf ggf. bestehende Auskunftsverweigerungsrechte aufmerksam gemacht. Bei Vordrucken ist mir außerdem aufgefallen, daß der Bürger des öfteren Erklärungen zu unterschreiben hat, mit denen er in die Einholung „aller notwendigen Auskünfte" bzw. in die Einsichtnahme in – nicht näher spezifizierte – Unterlagen oder Schweigepflichtentbindungen mehr oder minder pauschal einwilligt. Derartige Erklärungen sind weder hinreichend präzise noch gewährleisten sie die notwendige Transparenz über den Umfang der Datenerhebungen im Einzelfall. Meine Anmerkungen und Hinweise haben dazu geführt, daß gegenwärtig eine grundsätzliche Überarbeitung der Formulare für die Jugendbehörden erfolgt.

Problematisch ist aus meiner Sicht auch die gegenwärtige Praxis, Jugendfürsorgeakten und Sammelmappen nach dem Familienprinzip zu führen. Dadurch werden die Geschwister eines betreuten Minderjährigen in der Akte und der Zentralkartei miterfaßt, um ggf. aus einem späteren Anlaß auf die Familienakte zugreifen zu können. Die BAJS hat in ihrer Stellungnahme hierzu zwar dargelegt, daß sie ein solches Verfahren auch zukünftig aus pädagogischer Sicht für erforderlich hält, um

- die Zahl der eventuellen Bezugspersonen,

- die Generationsfolge der Bezugspersonen und
- die Stellung des aufzunehmenden Kindes in der Geschwisterreihe feststellen zu können;

jedoch sieht die BAJS ebenfalls das bei einer Aktenübersendung auftretende Problem der Offenbarung nicht erforderlicher Daten. In den weiteren Gesprächen wird es deshalb darum gehen, eine Umsetzung des Sozialdatenschutzes bei der Aktenübersendung zu erreichen.

Im nächsten Tätigkeitsbericht werde ich eingehend über die Informationsverarbeitung im Bereiche der Jugendbehörden Hamburgs berichten.

4.14.4 Prüfung einer Betriebskrankenkasse (BKK)

Im Berichtszeitraum habe ich mich zu erstenmal eingehend mit der Datenverarbeitung in einer BKK, die als juristische Person des öffentlichen Rechts der Aufsicht der Freien und Hansestadt Hamburg untersteht, befaßt. Meine Gespräche über das Ergebnis der Prüfung sind noch nicht abgeschlossen. Deshalb beschränke ich mich an dieser Stelle darauf, erste Eindrücke als Zwischenbericht wiederzugeben. Im nächsten Jahr werde ich ausführlich über das Ergebnis berichten.

Die BKK sammelt nach meinen Erkenntnissen eine Vielzahl von Daten, die von der Geburt bis zum Tode reichen, ohne Vorsorge dafür zu treffen, daß veraltete bzw. nicht mehr benötigte Angaben aus dem Leistungsbereich und dem persönlichen Umfeld des Mitglieds sowie seiner Familienangehörigen gelöscht werden. Bei der Mitgliedsbestandsführung auf Karteikarten ist es zugegebenermaßen sehr mühsam, überholte Angaben zu entfernen. Die Nutzung der ADV, die in der von mir geprüften BKK gerade begonnen hat, bietet jedoch die Chance, veraltete Daten relativ mühelos zu löschen. Diese Gelegenheit sollte durch eine entsprechende Programmgestaltung genutzt werden. Die Umstellung auf ADV könnte es auch ermöglichen, die Krankenakten in Zukunft so zu führen, daß alte Leistungsfälle ständig aussortiert und vernichtet werden können.

Ich habe außerdem den Eindruck gewonnen, daß die BKK durch Formulare und Erhebungsbogen von ihren Mitgliedern vorsorglich möglichst viele Informationen abfragt, um erst danach zu entscheiden, was notwendig ist und was nicht. Es fehlt auf den Vordrucken durchweg der Hinweis, welche Fragen notwendigerweise aufgrund einer Rechtsgrundlage und welche Fragen freiwillig zu beantworten sind. Eine entsprechende Überarbeitung der Vordrucke ist deshalb erforderlich.

Weiterhin ist mir aufgefallen, daß die BKK eine große Anzahl medizinischer Daten in Form von Diagnosen, Befunden, Therapievorschlägen, Krankenhausberichten, Begutachtungen usw. anfordert und sammelt, um die Notwendigkeit einzelner Verordnungen und Leistungen zu überprüfen. Ich habe Zweifel, ob die Mitarbeiter der BKK über den medizinischen Sachverstand verfügen, um die behandelten Krankheiten eines Mitgliedes und die damit zusammenhängende Notwendigkeit von Verordnungen beurteilen zu können. Dies ist Aufgabe des Vertrauensärztlichen Dienstes. Informationen aus der Gesundheitssphäre der Mitglieder sollten grundsätzlich aus dem Herrschaftsbereich des Vertrauensarztes nicht hinausgelangen.

4.14.5 Datenerfassung im Verfahren Kriegsopferversorgung

Die hamburgische Versorgungsverwaltung (Behörde für Arbeit, Jugend und Soziales – Versorgungsamt Hamburg –) hat die Aufgabe, die Leistungen an Kriegsbeschädigte und deren Hinterbliebene nach dem Bundesversorgungsgesetz (BVG) sowie an andere Personenkreise nach Gesetzen des sozialen Entschädigungsrechts (Opferentschädigungsgesetz, Häftlingshilfegesetz, Soldatenversorgungsgesetz, Zivildienstgesetz) zu berechnen und zahlbar zu machen. Das Versorgungsamt Hamburg ist zuständig für Anspruchsberechtigte mit Wohnsitz oder gewöhnlichem Aufenthalt in Hamburg, im Bereich der Kriegsopferversorgung darüber hinaus für Berechtigte mit Wohnsitz oder gewöhnlichem Aufenthalt in bestimmten europäischen und außereuropäischen Staaten.

Zur Erledigung dieser Aufgabe hat der Senat der FHH mit dem Land Niedersachsen ein Abkommen getroffen (siehe Bürgerschaftsdrucksache 10/501 vom 11.11.1982), in dem die Inanspruchnahme des Rechenzentrums beim Landesversorgungsamt Niedersachsen für Zwecke der Versorgungsverwaltung Hamburg geregelt wird. Danach übernimmt das Rechenzentrum beim Landesversorgungsamt Niedersachsen im Wege der Auftragsdatenverarbeitung die maschinelle Verarbeitung der Daten der Anspruchsberechtigten des Versorgungsamtes Hamburg.

Für die maschinelle Erfassung der Daten im Versorgungsamt Hamburg und für die Übertragung der Daten zum Rechenzentrum in Hannover sowie für die Übertragung von Fehlerprotokollen aus Verarbeitungsläufen im RZ in umgekehrter Richtung wird ein intelligentes Datenerfassungssystem mit Anschluß an eine Datenfernübertragungsleitung eingesetzt. Die Kontrolle des Rechenzentrums in Hannover obliegt dem Niedersächsischen Datenschutzbeauftragten. Er ist auch zuständig für die Überwachung des automatisierten Verfahrens, (das von den Ländern Niedersachsen, Bremen, Hessen, Saarland und Schleswig-Holstein gemeinsam entwickelt worden ist und in diesen Ländern angewendet wird,) soweit es im Rechenzentrum in Hannover eingesetzt wird. Die Datenerhebung und -erfassung im Versorgungsamt Hamburg sowie die Datenfernübertragung nach Hannover unterliegen meiner Kontrolle. Außerdem habe ich zu kontrollieren, ob das Versorgungsamt als Sozialleistungsträger (§§ 24, 25 SGB I, §§ 79, 80 SGB X) die Bestimmungen über die Datenverarbeitung im Auftrag (§§ 8, 6 BDSG) beachtet hat.

Im Berichtsjahr habe ich geprüft, ob im Versorgungsamt Hamburg die nach § 6 BDSG erforderlichen technischen und organisatorischen Maßnahmen getroffen worden sind. Die wesentlichen Regelungen für das Datenerfassungssystem sind in einer Verwaltungsanordnung aus dem Jahr 1982 niedergelegt. Die einzelnen technischen und organisatorischen Maßnahmen wurden an den Anforderungen aus der Anlage zu § 6 BDSG gemessen mit dem Ergebnis, daß sie in ihrer Gesamtheit (als System) einen ausreichenden Stand der Datensicherung gewährleisten. Schwächen im Detail werden, wie ich festgestellt habe, durch erhöhte Aufsicht und Dokumentation der Aufträge ausgeglichen.

Die eigentliche Verarbeitung der Daten aus der Versorgungsverwaltung läuft in einem Rechenzentrum unter den für zentrale Verarbeitung geltenden Bedingungen (Sicherheitssystem, Dokumentation, Freigabeverfahren, Funktionstrennung usw.) ab. Die Anwendung ist nur hinsichtlich der Datenerfassung „dezentral".

Ich habe – entgegen meiner Absicht – noch keine Prüfung dezentraler autonomer DV-Anlagen durchgeführt. Dies wird im Hinblick auf die Ausführungen unter 3.3 im nächsten Jahr zwingend erforderlich.

4.15 Wissenschaft und Forschung

Nach wie vor bereitet die Lösung des Zielkonfliktes zwischen dem Schutz des informationellen Selbstbestimmungsrechts einerseits und Forschungsinteressen andererseits in der Praxis große Schwierigkeiten. Diese werden ohne eine klare gesetzliche Regelung auch nicht zu überwinden sein. In meinem 2. TB (3.16.1., S. 163) hatte ich bereits dargestellt, welche Modelle sich zur Lösung typischer Konflikte anbieten. In seiner Stellungnahme zum 3. TB (Bürgerschafts-Drucksache 11/3876, erklärte der Senat, der Konflikt lasse sich seiner Auffassung nach nur dadurch lösen, daß sog. Forschungsklauseln in das BDSG und das HmbDSG aufgenommen werden, die die Verwendung personenbezogener Daten für die Forschung regeln. Dieser Erkenntnis sind allerdings bislang keine sichtbaren Aktivitäten gefolgt.

Um die Diskussion zur Schaffung von Forschungsklauseln voranzubringen, möchte ich nachfolgend weitere Vorschläge unterbreiten und die speziellen Problembereiche verdeutlichen, die bei der Formulierung einer Forschungsklausel (im HmbDSG) zu berücksichtigen sind.

Für eine Forschungsklausel bietet sich – kurzgefaßt – die folgende abgestufte Konzeption an:

- Grundsätzlich sollte zu Forschungszwecken nur mit anonymisierten Daten gearbeitet werden, es sei denn, der Zweck des Forschungsvorhabens kann auf diese Weise nicht erreicht werden.
- Ist ein Personenbezug unvermeidbar, so ist grundsätzlich die Einwilligung der Betroffenen einzuholen.
- Eine Einwilligung ist ausnahmsweise verzichtbar, wenn deren Einholung unzumutbar ist und das Allgemeininteresse das Geheimhaltungsinteresse des Einzelnen erheblich überwiegt.

Neben diesem materiellen Konzept sollten flankierende Maßnahmen verfahrensrechtlicher (z.B. Genehmigungsvorbehalte) sowie organisatorisch-technischer Art (Anonymisierungsgebot, Löschungsfristen etc.) gesetzlich abgesichert werden.

Eine solche Konzeption bewirkt – jedenfalls auf einer solchen Abstraktionsebene – nach meiner Einschätzung einen angemessenen Ausgleich zwischen den Interessen der Forschung und des Persönlichkeitsschutzes. Sie hat sich etwa bei § 75 SGB X, der diese Elemente ebenfalls enthält, grundsätzlich bewährt. Die eigentlichen Probleme treten dann auf, wenn es darum geht, diese Konzeption in eine möglichst präzise Regelung umzusetzen. Welche Probleme hier zu lösen sind, möchte ich kurz skizzieren.

4.15.1 Forschung mit anonymisierten Daten

Bei der Regelung dieses Punktes stellt sich zunächst einmal die Frage, wann eigentlich Daten als „anonymisiert" anzusehen sind. Weitgehende Einigkeit besteht darüber, daß eine absolute Anonymisierung wegen deren praktischer Unmöglichkeit nicht gefordert werden kann. Nach dem Konzept der „faktischen Anonymisierung" soll Nichtidentifizierbarkeit vorliegen, wenn die Reidentifizierung einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde. Nicht schon jede theoretische Möglichkeit genügt für die Bestimmbarkeit, sondern erst eine solche Situation, in der der Wert der möglicherweise zu erlangenden Information zu dem zur Beschaffung des Zusatzwissens voraussichtlichen Aufwand in einer Relation steht, nach der es nicht ausgeschlossen werden kann, daß ein Interessent von diesen Möglichkeiten Gebrauch macht (Simitis/Dammann/u.a., BDSG, § 2, Rdnr. 36).

Die Problematik derartiger Formeln liegt aus der Sicht der Wissenschaft in ihrer aus Unbestimmtheit und Abstraktheit resultierenden Unberechenbarkeit.Es ist somit zu erwägen, ob und wie es möglich ist, die Anforderungen an eine hinreichende Anonymisierung weiter zu konkretisieren.

Die Schwierigkeiten, denen ein solches Unterfangen begegnet, sind allerdings immens. Da die Anforderungen, die an eine Anonymisierung zu stellen wären, der unterschiedlichen Sensitivität der Daten Rechnung tragen müßten, kann hier wohl allein eine nach Forschungszwecken differenzierende Lösung angemessen sein.

Eine weitere Schwierigkeit, die im Zusammenhang mit der Forderung nach konkretisierender Festschreibung von Anonymisierungsregeln bedacht werden muß, liegt in der permanenten Revisionsbedürftigkeit von derartigen Regeln. Angesichts der rasanten technischen Entwicklung auf dem Gebiet der Datenverarbeitung müßten solche Regeln fortlaufend adäquat zu den neu entstandenen Gefährdungspotentialen fortgeschrieben (ständig überwacht) werden.

Aus diesen Umständen folgt, daß eine Regelung auf der Ebene des Gesetzes nicht möglich sein wird. Hier kann allenfalls festgeschrieben werden, daß der Grad der Anonymisierung etwa dem Stand der Wissenschaft entsprechen muß.Anonymisierungsrichtlinien müßten auf einer Ebene unterhalb des Gesetzes entwickelt und fortgeschrieben werden.

4.15.2 Das Erfordernis der Einwilligung

Diese Stufe der Konzeption dürfte nach meiner Einschätzung die wenigsten Probleme aufwerfen. Erörtert wird lediglich, wann eine wirksame, sog. „informierte" Einwilligung (informed consent) vorliegt. Von Wissenschaftlern wird bisweilen beklagt, daß deren

Anforderungen nicht hinreichend klar und berechenbar seien. Dem ist entgegenzuhalten, daß zumindest § 5 Abs. 2 HmbDSG den Inhalt einer Einwilligungserklärung recht detailliert umschreibt und § 9 Abs. 2 HmbDSG einen Hinweis auf die Freiwilligkeit der Mitarbeit vorsieht.

Ferner weise ich auf die Empfehlung Nr. R (83) 10 des Europarats zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik vom 14.9.1983 hin. Danach liegt eine informierte Einwilligung vor, wenn

- jede Person, die Daten über sich mitteilt, ausreichend über die Art des Projektes, seine Ziele sowie über den Namen der Person oder die Stelle unterrichtet worden ist, für die die Forschungsarbeit durchgeführt wird;
- der Betroffene darüber unterrichtet worden ist, daß es ihm freisteht, die erbetenen Daten zur Verfügung zu stellen, mitzuarbeiten oder seine Mitwirkung abzulehnen. Darüber hinaus ist zu fordern, daß über die Aufbewahrungsdauer der Daten aufgeklärt werden muß.

Die nach dem Datenschutzrecht geforderte Schriftform der Einwilligung wird insbesondere von empirischen Sozialforschern mit dem Argument angegriffen, daß dadurch wesentlich höhere Verweigerungsraten entstehen, weil Unterschriften häufig mit dem Eingehen einer Verbindlichkeit identifiziert werden. Diese Argumentation überzeugt mich nicht. Jemand, der bereit ist, sich für ein Forschungsvorhaben interviewen zu lassen, über das er aufgeklärt worden ist, dürfte auch in der Lage sein, die Bedeutung einer schriftlichen Einwilligung einzuschätzen. Ein Verzicht auf das Schriftformerfordernis birgt demgegenüber die große Gefahr, daß die Erforderlichkeit einer Einwilligung auf informierter Basis umgangen wird, weil sie kaum kontrolliert werden kann.

4.15.3 Verzicht auf eine Einwilligung

Der Grundsatz, daß es Ausnahmefälle geben muß, in denen Einwilligungen verzichtbar sind, ist heute kaum noch umstritten. Unterschiedlich beantwortet wird jedoch die Frage, wie die Voraussetzungen für den Verzicht möglichst präzise in einem Gesetz zu umschreiben sind.

Um sicherzustellen, daß der Verzicht auf eine Einwilligung die Ausnahme bleibt, muß zunächst einmal ein Zumutbarkeits-Kriterium berücksichtigt werden; nur wenn die Einholung der Einwilligung unzumutbar ist, kann der Verzicht überhaupt in Erwägung gezogen werden. Die Unzumutbarkeit ist – im Gesetz – zu konkretisieren: sie kann gegeben sein, wenn die Einholung der Einwilligung das Forschungsziel gefährden würde – etwa wegen Voreingenommenheit der Probanden (z.B. bei teilnehmender Beobachtung). In diesen Fällen sollte aber wiederum die Europaratsempfehlung berücksichtigt werden. Diese verlangt für den Fall, daß in Anbetracht des verfolgten Ziels die geforderte Information ganz oder teilweise entfallen muß, den Betroffenen unmittelbar nach der Datenerfassung über den Inhalt des Forschungsvorhabens vollständig zu unterrichten. Es soll ihm dann freistehen, seine Mitwirkung fortzusetzen oder abzubrechen, und im letzteren Fall soll er die Löschung der erfaßten Daten verlangen können. Nach diesem Modell wird das Einwilligungserfordernis durch ein nachträgliches Genehmigungserfordernis ersetzt.

Das Problem der Zumutbarkeit wird ferner insbesondere bei der retrospektiven Forschung von Bedeutung sein. Bei solchen Forschungsvorhaben, die rückwirkend zu anderen Zwecken angelegte Datenbestände auswerten wollen, werden Einwilligungen häufig schon deswegen kaum eingeholt werden können, weil die gegenwärtige Anschrift der Betroffenen nicht oder nur mit unverhältnismäßigem Aufwand festgestellt werden kann. Auch in diesen Fällen kommt ein Verzicht auf eine Einwilligung in Betracht, wenn auch die im nächsten Absatz beschriebenen Voraussetzungen erfüllt sind.

Zusätzlich muß – neben der Zumutbarkeitsprüfung – immer noch abgewogen werden, ob das Allgemeininteresse an der Durchführung eines bestimmten Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. Um nichts anderes als diese Abwägung geht es im übrigen auch, wenn vorhandene Forschungs-

klauseln (etwa § 12 LDSG NRW, §15 HDSG) die Voraussetzung normieren, daß „schutzwürdige Belange" der Betroffenen nicht beeinträchtigt werden. Das Problem liegt allerdings jeweils darin – sowohl aus der Sicht des Betroffenen als auch der Sicht des Forschers –, daß diese unbestimmten Rechtsbegriffe wenig transparent und berechenbar sind. Ob und in welcher Form hier Konkretisierungen möglich sind, muß noch geklärt werden. Zu erwägen ist dabei z.B. als ein Kriterium, daß das Forschungsinteresse dann erheblich überwiegt (bzw. schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden), wenn zunächst personenbezogen erfaßte Daten unverzüglich nach Erhalt anonymisiert werden (so ein hessischer Erlaß aus 1981).

Klärungsbedürftig ist schließlich die Frage, wer darüber entscheidet, daß der Verzicht auf eine Einwilligung zulässig ist. Hier wird m.E. zu differenzieren sein: Erhebt ein Forscher selbst Daten bzw. wertet er die vorhandenen Daten aus, so wird er auch selbst die volle Verantwortung für einen etwaigen Verzicht auf Einwilligungen tragen müssen. Um eine Kontrolle zu ermöglichen, muß er allerdings verpflichtet werden, die Gründe für eine solche Entscheidung zu dokumentieren. Werden für ein Forschungsvorhaben Daten von öffentlichen Stellen weitergegeben, so ist eine Genehmigung erforderlich. Stammen diese Daten aus einem durch besondere Berufs- oder Amtspflichten geschützten Bereich, so ist zwingend vorzusehen, daß die Genehmigung einer obersten Landesbehörde vorbehalten bleibt (vgl. § 75 SGB X) oder aber, wie § 9 HmbKrebsRegG es für den Fall vorsieht, daß eine Fachbehörde selbst datenverarbeitende Stelle ist, der Präses oder der Staatsrat dieser Behörde das Vorhaben zu genehmigen hat.

4.15.4 Organisatorische und verfahrensrechtliche Sicherungen

Nach dem VZ-Urteil sind schon vom Gesetzgeber zusätzliche organisatorische und verfahrensrechtliche Sicherungen vorzusehen.

Zu denken ist dabei etwa an das Gebot, personenbezogene Daten grundsätzlich sobald wie möglich zu anonymisieren. Die Anonymisierung könnte in der Weise erfolgen, daß die Merkmale, mit deren Hilfe der Bezug der anonymisierten Daten zu den Betroffenen wiederhergestellt werden kann, zunächst gesondert gespeichert werden. Für den Fall, daß die personenbezogenen Daten dem Forscher von einer anderen Stelle zur Verfügung gestellt worden sind, sollte festgelegt werden, daß dieser Stelle der Reidentifizierungs-Code wieder zu übergeben ist.

Desweiteren ist zu regeln, wann personenbezogene Forschungsdaten zu löschen sind. Hier stellt sich das Problem der sog. Sekundäruntersuchungen. Wenn Daten zwingend zu löschen sind, sobald ein konkretes Forschungsvorhaben abgeschlossen ist, wären Kontrolluntersuchungen zur Überprüfung des Projektes nicht mehr möglich. Dies Problem läßt sich dadurch lösen, daß man die notwendigen Sekundäruntersuchungen bei einem Forschungsprojekt von vornherein mit einkalkuliert und eine Löschung erst für den Zeitpunkt zwingend vorschreibt, wenn alle Kontrollen abgeschlossen sind. Hier sind allerdings – auch in den Genehmigungsbescheiden – klare Fristen vorzusehen.

4.15.5 Resümee

Ich hoffe, mit meinen vorstehenden Ausführungen die wesentlichen Probleme, die bei der Formulierung von Forschungsklauseln zu berücksichtigen sind, umrissen zu haben. Zusätzlich wird zu klären sein, ob öffentliche und nicht-öffentliche Stellen in Forschungsklauseln gleichzubehandeln sind. Aus meiner Sicht wäre gegen eine Gleichbehandlung dann nichts einzuwenden, wenn die Möglichkeit einer gleich hohen Kontrolldichte gewährleistet ist. Die Datenschutzbeauftragten müßten also die Möglichkeit erhalten – was heute auf freiwilliger Basis bereits praktiziert wird –, auch bei nicht-öffentlichen Stellen die zweckgerechte Verwendung von – aus dem öffentlichen Bereich übermittelten – Daten zu kontrollieren.

Ich erwarte, daß der Senat seine bisherigen Erkenntnisse nun bald in die Tat umsetzt und die Schaffung einer Forschungsklausel – auch im Interesse der Forschung – zügig vorantreibt.

5. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

5.1 Versandhandel

Bereits in meinen letzten Tätigkeitsberichten habe ich die Problematik der Schufa-Anfragen des Versandhandels über die Ehegatten von Erstbestellern dargestellt (vgl. insb. 3. TB, 4.1.1, S. 100 f.). Ich habe weitere Gespräche mit Vertretern des Versandhandels geführt, um zu einer datenschutzrechtlichen einwandfreien Lösung dieses Problems zu kommen.

Der Versandhandel ist bereit, meinen Bedenken zumindest zum Teil Rechnung zu tragen. Seine Vertreter schlugen vor, eine Einigung dadurch herbeizuführen, daß in Zukunft die Anfrage bei der Schufa über den Ehegatten des Bestellers nicht mehr mit dem Merkmal VK („Versandhauskonto"), sondern mit dem Merkmal AH („Anfrage des Versandhandels wegen Lieferung oder Leistung mit kreditorischem oder geschäftlichem Risiko") erfolgen soll. Dies würde bedeuten, daß der Versandhandel eine aktuelle Auskunft von der Schufa erhält, daß aber keine Nachmeldungen von Negativmerkmalen über den Ehegatten durch die Schufa mehr erfolgen. Über den Ehegatten würde die Schufa in Zukunft nichts mehr speichern. Über den Besteller selbst würde weiterhin mit dem Merkmal VK bei der Schufa angefragt werden, so daß Nachmeldungen von Negativmerkmalen über diesen erfolgen würden.

Dieses Verfahren würde eine wesentliche Verbesserung bedeuten. Ich habe den Versandhandel jedoch darauf hingewiesen, daß dadurch noch nicht alle mit der Schufa-Anfrage über die Ehegatten von Erstbestellern verbundenen datenschutzrechtlichen Probleme gelöst werden. Auch bei diesem Verfahren kann nicht ausgeschlossen werden, daß –in beiden Richtungen– Daten unter Verstoß gegen §§ 24 Abs. 1 Satz 1 bzw. 32 Abs. 2 Satz 1 BDSG übermittelt werden, da schutzwürdige Belange Betroffener jedenfalls in den Fällen beeinträchtigt sein können, in denen eine Mitverpflichtung des Ehegatten aus § 1357 BGB nicht in Frage kommt. Ein weiteres Problem liegt darin, daß der Empfänger nach § 32 Abs. 2 BDSG sein berechtigtes Interesse an der Übermittlung glaubhaft darlegen muß, der Versandhandel sein berechtigtes Interesse durch die pauschale Meldung VK oder AH aber nicht darlegen kann, da die Ehegatten nur im Fall des § 1357 BGB aus den Geschäften mitverpflichtet werden.

Die verbleibenden juristischen Probleme müssen bald gelöst werden. Es wäre wünschenswert, daß im Zusammenhang mit der durch das BGH-Urteil zur Schufa-Klausel bewirkten Neuorganisation des gesamten Schufa-Anfragesystems auch die vertraglichen Beziehungen zwischen Schufa und Versandhandel neu gestaltet und die mit der Anfrage über Ehegatten verbundenen Probleme geklärt werden.

5.2 Direktwerbung

In meinen bisherigen Tätigkeitsberichten habe ich bereits über die Probleme berichtet, die mit der Direktwerbung verbunden sind. Nach wie vor erreichen mich immer wieder Anrufe und Schreiben von Bürgern, die sich über unverlangt zugesandte Werbesendungen beschweren und mich um Rat fragen, wie sie die Verwendung ihrer Anschrift für Zwecke der Direktwerbung verhindern können.

Neben der Aufklärung über die Zusammenhänge der Direktwerbung und des Adreßhandels bleibt mir regelmäßig nur der Hinweis auf die sog. Robinsonliste, in die sich eintragen lassen kann, wer keine Werbesendungen mehr erhalten möchte. Ich habe zur Aufklärung über diesen Problembereich zusammen mit der Verbraucherzentrale Hamburg ein Merkblatt herausgegeben, das bei mir angefordert werden kann.

Ich muß jedoch feststellen, daß ich den Ratsuchenden darüber hinaus nicht helfen kann. In meinem 3. TB (4.1.2, S. 101 ff.) hatte ich über einen Fall berichtet, in dem das werbende Unternehmen sich geweigert hatte, dem betroffenen Empfänger der

Werbesendung die Herkunft der Adresse mitzuteilen. Ich habe diesem Unternehmen meine im 3. TB dargestellte Rechtsauffassung vorgetragen, wonach der Betroffene einen Anspruch darauf hat, die Quelle seiner genutzten Adresse zu erfahren, damit er dort der weiteren Verwendung widersprechen kann. Das Unternehmen hat darauf ablehnend und später auf ein weiteres Schreiben gar nicht mehr reagiert. Auf eine Erinnerung hin teilte es dann mit, es beabsichtigte nicht, die Korrespondenz über diesen Fall fortzusetzen. Es war dem Betroffenen letztlich also nicht möglich, die Herkunft der Adresse zu erfahren, um sie bei der Quelle für weitere Werbeaktionen sperren zu lassen. Dies macht deutlich, daß der Bürger gegenwärtig der Direktwerbung hilflos ausgeliefert ist und – von der lückenhaft funktionierenden Robinsonliste abgesehen – keine Möglichkeit hat, wirksam gegen die Verwendung seines Namens, seiner Anschrift und zusätzlicher Angaben zur Zielgruppenauswahl für Zwecke der Direktwerbung vorzugehen.

Es hat sich somit nichts an dem unbefriedigenden Zustand geändert, der die Aufsichtsbehörden für den Datenschutz bereits 1981 dazu veranlaßt hatte, mit dem Adressenverleger- und Direktwerbeunternehmerverband (ADV) Gespräche zu führen, die zu einer Änderung führen sollten. Die damals getroffenen Vereinbarungen sind, wie bereits im 3. TB (4.1.2., S. 102 f.) berichtet, nicht in die Praxis umgesetzt worden.

Im einzelnen ist hier folgendes zu beanstanden:

1. Der Adressen-Nutzer teilt dem Umworbenen nicht mit, nach welchen Kriterien er in diese Werbung einbezogen worden ist. Der Vermittler begründet dies damit, daß die Angabe der Selektionskriterien die Wirkung der Werbemaßnahme beeinflussen würde. Wegen fehlender Bereitschaft der Kunden (Adressen-Nutzer) habe sich die Absicht des ADV deshalb nicht realisieren lassen.

2. Auch die Herkunft der Adressen wird dem Umworbenen weiterhin generell nicht offengelegt. Die Adressen-Nutzer verweisen lediglich auf den Vermittler, mit dem sie zusammengearbeitet haben, und auf die Robinson-Liste des ADV. In den Fällen, in denen die Adressen aus mehreren Quellen stammen, kann der Werbende die Quelle ohnehin nicht angeben, weil er sie selbst nicht genau kennt. In dem oben erwähnten Fall war das werbende Unternehmen nicht einmal bereit, dem Betroffenen den zwischengeschalteten Vermittler zu nennen.

3. In die Vertragstexte für Direktwerbe-Aufträge wurden – soweit ersichtlich – keine der mit dem ADV vereinbarten Regelungen übernommen. Die Kontrolle wird 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 eingerichtete und der Werbewirtschaft portosparende Robinson-Liste 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 Robinson-Liste verzeichnet sind.

Zur Klärung dieser Probleme haben die Aufsichtsbehörden für den Datenschutz ein Gespräch mit Vertretern des Zentralausschusses der Werbewirtschaft (ZAW) und des ADV geführt. Gegen die Rechtsauffassung der Aufsichtsbehörden, die ihren Niederschlag in den Vereinbarungen mit dem ADV im Jahre 1981 gefunden hatte, wandten die Vertreter der Werbewirtschaft jetzt ein, daß diese Vereinbarungen in der Praxis nicht umsetzbar seien. Zum einen würde die Mitteilung von Selektionskriterien in Werbeschreiben zu unvertretbar hohen Kosten führen, wenn etwa durch unterschiedliche Hinweise in den Schreiben einer Werbeaktion die von der Bundespost für die Einstufung als Massendrucksache geforderte Anzahl inhaltsgleicher Schreiben nicht mehr erreicht werden könne. Zum anderen könne der von den Aufsichtsbehörden geforderte Auskunftsanspruch des Umworbenen über die Herkunft der Daten schon aus wettbewerbsrechtlichen Gründen nicht akzeptiert werden. Woher ein Direktwerbeun-

ternehmen seine Adressen beziehe, sei ein Geschäftsgeheimnis, das im Rahmen der Konkurrenzbeobachtung dann offengelegt würde.

Die Vertreter der Aufsichtsbehörden betonten, daß die Zulässigkeit der durch die Reaktion des Umworbenen eintretenden Übermittlung weder aus § 24 noch aus § 32 BDSG abgeleitet werden könne. Die Zulässigkeit der Übermittlung könne nur erreicht werden, wenn der Betroffene in die Lage versetzt würde, aufgrund der Kenntnis der Selektionskriterien bewußt zu entscheiden, ob er seine Zugehörigkeit zu dem ausgewählten Personenkreis dem werbenden Unternehmen preisgeben wolle.

Die Vertreter der Aufsichtsbehörden sahen hinsichtlich der Genauigkeit der mitzuteilenden Auswahlkriterien Verhandlungsmöglichkeiten; die Kriterien müßten aber so genau bezeichnet sein, daß noch von einer informierten Einwilligung des Umworbenen ausgegangen werden könne. Auch zur Frage der Auskunftserteilung über die Herkunft der Adressen waren die Aufsichtsbehörden geneigt, den Interessen der Werbewirtschaft am Schutz ihrer Geschäftsgeheimnisse entgegenzukommen. So könne etwa entsprechend einem Vorschlag des ZAW in Erwägung gezogen werden, daß bei einem Löschungsverlangen des Umworbenen der Adressenmittler nicht die Herkunft der Adresse offenbart, sondern selbst bei dem Adresseneigentümer die Löschung sicherstellt.

Die Vertreter der Werbewirtschaft sagten zu, die Problematik in ihren Gremien zu erörtern und auf Lösungsvorschläge hinzuwirken. Die Gespräche zwischen Aufsichtsbehörden und Werbewirtschaft werden weitergeführt werden. Ich bin zuversichtlich, daß dabei nunmehr ein auch aus der Sicht des Datenschutzes befriedigendes Ergebnis wird erzielt werden können, denn die Werbewirtschaft ist selbst eher an freiwilligen Vereinbarungen als an Verschärfungen der Gesetze interessiert (vgl. Hörle, Bundesdatenschutzgesetz, Bedeutung und Auswirkungen auf die Direktwerbung, WRP 1985, S. 529, 536), die unumgänglich würden, wenn es nicht zu einer einvernehmlichen Lösung kommt.

5.3 Kreditwirtschaft

5.3.1 Prüfung bei der Verbraucherbank

Im Berichtszeitraum habe ich bei der Verbraucherbank u.a.

die Zugangssicherung für die Kontoführung über Btx

die Zugangssicherungs im Selbstbedienungsverfahren

geprüft. Die wesentlichenErgebnisse meiner Prüfung sind:

1. Zugangssicherung für die Kontoführung über Btx

1.1 Anforderungen

Die Zugangssicherung im Btx-Verfahren ist Teil der technischen und organisatorischen Maßnahmen (Datensicherung), die der Anbieter nach Art. 9 Abs. 1 StV-Btx, § 6 Abs. 1 BDSG zu treffen hat. Der Umfang der Datensicherung ergibt sich – da es sich um automatisierte Verarbeitung handelt – aus der Anlage zu § 6 Abs. 1 BDSG. Darüber hinaus stellt Art. 9 Abs. 8 StV-Btx weitere Anforderungen an die Datensicherung.

Insgesamt besteht die Verpflichtung zu Maßnahmen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

- die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
- die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern (Benutzerkontrolle),

- zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
- zu gewährleisten, daß bei der Übermittlung personenbezogener Daten... diese nicht unbefugt gelesen, verändert oder gelöscht werden können (Transportkontrolle);

dabei müssen die zu Zwecken der Datensicherung vergebenen Codes einen dem Stand der Technik entsprechenden Schutz vor unbefugter Verwendung bieten.

1.2 Maßnahmen

Der Zugang zum Konto ist durch folgende Maßnahmen gesichert:

- Eingabe einer Geheimzahl oder persönlichen Identitäts-Nummer (PIN)

  Die Geheimzahl ist ausreichend lang; triviale und bestimmte Kombinationen aus dem Umfeld des Kunden (z.B. Geburtsdatum, Telefonnr.) werden nicht zugelassen. Die Geheimzahl wird verdeckt eingegeben. Die Zahl der Fehlversuche ist begrenzt; nach Ausschöpfung der Fehlversuche wird derjenige, der eine Verbindung aufzubauen versucht, abgewiesen. Das Konto wird gesperrt und nur nach Einschaltung der Verbraucherbank entsperrt.

  Der Kontoinhaber kann seine Geheimzahl im Btx ohne Einschaltung der Bank jederzeit ändern.

  Die Geheimzahl wird im System verschlüsselt gespeichert.

- Eingabe einer Transaktionsnummer (TAN) mit Quittungsverfahren

  fakultativ, wenn keine Verfügungen getroffen werden,

  obligatorisch, wenn Verfügungen getroffen werden.

  Die TAN sind 10stellig und werden dem Kontoinhaber in einer größeren Anzahl vom Bankinstitut zur Verfügung gestellt. Der Kontoinhaber gibt auf Anforderung die ersten 6 Stellen ein und erhält die letzten 4 Stellen als Quittung angezeigt. Dadurch erhält der Kontoinhaber Gewißheit darüber, daß er mit seinem Bankinstitut kommuniziert,

- Eingabe von bis zu 3 zusätzlichen Paßwörtern, wenn der Kontoinhaber diese zusätzliche Zugangssperre einrichtet.

- Zeitschloß

  Der Kontoinhaber kann für eine bestimmte, von ihm mit Datum und Uhrzeit definierte Zeitspanne (z.B. Urlaub) den Btx-Zugang zu seinem Konto absolut sperren. Die Sperre kann während des Sperrzeitraumes auch vom Kontoinhaber nur aufgrund persönlicher Vorsprache in dem Bankinstitut aufgehoben werden.

Die benutzten Codes (PIN, Paßwort, TAN) entsprechen – wie Art. 9 Abs. 8 StV-Btx fordert – dem Stand der Technik:

- Sie sind ausreichend lang, um – insbesondere mit der Begrenzung der Fehlversuche – ein Ausprobieren zu verhindern.
- Sie können vom Benutzer jederzeit geändert bzw. können nur einmal verwendet werden (TAN).
- Sie werden verschlüsselt gespeichert.

Die Eingabekontrolle wird dadurch gewährleistet, daß aufgrund der handels- und steuerrechtlichen Buchführungspflicht alle ein Konto betreffenden Vorgänge aufgezeichnet werden.

Der Transportweg befindet sich außerhalb des Verantwortungsbereichs der Verbraucherbank; die Verbraucherbank mußte nämlich, wenn sie am Btx teil-

nehmen wollte, die Vorgaben der Deutschen Bundespost akzeptieren. Sie hat für den Kontoinhaber durch die fakultativen Möglichkeiten der Zugangssicherung und das Quittungsverfahren bei der TAN im Falle der Verfügung die Möglichkeit geschaffen, Sicherheitsmängel der Netze auszugleichen.

Die Verbraucherbank hat den Zugang zwischen Btx-Vermittlungsstellen und Verbraucherbank über Datex-P zusätzlich durch die Einrichtung einer Teilnehmerbetriebsklasse abgesichert (Teilnehmerbetriebsklasse bedeutet, daß nur zu dieser Teilnehmerbetriebsklasse gehörende Anschlüsse untereinander Verbindung aufnehmen können; fremde Anschlüsse werden abgewiesen).

1.3 Bewertung

Die getroffenen Maßnahmen gewährleisten einen angemessenen Stand der Datensicherung.

Im Btx-System ist der Zugang zu einem fremden Konto nur möglich, wenn der Unberechtigte die für den Zugang notwendigen Informationen (Geheimzahl, evtl. TAN oder Paßwort, TAN bei Verfügungen) kennt; denn über Btx kann der durch die Angebote der Verbraucherbank gezogene Rahmen nicht verlassen werden, weil Eingaben außerhalb der zulässigen abgewiesen oder ignoriert werden. Es kommt also darauf an, ob ein Unberechtigter in den Besitz der Informationen gelangen kann, die für den Zugang zu einem Konto erforderlich sind.

- Die für den Zugang notwendigen Informationen könnten auf „konventionelle" Weise (z.B. Belauschen, Diebstahl usw.) erlangt werden. Dies wird bei der Geheimzahl dadurch verhindert, daß die Geheimzahl verdeckt eingegeben wird, d.h. auf dem Bildschirm erscheinen statt der eingegebenen Zahlen Striche; die nur einmal verwendbare TAN wird offen eingegeben, sie wird auf dem Transport zum Kontoinhaber durch Versenden per Einschreiben geschützt.

  Da das Ausspähen aber überwiegend nur in der Sphäre des Kontoinhabers möglich ist, muß es der Kontoinhaber durch entsprechende Vorkehrungen (Ausnutzen der angebotenen fakultativen Zugangssicherungen) und sicherheitsbewußtes Verhalten verhindern. Die Verbraucherbank informiert den Kontoinhaber ausreichend über die Sicherheitsproblematik.
- Die für den Zugang notwendigen Informationen könnten auch durch „Anzapfen" (im weitesten Sinne) der Fernsprechleitung erlangt werden. Neben einer geeigneten technischen Einrichtung ist die Identifikation einer bestimmten Fernsprechleitung erforderlich; das ist im allgemeinen nur in räumlicher Nähe zum Anschluß möglich und kann durch sicherheitsbewußtes Verhalten des Kontoinhabers (gelegentliche Beobachtung) verhindert werden. Entsprechende Hinweise fehlen aber z.Z. noch. Da die Deutsche Bundespost hier ihren Pflichten nicht nachkommt, habe ich die Verbraucherbank gebeten, die Lücken auszufüllen.
- Wenn die Eingabe einer TAN erforderlich ist (fakultativ für den Zugang, obligatorisch für Verfügungen), ist bei dem von der Verbraucherbank gewählten Verfahren mit Quittung für das Anzapfen der Fernsprechleitung mit dem Ziel unberechtigter Verfügung ein hoher Aufwand zu leisten:

  Ein Unberechtigter muß sich induktiv auf die Fernsprechleitung aufschalten.

  Er muß eine Verfügung des Kontoinhabers auffangen und an den Empfänger zurückspiegeln („echoplexen"), also die Btx-Vermittlungsstelle simulieren.

  Wenn der Kontoinhaber den Auftrag mit einer TAN absendet, muß der Unberechtigte die Verfügung in seinem Sinne verändern (andere Empfänger, anderes Konto, anderer Betrag) und nach Veränderung an die Btx-Vermittlungsstelle weiterleiten. Dabei müssen Zeittakt und Protokolle des Btx-Verfahrens beachtet werden.

Da die Verfügungen ab einer bestimmten Höhe bankintern einem Prüfungsverfahren unterworfen werden und durch das angegebene andere (begünstigte) Konto Spuren gelegt werden, dürfte der Ertrag im Verhältnis zum Aufwand zu hoch und ein Mißbrauch daher nicht zu befürchten sein. Da der kriminellen Phantasie jedoch kaum Grenzen gesetzt sind, darf diese Feststellung keine Veranlassung geben, die Hände in den Schoß zu legen. Alle Beteiligten sind aufgerufen, die Situation aufmerksam zu beobachten.

Ich habe angregt, daß die Verbraucherbank den Kontoinhaber über alle registrierten Fehlversuche der Eingabe der Geheimzahl und einer TAN informiert, weil nur der Kontoinhaber erkennen kann, ob es sich um Versuche eines Unberechtigten handelte, und entsprechende Maßnahmen treffen kann.

2. Zugangssicherung im Selbstbedienungsverfahren

Die Verbraucherbank ermöglicht ihren Kunden, ihr Konto ohne Papierbelege und Inanspruchnahme von Mitarbeitern der Bank zu führen, indem sie in den Räumen der Bank aufgestellte Selbstbedienungsterminals benutzen, die mit der Datenverarbeitungsanlage der Verbraucherbank verbunden sind. Es gibt zwei Arten von Selbstbedienungsterminals:

Bildschirmgeräte mit Tastatur und Drucker für alle Aktionen außer Barabhebung;

Geldausgabeautomaten für Barabhebungen.

Die Selbstbedienungseinrichtungen können an allen Tagen und rund um die Uhr benutzt werden.

2.1 Anforderungen

Auch hier ist die Zugangssicherung Teil der Datensicherung, zu der die Verbraucherbank als speichernde Stelle gem. § 6 Abs. 1 BDSG verpflichtet ist. Der Umfang der Datensicherung ergibt sich ebenfalls – da es sich um automatisierte Verfahren handelt – aus der Anlage zu § 6 Abs. 1 BDSG.

Die in Art. 9 Abs. 8 StV-Btx für Btx-Anwendungen genannten Anforderungen an die Codes sind auch bei der Zugangssicherung im Selbstbedienungsverfahren zu berücksichtigen.

2.2 Maßnahmen

Der Zugang zum Konto im Selbstbedienungsverfahren ist durch Legitimationskarte und Geheimzahl abgesichert. Die Legitimationskarte ist eine Kunststoffkarte im Format der EC-Karte. Sie ist äußerlich deutlich von der EC-Karte unterschieden, als Karte der Verbraucherbank erkennbar und nur in den Geldautomaten der Verbraucherbank zu benutzen. Die Legitimationskarte enthält in einem Codierstreifen Informationen, die es ausschließen, daß die Legitimationskarte nachgemacht werden kann, ohne daß man in Besitz der ursprünglichen Legitimationskarte war.

Der Kontoinhaber ist zur sorgfältigen Aufbewahrung der Legitimationskarte – die Eigentum der Verbraucherbank bleibt – und dazu verpflichtet, einen etwaigen Verlust sofort zu melden. Die Legitimationskarte wird in diesem Fall gesperrt. Wenn gesperrte Legitimationskarten benutzt werden, werden sie am Geldausgabeautomaten eingezogen bzw. wird am Bildschirmgerät der Dialog abgebrochen.

Die Geheimzahl ist innerhalb einer vorgeschriebenen Länge vom Kontoinhaber frei wählbar, ohne Vorgaben von der Verbraucherbank.

Die Geheimzahl ist vom Kunden jederzeit, aber nur unter Mitwirkung der Verbraucherbank änderbar, weil die Verbraucherbank ein zweistufiges Verfahren eingerichtet hat. Die Geheimzahl kann daher nur während der Kassenstunden geändert werden.

Die Zahl der Fehlversuche bei der Eingabe der Geheimzahl ist sowohl bei den Geldausgabeautomaten als auch bei den Bildschirmterminals begrenzt. Für Btx- und Selbstbedienungsverfahren gilt dieselbe Geheimzahl. In einem Verfahren geänderte Geheimzahlen sind im jeweils anderen Verfahren mit Zeitversetzung wirksam. Die Geheimzahl als Code bietet einen dem Stand der Technik entsprechenden Schutz vor unbefugter Verwendung. Der Kontoinhaber hat außerdem die Möglichkeit, sein Konto für das Selbstbedienungsverfahren zu sperren. Das ist nur unter Mitwirkung der Verbraucherbank und damit nur während der Kassenstunden möglich.

Außerhalb der Kassenstunden und ohne Mitwirkung der Verbraucherbank kann der Kontoinhaber sein Konto für das Selbstbedienungsverfahren nur sperren, indem er absichtlich die zulässige Zahl von Fehlversuchen bei der Eingabe der Geheimzahl überschreitet und damit die Sperre des Kontos auslöst.

Ein Unberechtigter kann nur dann Zugang zu einem fremden Konto erlangen, wenn er im Besitz der für den Zugang erforderlichen Informationen ist.

Wenn der Kontoinhaber die Legitimationskarte und die Geheimzahl sorgfältig aufbewahrt (d.h. die Geheimzahl nicht oder nur an schwer zugänglicher Stelle aufzeichnet), ist es praktisch ausgeschlossen, daß ein Unberechtigter die für den Zugang erforderlichen Informationen erfährt.

Das Nachmachen einer Legitimationskarte ist nur möglich, wenn man sich entweder – vorübergehend – in den Besitz der echten Legitimationskarte setzt – was abhängig vom Verhalten des Kontoinhabers ist, siehe oben – oder die Mithilfe eines Mitarbeiters der Verbraucherbank gewinnt; ich halte es für unwahrscheinlich, daß dies bei dem kleinen und ausgesuchten Personenkreis gelingt, der Zugang zu diesen Informationen hat.

Da die Geheimzahl im DV-System der Verbraucherbank verschlüsselt gespeichert wird, kann ein Unberechtigter die Geheimzahl nur auf konventionellem Wege ausforschen; hierzu bestehen mehrere Möglichkeiten. Die Verbraucherbank sollte die Ausforschungsmöglichkeiten durch Abschirmung der Tastaturen an den Bildschirmgeräten und Geldausgabeautomaten sowie durch Markierung einer Wartelinie verringern und die Kunden durch entsprechende Hinweise sicherheitsbewußt machen. Die Verbraucherbank sollte den Kontoinhaber auch hier über registrierte Fehlversuche informieren, weil nur er übersehen kann, ob es sich um Versuche Unberechtigter handelt. Der Kontoinhaber sollte die Möglichkeit haben, seine Geheimzahl jederzeit über Terminal selbst und ohne Mitwirkung der Bank zu ändern. Außerdem sollten die Geheimzahlen im Btx-Verfahren und im Selbstbedienungsverfahren sofort synchronisiert werden.

Auch wenn bisher kein Fall bekannt geworden ist, in dem ein Unberechtigter trotz sicherheitsbewußten Verhaltens des Kontoinhabers die für den Zugang notwendigen Informationen erlangt hat – nach Auskunft der Verbraucherbank war in allen bisher bekanntgewordenen Fällen der Unberechtigte eine Person aus dem persönlichen Umfeld des Kontoinhabers, die sich wegen der persönlichen Nähe Legitimationskarte und Geheimzahl beschaffen konnte bzw. wußte –, bleibt ein Restrisiko, das nicht quantifiziert werden kann. Aber selbst, wenn es nur sehr gering ist, sollte die Verbraucherbank dem Kunden wie im Btx-Verfahren zusätzliche Sicherungen wie Paßwörter, TAN, Zeitschloß anbieten. Wahrscheinlich werden diese zusätzlichen Sicherungsmaßnahmen nur diejenigen Kontoinhaber in Anspruch nehmen, die sich ohnehin sicherheitsbewußt verhalten; dennoch können durch solche Angebote das subjektive Sicherheitsempfinden und die Sicherheit objektiv erhöht werden.

Ein Eindringen Fremder in die DV-Anlage der Verbraucherbank außerhalb des Btx-Verfahrens über die Einrichtungen der Datenfernverarbeitung ist so gut wie ausgeschlossen, weil

- es keine Wählanschlüsse gibt,
- die Daten verschlüsselt übertragen werden,
- keine Standard-Software für die Steuerung der Datenfernübertragung (über die man sich aus allgemein zugänglichen Broschüren informieren kann), sondern individuelle Software verwendet wird.

Damit sind die Barrieren für ein unberechtigtes Eindringen so hoch, daß sie selbst für einen DV-Experten nahezu unüberwindlich sind.

5.3.2 Bargeld- und belegloser Zahlungsverkehr

Ich habe im 3. TB (S. 17 f.) über damals erkennbare Entwicklungen in Richtung auf einen bargeld- und beleglosen Zahlungsverkehr berichtet. Dabei habe ich als eine mögliche Variante beschrieben, daß ein Lesegerät off-line arbeitet und der Kunde seine Schuld dadurch begleicht, daß der geschuldete Betrag von einem in der Karte gespeicherten Guthaben abgebucht wird. Nach dem gegenwärtigen Erkenntnisstand wird diese Variante in Verbindung mit der EC-Karte nicht mehr weiter verfolgt werden. (Wohl aber wird es spezielle Karten mit Guthaben geben, z.B. für die Benutzung von öffentlichen Münzfernsprechern.)

Z.Z. wird in Berlin in einem Versuch der bargeld- und beleglose Zahlungsverkehr mit POS (Point of Sale)–Terminals erprobt, die on-line, d.h. unter Steuerung einer DV-Anlage arbeiten werden. Für die Realisierung dieser on-line-Lösung gibt es wiederum zwei Varianten:

- Die dezentrale Lösung sieht vor, alle POS-Terminals an eine bundesweite Zentrale anzuschließen, die die Transaktionen zur weiteren Verarbeitung an das zuständige Bankinstitut weiterreicht.
- Nach der zentralen Lösung sollen alle POS-Terminals an eine Zentrale angeschlossen werden, die die Transaktionen verarbeitet und nach Verarbeitung an die zuständigen Bankinstitute weiterreicht.

Es ist z.Z. nicht absehbar, welche Lösung sich durchsetzen wird.

In beiden Lösungen wird die Persönliche-Identifikations-Nummer (PIN) in derselben Weise verwaltet wie auch jetzt beim Geldausgabeautomaten-Verfahren: Dem Karteninhaber wird eine feste PIN zugeteilt, die bei jeder Benutzung errechnet und mit der vom Benutzer eingegebenen verglichen wird.

Ich halte an meiner im 3. TB (S. 17) geäußerten Ansicht fest, daß bei dieser Lösung eine Gefahr darin besteht, daß der Schlüssel für die Errechnung der PIN entdeckt wird (der benutzte Verschlüsselungsalgorithmus ist ohnehin öffentlich). Ich füge hinzu, daß das Verfahren auch wenig benutzerfreundlich ist, weil der Benutzer eine neue EC-Karte und damit eine neue PIN beantragen muß, wenn er befürchtet, seine alte PIN sei ausgespäht worden.

Gegen die Alternative – vom Benutzer gewählte und von ihm jederzeit änderbare PIN – werden Bedenken hinsichtlich des Sicherheitsstands vorgetragen. Zum einen bestehe die Gefahr, daß viele Benutzer einfache, leicht erratbare PIN wählten; dem halte ich entgegen, daß solche Benutzer auch mit ihrer jetzigen PIN nicht sorgfältig umgehen. Zum anderen wird eine Gefahr darin gesehen, daß die PIN im Bankenbereich gespeichert wird und ausgelesen werden kann. Auch dieser Gefahr kann meiner Meinung nach dadurch begegnet werden, daß die PIN irreversibel verschlüsselt gespeichert werden.

Der Unterschied zwischen den beiden Konzeptionen besteht darin, daß bei

fest vergebener PIN grundsätzlich die Gefahr besteht, daß die PIN ohne Zutun des Betroffenen entdeckt wird, nämlich dadurch, daß die Geheimnisträger den Schlüssel für die Bildung der PIN verraten.

vom Benutzer vergebener und verwalteter PIN die Gefahr des Entdeckens ohne Zutun des Benutzers nicht besteht, wenn die PIN irreversibel verschlüsselt gespeichert wird.

Bei fest vergebener PIN hängt die Sicherheit mithin von den Vorkehrungen in der Kreditwirtschaft und beim Benutzer ab, bei der vom Benutzer verwalteten PIN ausschließlich vom Benutzer.

Dennoch halte ich es nicht für notwendig, das gegenwärtige System mit fest vergebener PIN unverzüglich durch ein System mit vom Benutzer verwalteter PIN abzulösen, weil die gegenwärtig in der Kreditwirtschaft getroffenen Maßnahmen nach meiner Überzeugung einen ausreichenden Sicherheitsstand bieten das bestätigen auch die bisherigen Erfahrungen, daß keine PIN ohne Zutun des Benutzers ausgeforscht werden konnte.

5.3.3 Personenbezogene Daten auf Kontoauszügen

Ein Bürger stellte mir die Frage, ob die Angabe des Verwendungszwecks bei Überweisungen und Lastschriften auf Kontoauszügen datenschutzrechtlich zulässig ist und ob diese Daten gespeichert und an andere Stellen übermittelt werden. Der Bürger hielt es für überflüssig und damit unzulässig, daß z.B. Versicherungsnummer, Steuernummer, HVV-Abonnementsnummer bei den jeweiligen Buchungsposten auf dem Kontoauszug erscheinen. Er war der Meinung, der Kontoinhaber könne die einzelnen Buchungen auch ohne diese Angaben zuordnen.

Ich habe diese Problematik mit dem beteiligten Kreditinstitut erörtert und bin danach zu folgender Beurteilung gekommen: Die Angabe des Verwendungszwecks auf den Kontoauszügen erfolgt nur bei Sollbuchungen im Lastschriftenverfahren und bei Habenbuchungen, sofern diese Buchungen im Rahmen des beleglosen Zahlungsverkehrs abgewickelt werden. In diesen Fällen leitet das Kreditinstitut nur die Daten an den Kontoinhaber weiter, die ihm vom Auftraggeber (Abbuchender oder Überweisender) zur Weitergabe an den Kontoinhaber übermittelt werden. Es nimmt also in keiner Weise Einfluß darauf, welche Daten der Kontoinhaber erhält. Es druckt lediglich das auf den Kontoauszügen aus, was es vom Auftraggeber erhalten hat. Es entscheidet also der Auftraggeber, nicht das Kreditinstitut, was als Verwendungszweck auf den Kontoauszügen erscheint.

Das Kreditinstitut ist verpflichtet, die Daten, die als Verwendungszweck angegeben werden, unverändert an den Kontoinhaber weiterzuleiten. Es wäre mit den Pflichten eines Kreditintitutes nicht zu vereinbaren, wollte es bei einzelnen Daten Veränderungen vornehmen. Bei arbeitstäglich fast 500.000 Aufträgen im Zahlungsverkehr bei einem – wenn auch großen – Kreditinstitut wäre es organisatorisch auch nicht möglich, die einzelnen Überweisungen daraufhin zu überprüfen, ob im Verwendungszweck Daten übermittelt werden, die überflüssig sind. Es ist auch nicht recht vorstellbar, wie das Kreditinstitut dies prüfen und entscheiden sollte.

Wenn ein Kontoinhaber die Angabe des Verwendungszwecks einer Buchung für überflüssig hält, weil er in der Lage ist, die Buchung auch ohne nähere Angaben zu identifizieren und zuzuordnen, so werden andere Kontoinhaber sicher nicht immer ohne Angabe des Verwendungszwecks die einzelnen Buchungen identifizieren können. Zum anderen müßte jeder, der die Angabe des Verwendungszwecks von Buchungen verhindern will, die jeweiligen Auftraggeber entsprechend anweisen, da das Kreditinstitut – wie ausgeführt – lediglich die Daten weiterleitet, die es von den Auftraggebern erhält. Die meisten Auftraggeber würden allerdings nicht bereit sein, auf die Angabe des Verwendungszwecks zu verzichten, da dies auch der Zuordnung der Buchung beim Auftraggeber selbst dient.

Zu der technischen Seite der Angelegenheit habe ich festgestellt, daß diese Daten – jedenfalls bei dem betroffenen Kreditinstitut – nicht auf Dauer gespeichert werden. Die Daten zum Verwendungszweck bleiben dort nur bis zum Ende des Tages gespeichert, an dem der Kunde den Kontoauszug erhält, und werden dann gelöscht. Wenn der Kunde dann den Kontoauszug verliert, ist das Kreditinstitut aufgrund der weiter für das Konto gespeicherten Daten lediglich in der Lage, die einzelnen Geldbewegungen zu

rekonstruieren, nicht aber den Verwendungszweck der Buchungen anzugeben. Die einzelnen Mitarbeiter des Kreditinstituts haben also keinen Zugang mehr zu diesen Daten.

Nach allem ist dieses Verfahren als datenschutzrechtlich unbedenklich anzusehen.

5.3.4 EC-Karte und Geldautomat

Die Eurocheque-Karte oder EC-Karte hat neben der Garantiefunktion in Verbindung mit einem Euroscheck-Vordruck, der manuell ausgefüllt wird, zunehmende Bedeutung als Ausweis für einen Geldautomaten gewonnen. Geldautomaten sind zwar in der Bundesrepublik noch nicht so weit verbreitet wie teilweise im Ausland; dennoch gibt es bereits jetzt besorgte Fragen nach ihrer Sicherheit.

Um das Ergebnis vorwegzunehmen: In allen bisher bekannt gewordenen Fällen, in denen Unberechtigte mit einer EC-Karte Geld aus einem Geldausgabeautomaten zu Lasten eines anderen Kontos erlangt haben, ist ihnen dies nur gelungen, wenn der EC-Karteninhaber beim Umgang mit der EC-Karte und der dazugehörigen „Persönlichen Identitäts-Nummer" (PIN) nicht genügend Sorgfalt aufgewendet hat, so daß ein Dritter die EC-Karte entwenden und die PIN ausspähen konnte. Es ist bisher nicht gelungen, eine EC-Karte nachzumachen oder die PIN ohne Mitwirkung des Inhaber auszuforschen.

Das Verfahren der Benutzung eines Geldausgabeautomaten wird im folgenden kurz dargestellt.

Wenn Geld über einen Geldausgabeautomaten abgehoben werden soll, muß zunächst die EC-Karte eingeführt werden. Die eingeführte EC-Karte wird auf Echtheit und darauf geprüft, ob sie gesperrt ist. Danach muß der Benutzer seine PIN über Tastatur eingeben; sie wird mit einer PIN verglichen, die in dem Geldausgabeautomaten errechnet wird. Mit der Geheimzahl identifiziert sich der Kontoinhaber und weist sich zugleich als Berechtigter aus.

Es ist einem Unberechtigten nahezu unmöglich, über Geldausgabeautomaten Geld von fremden Konten abzuheben.

1) Die EC-Karte ist nahezu fälschungssicher, weil sie unsichtbar Merkmale enthält, deren Auswertung beim Lesen im Geldausgabeautomat bestimmten Speicherinhalten im Codierstreifen entsprechen muß. Die EC-Karte wird im Auftrage der Banken speziell für einen Kunden beschriftet.

2) Bei der Beschriftung wird zugleich mit Hilfe eines anerkannten Verschlüsselungsalgorithmus und geheimer Schlüssel die PIN gebildet, die dem Kontoinhaber zusammen mit der EC-Karte in einem Briefumschlag übergeben wird, der es unmöglich macht, den Inhalt ohne Öffnung zu lesen.

   Die Kenntnis der Schlüssel wird äußerst restriktiv gehandhabt. Einige Schlüssel z.B. sind in den Bankinstituten nicht bekannt. Die Kenntnis anderer Schlüssel ist in jedem Bankinstitut auf sehr wenige Personen in hoher Führungsebene und immer nur auf Teile des Schlüssels beschränkt. Darüberhinaus sind die Schlüssel in den Geldausgabeautomaten gegen Auslesen geschützt.

3) Die PIN ist gegen Ausprobieren durch die Begrenzung der Fehlversuche geschützt. Die Zahl der Fehlversuche wird in der EC-Karte gespeichert und bei jedem tatsächlichen Fehlversuch entsprechend berichtigt.

Das Verfahren der Benutzung von Geldausgabeautomaten ist ausreichend sicher, wenn der Karteninhaber sich sicherheitsbewußt verhält:

- Er muß die EC-Karte sicher verwahren.
- Er muß dem Bankinstitut sofort melden, wenn eine EC-Karte abhanden gekommen ist. Die EC-Karte wird dann gesperrt; die Sperre wird frühestens am nächsten Tag wirksam.

- Die PIN darf nicht oder – wenn unumgänglich – nicht an leicht zugänglichen Orten aufgezeichnet werden; solche Orte sind z.B.
  die EC-Karte,
  das Adreßbuch unter B wie Bank.
- Die PIN darf auch an vertraute Dritte nicht weitergegeben werden.
- Bei der Eingabe der PIN sollte die Tastatur gegen Einblick Fremder geschützt werden. Hier müssen die Bankinstitute durch geeignete Vorkehrungen (z.B. waagerechte Anordnung der Tastatur, Sichtblenden, Absperrungen) die Geheimhaltung bei der Eingabe erleichtern.

Aber selbst wenn es einem Unberechtigten gelungen ist, eine EC-Karte zu entwenden und die dazugehörige PIN auszuspähen, sind der unzulässigen Abhebung Grenzen gesetzt.

1) Bei Geldausgabeautomaten des eigenen Bankinstituts wird aufgrund der im Konto gespeicherten Informationen geprüft, ob der gewünschte Betrag innerhalb des Guthabens oder des eingeräumten Dispositionsrahmens liegt.

2) Eine Sperre wird bei anderen Bankinstituten frühestens am nächsten Tag wirksam, weil sie an eine (bundesweite) Zentrale gegeben und von dort über Datenträgeraustausch oder über Leitung an alle Bankinstitute verteilt wird. Allerdings darf bei Geldausgabeautomaten fremder Bankinstitute nur einmal am Tag bis zu 400,– DM abgehoben werden. Die Einhaltung dieser Begrenzung wird überprüft und die EC-Karte eingezogen, wenn versucht wird, an einem Tag mehr als einmal zu verfügen.

   Vor kurzem ist es Journalisten gelungen, eine EC-Karte so zu verändern, daß mehrmals an einem Tag bei jeweils anderen Banken Geldbeträge abgehoben werden konnten. Voraussetzung hierfür ist eine geeignete technische Ausrüstung. Dann könnte unter Ausnutzung eines Wochenendes und Benutzung vieler, voneinander unabhängiger Geldausgabeautomaten der Verlust sehr hoch sein, wenn die EC-Karte entwendet und die PIN ausgespäht worden ist.

   Aufgrund dieser Erfahrung halte ich es für notwendig, daß die Bankinstitute ihre Kunden über die Sicherheitsrisiken intensiver als bisher aufklären und nur noch Geldausgabeautomaten einsetzen, bei denen die PIN verdeckt eingegeben werden kann; dazu gehört mindestens, daß die Tastatur waagerecht und in einer Nische angeordnet ist. Alle Geldausgabeautomaten, die diesen Anforderungen nicht entsprechen, sind gegen das Ausspähen der PIN nicht ausreichend gesichert.

   Die Veränderung der EC-Karte nützt dann nichts mehr, wenn alle Geldausgabeautomaten on-line an eine Zentrale angeschlossen werden, in der alle Verfügungen eines Tages gesammelt werden; denn in diesem Falle kann in den schon angefallenen Verfügungen nachgeprüft werden, ob die EC-Karte schon benutzt worden ist. Da eine bundesweite Zentrale sehr aufwendig sein dürfte, wären regionale Zentralen jedenfalls als Übergangslösung geeignet.

5.3.5 Kontenführung über Btx

Btx ermöglicht u.a., das Bankkonto unabhängig von Öffnungszeiten und ohne Verlassen der Wohnung zu führen. Diese Dienstleistung umfaßt eine im Vergleich zum Schalterdienst und zu Selbstbedienungsterminals eingeschränkte Kontenführung:

Informationen über Kontenstände und Bewegungen,

Überweisungen.

Voraussetzung für die Kontenführung über Btx – auch home-banking genannt – ist natürlich, daß das betreffende Bankinstitut seine Konten über Btx zugänglich macht. Über Btx sind Konten nur erreichbar, wenn die Bank – die die Konten verwaltet – am Btx mit einem externen Rechner teilnimmt und Zugriffe über Btx zuläßt.

Aber auch wenn die Konten einer Bank über Btx erreichbar sind, hat damit nicht jedermann Zugang zu jedem Konto, kann nicht jedermann z.B. sich über das Konto seines

Nachbarn informieren. Sicherheitsvorkehrungen wie „persönliche Identitäts-Nummer" (PIN) und „Transaktions-Nummer" (TAN) sowie u.U. weitere (Paßwörter, Zeitschloß) können bei entsprechendem Gebrauch verhindern, daß andere als der Kontoinhaber oder die von ihm bevollmächtigten Personen Zugang zu seinem Konto erlangen.

Die Kenntnis dieser schlichten Tatsachen ist aber leider nur sehr wenig verbreitet. Sonst hätte eine als Satire gedachte Fernsehsendung von Radio Bremen, in der jedermann über Btx Zugang zu jedem gewünschten Konto erhielt, nicht so viele besorgte Anfragen ausgelöst. Ich finde es schon bedenklich, daß ein so offensichtlicher Unsinn – für den Zugang zum Konto genügte es, wenn man den Namen des Kontoinhabers angab – ernst genommen wird. Für mich sind solche Dinge Veranlassung, meine relativ breite Berichterstattung über Anwendungen von Technik fortzusetzen und so dazu beizutragen, daß Informationsdefizite abgebaut werden.

Auf Fragen der Datensicherung bei home-banking bin ich in meinem 3. TB (s. S. 20 f.) ausführlicher eingegangen bzw. gehe ich in diesem Tätigkeitsbericht näher ein.

5.3.6 Das Notieren von personenbezogenen Daten auf der Rückseite eingelöster Schecks

Ein Bürger stellte mir die Frage, ob das Notieren personenbezogener Daten bei Scheckeinlösungen zulässig ist und ob diese Daten gespeichert und an andere Stellen übermittelt werden. Ich habe diese Angelegenheit mit dem beteiligten Kreditinstitut erörtert und bin danach zu folgendem Ergebnis gekommen:

Das Kreditinstitut läßt sich aus Sicherheitsgründen in bestimmten Fällen den Personalausweis vorlegen und notiert den Namen, die Anschrift, das Geburtsdatum und die Personalausweisnummer der Person, die den Scheck vorlegt, auf der Rückseite des Schecks. Dies hat den Zweck, dem Kontoinhaber später Auskunft über den Scheckverwender geben zu können, wenn der Scheck sich als gestohlen erweisen sollte.

Es handelt sich hier also um eine Sicherheitsmaßnahme, die im Interesse der Kontoinhaber getroffen worden ist. Gegen dieses Verfahren ist aus der Sicht des Datenschutzes nichts einzuwenden, da die Daten nur notiert werden, um bei späteren Rückfragen zugänglich zu sein, und ansonsten nicht weiterverwendet werden. Das Kreditinstitut überträgt die Daten nicht in eine Liste oder Datei, verwendet sie nicht für andere Zwecke und leitet sie auch nicht an andere Stellen weiter.

5.4 Versicherungswirtschaft

5.4.1 Zentrale Dateien der Versicherungsverbände

In meinem 2. TB habe ich ausführlich dargestellt, welche Datenübermittlungen zwischen Versicherungsunternehmen und einigen Versicherungsverbänden stattfinden (4.3.1, S. 113 ff). Dort habe ich ausgeführt, welchen rechtlichen Bedenken diese Datenübermittlungen im einzelnen begegnen.

In der Zwischenzeit haben verschiedene Gespräche über diese Thematik zwischen dem „Düsseldorfer Kreis" und Verbänden der Versicherungswirtschaft stattgefunden. Dabei konnten folgende Zwischenergebnisse erzielt werden:

Die Versicherungswirtschaft hält zwar an ihrer Rechtsauffassung fest, daß die Datenübermittlungen der einzelnen Versicherungsunternehmen an den jeweiligen Verband und die anschließenden Datenübermittlungen vom Verband an alle dem Verband angeschlossenen Versicherungen der Sparte versicherungsvertragsgesetzlich geboten und vom BDSG gedeckt seien. Mit Rücksicht auf die davon abweichende Rechtsauffassung der Datenschutz-Aufsichtsbehörden, nach der die Datenübermittlungen aus der Sonderwagnisdatei Leben und der Datei der Zentralen Registrierstelle Rechtsschutz an alle dem Lebens- bzw. dem HUK-Verband angeschlossenen Mitgliedsunternehmen und deren Vorratsspeicherung unzulässig sind, hat sich die Versicherungswirtschaft aber bereit erklärt, eine Neugestaltung der Meldeverfahren zu erproben und im Falle positiver Ergebnisse umzusetzen.

1. Bei der Sonderwagnisdatei der Lebensversicherer (vgl. 2. TB, 4.3.1.2, S. 115 f) sollen sich nach einem Änderungsvorschlag der Versicherungswirtschaft Verfahren und Umfang der Datenübermittlungen an den Verband nicht ändern. Das Verfahren der Datenübermittlungen des Verbandes an die einzelnen Versicherungsunternehmen soll allerdings insofern modifiziert werden, als der Verband aus bisher schon verwandten identifizierenden Angaben und einer Meldenummer einen verkürzten Suchbegriff bildet und nur diesen zu Zwecken einer Vorprüfung an die ihm angeschlossenen Versicherungsunternehmen übermittelt. Diese gleichen die empfangenen verkürzten Suchbegriffe mit ihrem Vertragsbestand ab.

   Nach Vermutungen der Versicherungswirtschaft werden die Versicherungsunternehmen in der weit überwiegenden Mehrzahl der Fälle feststellen, daß der Antragsteller mit dem neu gemeldeten Sonderwagnis nicht in ihrer Datei enthalten ist. In den verbleibenden wenigen Fällen, also insbesondere dann, wenn dem Versicherungsunternehmen ein Antrag vorliegt, dessen Daten mit dem Suchbegriff übereinstimmen, kann es sich entweder mit dem Verband oder dem Versicherungsunternehmen, das das Sonderwagnis eingemeldet hat, in Verbindung setzen, um die Identität zu klären.

   Bei kurzem Familiennamen kommt eine „Anonymisierung" durch eine sinnvolle Ergänzung auf 5 Stellen (programmgesteuertes Nachschieben zusätzlicher Buchstaben) in Betracht.

   Die Datenschutzaufsichtsbehörden halten dieses Matchcode-Verfahren für eine wesentliche Verbesserung, weil die einzelnen Versicherungsunternehmen eine vollständige Reidentifizierung des verkürzten Suchbegriffs nicht allein vornehmen können.

   Parallel zu dieser Änderung müßten nach Auffassung der Aufsichtsbehörden jedoch flankierende Maßnahmen (Konkretisierung der derzeit verwendeten Datenschutz-Ermächtigungsklausel, Verbesserung der Erläuterungen hierzu) ergriffen werden. Die Versicherungswirtschaft steht einer kundennäheren Unterrichtung über das neue Meldeverfahren nicht grundsätzlich ablehnend gegenüber.

   Die Überlegungen zur Verschlüsselung der Daten sind in der Versicherungswirtschaft noch nicht abschließend diskutiert worden. Die Einzelheiten müssen vielmehr noch getestet und auch in den zuständigen Verbandsgremien abgestimmt werden. Bei den bisherigen Testläufen haben sich allerdings keine größeren Bedenken gegen das Verfahren und auch die Art der Verschlüsselung ergeben.

2. Der HUK-Verband prüft, ob eine entsprechende Verfahrensänderung bei der Zentralen Registrierstelle Rechtsschutz (vgl. 2. TB, 4.3.1.1, S. 114 f) in Betracht kommt. Der dort gespeicherte Datensatz ist dem der Sonderwagnisstelle Leben vergleichbar, wenn er auch nicht das Geburtsdatum, dafür aber Anschrift und Beruf umfaßt.

   Der HUK-Verband hält das von den Lebensversicherern erwogene Matchcode-Modell ebenfalls für geeignet und erwägt, es mit folgenden Modifizierungen einzuführen. Die Versicherungsunternehmen sollen im Kündigungsfall eine Meldung mit etwas reduzierten Daten an den Verband geben. Der Verband verwandelt diese Daten dann in den Matchcode. Nur die Matchcodes werden dann pauschal an alle Rechtsschutzversicherer gegeben. Die an den HUK-Verband gegebenen Meldungen werden nach der Verwandlung in den Matchcode vernichtet. Bei den einzelnen Versicherungsunternehmen werden die Daten dann zusammengefaßt, wenn Anträge gestellt werden. Es wird erwartet, daß Paarigkeit nur in sehr seltenen Fällen auftreten wird. In Fällen von Paarigkeit kann das Versicherungsunternehmen bei dem jeweils anderen Versicherungsunternehmen anfragen. Das weitere Verfahren würde dann so ablaufen wie bisher.

5.4.2 Schweigepflichtentbindungsklausel

Im 3. TB (4.3.1, S. 105 f) hatte ich meine rechtlichen Bedenken gegenüber der derzeit bei Anträgen auf private Kranken-, Unfall- und Lebensversicherungen verwandten

Schweigepflichtentbindungsklausel dargestellt. Diese beziehen sich im wesentlichen darauf, daß die Klausel pauschal auch in der Zukunft liegende ärztliche Behandlungen umfaßt, und daß sie allgemein auch „Behörden" von der Schweigepflicht entbinden soll, obwohl nach § 67 Satz 1 SGB X die Betroffenen grundsätzlich im Einzelfall in eine Offenbarung von Daten eingewilligt haben müssen.

In einem Gespräch zwischen dem „Düsseldorfer Kreis" und Vertretern der Versicherungswirtschaft wurde diese Problematik inzwischen erörtert. Dabei konnte Einigkeit darüber hergestellt werden, daß eine Eingrenzung der durch die Schweigepflichtentbindungsklausel abzudeckenden Datenübermittlungen auf das jeweils versicherungsvertraglich Erforderliche anzustreben ist.

Gegenwärtig werden Neuformulierungen der Klausel für verschiedene Versicherungssparten zwischen Versicherungswirtschaft, Bundesaufsichtsamt für das Versicherungswesen und Datenschutz-Aufsichtsbehörden diskutiert. Bisher liegen Formulierungsvorschläge für Klauseln bei Unfall- und Krankenversicherungen vor. Entsprechende Änderungen werden auch für Lebensversicherungen erwogen.

5.4.3 Teilungsabkommen in der Versicherungswirtschaft

Versicherungsunternehmen haben vielfach Teilungsabkommen geschlossen, nach denen zwei oder mehr Versicherungen Schäden quotenmäßig ohne Rücksicht auf ihre tatsächliche Haftung tragen, wenn mehrere Versicherungsunternehmen wegen eines Schadens in Anspruch genommen werden. Ein derartiges Teilungsabkommen kommt z.B. zur Anwendung, wenn ein Kraftfahrer den ihm zugefügten Sachschaden nicht bei der Haftpflichtversicherung seines zahlungsverpflichteten Unfallgegners, sondern bei seiner ebenfalls zahlungsverpflichteten Vollkaskoversicherung geltend macht. Wenn zwischen diesen beiden Versicherungen ein Teilungsabkommen besteht, nach welchem derartige Schäden ohne Rücksicht auf die jeweiligen rechtlichen Verpflichtungen hälftig geteilt werden, dann meldet die Vollkaskoversicherung, die den gesamten Schaden des geschädigten Kraftfahrers reguliert hat, die Hälfte davon zur Zahlung bei der Haftpflichtversicherung des Unfallgegners an. Diese überweist ihre Hälfte ohne weitere rechtliche Prüfung an die Vollkaskoversicherung.

Diese Teilungsabkommen werden im allgemeinen nach Mustern abgeschlossen, die der HUK-Verband erarbeitet hat. Nach § 6 Nr. 2 des Standard-Teilungsabkommens (Stand 15.7.1985) für derartige Fälle muß der „bearbeitende" (also den Schaden regulierende) Abkommenspartner seine erstattungsfähigen Aufwendungen lediglich spezifizieren. Auf die Vorlage von Unterlagen zum Nachweis der Höhe der erstattungsfähigen Aufwendungen wird grundsätzlich verzichtet. Nach Nr. 14 der Erläuterungen zu diesem Standard-Teilungsabkommen wird dadurch nicht ausgeschlossen, daß der in Anspruch genommene Abkommenspartner die Übersendung derartiger Unterlagen im Einzelfall verlangen kann.

Dieses Verfahren wird zur Vereinfachung gewählt, weil umständliche Nachprüfungen der Haftungsfragen und der Höhe der verursachten Aufwendungen teurer wären, als eine quotenmäßige Aufteilung der Schadensersatzzahlungen.

Die anspruchstellende Versicherung muß also bei diesem Verfahren der jeweils anderen Versicherung nur mitteilen, um welchen Schaden es sich handelt, daß dieser unter das Teilungsabkommen fällt und in welcher Höhe sie gezahlt hat. Weiteres braucht nach dem Teilungsabkommen ausdrücklich nicht mitgeteilt zu werden.

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, daß eine Versicherung zur Anmeldung ihres Anspruches nach dem Teilungsabkommen die gesamte von dem Unfallopfer ausgefüllte Schadensmeldung in Kopie an die andere Versicherung gegeben hatte. Sie hatte damit mehr mitgeteilt, als nach dem Teilungsabkommen nötig war, u.a. auch die (wie sich später herausstellte: falsche) Einschätzung des Unfallopfers hinsichtlich der medizinischen Folgen des Unfalls. Diese Informationen, die für den Sachschaden am Kraftfahrzeug unerheblich waren, wurden von der anderen Versicherung später gegen das Unfallopfer verwandt, als dieses von ihr Schadensersatz

wegen der ebenfalls erlittenen Körperschäden verlangte. Dazu war diese Versicherung nur in der Lage, weil sie die gesamte Schadensmeldung in Kopie erhalten hatte.

Über diese Problematik habe ich ein Gespräch mit dem HUK-Verband geführt, der das Standard-Teilungsabkommen ausgearbeitet hat.

Ich bin der Meinung, daß deutlich getrennt werden muß zwischen den Angaben, die der Versicherungsnehmer zur Geltendmachung seines Schadens bei seiner Versicherung machen muß, und den Angaben, die die Versicherung nach dem Teilungsabkommen zur Darlegung des Vorliegens der Voraussetzungen des Teilungsabkommens gegenüber der jeweils anderen Versicherung machen muß. Da der Umfang der letzteren Angaben erheblich geringer ist als der Umfang der zuerst genannten Angaben, geht es nicht an, sämtliche von dem Versicherungsnehmer gegenüber seiner Versicherung gemachten Angaben komplett bei der Darlegung eines Anspruchs aus dem Teilungsabkommen an eine andere Versicherung zu übermitteln. Dann wird mehr übermittelt, als nötig ist.

Weiter habe ich die Vertreter des HUK-Verbandes darauf hingewiesen, daß die Empfänger der Daten auf das Zweckbindungsprinzip hingewiesen werden müssen. Die Versicherungsunternehmen, die im Rahmen von Teilungsabkommen Daten übermittelt bekommen, dürfen diese nur für Zwecke verwenden, für die sie die Daten erhalten haben.

Der HUK-Verband hat eine Überprüfung zugesagt. Die Gespräche dauern an.

5.4.4 Datenübermittlungen im Rahmen von fakultativen Gruppenversicherungsverträgen

Seit zwei Jahren beschäftigte ich mich mit dem Problem, daß Vereine oder Verbände im Rahmen fakultativer Gruppenversicherungsverträge personenbezogene Daten ihrer Mitglieder an Versicherungsgesellschaften übermitteln, ohne daß die Einwilligung der Betroffenen vorliegt (vgl. 2. TB, 4.3.3, S. 119 f).

Durch fakultative Gruppenversicherungsverträge erhalten die Vereinsmitglieder die Möglichkeit zum Abschluß von Einzelverträgen zu günstigeren Konditionen. Nach den Auflagen des BAV werden die Einzelverträge nur wirksam, wenn mindestens 50% der Mitglieder des jeweiligen Vereins derartige Verträge abgeschlossen haben.

Bisher übermitteln die Vereine aufgrund des Gruppenversicherungsvertrages den Namen, die Anschrift und teilweise das Geburtsdatum ihrer Mitglieder an die Versicherung, damit diese die Mitglieder wegen Neuabschluß oder Erhöhung eines bereits bestehenden Versicherungsvertrages umwerben kann. Die Mitglieder erfahren lediglich, daß sie im Rahmen des fakultativen Gruppenversicherungsvertrages eine günstige Sterbegeld- und Unfallversicherung abschließen können.

Der „Düsseldorfer Kreis" hatte sich bereits 1979 mit einem Vorschlag des BAV einverstanden erklärt, daß im Rahmen von fakultativen Gruppenversicherungsverträgen entweder der Verein die Werbung für den Abschluß einer Versicherung selbst übernimmt oder daß er nur Daten von Mitgliedern übermittelt, die sich schriftlich damit einverstanden erklärt haben.

Nach Auffassung des beteiligten Versicherungsunternehmens richtet sich die Zulässigkeit der Übermittlung nach § 24 Abs. 1 Satz 1 letzte Alt. BDSG, d.h. die berechtigten Interessen des werbenden Unternehmens sind gegen die schutzwürdigen Belange des Betroffenen abzuwägen.

In den letzten beiden Jahren habe ich verschiedene Gespräche geführt, die bisher folgenden Diskussionsstand erbracht haben:

Es konnte Einigkeit darüber erzielt werden, daß die Daten neu eintretender Mitglieder der Vereine grundsätzlich nur mit schriftlicher Einwilligung an die Versicherung übermittelt werden dürfen. Es wird sichergestellt, daß Beitrittswillige den Vereinen auch bei Streichung dieser Einwilligungsklausel im Aufnahmeantrag beitreten können.

Für die „Altmitglieder" wurde eine Widerspruchslösung vereinbart. Ihnen soll vor Beginn von Werbeaktionen des Versicherungsunternehmens, zu dessen Vorberei-

tung eine Liste mit den Adressen der zu umwerbenden Mitglieder an die Versicherung übermittelt werden soll, Gelegenheit gegeben werden, dieser Übermittlung zu widersprechen.

Diese Widerspruchslösung für die „Altmitglieder" erscheint mir als vertretbar, da es mit einem unverhältnismäßigen Aufwand verbunden wäre, von allen Personen, die bereits Mitglieder der Vereine sind, Einwilligungserklärungen für die Datenübermittlungen unterschreiben zu lassen, und i.ü. die Versicherungen i.d.R. nicht in der Lage wären, die oben erwähnte Auflage des BAV zu erfüllen.

Das Recht dieses Personenkreises auf informationelle Selbstbestimmung wird gewahrt, da jeder der Datenübermittlung widersprechen kann.

Das beteiligte Hamburger Versicherungsunternehmen hat sich mit diesem Verfahren im Prinzip einverstanden erklärt. Es möchte sich allerdings einen zweiten Weg offenhalten. Die Vereine könnten – so meint die Versicherungsgesellschaft – die Datenübermittlungen auch in ihren Satzungen absichern, so daß sie auch ohne besondere Einwilligung nach § 24 Abs. 1 Satz 1 Alt. 1 BDSG („Die Übermittlung personenbezogener Daten ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen") erfolgen dürften. Diese Alternative halte ich für problematisch.

Derartige Satzungsänderungen wären m.E. praktisch nicht durchführbar, weil sie in aller Regel Änderungen des Vereinszwecks wären, die nach § 33 Abs. 1 Satz 2 BGB grundsätzlich nur einstimmig beschlosssen werden könnten. Einstimmige Beschlüsse der Mitgliederversammlungen dürften jedoch bei größeren Vereinen praktisch nicht oder nur unter größten Schwierigkeiten durchsetzbar sein.

Im übrigen würde wohl auch das informationelle Selbstbestimmungsrecht der Betroffenen einem Lösungsversuch über eine Satzungsänderung entgegenstehen, in das nur aufgrund einer ausreichend klaren und verhältnismäßigen Rechtsgrundlage eingegriffen werden darf.

Das Versicherungsunternehmen vertritt die Auffassung, daß die erwogenen Satzungsänderungen häufig keine Änderungen des jeweiligen Vereinszwecks wären, so daß sie nicht unter den erschwerenden Bedingungen des § 33 Abs. 1 BGB für Änderungen des Vereinszwecks herbeigeführt werden müßten, daß sie vielmehr mit der Dreiviertelmehrheit für sonstige Satzungsänderungen beschlossen werden könnten.

Ich rechne damit, daß die Diskussion in Kürze zu einer Lösung führen wird, die zugleich den Belangen des Datenschutzes als auch den wirtschaftlichen Interessen der Versicherungen gerecht wird.

5.5 Auskunfteien

5.5.1 Allgemeine Probleme

5.5.1.1 Angebot von bonitätsgeprüften Adressen durch Handels- und Wirtschaftsauskunfteien

In einem Gespräch, das der „Düsseldorfer Kreis" Anfang 1985 mit Vertretern der Handelsauskunfteien geführt hat, wurde vor allem die Weitergabe EDV-mäßig insbesondere unter Bonitätskriterien selektierter Marketingadressen erörtert (3. TB, 4.4.1, S. 107 f.). Über dieses Thema habe ich ein gesondertes Gespräch mit der Auskunftei geführt, die inzwischen auch ihren Hamburger Adreßbestand für diese Nutzungsform anbietet. Eine abschließende rechtliche Beurteilung durch die Datenschutzaufsichtsbehörden ist noch nicht erfolgt. Ich habe bei meinem Gespräch vereinbart, daß ich zur Klärung des Sachverhalts bei dem Hamburger Büro dieser Auskunftei eine Prüfung gem. § 40 BDSG vornehmen werde. Die Zentrale dieser Auskunftei soll ebenfalls von der örtlich zuständigen Aufsichtsbehörde überprüft werden. Aufgrund des bei diesen Prüfungen festgestellten Sachverhalts kann dann eine endgültige rechtliche Beurteilung dieser Datenübermittlungen vorgenommen werden.

5.5.1.2 Aufforderung zur Selbstauskunft

Auskunfteien sind,gem. § 34 Abs. 1 BDSG verpflichtet, Betroffene über die Speicherung von Daten zu benachrichtigen, wenn sie erstmals Daten dieser Personen an einen Dritten übermitteln. Diese Benachrichtigung wird oft mit der Bitte verbunden, einen Fragebogen als Selbstauskunft auszufüllen und an die Auskunftei zurückzuschicken. Bereits in meinem 1. TB (7.1.1, S. 51) hatte ich darauf hingewiesen, daß Benachrichtigung und die Bitte um mehr Daten deutlicher voneinander abgesetzt werden müssen, damit dem Angeschriebenen klar wird, daß er nicht etwa eine gesetzliche Pflicht zum Ausfüllen und Zurücksenden des beigefügten Fragebogens hat. Auf die Freiwilligkeit dieser Leistung ist besonders hinzuweisen.

Die Formschreiben zur Benachrichtigung sind zwar neugestaltet und insoweit verbessert worden, als darüber aufgeklärt wird, daß keine Verpflichtung zur Selbstauskunft besteht. Gleichwohl erreichen mich nach wie vor zahlreiche Anfragen, die zeigen, daß viele der Angeschriebenen meinen, sie müßten die Fragebogen zurückschicken. Deshalb habe ich mir vorgenommen, diese Problematik erneut über den „Düsseldorfer Kreis" an die Wirtschaftsauskunfteien heranzutragen.

5.5.2 Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD)

In meinen letzten Tätigkeitsberichten habe ich bereits ausführlich über die mit dem AVAD-Meldeverfahren verbundenen datenschutzrechtlichen Probleme berichtet (1. TB, 7.1.2, S. 52; 2. TB, 4.4.2, S. 123 f.; 3. TB, 4.4.2, S. 108). Das im 3. TB angesprochene neue Verfahren ist jetzt mit Wirkung vom 1.8.1985 in die Praxis umgesetzt worden. Dieses Verfahren, über das ich mich in mehreren Gesprächen mit der AVAD und der Versicherungswirtschaft geeinigt habe, sieht im einzelnen folgende Verbesserungen vor:

Die Datenübermittlungen im Rahmen des AVAD-Auskunftsverfahrens werden Gegenstand des Anstellungsvertrages mit den Außendienstmitarbeitern, die nach dem 1.8.1985 (als Angestellter oder Handelsvertreter) eingestellt werden. Den neuen Mitarbeitern wird ein „Informationsblatt über den AVAD-Auskunftsverkehr" ausgehändigt, in dem das gesamte Verfahren erläutert wird. Außendienstmitarbeiter, die vor dem 1.8.1985 eingestellt waren, müssen keine ausdrückliche Einwilligung erklären. Sie werden durch Übersendung des Informationsblattes und durch Veröffentlichungen in Hauszeitschriften oder anderen Informationsdiensten unterrichtet.

Das Auskunftsverfahren läuft jetzt wie folgt ab:

Das Formular für AVAD-Auskünfte ist insofern geändert worden, als nur noch nach rückforderbaren Salden aus nicht verdienter Provision gefragt wird. Nicht rückforderbare Salden tauchen jetzt nicht mehr in den Auskünften auf.

Beim Ausscheiden eines Außendienstmitarbeiters wird die AVAD-Auskunft gleichzeitig an die AVAD und an den betroffenen Mitarbeiter gegeben. Dieser hat dadurch die Möglichkeit, sofort auf unrichtige Angaben hinzuweisen und seine Einwände gegen den Inhalt der Auskunft und/oder das Speichern bei der AVAD vorzutragen. Von Nachmeldungen, Korrekturen und Ergänzungen erhält der betroffene Mitarbeiter ebenfalls sofort eine Kopie.

Wenn ein Außendienstmitarbeiter gegen Teile der Auskunft Einspruch bei dem Versicherungsunternehmen einlegt, das die AVAD-Auskunft ausgefüllt hat, wird die AVAD darüber von dem Unternehmen unterrichtet unter gleichzeitiger Mitteilung, wie es auf den Einspruch reagieren will. Der betroffene Mitarbeiter erhält eine Kopie dieses Schreibens an die AVAD. Ist der Einspruch nicht völlig pauschal und unspezifiziert, werden die betroffenen Teile der Auskunft vorläufig bis zur Klärung gesperrt. Die übrige Auskunft bleibt davon unberührt und wird weiterhin von der AVAD vermittelt. Erweisen sich die Einwände des Betroffenen als begründet, erfolgt insoweit eine Löschung oder Berichtigung.

Wenn andere Versicherungsunternehmen bereits die AVAD-Auskunft erhalten haben, gegen die Einspruch erhoben wird, werden sie sofort von der AVAD über den Einspruch informiert.

Hierdurch ist sichergestellt, daß Betroffene sowohl über das gesamte Meldeverfahren als auch über die sie betreffenden Auskünfte umfassend und schnell informiert werden. Die Betroffenen haben dadurch die Möglichkeit, gegen Unrichtigkeiten sofort vorzugehen, ohne daß das Auskunftssystem dadurch nennenswert beeinträchtigt wird.

Eine Eingabe, die mir vor einigen Wochen zuging, hat gezeigt, daß das neue Verfahren offenbar noch nicht richtig eingespielt ist. Ein Versicherungsunternehmen hat mehrere Monate vor dem Ausscheiden zweier Außendienstmitarbeiter „anstelle einer Auskunft" ein formloses Schreiben an die AVAD gerichtet, in dem es darüber informierte, daß es kein Neugeschäft mehr von diesen Mitarbeitern annehmen wolle und daß es die Geschäftsbeziehungen mit diesen beiden Mitarbeitern auf die unumgänglich notwendigen Beziehungen aus den vorhandenen Versicherungsbeständen beschränke. Zur Beantwortung schriftlicher Anfragen anderer Gesellschaften sei dieses Unternehmen bereit. Die AVAD hat dieses Schreiben als Auskunft gewertet und anderen Gesellschaften vermittelt. Die Betroffenen haben keine Kopie dieses Schreibens erhalten.

Das beteiligte Versicherungsunternehmen hat erklärt, die Erstellung der AVAD-Auskunft sei zum Zeitpunkt des Versendens des Schreibens noch nicht möglich gewesen, da ein zu erwartender Saldo noch nicht exakt habe ermittelt werden können. Man habe deshalb nach Rückprache mit der AVAD ausnahmsweise die Form der Vormerkung gewählt. Da darin detaillierte Daten nicht enthalten seien, habe das Unternehmen es nicht für nötig erachtet, den beiden Mitarbeitern eine Kopie zukommen zu lassen.

Die AVAD hat zu diesem Fall erkärt, sie habe das Schreiben des Versicherungsunternehmens weitergeleitet, da das Unternehmen keinen Hinweis darauf gegeben habe, daß die Information vertraulich zu behandeln sei. Ein Gespräch mit der AVAD ist verabredet.

Aufgrund einer anderen Eingabe habe ich mich mit der Frage befaßt, ob das AVAD-Auskunftsverfahren dazu führt, daß die restriktive Rechtssprechung der Arbeitsgerichte zum zulässigen Inhalt von Zeugnissen und zum Fragerecht des Arbeitgebers umgangen wird, indem potentielle neue Arbeitgeber durch die AVAD-Auskünfte Details erfahren, die in Zeugnisse nicht aufgenommen werden dürfen und die der Arbeitgeber bei der Einstellung auch nicht erfragen darf. Die Prüfung dieser Problematik ist noch nicht abgeschlossen.

5.5.3 Schufa

5.5.3.1 BGH-Urteil zur Schufa-Klausel

Bereits in meinen beiden letzten Tätigkeitsberichten habe ich die mit der Schufa-Klausel verbundenen datenschutzrechtlichen Probleme erörtert (2. TB, 4.4.3.3, S. 126 f.; 3. TB, 4.4.3.3, S. 113 ff.). Die Klausel, die bisher bei der Beantragung von Krediten unterschrieben werden mußte, ist jetzt durch Urteil des BGH vom 19.9.1985 (III ZR 213/83; BB 1985, S. 1998) für unwirksam erklärt worden. Dieses Urteil hat nicht nur zur Folge, daß eine neue Schufa-Klausel erarbeitet werden muß, sondern auch, daß es Änderungen des Schufa-Auskunfts-Verfahrens geben wird.

Der BGH hat in seinem Urteil ausgeführt, das BDSG gestatte zwar „auch die Übermittlung bestimmter Kreditdaten an ein Kreditinformationssystem, das eine Kreditvergabe an Kreditunwürdige verhindern und damit den Interessen der Banken, aber auch der Allgemeinheit und der Kreditnehmer selbst dienen will. Notwendig ist jedoch, daß die übermittelnde Bank Aussagekraft und Berechtigung einer bestimmten Einzelmitteilung unter sorgfältiger Interessenabwägung prüft und außerdem das Kreditinformationssystem so organisiert ist, daß die gespeicherten Daten insgesamt ein möglichst vollständiges, aktuelles Bild der Kreditwürdigkeit bieten und die Weitergabe sich auf Anschlußnehmer beschränkt, die ein berechtigtes Interesse haben, über die Kreditwürdigkeit eines Betroffenen unterrichtet zu werden." Daraus folgt, daß sowohl der Katalog der an die Schufa zu übermittelnden Merkmale als auch der Kreis der Schufa-Vertragspartner eingeschränkt werden müssen. Anders wird dem zitierten Postulat des BGH nicht Rechnung getragen werden können.

5.5.3.1.1 Neufassung der Schufa-Klausel

Bisher wurden folgende Schufa-Klauseln verwandt:

Für Kreditanträge und Kreditverträge:

Das Kreditinstitut ist berechtigt, der Schufa Schutzgemeinschaft für allgemeine Kreditsicherung Daten des Kreditnehmers und etwaiger Mitschuldner über die Aufnahme (Kreditbetrag, Laufzeit, Ratenbeginn) und Abwicklung dieses Kredites zur Speicherung zu übermitteln. Die Adresse der Schufa lautet (folgt: Anschrift der zuständigen Schufa GmbH).

Für Kontoeröffnungsanträge:

Das Kreditinstitut ist berechtigt, der Schufa Schutzgemeinschaft für allgemeine Kreditsicherung Daten des Kontoinhabers über die Errichtung und nicht vertragsgemäße Nutzung dieser Kontoverbindung zur Speicherung zu übermitteln. Die Adresse der Schufa lautet: (folgt: Anschrift der zuständigen Schufa GmbH).

Für Bürgschaftserklärungen:

Das Kreditinstitut ist berechtigt, der Schufa Schutzgemeinschaft für allgemeine Kreditsicherung Daten des Bürgen über die Übernahme und Abwicklung dieser Bürgschaft zur Speicherung zu übermitteln. Die Adresse der Schufa lautet: (folgt: Anschrift der zuständigen Schufa GmbH).

Die Schufa und die Kreditwirtschaft sind bisher der Auffassung gewesen, daß diese Klausel lediglich der Benachrichtigung des Kunden über die Speicherung seiner Daten bei der Schufa dient. Die Datenschutz-Aufsichtsbehörden vertreten dagegen – jetzt durch das BGH-Urteil vom 19.9.1985 bestätigt– die Ansicht, daß die Klausel auch eine Erklärung über die Berechtigung des Kreditinstitutes zu der Datenübermittlung an die Schufa enthält. Der Kunde willigt also durch seine Unterschrift unter diese Klausel in die Verarbeitung seiner Daten im Rahmen des Schufa-Auskunftssystems ein. Wenn er dazu nicht bereit ist, kann er –jedenfalls bei Banken und Sparkassen– i.d.R. kein Girokonto eröffnen und bekommt keinen Kredit. Angesichts dieses faktischen Zwangs zur „freiwilligen" Einwilligung sind hohe Anforderungen an die inhaltliche Klarheit und Ausgewogenheit der Klausel zu stellen.

Der BGH hat jetzt die von einer Teilzahlungsbank verwendete Schufa-Klausel für unwirksam erklärt, deren Formulierung unwesentlich von der oben zitierten Klausel für Kreditanträge und Kreditverträge abweicht. Auch wenn das Urteil lediglich für den konkreten Fall gilt, ist doch wegen der Gleichheit der von allen Banken und Sparkassen verwandten Schufa-Klauseln davon auszugehen, daß alle diese Klauseln nun als unwirksam zu betrachten sind.

Nach dem BGH-Urteil verstößt die Klausel gegen § 9 des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, weil sie den Kunden unangemessen benachteiligt. Diese Benachteiligung liegt darin, daß die Klausel mit wesentlichen Grundgedanken des BDSG nicht vereinbar ist. Nach dem BGH-Urteil liegt eine wesentliche Benachteiligung vor, „wenn eine formularmäßige Einwilligung sich nicht auf bestimmte Kreditdaten beschränkt, sondern pauschal unter der Bezeichnung „Daten des Kreditnehmers über die Abwicklung des Kredits" auch Angaben über einseitige Maßnahmen des Kredigebers zur Durchsetzung vermeintlicher Ansprüche gegen den Kreditnehmer, beispielsweise Mahnungen, Kündigungen, Mahnbescheide .... umfassen soll und den Kreditgeber uneingeschränkt ermächtigt, auch derartige Negativmerkmale ohne Interessenabwägung im Einzelfall und sogar in Fällen, in denen eine solche Abwägung negativ ausfallen würde, an ein Kreditinformationssystem zu übermitteln."

Dies bedeutet zum einen, daß eine Schufa-Klausel keine pauschale Ermächtigung zur Übermittlung nicht näher spezifizierter Merkmale enthalten darf, sondern aufzählen muß, welche Merkmale an die Schufa übermittelt werden dürfen. Es bedeutet aber zum zweiten auch, daß bestimmte problematische Negativmerkmale nicht mit einer differenzierteren Einwilligung, sondern nur nach einer Einzelfallabwägung der Interessen der übermittelnden Stelle, eines Dritten oder der Allgemeinheit mit den schutzwürdi-

gen Belangen des Betroffenen an die Schufa übermittelt werden dürfen (§ 24 Abs. 1 S. 1 BDSG).

Unter Berücksichtigung dieser Grundsätze müssen die Schufa-Klauseln neu gefaßt werden. Dazu haben sich in den letzten Monaten des Jahres 1985 Vertreter der Kreditinstitute, der Schufa und der Datenschutz-Aufsichtsbehörden zusammengefunden, nachdem bereits im Jahre 1984 Gespräche geführt und Ergebnisse erzielt worden waren, die jetzt im Lichte des BGH-Urteils vom 19.9.1985 zu überprüfen waren. Neue Klauseln werden voraussichtlich ab Februar/März 1986 eingesetzt werden können.

Die neuen Schufa-Klauseln müssen die BGH-Rechtsprechung berücksichtigen, nach der die Übermittlung der einzelnen Merkmalarten differenziert zu beurteilen ist: Mit der Klausel wird die Einwilligung zur Datenübermittlung i.S.d. § 3 BDSG nur noch für die positiven Merkmale erklärt (z.B. Eröffnung eines Girokontos und Beendigung der Kontoverbindung, Aufnahme und Abwicklung eines Kredits). Die Übermittlung und Speicherung von Negativmerkmalen kann bei Berücksichtigung der BGH-Rechtssprechung nicht aufgrund einer Einwilligung, sondern nur noch nach Abwägung der schutzwürdigen Belange der Betroffenen mit den berechtigten Interessen der übermittelnden Stelle, eines Dritten oder der Allgemeinheit (§ 24 Abs. 1 Satz 1 BDSG) erfolgen. Dabei ist zwischen „harten" und „weichen" Negativmerkmalen zu unterscheiden. Die Übermittlung „harter" Negativmerkmale (wie z.B. Zwangsvollstreckung, Lohnpfändung) wird in aller Regel gerechtfertigt sein und kann deshalb aufgrund einer pauschalen Prüfung erfolgen, da die berechtigten Interessen der Allgemeinheit an einem Schutz vor der Vergabe von Krediten an Zahlungsunfähige oder -unwillige schwerer wiegen als die jeweils zu berücksichtigenden Belange der Betroffenen (vgl. BGH, Urteil vom 7.7.1983, III ZR 159/82, NJW 1984, S. 436, 437). Für die Übermittlung der „weichen" Negativmerkmale, also solcher Maßnahmen, die einseitig auf Veranlassung des Gläubigers und ohne gerichtliche Prüfung ergriffen werden (wie z.B. beantragter Mahnbescheid), wird dagegen eine sehr sorgfältige Interessenabwägung im Einzelfall vorgenommen werden müssen, da bei diesen Merkmalen sehr viel eher als bei den „harten" Negativmerkmalen eine Verletzung der schutzwürdigen Belange Betroffener denkbar ist (vgl. BGH, Urteil vom 15.12.1983, III ZR 207/82, NJW 1984, S. 1889, 1890). Für diese Einzelfallabwägung müssen die Kreditinstitute ihren Sachbearbeitern eine Aufstellung dafür relevanter Kriterien an die Hand geben.

5.5.3.1.2 Neuorganisation des Schufa-Auskunftsverfahrens

Der BGH hat in seinem Urteil vom 19.9.1985 ausgeführt, daß die übermittelnde Bank Aussagekraft und Berechtigung einer bestimmten Einzelmitteilung an die Schufa unter sorgfältiger Interessenabwägung prüfen muß. Daraus ist zu folgern, daß insgesamt die Aussagekraft der von den Kreditinstituten übermittelten Merkmale überdacht werden muß.

Die Vertreter der Kreditinstitute haben selbst eingeräumt, daß der Katalog der zur Übermittlung an die Schufa bestimmten Merkmale verringert werden muß. Es besteht Einigkeit darüber, daß die Merkmale „Klageerhebung" und „letzte außergerichtliche Mahnung" in Zukunft generell nicht mehr an die Schufa übermittelt werden dürfen, weil sie eine zu geringe Aussagekraft über das tatsächliche Bestehen einer Forderung haben. Das Merkmal „Mahnbescheid" kann jedenfalls bei der Übermittlung durch Kreditinstitute anders bewertet werden. Mahnbescheide werden von den Kreditinstituten nach Angaben ihrer Verbände nur beantragt, wenn aufgrund des Verlaufs der Auseinandersetzung mit dem Schuldner davon ausgegangen werden kann, daß dieser die Forderung als solche akzeptiert und lediglich im Moment nicht zahlen kann oder will. Anders als bei der Klageerhebung und bei der letzten außergerichtlichen Mahnung ist deswegen bei der Meldung „Mahnbescheid" durch ein Kreditinstitut nicht von vornherein eine Beeinträchtigung der schutzwürdigen Belange des Kunden zu befürchten. Dieses Merkmal wird deswegen nicht aus dem Katalog der von Kreditinstituten an die Schufa zu übermittelnden Merkmale gestrichen werden müssen.

Nach Darstellung der Schufa beantragen auch ihre sonstigen Vertragspartner in aller Regel keinen Mahnbescheid, wenn die Forderung selbst streitig ist. Die Datenschutz-

Aufsichtsbehörden haben sich deshalb damit einverstanden erklärt, daß das Merkmal „Mahnbescheid" weiter übermittelt werden darf, fordern aber, daß vor der Meldung an die Schufa die Betroffenen über die Absicht einer Übermittlung unterrichtet werden, um sich hiergegen zur Wehr setzen zu können. Im übrigen muß es selbstverständlich dabei bleiben, daß eine Nachmeldung an die Schufa erfolgt, wenn der Betroffene Widerspruch gegen einen Mahnbescheid eingelegt hat.

Eine weitere Forderung der Aufsichtsbehörden geht dahin, daß die Schufa sich von Vertragspartnern trennen soll, die selbst keine Kredite gewähren. Die mit der Übermittlung von Daten durch die Schufa z.B. an Wohnungsvermittler, Kfz-Vermieter, Einzelhändler verbundenen datenschutzrechtlichen Probleme habe ich bereits in meinen letzten beiden Tätigkeitsberichten dargelegt (2. TB, 4.5.2.1, S. 128 f.; 3. TB, Nr. 4.4.3.3, S. 114 f.). Die Schufa hat inzwischen einigen dieser Vertragspartner gekündigt oder führt mit anderen Verhandlungen zur Lösung des Vertragsverhältnisses. Die Schufa Hamburg hat z.B. rund 130 Vertragspartnern, die Wohnungen aus eigenem Bestand vermieten, zum 31.12.1985 gekündigt. Ich begrüße, daß sich auf diese Weise der Kreis derjenigen Schufa-Vertragspartner deutlich verringert, die keine Kredite vergeben und somit vom Geschäftszweck der Schufa (Schutzgemeinschaft für **Kredit**sicherung) nicht umfaßt werden. Es muß allerdings darauf hingewiesen werden, daß es auch nach dieser Änderung noch Schufa-Vertragspartner geben wird, die zunächst nicht wegen einer Kreditgewährung, sondern wegen einer sonstigen „wirtschaftlichen Vorleistung" bei der Schufa anfragen (z.B. ein Handwerker kauft Material ein, um für einen Kunden Ware herzustellen), die dann bei Auslieferung der Ware vielleicht einen Kredit gewähren (und sei es auch nur in der Weise, daß sie eine Zahlungsfrist von 30 Tagen einräumen), und die die zuerst zu einem anderen Zweck eingeholte Schufa-Auskunft tatsächlich für Kreditzwecke verwenden. Ich meine aber, daß zumindest diejenigen, die keinerlei Kredit geben, nicht an dieses hochsensible Auskunftssystem angeschlossen sein sollten (wie etwa viele Handwerker, Kfz-Vermieter und sonstige Dienstleistungsunternehmen). Wenn diese Unternehmer aber Vertragspartner der Schufa bleiben, dürfen ihnen künftig – und das ist positiv zu vermerken – Daten nur noch übermittelt werden, wenn der Kunde im Einzelfall ausdrücklich seine Einwilligung hierzu gegeben hat.

Eine weitere Verbesserung des Schufa-Verfahrens wird dadurch herbeigeführt werden müssen, daß die stichprobenweise Überprüfung des vom Anfragenden gegenüber der Schufa dargelegten „berechtigten Interesses" deutlich verstärkt wird (vgl. dazu auch 5.5.3.2).

Eine weitere Forderung zur Verbesserung des Schufa-Verfahrens ist die deutliche Steigerung seiner Transparenz. Dies soll bewirken, daß der Betroffene seine Überlegungen in die Abwägung seiner schutzwürdigen Belange mit den berechtigten Interessen anderer an der Übermittlung und Speicherung seiner Daten soll einbringen können. Dies kann er jedoch nur, wenn er das gesamte Verfahren durchschaut.

Das Schufa-Verfahren sollte durch folgende Maßnahmen transparenter gestaltet werden:

- Die Änderungen der Schufa-Klausel werden zu einer Verbesserung der Information der Kunden führen.
- In das Schufa-Merkblatt, das künftig allen Kunden ausgehändigt werden sollte, sind mehr Erläuterungen als bisher aufzunehmen.
- Möglichst vor der Übermittlung „weicher" Negativmerkmale an die Schufa ist der Kunde über die Absicht der Übermittlung zu unterrichten, damit er Gelegenheit hat, notfalls dagegen vorzugehen.
- Die Benachrichtigung Betroffener über die Speicherung von Daten bei der Schufa, die die sog. B-Vertragspartner (ohne Einwilligung) gemeldet haben, und die von der Schufa selbst vorgenommen werden muß, sollte mit deutlich vermehrter Aufklärung über das gesamte Verfahren versehen werden. Damit soll den Betroffenen klar gemacht werden, was mit ihren bei der Schufa gespeicherten Daten geschieht.

- Im Vorgriff auf die Novellierung des BDSG sollten alle am Schufa-Verfahren Beteiligten dem Betroffenen Auskunft über Herkunft und Empfänger seiner Daten geben, wie es die Entwürfe von SPD und Koalition zur Neufassung des BDSG in den §§ 26 Abs. 2 und 34 Abs. 2 vorsehen.
- Schließlich sollte der Betroffene darüber informiert werden, wenn eine negative Schufa-Auskunft den Ausschlag für eine negative geschäftliche oder sonstige Entscheidung des Schufa-Vertragspartners gegeben hat, so wie es einige Schufa-Vertragspartner bereits jetzt praktizieren und es auch der SPD-Entwurf zur Novellierung des BDSG in § 32 Abs. 4 vorsieht. In den Verträgen zwischen Schufa und Vertragspartnern müßte die Pflicht der Vertragspartner zu dieser Unterrichtung abgesichert werden.

5.5.3.1.3 Behandlung der bereits bei der Schufa gespeicherten Daten

Nach dem Urteil des BGH zur Schufa-Klausel muß schließlich geklärt werden, wie die derzeitige Speicherung von Daten bei der Schufa rechtlich zu beurteilen ist. Ich vertrete dazu folgende Ansicht:

Die sog. A-Partner haben in der Vergangenheit die Daten aufgrund einer – wie sich jetzt herausgestellt hat – unwirksamen Schufa-Klausel und somit ohne wirksame Einwilligung an die Schufa übermittelt. Die Zulässigkeit der Speicherung dieser Daten bei der Schufa ist differenziert zu beurteilen.

Die Übermittlung „harter" Negativmerkmale an die Schufa und die Speicherung dort wird in aller Regel zulässig gewesen sein, denn die berechtigten Interessen der Allgemeinheit an einem Schutz vor der Vergabe von Krediten an Zahlungsunfähige oder -unwillige rechtfertigen in aller Regel die Weitergabe der Daten z.B. über eine Lohnpfändung oder eine Zwangsvollstreckung in sein sonstiges Vermögen (vgl. BGH, Urteil vom 7.7.83, a.a.O.).

Hinsichtlich der „weichen" Negativmerkmale wird man dagegen nur nach einer Einzelfallabwägung entscheiden können, ob die Belange des Betroffenen Schutz verdienen. Bei diesen Daten (beantragter Mahnbescheid, Klageerhebung und letzte außergerichtliche Mahnung) läßt sich dies nur beurteilen, wenn man die Belange des Betroffenen den Interessen der übermittelnden und der speichernden Stelle, Dritter oder der Allgemeinheit gegenüberstellt (vgl. BGH, Urteil vom 15.12.1983, a.a.O.). Dies setzt wohl voraus, daß die Betroffenen darüber unterrichtet werden, welche „weichen" Negativmerkmale über sie gespeichert sind.

Auch positive Merkmale wie z.B. Eröffnung eines Girokontos und Ausgabe einer Kreditkarte können unter Verletzung schutzwürdiger Belange der Betroffenen an die Schufa gemeldet worden sein. In der Unterzeichnung der – unwirksamen – Schufa-Klausel ist allerdings eine Unterrichtung des Betroffenen über das Schufa-Meldeverfahren zu sehen. Wenn der Betroffene in Kenntnis dieses Verfahrens der Übermittlung positiver Daten nicht widersprochen hat, so ist dies als – allerdings wiederlegliches – Indiz dafür zu werten, daß er selbst seine schutzwürdigen Belange dadurch nicht beeinträchtigt sieht. Die Unterzeichnung der unwirksamen Schufa-Klausel kann somit als mutmaßliche Einwilligung des Betroffenen betrachtet werden, nach der die Übermittlung positiver Daten zulässig war.

Auch für die jetzt schon bei der Schufa gespeicherten positiven Merkmale muß also geklärt werden, ob die weitere Speicherung zulässig ist. Dies könnte dadurch geschehen, daß – nachdem die neuen Schufa-Klauseln erarbeitet sind – den Betroffenen Gelegenheit gegeben wird, der weiteren Speicherung ihrer Daten zu widersprechen. Wenn dann innerhalb eines bestimmten Zeitraumes kein Widerspruch der Betroffenen erfolgt, kann vermutet werden, daß sie durch die Speicherung ihre schutzwürdigen Belange nicht beeinträchtigt sehen. Die weitere Speicherung wäre dann rechtlich nicht zu beanstanden. Wird Widerspruch eingelegt, muß eine sorgfältige Abwägung der gegenseitigen Interessen unter besonderer Berücksichtigung der Argumente des Betroffenen stattfinden.

Dies wäre ein Weg, der zwar ausdrücklich im BDSG nicht vorgesehen ist, der aber angesichts der erheblichen praktischen Schwierigkeiten bei der Einführung einer neuen Schufa-Klausel noch hingenommen werden kann.

5.5.3.2 Unberechtigte Schufa-Anfragen

Ein Beschwerdefall, mit dem ich mich vor einigen Wochen zu beschäftigen hatte, hat mich veranlaßt, erneut eine verstärkte Überprüfung des vom Anfragenden dargelegten „berechtigten Interesses" zu fordern.

Bei der Schufa Hamburg wird monatlich lediglich in 10 Fällen das Vorliegen eines berechtigten Interesses für Anfragen nachträglich überprüft. Ich hatte bereits in meinem letzten Tätigkeitsbericht darauf hingewiesen, daß diese Zahl angesichts von über 360.000 Auskünften, die die Schufa Hamburg z.B. im Jahre 1983 erteilt hat, viel zu niedrig ist und wesentlich erhöht werden muß (3. TB, 4.4.3.2.4, S. 112).

In dem erwähnten Beschwerdefall hatte ein Mitarbeiter eines Kreditinstitutes unter Darlegung des „berechtigten Interesses" (mit der „Anfrage Girokonto") bei der Schufa über einen Bürger angefragt und den Eindruck erweckt, dieser Bürger habe sich um ein Girokonto bemüht. Dies war jedoch nicht der Fall. In Wirklichkeit hat der Mitarbeiter des Kreditinstitutes diese Schufa-Auskunft für einen Wohnungsvermieter erfragt, für den er der Kundenbetreuer des Kreditinstitutes war. Der Wohnungsvermieter wollte die Auskunft haben, weil der betroffene Bürger eine seiner Wohnungen mieten wollte. Aufgrund der negativen Schufa-Auskunft hat der Bürger die Wohnung nicht mieten können.

Dieser Fall hat zwar dazu geführt, daß das beteiligte Kreditinstitut alle Mitarbeiter noch einmal intensiv auf ihre Pflichten aus dem Bankgeheimnis und dem BDSG hingewiesen hat. Damit kann es jedoch m.E. nicht sein Bewenden haben. Ich habe diesen Fall zum Anlaß genommen, von der Schufa Hamburg erneut eine deutliche Erhöhung der stichprobenartigen Überprüfungen des „berechtigten Interesses" zu fordern.

Die Schufa Hamburg ist der Meinung, daß dies nicht nötig ist, weil unberechtigte Schufa-Anfragen meist durch die Anfragenden selbst offenbart würden und weil jeder Vertragspartner der Schufa wisse, daß er mit einer Prüfung des von ihm dargelegten „berechtigten Interesses" rechnen muß. Die Schufa Hamburg hält es für effektiver, wenn die Vertragspartner der Schufa ihr Personal von Zeit zu Zeit auf die Folgen von Datenmißbrauch hinweisen, als daß die Schufa einige hundert Stichproben mehr durchführt.

Ich kann dieser Ansicht nicht folgen und habe daher in die Verhandlungen mit der Kreditwirtschaft und der Schufa die Forderung eingebracht, die Anzahl der Stichproben deutlich zu erhöhen.

5.5.3.3 Negative Bewertung des Schufa-Merkmals KI

Eine Eingabe hat mich darauf aufmerksam gemacht, daß das Fehlen von Informationen über eine Person bei der Schufa von deren Vertragspartnern teilweise negativ bewertet wird.

Die Schufa hat beispielsweise keine Daten von Bürgern gespeichert, die nur ein Postgirokonto haben. Es gibt aber auch Kreditinstitute, die – obwohl der Schufa angeschlossen – die von ihnen geführten Girokonten der Schufa nicht zur Beobachtung einmelden. Wenn Schufa-Vertragspartner über diese Personen bei der Schufa anfragen, wird ihnen das – neutrale – Merkmal KI gemeldet, d.h. „keine Information über die angefragte Person im Schufa-Datenbestand vorhanden."

Diese Meldung KI verstehen manche Schufa-Vertragspartner fälschlicherweise so, daß die betroffene Person kein Girokonto habe. Daraus wird z.B. von einem Kfz-Vermieter der Schluß gezogen, daß – wenn auch andere von diesem Vermieter anerkannte Referenzen nicht vorgelegt werden können wie z.B. Euroscheckkarte, Kreditkarte – kein Auto an diese Person vermietet wird. Hintergrund ist die Erfahrung, daß häufig gefälschte Personalpapiere vorgelegt werden und in diesen Fällen ein Verlust eintritt.

Die Schufa-Anfrage über die in den gefälschten Papieren angegebenen Namen führt in der Tat zu der Auskunft KI, wenn es sich um erfundene Namen handelt. Insofern ist die Meldung KI immer mit dem Risiko verbunden, daß es diese Person nicht wirklich gibt und daß die vorgelegten Papiere gefälscht sind. In aller Regel sind die Papiere aber nicht gefälscht, und die betreffende Person hat ein Girokonto, das bei der Schufa nicht eingemeldet wird.

Die dargestellte Vorgehensweise führt somit zu einer Diskriminierung der Bürger, die über ein Girokonto verfügen, das nicht bei der Schufa gemeldet ist. Es wäre nicht sachgerecht, die Beseitigung dieser Diskriminierung dadurch erreichen zu wollen, daß alle bisher noch nicht bei der Schufa gemeldeten Girokonten dort gemeldet werden müssen. Dies würde u.a. die jetzt noch bestehende Möglichkeit entfallen lassen, der Speicherung bei der Schufa durch die Einrichtung eines Postgirokontos zu entgehen. Gefordert werden muß vielmehr, daß die Schufa-Meldung KI nicht generell in der negativen Weise verstanden wird, wie der erwähnte Kfz-Vermieter sie auslegt. Die Schufa-Vertragspartner sind aufgerufen, sich weniger diskriminierende Sicherungsmaßnahmen gegen die Vorlage gefälschter Papiere einfallen zu lassen als die alleinige Orientierung an dem Umstand, daß eine Person bei der Schufa nicht im Datenbestand vorhanden ist.

5.6 Prüfungen von Datenerfassungsbetrieben

Im Berichtszeitraum wollte ich die bei mir registrierten Datenerfassungsbetriebe nach § 40 BDSG prüfen, die vornehmlich auftragsgebundene Datenerfassung betreiben. In mehreren Fällen mußte ich feststellen, daß die Unternehmen nicht mehr existieren. Sie hatten sich zwar – großenteils erst nach Aufforderung – ursprünglich zum Register der Aufsichtsbehörde angemeldet, nicht aber die Beendigung ihrer Tätigkeit angezeigt, obwohl auch diese nach § 39 BDSG meldepflichtig ist. Diese Unterlassung ist eine Ordnungswidrigkeit, und ich habe in den Fällen, in denen die Verantwortlichen noch zu erreichen waren, Ermittlungsverfahren eingeleitet.

Die Meldepflichten nach § 39 BDSG sind auch im übrigen sehr häufig nicht beachtet worden. In einigen Fällen wurden Adressen-Änderungen nicht mitgeteilt, und in weiteren Fällen wurde nicht angezeigt, daß ein Wechsel in der Person der Verantwortlichen oder eine Änderung in der Firmenbezeichnung eingetreten ist. Da diese Angaben für die regelmäßige Überwachung durch die Aufsichtsbehörde unbedingt notwendig sind, prüfe ich, ob Bußgeld-Verfahren eingeleitet werden müssen.

Bei fast allen geprüften Unternehmen waren die Mitarbeiter nur allgemein oder nach Vorgaben der Auftraggeber auf ihre Verschwiegenheit verpflichtet worden. In diesen Fällen wurde die korrekte Verpflichtung nach § 5 Abs. 2 BDSG mit einem von mir vorgeschlagenen Text schriftlich nachgeholt.

Die Rechtsbeziehungen zwischen Auftraggebern und den geprüften Datenerfassungsbetrieben sind sehr unterschiedlich gestaltet. Nur mit wenigen Unternehmen wird ein Rahmenvertrag geschlossen, der die Grundzüge des Auftrags regelt und der jeweils bei einer anfallenden Arbeit hinsichtlich der Datenarten, der Menge, der Terminierung und ggf. der Transportregelungen konkretisiert wird. Vielfach ist der Auftraggeber der faktisch Stärkere, so daß dieser dem Datenerfassungsunternehmen die Auftragsausgestaltung vorgibt. Dabei sind Datenschutz und Datensicherung durchweg nicht genau genug geregelt.

In sehr vielen Fällen bestehen langjährige Geschäftsbeziehungen, bei denen nur mündliche Aufträge erteilt werden. Diese Abmachungen werden dann durch schriftliche Beschreibungen der erwarteten Datensätze und durch Muster-Belege und Erfassungsbeispiele ergänzt. Zur genauen Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer empfehle ich die Schriftform des Auftrages, damit über wesentliche Fragen kein Zweifel besteht. Sollte sich dies bei den Auftraggebern nicht durchsetzen lassen, sollte der Auftragnehmer jeden Auftrag schriftlich

bestätigen und dabei konkret angeben, wie weit er sich hinsichtlich des Transportes und der Übergabe von Belegen und Datenträgern, der Richtigkeit der Datenerfassung und der Datensicherungsmaßnahmen verantwortlich fühlt.

5.7 Sonstige Probleme

5.7.1 Drittschuldner-Auskunft

Bei Pfändung einer Geldforderung (z.B. des Gehalts eines Schuldners) hat der Gläubiger nach Vorliegen des gerichtlichen Pfändungsbeschlusses gem. § 840 Abs. 1 ZPO das Recht, von dem sog. Drittschuldner (also bei Lohn- oder Gehaltsempfängern von dem Arbeitgeber) Antwort auf folgende Fragen zu bekommen:

1. ob und inwieweit er die Forderung als begründet anerkennt und Zahlung zu leisten bereit ist;
2. ob und welche Ansprüche andere Personen an die Forderung stellen;
3. ob und wegen welcher Ansprüche die Forderung bereits für andere Gläubiger gepfändet ist.

Durch eine Eingabe wurde mir bekannt, daß ein Anwaltsbüro bereits vor dem Erwirken des Pfändungsbeschlusses an die potentiellen Drittschuldner zu schreiben pflegt und diesen folgende Fragen stellt:

1. Besteht das Beschäftigungsverhältnis noch?
2. Ist der Verdienst vorgepfändet oder abgetreten?
   Wenn ja, in welcher Höhe? ca.: DM
   Monatlich pfändbarer Betrag, ca.: DM
3. Werden Lohnabtretungen anerkannt?
4. Können angemessene mtl. Zahlungen im Einvernehmen mit Ihrem Mitarbeiter geleistet werden?
5. An wen muß eine eventuelle Lohnpfändung gerichtet werden (genaue Anschrift bitten wir auf der Rückseite anzugeben)?

Zur Begründung der Fragen werden lediglich Kostenersparnisgründe angeführt; auf die Freiwilligkeit der Beantwortung wird nicht hingewiesen. In einer Stellungnahme hat das Anwaltsbüro erklärt, die Fragen würden nur gestellt werden, wenn ein Titel gegen den Schuldner vorliegt, so daß die Voraussetzungen für die Erwirkung eines Pfändungs- und Überweisungsbeschlusses vorliegen. Es könnten in allen diesen Fällen also ohne weiteres die Voraussetzungen für die nach § 840 Abs. 1 ZPO zulässigen Fragen geschaffen werden. Die Fragen würden in vielen Fällen zu Zahlungsvereinbarungen mit den Schuldnern und deren Arbeitgebern führen, durch die die Zwangsvollstreckung und die damit für den Schuldner verbundenen Kosten vermieden würden.

Ich habe dem Anwaltsbüro dazu mitgeteilt, daß ich einen Hinweis auf die Freiwilligkeit der Fragenbeantwortung für sachdienlich halte. Um Zweifel an der Zulässigkeit der Übermittlung der Daten durch den Drittschuldner von vornherein auszuschließen, rate ich weiter, die Bitte um Beantwortung der Fragen im Einvernehmen mit dem Betroffenen in das Schreiben aufzunehmen. Wenn der Betroffene bei der Beantwortung nicht beteiligt ist, wird sich nicht in jedem Fall ausschließen lassen, daß die Übermittlung der Daten durch den Drittschuldner schutzwürdige Belange des Betroffenen beeinträchtigt. Die Übermittlung wäre dann wegen Unvereinbarkeit mit § 24 Abs. 1 BDSG unzulässig.

5.7.2 Datenschutz bei Mietnebenkostenabrechnungen

Mehrfach wurde mir die Frage gestellt, ob durch die Offenlegung einzelner Daten, die Nachbarn oder Hausmeister in Mietwohnungs- oder Wohnungseigentumsanlagen betreffen, Datenschutzbestimmungen verletzt werden. Dieses Problem taucht auf, wenn für Mieter oder Miteigentümer die Nebenkosten abgerechnet werden.

Der Mieter hat nach der Abrechnung der Nebenkosten einen Anspruch auf Einsicht in die Abrechnungsunterlagen, um die Abrechnung nachprüfen zu können. Dieser Anspruch ergibt sich meist direkt aus dem Mietvertrag (z.B. § 5 Nr. 6 des Hamburger Mietvertrages für Wohnraum). Im übrigen folgt er aus den Nebenpflichten des Vermieters. Auch der Wohnungseigentümer hat unter bestimmten Voraussetzungen das Recht auf Einsicht in die Abrechnungsunterlagen.

Die Offenlegung der Abrechnungsunterlagen soll es dem Mieter bzw. Wohnungseigentümer ermöglichen, die Abrechnung für seine Wohnung nachzuvollziehen. Dabei kann es auch notwendig sein, Abrechnungsdaten der Nachbarn heranzuziehen, sofern nur aus der Summe der Einzeldaten ein Rückschluß auf den eigenen Anteil gezogen werden kann.

Relevant wird dieses Problem vor allem bei Heizkostenabrechnungen. Die Röhrchen an den Heizkörpern lassen keinen direkten Schluß auf die Höhe der Heizkosten zu. Erst aus der Summe aller abgelesenen Werte und den insgesamt aufgewendeten Heizkosten läßt sich der Anteil jedes Einzelnen errechnen.

Daraus folgt, daß dem Mieter bzw. Wohnungseigentümer unter Offenlegung aller Ablese- und Abrechungsunterlagen auch gezeigt werden muß, wieviel die anderen Hausbewohner an Heizkosten verbraucht haben. Anders kann er nicht prüfen, ob die Berechnung seiner eigenen Heizkosten korrekt vorgenommen worden ist. Die schutzwürdigen Belange der Nachbarn müssen insoweit zurückstehen.

Ein weiteres Problem ist in diesem Zusammenhang, daß auch die auf alle Parteien umgelegten Kosten für die Hausverwaltung bzw. den Hausmeister nachvollziehbar sein müssen. Dies kann nur gewährleistet werden, wenn den Mietern bzw. Wohnungseigentümern Einblick in die Abrechnung aller Kosten des Hausmeisters und der Wohnungsverwaltung gewährt wird. Dies kann auch Einblick in den Arbeitsvertrag des Hausmeisters bedeuten. Dessen schutzwürdige Belange müssen insoweit zurücktreten, weil anders die Abrechnung der Nebenkosten der Hausverwaltung für die Mieter und Wohnungseigentümer nicht nachgeprüft werden kann.

5.7.3 Angebot zum Kauf vermieteter Wohnungen mit personenbezogenen Daten der Mieter

Von einem Bürger wurde mir das Angebot eines Immobilienmaklers zum Kauf vermieteter Eigentumswohnungen zugesandt, in dem für die einzelnen Wohnungen neben der Lage im Haus, der Größe und dem Kaufpreis auch die Namen der Mieter, die von diesen gezahlte Kaltmiete und das Datum des Mietvertragsbeginns angegeben waren. Auf Befragen erklärte der Immobilienmakler, er habe diese Liste an Kaufinteressenten versandt, ohne sich Gedanken über die damit verbundene datenschutzrechtliche Problematik zu machen. In Zukunft werde er derartige Listen nicht mehr mit personenbezogenen Daten von Mietern versenden.

Dieser Vorgang macht deutlich, wie wenig ausgeprägt das Datenschutzbewußtsein teilweise noch ist. Für die Versendung des Kaufangebots wurde einfach ein Ausdruck der in der Datenverarbeitungsanlage des Immobilienmaklers gespeicherten Daten verwandt, ohne Rücksicht darauf, daß darin auch Mieter-Daten enthalten waren. Das Speichern dieser Daten wird man noch für zulässig halten können, da der Name des jeweiligen Mieters für Kontaktaufnahmen benötigt wird und da die Höhe der gezahlten Miete im Zusammenhang mit dem Zeitpunkt, seit dem der Mietvertrag besteht, für die Bewertung der jeweiligen Wohnung nötig ist. Eine Weiterleitung dieser Daten an beliebige Interessenten verletzt jedoch eindeutig die schutzwürdigen Belange der betroffenen Mieter, weil auf diese Weise nicht nur diejenigen Personen Kenntnis der Daten erhalten können, die ein konkretes Interesse am Kauf einer der Wohnungen haben.

Als bemerkenswert an diesem Vorgang erscheint mir aber insbesondere, daß das Immobilienmaklerbüro noch nicht einmal daran gedacht hat, daß hier die Persönlichkeitsrechte der Mieter berührt sein könnten. Dies zeigt, wie wenig Sensibilität es auf diesem Gebiet teilweise immer noch gibt.

5.7.4 Inhalt der Benachrichtigung über gespeicherte Daten bei Konzerngesellschaften

Durch eine Eingabe wurde ich darauf aufmerksam, daß ein Versicherungsunternehmen die Benachrichtigung über die Speicherung von Daten (§ 26 Abs.1 BDSG) in einer Weise vornimmt, die für den Betroffenen nicht erkennbar werden läßt, wo genau seine Daten gespeichert werden. Dieser Konzern, der in mehrere rechtlich selbständige Versicherungsgesellschaften aufgegliedert ist, benachrichtigt Betroffene unter dem Briefkopf der jeweiligen Gesellschaft so:

> „Zu diesem Schaden sind Sie uns als Beteiligter angegeben. Diesbezügliche Daten sind bei den (Name des Konzerns)-Gesellschaften gespeichert."

Der Betroffene muß daraus entnehmen, daß seine Daten nicht nur bei der Gesellschaft gespeichert sind, die im Briefkopf erscheint, sondern auch bei allen anderen Gesellschaften des Konzerns.

Abgesehen davon, daß hierdurch ein unzutreffender Eindruck vermittelt wird (nach Auskunft des Unternehmens sind die Daten nur bei der Gesellschaft gespeichert, die im Briefkopf erscheint), genügt diese Form der Benachrichtigung nicht den Anforderungen des § 26 Abs. 1 BDSG. Durch die Benachrichtigung soll der Betroffene in die Lage versetzt werden, von seinem Recht auf Auskunft über die zu seiner Person gespeicherten Daten Gebrauch zu machen. Das kann er jedoch nur, wenn er genau darüber benachrichtigt wird, welche Stelle seine Daten gespeichert hat. Die dargestellte Form der Benachrichtigung klärt den Betroffenen aber nicht darüber auf, welche – von mehreren in Betracht kommenden – Gesellschaften seine Daten gespeichert hat und bei welcher genau er anfragen muß, wenn er Auskunft über die zu seiner Person gespeicherten Daten erhalten will, und welche ggf. Adressat weiterer Ansprüche ist.

Das beteiligte Versicherungsunternehmen hatte sich zunächst bereit erklärt, die Ausgestaltung der Benachrichtigung zu überdenken. Schließlich hat es sich bedauerlicherweise doch nicht dazu bereitgefunden und mitgeteilt, es sei nach nochmaliger Überprüfung der Angelegenheit der Auffassung, daß die von ihm verwendete Formulierung den Erfordernissen des § 26 Abs. 1 BDSG genüge. Seine Benachrichtigungsformel stelle sicher, daß der Betroffene durch Anfrage beim Absender des Mitteilungsschreibens seinen Auskunftsanspruch ohne Schwierigkeiten realisieren könne. –

Meine Bedenken gegenüber der von diesem Versicherungsunternehmen verwandten Benachrichtigung sind dadurch nicht entkräftet worden.

5.8 Arbeitnehmerdatenschutz

5.8.1 Datenschutz contra Datensicherung – Das Verhältnis von § 6 BDSG zu § 87 BetrVG

Im 1. TB (7.5.2, S. 58 f.) hatte ich auf das Spannungsverhältnis zwischen § 6 BDSG (Datensicherungsmaßnahmen) und § 87 Abs. 1 Ziff. 6 BetrVG (automatische Verhaltens- und Leistungskontrolle der Arbeitnehmer) hingewiesen, das immer dann konkret wird, wenn Maßnahmen zur Verwirklichung der Datensicherheitsanforderungen gleichzeitig geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Ich hatte indessen keine Zweifel, daß auch diese Fälle der Mitbestimmung des Betriebsrates unterliegen. § 6 Abs. 1 BDSG räumt dem Unternehmen einen Ermessensspielraum für die zu treffenden Sicherungsmaßnahmen ein; diese Gestaltungsmöglichkeiten sind der Mitbestimmung voll zugänglich.

Diese Auffassung, die in der Fachliteratur nicht unumstritten war, ist nunmehr vom BAG durch Urteil vom 23.4.1985 (1 ABR 2/82, BB 1985, S. 1664) bestätigt worden. Das BAG führt, nachdem es das Mitbestimmungsrecht des Betriebsrates für die in dem konkreten Fall geplante Maßnahme dem Grunde nach bejaht hat, weiter aus:

> „Diesem Mitbestimmungsrecht stehen entgegen der Ansicht der Antragsgegnerin Vorschriften des Datenschutzrechts nicht entgegen. Zwar hat die Antragsgegnerin nach § 6 BDSG diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vor-

schriften des Bundesdatenschutzgesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. § 6 BDSG und die Anlage dazu regeln jedoch nicht, auf welche Weise diesen Anforderungen des Gesetzes genügt werden muß. Das Gesetz fordert keine bestimmten Maßnahmen, sondern die erforderlichen Maßnahmen... Damit ist nicht gesetzlich vorgeschrieben, daß das Namenskürzel als Identifikationsmerkmal für den Dateneingeber selbst in das System eingegeben und in diesem zusammen mit eingegebenen personenbezogenen Daten gespeichert wird und abgerufen werden kann. Das Erfordernis der Identifizierung desjenigen, der personenbezogene Daten eingegeben hat, kann vielmehr auch auf andere Weise erfolgen."

Wenn Arbeitgeber und Arbeitnehmervertreter über die einzuführenden Datensicherungsmaßnahmen verhandeln, ist darauf zu achten, daß die im Rahmen der Datensicherung nach § 6 BDSG anfallenden Daten nicht zugleich auch für andere Zwecke genutzt, insbesondere nicht zur Überwachung der Leistung und des Verhaltens der Arbeitnehmer verwendet werden (vgl. auch § 25 a Abs. 5 des von der SPD-Fraktion im Bundestag eingebrachten Gesetzentwurfes zur Novellierung des BDSG, Bundestags-Drucksache 10/1180).

5.8.2 Einblick des Betriebsrates in Bruttolohnlisten

Mir wurde die Frage gestellt, ob das dem Betriebsrat nach dem BetrVG zustehende Einsichtsrecht in Bruttolohnlisten mit den Rechten der betroffenen Arbeitnehmer nach dem BDSG vereinbar ist.

Ich vertrete dazu die Ansicht, daß die Unterrichtungspflicht des Arbeitgebers gegenüber dem Betriebsrat nach § 80 BetrVG nicht durch das BDSG eingeschränkt wird (vgl. Dietz/Richardi, Kommentar zum BetrVG, 6. Aufl., § 80, Rdnrn. 39 und 83 ff., Fitting/Auffahrth/Kaiser, Kommentar zum BetrVG, 14. Aufl., § 80 Rdnr. 19 d).

Das gilt auch für das aus § 80 Abs. 2 BetrVG folgende Recht, Einblick in die Bruttolohnlisten zu nehmen. (Anzumerken ist hier, daß nach dem Gesetzeswortlaut nur ein Betriebsausschuß oder ein nach § 28 BetrVG gebildeter Ausschuß dieses Recht hat, was die Vermutung nahelegt, daß dieses Recht nur in Betrieben mit mehr als 300 Beschäftigten gilt. In der Literatur wird aber –soweit ersichtlich– davon ausgegangen, daß dieses Einsichtsrecht auch in Betrieben mit weniger als 300 Beschäftigten gilt. Im letzteren Fall hat der Betriebsratsvorsitzende, sein Stellvertreter oder ein besonders beauftragtes anderes Betriebsratsmitglied – also nicht der gesamte Betriebsrat – das Einblicksrecht.)

Das Einsichtsrecht erstreckt sich auf die effektiven Bruttobezüge einschließlich der übertariflichen Zahlungen. Der Betriebsrat hat keinen Anspruch auf Unterrichtung über die sich meist aus den familiären Verhältnissen oder persönlichen Umständen ergebende Höhe der Abzüge. Wenn wegen der Struktur eines Tarifvertrages trotzdem auch aus dem Bruttoentgelt Rückschlüsse auf persönliche Verhältnisse der einzelnen Arbeitnehmer möglich sind, so ist dies hinzunehmen, weil der Betriebsrat anders nicht überprüfen kann, ob die Regelungen des Tarifvertrages bei der Berechnung der Bezüge eingehalten werden. Das BDSG steht dem nicht entgegen.

5.8.3 Telefondatenerfassung von Arbeitnehmern

In meinem letzten TB (3. TB, 4.7.5, S. 125 ff.) hatte ich über die mit der Telefondatenerfassung von Arbeitnehmern verbundenen datenschutzrechtlichen Probleme berichtet. Gegen die Beschlüsse des Arbeitsgerichts Hamburg vom 3.10.1984 (23 Bv 6/84) und vom 19.12.1984 (6 Bv 14/83), die die Speicherung der von Arbeitnehmern angerufenen Telefonnnummern für unrechtmäßig halten, ist Beschwerde eingelegt worden, über die das Landesarbeitsgericht Hamburg noch nicht entschieden hat.

5.8.4 Sicherheitsüberprüfungen im privaten Bereich

Im Berichtszeitraum war die Zusammenarbeit von Betrieben mit Verfassungsschutzbehörden mehrfach Gegenstand von Eingaben. Beanstandungen hatte ich im Rahmen

meiner Zuständigkeit in keinem Fall auszusprechen. Ich mußte allerdings feststellen, daß den Betroffenen häufig unklar war, wann sie mit einer Sicherheitsüberprüfung zu rechnen haben, und sie falsche Vorstellungen darüber hatten, was im Falle einer Sicherheitsüberprüfung geschieht. Ich nehme daher diesen Bericht zum Anlaß, einige allgemeine Informationen zu geben.

Grundsätzlich ist zwischen zwei Arten von Sicherheitsüberprüfungen zu unterscheiden, an denen Verfassungsschutzbehörden mitwirken:

- die Überprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich dienstlich verschaffen können (§ 3 Abs. 2 Nr. 1 HmbVerfSchG);
- die Überprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen (§ 3 Abs. 2 Nr. 2 HmbVerfSchG).

Die zweitgenannte Überprüfung, die zum Zwecke des personellen Sabotageschutzes erfolgt, spielte bei der Aufsichtsbehörde keine Rolle. Sie kommt in Hamburg auch nur in eng abgegrenzten Bereichen sehr weniger Betriebe zur Anwendung, ist dem Betroffenen bekannt und führt offenbar nicht zu Problemen.

Gegenstand von Eingaben war nur die erste Überprüfungsart, die zum Zwecke des personellen Geheimschutzes erfolgt. Sie kommt vornehmlich in Betrieben der Rüstungsindustrie zur Anwendung. Solche Unternehmen benötigen zur Durchführung bestimmter Aufträge Kenntnis von geheimhaltungsbedürftigen Angelegenheiten und müssen sich ihren Auftraggebern (zumeist dem Bundesverteidigungsministerium) gegenüber verpflichten, die in Frage kommenden Arbeitnehmer beim Bundeswirtschaftsminister zur Sicherheitsüberprüfung aufzugeben.

Eine solche Sicherheitsüberprüfung muß konkret erforderlich sein (nicht auf Vorrat!) und setzt die Kenntnis und Einwilligung der betroffenen Arbeitnehmer voraus. Vor der Überprüfung müssen sie einen Fragebogen ausfüllen, in dem sie u.a. Auskünfte zu Mitgliedschaften in extremistischen Organisationen, Kontakte zu Personen in Ostblockstaaten und ähnliche Fragen, die Sicherheitrisiken darstellen könnten, beantworten müssen. Ferner müssen sie in Einzelfällen Referenzpersonen angeben, die von Beamten des Verfassungsschutzes zu den persönlichen Verhältnissen des Betroffenen befragt werden können. Neben der Befragung dieser Auskunftspersonen werden die Informationssysteme des Verfassungsschutzes abgefragt sowie Auskünfte von der Polizei eingeholt.

Neben Unklarheiten bezüglich des Verfahrens bestand das Hauptproblem der Betroffenen zumeist darin, daß sie nicht wußten, ob bzw. wann sie arbeitsvertraglich zur Einwilligung in die Sicherheitsüberprüfung verpflichtet sind. Diese Frage kann zwar sachgerecht nur in jedem Einzelfall geklärt werden, grundsätzlich festzuhalten ist jedoch folgendes: Einer Sicherheitsüberprüfung sind nur solche Arbeitnehmer zu unterziehen, die Zugang zu bzw. Umgang mit Verschlußsachen (VS) der Geheimhaltungsgrade „Streng Geheim", „Geheim" oder „VS-Vertraulich" erhalten sollen. Nur wenn im jeweiligen Einzelfall eine entsprechende Verwendung des Arbeitnehmers konkret beabsichtigt ist, muß er ggf. eine Überprüfung über sich ergehen lassen. Zu Überprüfungen ganzer Abteilungen oder einzelner Personen auf Vorrat ohne konkrete Veranlassung muß niemand seine Zustimmung erteilen.

(Zu meinen rechtspolitischen Forderungen bezüglich der Sicherheitsüberprüfung vgl. 4.10.2.2.)

5.9 Befugnisse der Aufsichtsbehörde

Bei den Stellen des nicht-öffentlichen Bereichs, die Datenverarbeitung für eigene Zwecke betreiben, kann die Aufsichtsbehörde nach § 30 Abs. 1 BDSG die Ausführung des BDSG und anderer Vorschriften über den Datenschutz nur überprüfen, wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung seiner personenbezoge-

nen Daten in seinen Rechten verletzt worden ist. Diese Regelung führt in manchen Beschwerdefällen zu Diskussionen mit den beteiligten speichernden Stellen über die Reichweite der Zuständigkeit der Aufsichtsbehörde. Gelegentlich kommt es vor, daß eine dieser Stellen es zunächst ablehnt, alle von der Aufsichtsbehörde gestellten Fragen zu beantworten.

Ich muß ihr dann deutlich machen, daß die Aufsichtsbehörde nach § 30 Abs. 2 Satz 1 BDSG berechtigt ist, alle Fragen zu stellen, die sie zur Bearbeitung der jeweiligen Eingabe geklärt wissen muß. Da in Eingaben der Sachverhalt oft nur unzureichend dargestellt ist, muß die Aufsichtsbehörde häufig Fragen stellen, um beurteilen zu können, ob das BDSG überhaupt anwendbar ist. So darf die Aufsichtsbehörde nur tätig werden, wenn Daten in einer Datei verarbeitet werden. „Es gehört allerdings durchaus zum Aufgabenbereich der Aufsichtsbehörde, sich selbst ein Bild davon zu machen, ob und in welchem Umfang sich die speichernde Stelle auf diese Einschränkungen berufen darf" (Simitis in : Simitis/Dammann/Mallmann/Reh, Kommentar zum BDSG, 3. Aufl., § 30 Rdnr. 27). Das kann die Aufsichtsbehörde aber nur tun, wenn ihr umfassend Auskunft gegeben wird.

Da die Aufsichtsbehörde neben der Einhaltung des BDSG auch die Anwendung anderer Datenschutzvorschriften zu überprüfen hat (§ 30 Abs. 1 Satz 1 BDSG), muß sie im Einzelfall auch Fragen stellen, um feststellen zu können, ob neben dem BDSG andere Datenschutzbestimmungen verletzt sein können.

Die Aufsichtsbehörde darf im Bereich des 3. Abschnitts des BDSG somit zwar nur Fragen stellen, die im Hinblick auf den spezifischen Anlaß der Eingabe erforderlich sind. „Innerhalb dieser Grenzen hat die Behörde freilich das Recht, ihre Fragen so zu formulieren, wie sie es für richtig hält, um eine möglichst wirksame Kontrolle zu gewährleisten" (Simitis, a.a.O., Rdnr. 50). Sie ist also berechtigt, alle ihr zur Aufklärung des Falles notwendig erscheinenden Fragen zu stellen, auch wenn diese sich auf das Umfeld des Falles beziehen.

Wenn nicht alle von mir zur Klärung des jeweiligen Einzelfalles für notwendig gehaltenen Fragen vollständig und erschöpfend beantwortet werden, bin ich gezwungen, von meinen Rechten nach § 30 Abs. 3 BDSG Gebrauch zu machen und eine Prüfung vor Ort vorzunehmen. Bisher ist dies nicht notwendig geworden und ich würde es begrüßen, wenn es auch künftig nicht notwendig würde. Ich halte es auch im Interesse der jeweils beteiligten speichernden Stellen für wünschenswert, wenn einzelne Beschwerden einvernehmlich zwischen diesen und der Aufsichtsbehörde geklärt werden.

6. Entwicklung des allgemeinen Datenschutzrechts

Nach der Verdeutlichung der verfassungsrechtlichen Grundlagen des Datenschutzes sind auch Veränderungen der Datenschutzgesetze unumgänglich geworden. Davon kann auch das HmbDSG nicht ausgenommen werden, wenngleich es als jüngstes der Datenschutzgesetze schon in einer Reihe von Vorschriften Regelungen enthält, die den vom BVerfG formulierten Ansprüchen schon näher kommen als andere Ländergesetze (vgl. 1. TB. 2.1, 5.10). Die Diskussion über die Fortschreibung der Datenschutzgesetze ist im Berichtszeitraum bereits auf vielen Ebenen in Gang gekommen. Von den Ländern Nordrhein-Westfalen und Hessen sind bereits Entwürfe für die Novellierung ihrer Landesdatenschutzgesetze vorgelegt worden. Der Innenausschuß des Bundestages hat im Juni 1985 ein Sachverständigen-Hearing zur BDSG-Novellierung veranstaltet, zu dem auch ich meinen Beitrag leisten konnte.

Nachfolgend will ich nun versuchen, den Änderungsbedarf aufzuzeigen, der sich für das HmbDSG sowie für das BDSG – insbesondere im nicht-öffentlichen Bereich – ergibt.

6.1 Novellierung des HmbDSG

Vorab möchte ich klarstellen:

Das HmbDSG kann – auch nach dem Volkszählungsurteil – seine Auffang- und seine Rahmenfunktion zur Regelung der Zulässigkeit der Datenverarbeitung behalten, denn es wird faktisch nicht möglich sein, für jede denkbare Form der Datenverarbeitung ein eigenes Gesetz zu schaffen. Informationseingriffe, die nach Art, Umfang und denkbarer Verwendung der erhobenen Daten sowie nach der Gefahr eines Mißbrauchs nicht als besonders tiefgehend zu bewerten sind, brauchen auch in Zukunft nicht auf präzisere bereichspezifische Regelungen, sondern können auf das HmbDSG gestützt werden.

Ferner wird man in das HmbDSG nach wie vor all diejenigen Regelungen aufzunehmen haben, die die Datenverarbeitung in allen Bereichen gleichermaßen betreffen.

6.1.1 Neuformulierung von Aufgabe und Gegenstand des Datenschutzes (§ 1 Abs. 1 HmbDSG)

Nach dem VZ-Urteil ist es zunächst erforderlich, Aufgabe und Gegenstand des Datenschutzes (§ 1) neu und umfassender als bisher zu definieren. Die Aufgabe des Datenschutzes umfaßt mehr als den Schutz vor Mißbrauch, wie der bisherige § 1 Abs. 1 HmbDSG es mißverständlich formuliert. Das Bundesverfassungsgericht hat klargestellt, daß der rechtmäßige Umgang mit Daten schlechthin und nicht nur die Verhinderung vorwerfbaren Fehlverhaltens Gegenstand des Datenschutzes ist. Dies muß in der Aufgabenbestimmung zum Ausdruck gebracht werden: Der Einzelne ist davor zu schützen, daß er durch die Verarbeitung oder sonstige Nutzung personenbezogener Daten in seinem Persönlichkeitsrecht – um auch den verfassungsrechtlichen Ansatz zu verdeutlichen – beeinträchtigt wird.

6.1.2 Ausweitung des Anwendungsbereichs (§ 1 Abs. 2 HmbDSG)

Nach dem bisherigen § 1 Abs. 2 HmbDSG schützt das Gesetz nur personenbezogene Daten, die in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. In § 1 Abs. 2 Satz 2 wird die Geltung des Gesetzes für sog. interne Dateien weiter beschränkt.

Diese Einschränkung des Anwendungsbereiches des Datenschutzgesetzes ist mit den im VZ-Urteil formulierten Grundsätzen nicht vereinbar. Vielmehr sind folgende Erweiterungen vorzunehmen:

6.1.2.1 Einbeziehung der Datenerhebung

Das Recht auf informationelle Selbstbestimmung ist nach dem VZ-Urteil nur dann gewährleistet, wenn der Einzelne bewußt über die Preisgabe und Verwendung seiner

persönlichen Daten entscheiden kann. Er muß wissen, für welche Zwecke er ggf. Angaben macht und welche Verarbeitungsmaßnahmen beabsichtigt sind, denn nur dann kann er die Konsequenzen einer Auskunftserteilung abschätzen.

Im Stadium der Gewinnung von Informationen besteht für den Betroffenen oft die einzige Möglichkeit, sein informationelles Selbstbestimmungsrecht wirksam auszuüben. Später kann er das Datenverarbeitungsverfahren kaum noch beeinflussen.

Es ist daher unabweisbar, im HmbDSG auch die Erhebung als besondere Phase der Datenverarbeitung zu regeln. Dabei kann das HmbDSG in seiner Funktion als Auffang- und Rahmengesetz zwar nicht allen Anforderungen, die nach dem VZ-Urteil bei der Erhebung zu berücksichtigen sind (normenklare Regelung des Umfangs der Auskunftspflicht, präzise Bestimmung des Verwendungszwecks, Festlegung der geeigneten Daten, Auskunfts- und Belehrungspflichten, Weitergabe- und Verwertungsverbote), Rechnung tragen. So können etwa Auskunftsverpflichtungen eines Bürgers, die konkret zu bestimmenden Verwendungszwecke und die dabei jeweils erfaßten Daten nur bereichsspezifisch normiert werden. Die allgemeinen Anforderungen an Erhebungsmaßnahmen sowie die verfassungsmäßigen Grenzen der Befragung von Betroffenen müssen jedoch in das HmbDSG aufgenommen werden.

Im einzelnen sollte das HmbDSG daher mindestens folgende Grundsätze festschreiben:

- Die Erhebung muß grundsätzlich beim Betroffenen erfolgen, um die Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, so wenig wie möglich einzuschränken.

  Ohne Mitwirkung des Betroffenen sollte eine Erhebung nur ausnahmsweise zulässig sein, soweit die zu erfüllende Verwaltungsaufgabe es ihrer Art nach erforderlich macht. Dies ist etwa der Fall, wenn der Betroffene durch die Stellung eines Antrages zum Ausdruck gebracht hat, daß die Behörde alle Ermittlungen anstellen darf, ohne die der Antrag nicht bearbeitet werden kann. Oder aber, wenn durch die anderweitige Erhebung schwerwiegende Nachteile für die Allgemeinheit oder den Betroffenen abzuwenden sind.

- Schließlich sollte ausdrücklich klargestellt werden, daß durch die Art und Weise der Erhebung – entsprechend der neuen Aufgabenbestimmung – nicht in unangemessener Weise in das Persönlichkeitsrecht des Betroffenen eingegriffen werden darf.

6.1.2.2 Einbeziehung der nicht-dateimäßigen Verarbeitung

Nach dem VZ-Urteil gilt das Recht auf informationelle Selbstbestimmung für jede Datenverwendung, unabhängig davon, ob diese Daten in Dateien verarbeitet werden oder nicht. Die Gefahr einer Beeinträchtigung des allgemeinen Persönlichkeitsrechts besteht bei jeder Ausgestaltung der Datenverarbeitung und -nutzung.

Um dem HmbDSG die Funktion einer allgemeinen Auffang- und Rahmenvorschrift zu erhalten, ist es daher unverzichtbar, auch die nicht-dateimäßige Verarbeitung zu regeln und den Anwendungsbereich entsprechend zu erweitern. Das bedeutet nicht, daß für alle Formen der Datenverarbeitung generell dieselben Vorschriften gelten müssen. Da die Gefährdungen für die Rechte der Betroffenen und die angemessenen Maßnahmen zu ihrem Schutz je nach Art der Datenträger bzw. der eingesetzten Informationstechnologie sehr unterschiedlich sein können, sollten differenzierte Regelungen für verschiedene Verarbeitungsformen berücksichtigt werden (z.B. Verwertungsverbote anstelle von Löschungsansprüchen bei schwer trennbaren Aktenvorgängen).

6.1.2.3 Einbeziehung der Verwendung von Daten

Der Verwendung personenbezogener Daten – die im geltenden HmbDSG nur unvollkommen in der Weise geregelt ist, daß sie nicht unbefugt und zweckwidrig erfolgen darf, wohingegen eine Erlaubnisvorschrift fehlt – mißt das Bundesverfassungsgericht

besondere Bedeutung bei. Hiervon wird der Bürger – sei es bei belastenden Verwaltungsmaßnahmen oder bei der Gewährung von Leistungen – unmittelbar berührt. Bei der Verwendung von Daten handelt es sich – wenn man sie nicht als Oberbegriff für alle im HmbDSG geregelten Phasen der Datenverarbeitung ansieht – i.d.R. nicht um eine Phase des Datenverarbeitungsprozesses (Ausnahme: z.B. der interne Datenabgleich), sondern um die Erfüllung des Zwecks der Datenerhebung. Die vom BVerfG gewählten allgemeinen Anforderungen an Einschränkungen des Rechts auf informationelle Selbstbestimmung haben sich auf jeglichen Umgang mit personenbezogenen Daten zu erstrecken. Dabei sollte im HmbDSG vor allem der Grundsatz fixiert werden, daß die Verwendung der Daten auf den gesetzlich bestimmten Zweck begrenzt ist.

6.1.2.4 Einbeziehung der sog. internen Datenverarbeitung

Die nach dem geltenden Recht vorgenommene Differenzierung zwischen sog. internen und externen Dateien kann nicht beibehalten werden. Das informationelle Selbstbestimmungsrecht gestattet keine Ausnahmen für Daten, die nicht zur Übermittlung an Dritte bestimmt sind, sondern lediglich intern verwendet werden. Im übrigen verliert die bisherige Differenzierung jegliche Berechtigung, wenn auch die Datenverarbeitung in Akten und sonstigen Unterlagen in den Geltungsbereich des Datenschutzgesetzes einbezogen wird. Wegen der gesteigerten Nutzungsmöglichkeiten dürfen die in internen Dateien gespeicherten Daten auch nicht an der Privilegierung der in Akten gesammelten Daten teilhaben.

6.1.2.5 Sonderregelungen für Bagatellfälle (triviale Datenverarbeitung)?

Verschiedentlich wird gefordert, daß für die Verarbeitung sog. Trivialdaten die Vorschriften der Datenschutzgesetze nur eingeschränkt zur Anwendung kommen sollen. Ich halte dies für einen prüfungswerten Vorschlag, weil er u.U. bürokratisierende Tendenzen verhindern und zur Erhöhung der Akzeptanz des Datenschutzes insgesamt beitragen könnte.

Schwierigkeiten bereitet allerdings die Definition der trivialen Datenverarbeitung. In Erwägung zu ziehen ist etwa die in § 2 Abs. 2 Satz 1 des Entwurfs zur Änderung des HessDSG vorgenommene Abgrenzung: Danach erfaßt das HessDSG nur „die Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten".

Damit fiele jedenfalls ein rein mündlicher Umgang mit Daten, die weder in Akten noch auf einem anderen Datenträger festgehalten sind oder festgehalten werden sollen, nicht unter das Gesetz.

Die Abgrenzung ist nach meiner Ansicht wichtig, weil den Stellen, die triviale Datenverarbeitung betreiben, die Angst vor Restriktionen und Verpflichtungen genommen werden sollte, auch wenn im allgemeinen die gesetzlichen Voraussetzungen für die vorgesehene Verarbeitung von Daten erfüllt sein dürften.

6.1.3 Sicherstellung der Zweckbindung

Bisher haben sich die Speicherungs- und Übermittlungsvorschriften des Datenschutzrechts in erster Linie am Maßstab der „Erforderlichkeit der Daten für die rechtmäßige Aufgabenerfüllung" für die jeweilige öffentliche Stelle orientiert (vgl. §§ 9 Abs. 1, 10 Abs. 1, 15 Abs. 2, 3 HmbDSG). Diese Konzeption ist nach dem VZ-Urteil nicht mehr haltbar: Das BVerfG hat festgestellt, daß die Verwendung von Daten grundsätzlich auf den gesetzlich bestimmten Zweck begrenzt ist. Das ist der Zweck, der entweder in einer bereichsspezifischen Erhebungsvorschrift festgelegt ist bzw. – bei freiwilligen Datenangaben – der Zweck, der dem Betroffenen genannt wurde.

6.1.3.1 Zweckbindungsregelungen im geltenden Datenschutzrecht

In den meisten Datenschutzgesetzen sind Zweckbindungen nur bei den Daten vorgesehen, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und im Rahmen einer Berufs- oder Amtspflicht weitergegeben werden (vgl. z.B. §§ 10 Abs. 1 Satz

3, 12 Abs. 4 HmbDSG oder §§ 10 Abs. 1 Satz 2, 11 Satz 2 BDSG). Die Weitergabe wird hier davon abhängig gemacht, daß der Weitergabezweck mit dem Hergabezweck übereinstimmt.

Das HmbDSG hat den vom BVerfG postulierten Grundsatz der Zweckbindung darüber hinaus in einer Reihe von weiteren Regelungen bereits ansatzweise umgesetzt. So wird in § 9 Abs. 1 Satz 2 HmbDSG statuiert, daß die mehrfache Verwendung von Daten dem Betroffenen bekannt sein muß; § 9 Abs. 2 HmbDSG schränkt die Verwendung von Daten innerhalb einzelner speichernder Stellen ein; nach § 12 Abs. 2 HmbDSG dürfen Datenempfänger im nicht-öffentlichen Bereich die übermittelten Daten nur für den Zweck verwenden, zu dem sie übermittelt wurden. Alle diese Regelungen zielen in die richtige Richtung und können beibehalten werden.

Als weitsichtige Regelung, die ebenfalls zentrale Anliegen des BVerfG bereits vorweggenommen hat, hat sich ferner § 6 Abs. 1 Nr. 4 HmbDSG erwiesen. Diese Vorschrift ermöglicht es Bürgern, Datenübermittlungen zwischen verschiedenen öffentlichen Stellen zu sperren, soweit diese Übermittlungen nicht durch – bereichsspezifische – Gesetze zugelassen sind. Damit sollte die Verwaltung veranlaßt werden, ihre Datenübermittlungen einer kritischen Überprüfung zu unterziehen und ggf. gesetzliche Regelungen, die die Übermittlungsvoraussetzungen präzise regeln, vorzubereiten.

Leider ist die lobenswerte Intention des Gesetzgebers von der Verwaltung nicht in dem Maße realisiert worden, wie es wünschenswert gewesen wäre (vgl. 3. TB, 1.2, S. 3). Bereichsspezifische Übermittlungsregelungen sind kaum geschaffen worden. Dies wird sich allerdings zwangsläufig ändern müssen, wenn eine Novellierung des HmbDSG der Verwaltung den Rückzug auf die Generalklausel des § 10 Abs. 1 HmbDSG abschneidet und den bisherigen Ansatz durch die umfassende Orientierung am Grundsatz der Zweckbindung ersetzt. § 6 Abs. 1 Nr. 4 HmbDSG wird dann entfallen können.

6.1.3.2 Notwendige Neuregelungen im HmbDSG

Im HmbDSG sollten künftig folgende Grundsätze geregelt werden:
Wenn auch die denkbaren Verwendungszwecke im DSG als einer Auffang- und Rahmenregelung nicht im einzelnen normiert werden können, so sollte doch zunächst einmal klargestellt werden, daß personenbezogene Daten grundsätzlich nur zu dem Zweck weiterverarbeitet werden dürfen, für den sie erhoben oder gespeichert worden sind. Dementsprechend ist bei den Löschungsregelungen (§ 15 Abs. 3 HmbDSG) klarzustellen, daß Daten nach Wegfall des Verwendungszwecks zu löschen sind.

Dieser Grundsatz muß für alle Verarbeitungsphasen gelten, d.h. er ist gleichermaßen zu beachten

- bei der Nutzung durch die speichernde Stelle,
- bei einer Übermittlung innerhalb des öffentlichen Bereichs,
- bei einer Übermittlung aus dem öffentlichen in den privaten Bereich und
- bei der Nutzung durch die empfangende Stelle.

Nach dem VZ-Urteil ist die Einhaltung des Zweckbindungsprinzips durch – amtshilfefeste – Weitergabe- und Verwertungsverbote abzusichern. Dementsprechend ist im HmbBDSG zu regeln, daß (insbesondere bei einer Datenverarbeitung in Akten), ein Verwertungsverbot für solche Daten gilt, die nicht dem Zweck der jeweiligen Verarbeitung dienen.

6.1.3.3 Ausnahmen von der Zweckbindung

Wie jeder Grundsatz wird allerdings auch das Zweckbindungsprinzip nicht ausnahmslos gelten können. Das HmbDSG muß aber die zulässigen Ausnahmetatbestände – in allgemeiner Form – abschließend umschreiben, damit die Bürger wissen können, unter welchen Voraussetzungen sie mit Zweckänderungen zu rechnen haben.

Zu weitgehend ist es, eine Datenverwendung schon immer dann zuzulassen, wenn sie

mit dem Erhebungs- bzw. Speicherungszweck nicht unvereinbar ist (vgl. Art. 5 c der Datenschutzkonvention des Europarats).

Ein solches Zweckvereinbarkeitsprinzip trägt dem VZ-Urteil nicht hinreichend Rechnung: Es würde den fundamentalen Satz von der präzisen und konkreten Zweckbindung der Datenerhebung und -verarbeitung in seinen konkreten Auswirkungen zunichtemachen.

Ausnahmen von der Zweckbindung kommen vielmehr grundsätzlich nur in Betracht, wenn sie im überwiegenden Allgemeininteresse geboten sind und die notwendige Transparenz für den Bürger sichergestellt bleibt bzw. – ausnahmsweise – vernachlässigt werden kann.

Folgende Fallgruppen z.B. könnten im HmbDSG geregelt werden:

- Zweckdurchbrechungen sind zulässig mit entsprechender Einwilligung des Betroffenen;
- sie können ferner zugelassen werden, wenn keine schutzwürdigen Belange des Betroffenen beeinträchtigt werden können.

  Dies ist etwa der Fall, wenn davon ausgegangen werden kann, daß die zweckentfremdete Nutzung im alleinigen Interesse des Betroffenen liegt und dieser in Kenntnis des Verwendungszwecks seine Einwilligung hierzu erteilt hätte (etwa weil die Bearbeitung eines vom Betroffenen gestellten Antrages ohne Kenntnis der Daten nicht möglich ist). Diese Fallgruppe umfaßt auch Fälle „trivialer" Kommunikation sowie Fälle mit minimalen Zweckabweichungen.
- Im überwiegenden Allgemeininteresse kommen Zweckdurchbrechungen ferner in Betracht, wenn eine bereichsspezifische Regelung dies vorsieht. Zu denken ist hierbei an die Fälle, in denen eine Datenerhebung durch die empfangende Stelle ohne Mitwirkung des Betroffenen erfolgen dürfte.
- Schließlich erscheint es unvermeidbar, Zweckdurchbrechungen zuzulassen, wenn die Abwehr erheblicher Gefahren für das Gemeinwohl oder einer schwerwiegenden Beeinträchtigung eines Einzelnen dies gebietet. Eine solche Notstands-Generalklausel wird nicht verzichtbar sein, sollte aber so eng wie möglich gefaßt werden.

6.1.3.4 Sonderregelungen für Direktzugriffsverfahren

Besondere Probleme für die Einhaltung der Zweckbindung ergeben sich auch bei der Einrichtung von Direkt-Zugriffs-Verfahren (on-line-Verbindungen) zwischen verschiedenen speichernden Stellen. Diese bedürfen daher ergänzender gesetzlicher Regelungen.

Das BVerfG hat im VZ-Urteil ausdrücklich klargestellt, daß bei der Beurteilung der Zulässigkeit von Eingriffen in das Recht auf informationelle Selbstbestimmung nicht allein auf die Art der Angaben abgestellt werden kann. Entscheidend sind vielmehr ihre Nutzbarkeit und Verwendungsmöglichkeit. Die Beurteilung dieser beiden Kriterien hängt wiederum von zwei Gesichtspunkten ab:

- einerseits von dem Zweck, dem eine Erhebung dient;
- andererseits von den der jeweils eingesetzten Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten.

Daraus folgt, daß die Zulässigkeit von Informationseingriffen (wie die Weitergabe von personenbezogenen Daten) nicht lediglich an die Voraussetzung gebunden werden darf, ob und wann eine Behörde – in welcher Form auch immer – bestimmte personenbezogene Daten verarbeiten darf (so noch § 10 HmbDSG); darüber hinaus ist vielmehr – neben dem Zweck – auch festzulegen, in welcher Form die Übermittlung zulässig ist. Wenn diese Frage offenbleibt, können Nutzbarkeit und Verwendungsmöglichkeiten bestimmter Angaben (und damit die Zulässigkeit eines Eingriffs in das Recht auf informationelle Selbstbestimmung) nicht umfassend beurteilt werden.

Da die Nutzbarkeit von Daten bei der Einrichtung von Direktzugriffsverfahren (=Übermittlungen im Wege der Datenfernübertragung) regelmäßig erheblich größer ist als etwa bei der manuellen Informationssammlung in Akten oder Karteien (erweiterte Zugriffsmöglichkeiten, bessere Erschließbarkeit sind auch andere gesetzliche Voraussetzungen für deren Einrichtung zu definieren.

Folgende Grundsätze für on-line-Verbindungen sollten daher im HmbDSG festgelegt werden:

1. Die Voraussetzungen für eine Übermittlung von Daten, die abgefragt werden können, müssen generell vorliegen.

2. Das Bereithalten der Daten zum sofortigen Abruf muß unter Abwägung der schutzwürdigen Belange der Betroffenen einerseits mit der Dringlichkeit des Übermittlungsbedürfnisses der beteiligten Stellen andererseits angemessen sein.

3. Ferner sollte klargestellt werden, daß die Einrichtung jedes on-line-Anschlusses im öffentlichen Bereich einer Regelung durch Rechtsvorschrift bedarf, die das Abwägungsergebnis dokumentiert und die jeweils gebotenen Sicherungsmaßnahmen festlegt.

6.1.4. Mehr Transparenz der Informationsverarbeitung für die Betroffenen

Das vom BVerfG im VZ-Urteil anerkannte Recht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Dies setzt voraus, daß ein Bürger wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß. Ein solches Wissen ist ihm wiederum nur möglich, wenn er hinreichende Aufklärungs- und Auskunftsrechte in Anspruch nehmen kann. Diesem Anspruch werden die bestehenden Datenschutzgesetze mit ihren Regelungen (vgl. z.B. §§ 5 Abs. 2, 9 Abs. 2, 10 Abs. 1 S. 2, 13 Abs. 2 und 14 HmbDSG) noch nicht im gebotenen Umfang gerecht. Es erscheint vielmehr notwendig, Aufklärungspflichten bei der Erhebung und Verwendung von Daten abzusichern, den Umfang des Auskunftsrechts zu erweitern sowie u.U. durch ein Akteneinsichtsrecht zu ergänzen.

6.1.4.1 Erweiterung des Umfangs von Auskunftsrechten

Es erscheint nach den Grundsätzen des VZ-Urteils unzureichend, wenn die Auskunft – wie in § 14 Abs. 1 HmbDSG vorgesehen – auf die über den Betroffenen gespeicherten Daten sowie die Stellen, denen Daten regelmäßig übermittelt werden, beschränkt wird. Auskunft muß vielmehr auch über den Zweck und die Rechtsgrundlage der Speicherung sowie über die Herkunft der Daten gegeben werden.

Die Auskunft soll also um Angaben erweitert werden, die bislang bereits teilweise Gegenstand des Datenschutzregisters nach § 13 HmbDSG waren und über die Betroffene künftig auch bei der Erhebung unterrichtet werden sollen.

Es würde die Regelung unnötig kompliziert machen, wenn die Auskunft über Zweck, Rechtsgrundlage und ggf. Empfänger auf die Fälle beschränkt würde, in denen die Daten nicht beim Betroffenen erhoben worden sind. Hinzu kommt, daß der Aufwand für diese Auskunft gering ist.

Dagegen verursacht eine Auskunft über die Herkunft der Daten möglicherweise zusätzlichen Aufwand; denn die Pflicht, hierüber Auskunft zu erteilen, zwingt die speichernde Stelle zu Aufzeichnungen. Andererseits haben die bisherigen Erfahrungen gezeigt, daß erst eine Auskunft über die Herkunft der Daten den Betroffenen in die Lage versetzt, „Wanderungen" seiner Daten auf die Spur zu kommen und seine sonstigen Rechte gegenüber allen Stellen wahrzunehmen, die Daten über ihn speichern. Der Aufwand für die Speicherung von Angaben über die Herkunft der Daten sollte daher in Kauf genommen werden; er kann u.U. Anlaß sein, die Speicherung personenbezogener Daten zu begrenzen.

Schließlich wäre zu erwägen, den Auskunftsanspruch auch auf die Empfänger nicht regelmäßiger Übermittlungen auszudehnen, soweit diese mit vertretbarem Aufwand festgestellt werden können.

6.1.4.2 Auskunftsrecht bei Aktenverarbeitung

Auch das Auskunftsrecht darf nicht wie bisher auf Dateien beschränkt bleiben, sondern muß auch auf die personenbezogenen Daten erstreckt werden, die in Akten oder sonstigen amtlichen Unterlagen gespeichert werden. Allerdings bedarf es einiger Modifizierungen, die sich aus der Besonderheit der Datenverarbeitung in nicht dateimäßiger Form ergeben und vor allem dem Problem der Auffindbarkeit personenbezogener Daten in Akten Rechnung tragen:

- Das Auskunftsrecht kann nur insoweit bestehen, als nicht in Rechte Dritter eingegriffen wird.
- Wenn Akten oder sonstige Unterlagen zur Person des Betroffenen geführt werden, braucht im Antrag auf Auskunft nur die Aktensammlung oder die Aufgabe bezeichnet zu werden, für die die in Akten oder sonstigen Unterlagen gespeicherten personenbezogenen Daten verwendet werden.
- Wenn sich die Auskunft auf Teile von Akten oder sonstigen Unterlagen beziehen soll, müssen im Antrag nähere Angaben darüber gemacht werden, aus welchem Anlaß und in welchem Zusammenhang die Vorgänge entstanden sind.

Diese Beschränkungen ermöglichen es, den Aufwand für die Auskunft aus Akten und sonstigen Unterlagen in Grenzen zu halten.

6.1.4.3 Ausnahmen für Sicherheitsbehörden

Es entspricht nicht den Vorgaben des Bundesverfassungsgerichts, daß bestimmte Behörden generell von der Auskunftsverpflichtung ausgenommen werden. § 14 Abs. 2 HmbDSG sollte daher gestrichen werden. Die in Abs. 3 genannten Ausnahmen reichen aus, um auch den Sicherheitsbehörden aufgrund einer Interessenabwägung im Einzelfall eine Auskunftsverweigerung zu ermöglichen, wie ich schon in meinem 2. TB, 3.9.2, S. 74 ff ausführlich dargelegt habe. Dies entspricht i.ü. der seit Jahren zumindest von der Polizei in Hamburg geübten Praxis.

Etwaige Ablehnungen eines Antrages auf Auskunft müssen begründet werden, damit sie durch die Verwaltungsgerichte nachgeprüft werden können. Nur wenn die Mitteilung der Gründe für die Verweigerung der Auskunft den mit der Auskunftsverweigerung verfolgten Zweck gefährden würde, kann eine Begründung unterbleiben. Die speichernde Stelle muß aber die wesentlichen Gründe für die Unterbindung intern in einer Weise aufzeichnen, die eine Überprüfung u.a. auch durch den Datenschutzbeauftragten ermöglicht.

Die bisher in § 14 Abs. 3 HmbDSG normierten Ausnahmen von der Auskunftspflicht können im wesentlichen erhalten bleiben:

- Gefährdung der Aufgabenerfüllung;
- Gefährdung der öffentlichen Sicherheit oder Nachteile für das Wohl des Bundes oder eines Landes;
- Geheimhaltung wegen einer Rechtsvorschrift oder wegen der überwiegenden Interessen einer dritten Person.

Entfallen muß allerdings die generelle Ausnahme für die Übermittlung an bestimmte Behörden (§ 14 Abs. 3 Nr. 4 HmbDSG). Genausowenig wie Behörden schlechthin von der Auskunftsverpflichtung freigestellt werden dürfen, dürfen die Übermittlungen an bestimmte Empfänger generell von dieser Verpflichtung ausgenommen werden.

6.1.4.4 Benachrichtigungspflichten

In der Novellierungsdiskussion ist verschiedentlich die Frage erörtert worden, ob Betroffene auch im öffentlichen Bereich über die erstmalige Speicherung ihrer Daten –

ähnlich wie im nicht-öffentlichen Bereich (vgl. §§ 26 Abs. 1, 34 Abs. 1 BDSG) – benachrichtigt werden sollten.

Ich halte eine solche generelle Benachrichtigungspflicht für verzichtbar, wenn die Daten, wie es die Regel sein sollte, beim Betroffenen erhoben werden, und er bei dieser Gelegenheit über den Verwendungszweck aufgeklärt und auf eine beabsichtigte Speicherung hingewiesen wurde. In diesen Fällen reicht es zur Herstellung der gebotenen Transparenz aus, wenn der Betroffene sich im Wege eines – allerdings bürgerfreundlich und umfassend auszugestalteten – Auskunftsanspruchs von sich aus einen Überblick über die gespeicherten Daten verschafft.

Zu beachten ist aber die gesetzliche Anforderung des § 10 Abs. 1 Satz 2 HmbDSG, wonach dem Bürger die Zulässigkeit mehrfacher Verwendung seiner Daten bekannt sein muß. Diese Regelung sollte insoweit ergänzt werden, als der Bürger über jede Verwendung von Daten (einschl. Übermittlung) benachrichtigt werden sollte, die mit dem ihm bekannten Verwendungszweck nicht übereinstimmt und in die er auch nicht eingewilligt hat.

Ausnahmen von dieser Benachrichtigungspflicht kommen nur für die Fallgruppen in Betracht, in denen das Geheimhaltungsinteresse der Verwaltung das Informationsinteresse des Betroffenen überwiegt und somit auch keine Auskunftsverpflichtung bestünde. Dies sind etwa Fälle, in denen eine Unterrichtung die Aufgabenerfüllung einer Behörde oder das Wohl des Bundes oder eines Landes gefährden würde. In diesen Fällen ist eine Benachrichtigung allerdings nachzuholen, sobald der Hinderungsgrund weggefallen ist.

Zu erwägen ist schließlich, ob eine Benachrichtigung auch in den Fällen verzichtbar ist, in denen die Zweckänderung keine schutzwürdigen Belange des Betroffenen beeinträchtigt. Es ist nicht auszuschließen, daß der Betroffene sich in solchen geringfügigen Fällen durch Benachrichtigungen eher belästigt als informiert fühlt. Ich halte es daher für sachgerecht, daß der Betroffene auch in solchen Fällen darauf verwiesen wird, sein Informationsbedürfnis selbst – durch ein Auskunftsbegehren – zu befriedigen.

6.1.4.5 Aufklärungspflichten bei der Erhebung

Für den Fall einer Datenerhebung beim Betroffenen gibt es nach geltendem Recht bereits eine Reihe von Aufklärungspflichten. Diese sind jedoch z.T. – insbesondere im Hinblich auf den Grundsatz der Zweckbindung – zu ergänzen.

§ 9 Abs. 2 HmbDSG verlangt u.a. einen Hinweis auf die Rechtsgrundlage der Datenerhebung, wenn Daten beim Betroffenen erhoben werden. Bei diesem Hinweis sollte differenziert werden danach, ob eine Auskunftspflicht besteht, ob die Angaben lediglich eine Voraussetzung für die Gewährung von Rechtsvorteilen bzw. Vermeidung von Rechtsnachteilen (Obliegenheit) oder aber völlig freiwillig sind. In diesem Zusammenhang sollte ferner vorgesehen werden, daß auch über den Verwendungszweck der zu erhebenden Daten in geeigneter Weise aufgeklärt wird.

Bei der Erteilung einer Einwilligung ist die Information über den Verwendungszweck bereits vorgesehen (vgl. § 5 Abs. 2 HmbDSG). Hier sollte noch klargestellt werden, daß der Betroffene unter Hinweis auf etwaige Rechtsfolgen darüber aufgeklärt wird, daß er die Einwilligung verweigern kann.

6.1.4.6 Allgemeines Akteneinsichtsrecht

Verschiedentlich ist in der Novellierungsdiskussion auch die Frage aufgeworfen worden, ob die Auskunftsregelungen des Datenschutzgesetzes durch ein allgemeines, nicht nur einzelnen Betroffenen zustehendes Akteneinsichtsrecht ergänzt werden sollte, weil mir so das demokratische Gebot einer transparenten Verwaltung realisiert werden könnte.

Ich kann diese Frage z.Z. nicht klären, möchte aber den Anstoß geben, diesem Problem im Zusammenhang mit der Novellierung des HmbDSG nachzugehen.

In der Praxis stellen sich für Bürger, die ihre in den Datenschutz- und Verwaltungsverfahrensgesetzen verankerten Auskunfts- und Akteneinsichtsrechte durchsetzen wollen, vielfältige Schwierigkeiten. Gemessen am Ziel der Aktenöffentlichkeit, wie es etwa im Freedom of Information Act der USA weitgehende Anerkennung gefunden hat, sind die Defizite unseres nach wie vor am Geheimhaltungsprinzip orientierten Verwaltungssystems noch größer. Weder Auskunftsrechte noch das Akteneinsichtsrecht nach § 29 VwVfG haben – in ihrer jetzigen begrenzten Ausgestaltung (weit enger als die vergleichbare Vorschrift des § 99 VwGO) – zur Kontrolle der Verwaltung durch die Öffentlichkeit entscheidend beigetragen. Wesentliche Voraussetzung für ein Vertrauensverhältnis zwischen Staat und Bürger sowie für Partizipationschancen des einzelnen ist jedoch Verwaltungstransparenz.

Die bestehenden Auskunfts- und Akteneinsichtsrechte, die nur punktuell den überkommenden Grundsatz des Amtsgeheimnisses durchbrechen, werden diesem Grundverständnis nicht gerecht. Anders als in der Bundesrepublik ist in anderen westlichen Staaten (z.B. Schweden, Norwegen, Dänemark, Niederlande, USA, Kanada, Australien, Neuseeland) der Anspruch der Bürger (von denen ja die Staatsgewalt ausgeht), von der Verwaltung zu erfahren, welche Informationen sich in Akten und anderen Speichermedien befinden, unabhängig davon anerkannt, ob sie betroffen sind oder ob ein Verwaltungsverfahren anhängig ist oder nicht.

Spricht der Transparenzgedanke des Datenschutzes insofern für die Erweiterung bestehender Auskunftsrechte und für die Schaffung eines allgemeinen Akteneinsichtsrechts, so bedingt die andere, die „defensive" Facette des Datenschutzes, nämlich der Schutz der Persönlichkeitssphäre, daß ein solches Informations- und Akteneinsichtsrecht seine Grenze findet an den schutzwürdigen Belangen – insbesondere dem Persönlichkeitsrecht, aber auch an Betriebs- und Geschäftsgeheimnissen – Dritter. Die nicht zu umgehende und im Einzelfall höchst schwierige Aufgabe der notwendigen Grenzziehung obliegt zunächst dem Gesetzgeber, dann aber auch der Gesetzesanwendung.

6.1.5. Weitere Stärkung von Rechten der Betroffenen

Die Sicherung des Rechts auf informationelle Selbstbestimmung – also der Befugnis des Einzelnen, grundsätzlich selbst über die Verwendung seiner persönlichen Daten zu bestimmten – erfordert neben einem Ausbau der Auskunftsrechte (s.o.6.1.4.1) auch eine Verstärkung der sonstigen Rechte, mit denen Bürger sich gegen eine Beeinträchtigung ihrer Persönlichkeitssphäre selbst zur Wehr setzen können (vgl. § 6 HmbDSG).

6.1.5.1 Rechte auf Berichtigung, Sperrung und Löschung bei Aktenverarbeitung

Vorrangig ist sicherzustellen, daß die Rechte der Betroffenen

- auf Berichtigung (§ 6 Abs. 1 Nr. 5 i.V.m. § 15 Abs. 2),
- auf Sperrung (§ 6 Abs. 1 Nr. 6 i.V.m. § 15 Abs. 2) und
- auf Löschung (§ 6 Abs. 1 Nr. 7 i.V.m. § 15 Abs. 3)

auch bei der Datenverarbeitung in Akten gelten. Dabei wird allerdings Besonderheiten dieser Verarbeitungsform Rechnung zu tragen sein.

So kann eine Berichtigung – im Hinblick auf die Pflicht zur vollständigen Aktenführung – sicherlich nicht einfach in der Weise erfolgen, daß eine unrichtige Information durch eine richtige ersetzt wird. Auch wird eine punktuelle Berichtigung nicht immer möglich sein. In diesen Fällen muß aber in geeigneter Weise vermerkt werden, zu welchem Zeitpunkt und aus welchem Grund die personenbezogenen Daten unrichtig waren oder geworden sind. In diesem Sinn sollte § 15 Abs. 1 HmbDSG ergänzt werden.

Für die Sperrung von Daten, die in Akten gespeichert sind, gibt es keine Besonderheiten: Die Sperrung hat in geeigneter Weise zu erfolgen, d.h. – bei Einzelfällen – durch Sperrvermerk und – bei einer Vielzahl von Fällen – durch Dienstanweisung. Für die gesperrten Daten gilt ein Verwertungsverbot.

Besonderer Regelungen bedarf – wiederum im Hinblick auf die Pflicht zur vollständigen Aktenführung – die Löschung von Daten: Diese ist nur durchzuführen, wenn der ganze zur Person eines Betroffenen geführte Aktenvorgang zur Aufgabenerfüllung nicht mehr benötigt wird; im übrigen können die Daten nur gesperrt werden. Dies sollte in § 15 Abs. 3 HmbDSG ergänzend geregelt werden.

6.1.5.2 Regelfristen für die Überprüfung und Löschung von Daten

In der bisherigen Novellierungsdiskussion wurde erwogen, daß die o.g. Rechte der Betroffenen durch die Festlegung von regelmäßigen Löschungsfristen für gespeicherte Daten im Datenschutzgesetz ergänzt werden sollen. Ich halte dies nicht für geboten, denn Löschungsfristen können sachgerecht nur in bereichsspezifischen Datenschutzvorschriften festgelegt werden, wie z.B. im Bundeszentralregistergesetz und in den Meldegesetzen geschehen. Ich halte es allerdings für notwendig, weitere bereichsspezifische Vorschriften für die Löschung von personenbezogenen Daten zu schaffen.

Bereichsspezifisch sollten ferner Verpflichtungen der Verwaltung begründet werden, in bestimmten Abständen die gespeicherten Daten darauf zu überprüfen, ob sie noch für die rechtmäßige Erfüllung der Aufgaben erforderlich sind.

Eine entsprechende Regelung gibt es in § 15 Abs. 4 HmbDSG bereits. Danach gilt generell eine Überprüfungsfrist von vier Jahren. Diese Regelung hat in den vergangenen Jahren richtungsweisende Funktion gehabt und eine Reihe von Veränderungen zu Positiven bewirkt (vgl. 1. TB, 8.2, S. 60, 2. TB, 3.12.1, S. 98 betr. die Zentralkartei der Staatsanwaltschaft). Sie stößt allerdings – insbesondere bei einer weiteren Zunahme bereichsspezifischer Regelungen – materiell in Leere: Dies gilt etwa, wenn gesetzliche Aufbewahrungsvorschriften vorschreiben, daß der Bestand einer Datei über den Prüftermin hinaus zur Verfügung stehen kann. Dann kann das mit der Überprüfung verfolgte Ziel, nicht mehr erforderliche Daten zu löschen, nicht erreicht werden.

Eine Überprüfung dürfte auch entbehrlich sein, wenn Daten von einem Antragsteller freiwillig und in der Erwartung einer Gegenleistung abgegeben werden. Hier erwartet der Betroffene eine Leistung der Verwaltung. Es ist davon auszugehen, daß er daran interessiert ist, daß seine Daten weiterhin gespeichert werden; andernfalls kann er selbst die Löschung verlangen. Eine Nachfrage beim Betroffenen, ob die Datenspeicherung noch erforderlich ist, würde i.d.R. auf Unverständnis stoßen.

In den Fällen, in denen der Betroffene gesetzlichen Meldepflichten nachkommen muß, kann es nicht Aufgabe der Verwaltung sein, aus Gründen des Datenschutzes die Erfüllung von Meldepflichten des Betroffenen zu kontrollieren.

6.1.5.3 Schadensersatz

Das HmbDSG sieht in seinem § 17 zwar bereits einen verschuldensunabhängigen Schadensersatzanspruch ohne summenmäßige Begrenzung vor und geht insofern bereits über andere Datenschutzgesetze hinaus; auch diese Regelung sollte bei einer Novellierung im Interesse eines möglichst effektiven Schutzes für betroffene Bürger abgerundet werden. Es sollte klargestellt werden,

- daß der Begriff rechtswidrige Datenverarbeitung sowohl die unzulässige als auch die unrichtige Verarbeitung personenbezogener Daten umfaßt und
- daß der Schadensersatzanspruch sich auch auf immaterielle Schäden erstreckt. Diese aus der Ersatzpflicht herauszunehmen, hieße, typische und häufig auftretende Schäden unberücksichtigt zu lassen.

6.1.6. Klarstellung der Kompetenzen des DSB

In Hamburg habe ich bislang im Ergebnis alle Unterlagen einsehen können, deren Überprüfung ich zur Erfüllung meiner Aufgaben für erforderlich hielt. Gelegentlich ist es allerdings zu Verzögerungen gekommen, insbesondere weil einzelne Stellen mir

unter Berufung auf das Arzt- und Sozialgeheimnis zunächst keine Einsicht gewähren wollten. Aus dem Bund und aus anderen Ländern sind ähnliche Schwierigkeiten bekannt (vgl. dazu meinen 2. TB, 3.9.1, S. 72 ff).

Um derartige Streitigkeiten, deren Lösung heute letztlich von politischen Entscheidungen abhängig ist, für die Zukunft auszuschließen, halte ich eine Klarstellung meiner Kontrollbefugnisse – bei Gelegenheit einer Novellierung des HmbDSG insgesamt – für wünschenswert.

Maßgeblich für den Umfang der Kontrollkompetenzen muß der Inhalt und Anwendungsbereich des Rechts auf informationelle Selbstbestimmung sein. Der Datenschutzbeauftragte kann nur dann effektiv arbeiten, wenn er alle Eingriffe in dieses Recht überprüfen kann und darf. Bereiche, in denen keine Kontrolle stattfindet, sind daher nicht akzeptabel.

Daraus folgt:

Die Kontrollbefugnis des Datenschutzbeauftragten umfaßt die Einhaltung der Datenschutzgesetze und aller anderen datenschutzrechtlichen Vorschriften, unabhängig davon, ob Daten in Dateien, in Akten oder in sonstiger Form festgehalten werden.

Dem Datenschutzbeauftragten dürfen nicht die speziellen Geheimhaltungspflichten entgegengehalten werden können, deren Befolgung er nach seinem gesetzlichen, durch das BVerfG bekräftigten Auftrag sicherzustellen hat. Deshalb ist klarzustellen, daß besondere Geheimhaltungspflichten (wie z.B. das Steuer-, Sozial- oder Arztgeheimnis) eine Datenschutzkontrolle nicht ausschließen oder einschränken.

6.1 Novellierung des BDSG

Bei meiner Darstellung des Novellierungsbedarfs im BDSG möchte ich die für meine Tätigkeit als Aufsichtsbehörde maßgeblichen Regelungen für den nicht-öffentlichen Bereich (3. und 4. Abschnitt des BDSG) in den Vordergrund rücken.

Auch die Regelungen des BDSG für den öffentlichen Bereich sind für die Länder jedoch nicht ohne Bedeutung. Bislang hat das BDSG auch für die Landesdatenschutzgesetze Leitfunktionen übernommen, und diese Rolle sollte es nach Möglichkeit auch in Zukunft behalten. Dementsprechend werden Änderungen der Abschnitte 1 (Allgemeine Vorschriften) und 2 (Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen) des BDSG die Entwicklung des Datenschutzrechts in Hamburg in starkem Maße beeinflussen. Ich habe mich daher auch an diesem Teil der Novellierungsdiskussion intensiv beteiligt und mich u.a. im Juni 1985 auf Einladung des Bundestags-Innenausschusses auf einer Sachverständigen-Anhörung geäußert (vgl. BT-Drs. 10/1186).

6.2.1 Öffentlicher Bereich

Für die Novellierung der für die öffentliche Verwaltung geltenden Vorschriften des BDSG sind die gleichen Grundsätze maßgeblich, die ich vorstehend für die Novellierung des HmbDSG entwickelt habe. An dieser Stelle möchte ich daher nur einige Punkte hervorheben, die mir bei den von den Koalitions-Parteien im Bund entwickelten Novellierungs-Vorschlägen –soweit sie mir bislang bekannt sind– als besonders problematisch erscheinen. Zu nennen sind hier folgende Punkte:

- Kontrollkompetenzen des Datenschutzbeauftragten:

  Alle Streitfragen, die in der Vergangenheit gelegentlich entstanden sind, wenn die Verwaltung versuchte, die Kontrolltätigkeit des Datenschutzbeauftragten zu beschränken, sollen weitgehend im Sinne der Verwaltung entschieden werden.

  Zunächst wird festgelegt, daß der BfD die Einhaltung datenschutzrechtlicher Vorschriften grundsätzlich nur insoweit überprüfen darf, als sie die Verarbeitung personenbezogener Daten in Dateien oder ihre unmittelbare Nutzung aus Dateien regeln. Die Datenverarbeitung in Akten soll er nur überprüfen können, wenn er konkrete Anhaltspunkte für die Verletzung von Datenschutzvorschriften hat. Ferner

wird der Dateibegriff neu definiert mit der Folge, daß auch Akten, die mit Hilfe automatisierter Verfahren nachgewiesen werden (z.B. NADIS, KAN), nicht als Dateien angesehen werden und somit nicht der allgemeinen, routinemäßigen Datenschutzkontrolle unterliegen. Diese Einschränkungen sind nicht akzeptabel; der Datenschutzbeauftragte kann seinen –vom Bundesverfassungsgericht im VZ-Urteil ausdrücklich bekräftigten– Auftrag zu einem effektiven Schutz des Rechts auf informationelle Selbstbestimmung nur ausführen, wenn seine Kontrollkompetenz unmißverständlich auf jede Form der Datenverarbeitung erstreckt wird.

Weiter sollen sich die Koalitionsparteien –nach meinen Informationen– darauf verständigt haben, daß der Betroffene die Möglichkeit erhalten soll, in bestimmten Fällen der Kontrolle seiner Daten durch den Datenschutzbeauftragten zu widersprechen, und zwar bei personenbezogenen Daten, die dem Steuergeheimnis oder der ärztlichen Schweigepflicht unterliegen sowie bei Daten in Personalakten oder in den Sicherheitsakten einer Beschäftigungsbehörde. Bei diesem Vorbehalt bleibt völlig unklar, wie er in der Praxis geltend gemacht werden soll: Müssen alle Betroffenen bei der Erhebung oder vor jedem Kontrollbesuch des Datenschutzbeauftragten eine Erklärung dazu abgeben, ob sie widersprechen wollen? Nicht nachvollziehbar ist es i.ü., daß etwa Fachaufsichts- und Rechnungsprüfungsbehörden im Rahmen ihrer Aufgabenstellung auch die o.g. Unterlagen überprüfen dürfen, ausgerechnet dem Datenschutzbeauftragten jedoch, der die Einhaltung der besonderen Datenschutzvorschriften zu überwachen hat, Datenschutzgesichtspunkte sollen entgegengehalten werden können. So wird Datenschutz-Kontrolle ad absurdum geführt (vgl. a. 2. TB, 3.9.1.5).

Schließlich sollen personenbezogene Daten von der Datenschutz-Kontrolle ausgespart bleiben, wenn sie der Kontrolle nach dem Gesetz zur Ausführung des Art. 10 GG (G-10) unterliegen, also aus einer Überwachung des Brief- und Fernmeldeverkehrs durch die Nachrichtendienste stammen. Auch hierdurch wird der verfassungsgerichtlich anerkannte Auftrag des Datenschutzbeauftragten in Frage gestellt. Das Bundesverfassungsgericht hat in seinem "BND-Urteil" vom 20.6.1984 (NJW 1984, 121, 125) deutlich zum Ausdruck gebracht, daß die "strategische" Telefonüberwachung u.a. nur deshalb hingenommen werden kann, "weil die Kontrolle der Maßnahmen (...) durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane (Kontrollkommission und Datenschutzbeauftragte) sichergestellt ist". Keineswegs ist wegen der "besonderen Empfindlichkeit und Geheimhaltungsbedürftigkeit der Materie" –wie die Bundesregierung meint– die Kontrolle durch den DSB ausgeschlossen.

- Transparenz für den Bürger:

  Nach wie vor sollen Sicherheitsbehörden weitgehend von Auskunftsverpflichtungen gegenüber den Bürgern ausgenommen werden: Für Geheimdienste soll keine Auskunftspflicht bestehen, soweit die Sicherheit des Bundes berührt wird. Eine solche "Berührung" dürfte in diesem Bereich immer gegeben sein. Strafverfolgungsbehörden sollen keine Auskunft erteilen müssen, wenn eine Abwägung ergibt, daß die schutzwürdigen Belange des Betroffenen hinter den öffentlichen Interessen, die Auskunft nicht zu erteilen, zurücktreten müssen. Daneben sollen die weiteren, schon bisher in § 14 Abs. 3 BDSG vorgesehenen Ausnahmen weiterbestehen. Derartig weitgehende Ausnahmen werden dem Recht auf informationelle Selbstbestimmung nicht gerecht. Darüber ist bislang nicht sichergestellt, daß die Gründe für eine Auskunftsverweigerung im einzelnen dokumentiert werden.

- Ausnahmen von der Zweckbindung:

  Der Grundsatz der Zweckbindung wird in den mir bekannten Novellierungsvorstellungen zwar anerkannt, zugleich soll allerdings ein langer Katalog von Ausnahmeregelungen gelten: so sollen Zweckdurchbrechungen schon zulässig sein, wenn angenommen werden kann, daß sie im Interesse des Betroffenen liegen und er in Kenntnis des Verwendungszwecks einwilligen würde bzw. wenn die Daten für den anderen Zweck nach einer anderen Rechtsvorschrift erhoben werden dürften. Diese Ausnahmetatbestände sind zu unbestimmt und zu weitgehend, sie geben

weder dem Bürger noch der speichernden Stelle selbst klar zu erkennen, wo die Verarbeitungsbefugnis beginnt und wo ihre Grenzen verlaufen.

- Regelungen für on-line-Verfahren:

  Die bisher bekannten Koalitionsvorstellungen verzichten darauf, die Einrichtung von einzelnen on-line-Verfahren (automatisiertes Abrufverfahren) durch Rechtsvorschriften abzusichern, sondern überlassen die erforderlichen Festlegungen jeweils den speichernden Stellen und den Datenempfängern. Dieses Verfahren trägt dem Grundsatz der Zweckbindung nicht hinreichend Rechnung (s.o.6.1.3.4).

6.2.2 Nicht-öffentlicher Bereich

6.2.2.1 Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts

Das Volkszählungsurteil hat Konsequenzen auch für die Datenverarbeitung im nicht-öffentlichen Bereich. Die vom Bundesverfassungsgericht 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. Moderne Personalinformationssysteme etwa liefern die Möglichkeit zu einer umfassenden Normung und Kontrolle des Verhaltens und der Leistung der Beschäftigten. Angesichts dieser Gefährdungen reicht es nicht aus, daß das Recht auf informationelle Selbstbestimmung als Ordnungsgrundsatz und objektive Wertentscheidung der Verfassung Drittwirkung insofern entfaltet, als Regelungen der Rechtsbeziehungen zwischen Privaten in seinem Geiste ausgelegt werden. Die Aussage des Bundesverfassungsgerichtes, mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß, schließt in ihrem Sinngehalt auch private Stellen als solche Wissensträger ein und verpflichtet den Gesetzgeber, den Bürger vor freiheitsbedrohender Datenverarbeitung auch im privaten Bereich stärker zu schützen, als dies im Bundesdatenschutzgesetz bislang geschehen ist.

Auch die Bundesregierung hat in ihrer vom Bundesminister für Arbeit und Sozialordnung erarbeiteten Stellungnahme vom 30.4.1985 gegenüber dem Innenausschuß des Deutschen Bundestages anerkannt, daß das Urteil des Bundesverfassungsgerichts auch für den Schutz der informationellen Selbstbestimmung im nicht-öffentlichen Bereich Bedeutung hat, und leitet daraus das Gebot ab, den Schutz von Arbeitnehmerdaten gesetzlich zu regeln.

Es muß allerdings – wie auch die Bundesregierung in ihrer Stellungnahme betont hat – berücksichtigt werden, daß das Recht auf informationelle Selbstbestimmung im privaten Bereich mit anderen Grundrechten (z.B. Art. 5 Abs. 1 und 2 und Art. 2 Abs. 1 Grundgesetz) kollidieren kann. Private Datenverarbeiter z.B. können sich gegenüber dem Recht auf informationelle Selbstbestimmung ihrerseits auf das Grundrecht der allgemeinen Handlungsfreiheit und andere Grundrechte berufen. Bei derartigen Kollisionen ist dann ein Ausgleich zwischen den verschiedenen Grundrechtspositionen vorzunehmen.

Ziel der Novellierung des BDSG muß es auch im privaten Bereich sein, das informationelle Selbstbestimmungsrecht des Einzelnen zu stärken. Gesetzliche Korrekturen sind dort geboten, wo sich die bisherigen Regelungsansätze des BDSG – Einwilligung und Vertragsverhältnis – als wirkungslos erwiesen haben.

Vordringlich sind namentlich folgende Regelungen:

6.2.2.2 Ausweitung des Anwendungsbereichs

Auch im nicht-öffentlichen Bereich muß das Bundesdatenschutzgesetz vom Dateibezug abrücken und die Datenverarbeitung in Akten und sonstigen Datensammlungen

mit einbeziehen. Wie im öffentlichen Bereich (s. 6.1.2.2, 6.1.4.2) müssen hier natürlich differenzierte Regelungen für verschiedene Verarbeitungsformen gefunden werden.

Auch kann es nicht bei einer Beschränkung auf einige Phasen der Datenverarbeitung bleiben. Deshalb muß auch für den nicht-öffentlichen Bereich die Geltung des BDSG auf die Erhebung und sonstige Nutzung von Daten ausgedehnt werden.

6.2.2.3 Grundsatz der Zweckbindung

Der Grundsatz der Zweckbindung muß im BDSG auch für den nicht-öffentlichen Bereich verankert werden, da ansonsten die Entscheidung des Betroffenen oder des Gesetzgebers, die Verarbeitung von Daten jeweils für einen konkret bestimmten Zweck zuzulassen, gegenstandslos würde, wenn die weitere Verwendung der Daten nicht grundsätzlich an diesen Zweck gebunden wäre.

Von einer so strikten Zweckbindung, wie sie im öffentlichen Bereich geboten ist, kann im nicht-öffentlichen Bereich aber abgesehen werden. Meines Erachtens kann deshalb sowohl bei der Speicherung als auch bei der Übermittlung der Erlaubnistatbestand der Abwägung zwischen berechtigten Interessen der einen Seite und schutzwürdigen Belangen der Betroffenen beibehalten werden. Auch die Privilegierung der Übermittlung listenmäßig oder sonst zusammengefaßter Daten muß nicht gänzlich aufgegeben werden. Als Ausgleich dafür müssen die Nutzung der Daten konkreter geregelt und die Abwehrrechte der Betroffenen gestärkt werden.

6.2.2.4 Verbesserung der Rechte der Bürger

Auch im nicht-öffentlichen Bereich sind die Ansprüche der Betroffenen auf Auskunft, Berichtigung, Sperrung und Löschung zu erweitern. Dem Betroffenen ist nicht nur wie bisher Auskunft über die zu seiner Person gespeicherten Daten zu geben, vielmehr wird auch der Zweck der Speicherung, die Herkunft der Daten und die Empfänger von Übermittlungen mitzuteilen sein, und dies auch dann, wenn diese Angaben nicht in einer Datei gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können.

Bereits bei der Benachrichtigung sollten die Art der gespeicherten Daten und die Empfänger regelmäßiger Übermittlungen mitgeteilt werden. Wenn die Daten automatisiert verarbeitet werden, sollten darüber hinaus der Zweck der Speicherung und die Herkunft der Daten angegeben werden.

Aus Akten oder sonstigen Unterlagen ist dem Betroffenen Auskunft über personenbezogene Daten zu erteilen, soweit er Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem Auskunftsinteresse des Betroffenen steht.

Auch im nicht-öffentlichen Bereich darf für die Auskunft ein Entgelt künftig nicht verlangt werden. Im 4. Abschnitt des BDSG sollte jedoch eine Klausel vorgesehen werden, nach der Dritte vom Betroffenen die Geltendmachung eines Auskunftsrechts nicht verlangen dürfen. Damit könnte auch verhindert werden, daß Unternehmen nicht selbst eine entgeltpflichtige Auskunft bei der Schufa oder vergleichbaren Stellen einholen, sondern den Betroffenen als Werkzeug nutzen, um an eine unentgeltliche Auskunft heranzukommen.

Von einer Berichtigung, Sperrung oder Löschung sind unverzüglich die Stellen – soweit bekannt – zu verständigen, denen die Daten im Rahmen regelmäßiger Datenübermittlung übermittelt wurden, es sei denn, daß die schutzwürdigen Belange des Betroffenen berührt sind.

Ferner muß folgendes Problem gelöst werden, das auch für die Datenverarbeitung öffentlicher Stellen Bedeutung erlangen kann, sich aber vor allem im nicht-öffentlichen Bereich auswirkt: Das BDSG fragt nicht danach, ob die Datenverarbeitung, in die eingewilligt worden ist, zu dem angestrebten wirtschaftlichen Zweck erforderlich oder auch nur geeignet und angemessen ist.

Die eine fast uneingeschränkte Datenverarbeitung ermöglichende Einwilligung beruht wegen vielfältiger sozialer oder wirtschaftlicher Zwänge oft auf einer Schein-Freiwilligkeit. Der Verzicht auf Strom-, Gas- und Wasserlieferungen, auf ein Bankkonto, auf Versicherungsschutz oder Krankenhausversorgung ist keine reale Alternative. Wenn das BDSG der Einwilligung eine Schlüsselrolle einräumt, dann muß es auch dafür sorgen, daß der Betroffene vor Benachteiligungen bei Verweigerung des Einverständnisses geschützt und die Widerruflichkeit der Einwilligung garantiert wird, da es andernfalls seinem Schutzzweck nicht genügt. Es kann keine die Zulässigkeit begründende „freiwillige" Einwilligung angenommen werden, wenn sie durch unangemessenen Druck bewirkt wurde.

Deshalb muß im Gesetz klargestellt werden, daß eine Einwilligung unwirksam ist, wenn sie den Betroffenen entgegen den Grundsätzen von Treu und Glauben unangemessen benachteiligt. Eine unangemessene Benachteiligung ist dann anzunehmen, wenn die Einwilligung wesentliche Rechte oder Pflichten einschränkt, die sich aus der Natur des Rechtsverhältnisses zwischen Betroffenem und speichernder Stelle ergeben.

6.2.2.4 Stellung des betrieblichen Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte (bDSB) sollte zur Stärkung seiner Unabhängigkeit einen verbesserten Kündigungsschutz erhalten, etwa in der Weise, daß die Kündigung seines Arbeitsverhältnisses bis zu einem Jahr nach Beendigung seiner Aufgaben nur aus wichtigem Grund (§ 626 BGB) zulässig wäre. Ferner sollte das Vertrauensverhältnis zwischen bDSB und Betriebsrat gestärkt werden. Dies könnte dadurch erreicht werden, daß Bestellung und Abberufung des bDSB an die Zustimmung des Betriebsrates geknüpft werden und eine gesetzliche Verpflichtung zur engen Zusammenarbeit zwischen bDSB und Betriebsrat mit gegenseitigen Informationspflichten eingeführt wird.

Darüber hinaus sollte gesetzlich festgelegt werden, daß der bDSB sich ständig über die Entwicklung neuer Datenverarbeitungsanwendungen und die technischen und organisatorischen Veränderungen in der Datenverarbeitung zu informieren und gegenüber allen Beteiligten beratend mitzuwirken hat. Sinnvoll wäre schließlich die Einführung einer Pflicht zur Berichterstattung über seine Tätigkeit.

6.2.2.5 Befugnisse der Aufsichtsbehörde

Im 3. Abschnitt des BDSG sollte die Aufsichtsbehörde nicht nur auf die Beschwerde des Betroffenen hin, sondern immer dann tätig werden können, wenn Anhaltspunkte dafür vorliegen, daß gegen eine Vorschrift des BDSG oder eine andere Vorschrift über den Datenschutz verstoßen worden ist. Die Aufsichtsbehörde sollte die Betroffenen über eine unzulässige Verarbeitung ihrer Daten unterrichten dürfen.

Weiter ist unbefriedigend, daß die Aufsichtsbehörden über keine Instrumente verfügen, um festgestellte Mißstände zu beseitigen. Zu einem wirksamen Datenschutz gehört auch, daß die Aufsichtsbehörden über ihre jetzigen Befugnisse hinaus (Zutritts- und Auskunftsrechte, Möglichkeit zur Äußerung von unverbindlichen Rechtsansichten) Anordnungs- und Untersagungsbefugnisse erhalten. Im einzelnen sollten dies folgende Befugnisse sein:

- Maßnahmen zum Vollzug des § 6 BDSG (technische Maßnahmen zur Datensicherung) anzuordnen;
- den Einsatz einzelner Verfahren zu verbieten, soweit durch solche Anordnungen ausreichender Datenschutz nicht zu bewirken ist;
- den Betrieb bestimmter Datenverarbeitungsanlagen zu untersagen, wenn ausreichender Datenschutz sonst nicht zu bewirken ist;
- einen betrieblichen Beauftragten für den Datenschutz abzuberufen, wenn dieser seine Aufgaben nicht wahrnimmt oder erhebliche Mängel bei der Aufgabenwahrnehmung festgestellt werden.

Meines Erachtens liegt es im Interesse von Öffentlichkeit, Parlamenten und Regierungen, daß die Aufsichtsbehörden über die Datenverarbeitung im nicht-öffentlichen

Bereich regelmäßig berichten; denn diese Probleme sind bisher noch viel zu wenig bekannt. Der Deutsche Bundestag hat bei der Beratung des 5. Tätigkeitsberichtes des Bundesbeauftragten für den Datenschutz zu Recht darauf hingewiesen, 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.

Grenzen der Berichterstattung über die Datenverarbeitung im nicht-öffentlichen Bereich ergeben sich allerdings aus den Vorschriften über die Geheimhaltung (z.B. Steuergeheimnis, Betriebs- und Geschäftsgeheimisse) oder die Amtsverschwiegenheit sowie dem Gebot, überwiegende öffentliche oder schutzwürdige private Interessen nicht zu verletzen und nicht in schwebende Gerichtsverfahren einzugreifen (vgl. z.B. § 4 Hamburgisches Pressegesetz).

6.2.2.7 Arbeitnehmerdatenschutz

Zu dem Themenbereich des Arbeitnehmerdatenschutzes hat die Bundesregierung in der oben genannten Stellungnahme vom 30.4.1985 gegenüber dem Bundestagsinnenausschuß folgende Aussagen gemacht:

- Bei der Anwendung des geltenden Rechts ergeben sich in Einzelfragen Probleme, zu deren Lösung eine bereichsspezifische Regelung des Arbeitnehmerdatenschutzes beitragen könnte;
- die vielfältigen Einsatzmöglichkeiten von Personalinformationssystemen führen je nach Ausgestaltung im Einzelfall zu Gefährdungen des informationellen Selbstbestimmungsrechts der Arbeitnehmer, denen durch gesetzliche Regelungen insbesondere zum Schutz der Zweckbindung und der Transparenz von Arbeitnehmerdaten entgegengewirkt werden könnte;
- darüber hindaus wäre dann auch eine gesetzliche Klarstellung und Ergänzung der bisherigen Rechtsprechung zum Fragerecht des Arbeitgebers, zur Zulässigkeit von Anstellungsuntersuchungen und psychologischen Tests, zum Zeugnisrecht und zur Erteilung von Auskünften an Dritte sinnvoll;
- gesetzliche Regelungen zum Schutz von Arbeitnehmerdaten könnten sich jedoch nicht auf Regelungen im Bereich des Individualarbeitsrechts beschränken;
- ein geschlossenes Konzept zur Gewährleistung eines wirksamen Datenschutzes für Arbeitnehmer bedürfte der Ergänzung durch effektive Kontrollinstanzen.
- Im Hinblick auf eine solche gesetzliche Regelung ist das grundlegende Urteil des Bundesverfassungsgerichts vom 15.12.1983 zu berücksichtigen.

Dem allem stimme ich zu und halte es wie die Bundesregierung für geboten, den Schutz von Arbeitnehmerdaten durch bereichsspezifische und präzise gesetzliche Bestimmungen zu regeln.

Ausgehend von dem Entwurf der SPD-Fraktion für ein Gesetz zur Änderung des Bundesdatenschutzgesetzes (BT-Drs. 10/1180) könnte die Datenverarbeitung im Rahmen des Arbeitsverhältnisses wie folgt geregelt werden:

- Der Arbeitgeber darf personenbezogene Daten des Arbeitnehmers vor Abschluß des Arbeitsvertrages oder im Rahmen eines bestehenden Arbeitsvertrages abweichend von §§ 23 und 24 BDSG nur erheben, verarbeiten oder sonst nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich ist oder eine andere Rechtsvorschrift dies vorschreibt. Der Arbeitgeber darf vom Arbeitnehmer die Einwilligung für eine darüber hinausgehende Datenverarbeitung nicht verlangen. Wenn ein Personalfragebogen (§ 94 Abs. 1 Betriebsverfassungsgesetz) verwendet wird, so beschränkt sich die Datenerhebung auf die darin enthaltenen Fragen; gleiches gilt für persönliche Angaben in schriftlichen Arbeitsverträgen, die allgemein für den Betrieb verwendet werden (§ 94 Abs. 2 Betriebsverfassungsgesetz).

- Der Arbeitgeber darf beim Arbeitnehmer vor Abschluß des Arbeitsvertrages Daten über berufliche und fachliche Kenntnisse, Erfahrungen und Fähigkeiten erheben. Sonstige Daten, insbesondere hinsichtlich persönlicher und wirtschaftlicher Verhältnisse, darf der Arbeitgeber nur erheben, soweit die zu besetzende Arbeitsstelle oder die zu leistende Arbeit dies erfordert.

- Die Erhebung medizinischer Daten bei ärztlichen Untersuchungen des Arbeitnehmers vor Abschluß des Arbeitsvertrages ist nur zulässig, soweit dadurch seine Eignung für die von ihm zu leistende Arbeit festgestellt wird und er vorher sein Einverständnis zu Art und Umfang der Datenerhebung erteilt hat. Der untersuchende Arzt darf dem Arbeitgeber i.d.R. nur das Ergebnis der Eignungsuntersuchung mitteilen.

- Die Erhebung psychologischer Daten ist nur zulässig, soweit sie wegen besonderer Anforderungen an den Arbeitnehmer im Hinblick auf die von ihm zu leistende Arbeit erforderlich sind, vorhandene Bewerbungsunterlagen zur Beurteilung nicht bereits ausreichen, der Arbeitnehmer zuvor über Art und Umfang der Datenerhebung informiert wurde und sein Einverständnis hierzu erklärt hat. Daten im Zusammenhang mit psychologischen Tests dürfen nur von Psychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung erhoben werden; sie sind nach Feststellung des Ergebnisses unverzüglich zu sperren.

- Die Ergebnisse medizinischer und psychologischer Untersuchungen des Arbeitnehmers dürfen nur automatisiert verarbeitet werden, wenn dies dem Schutz des Arbeitnehmers dient. Arbeitsrechtliche Beurteilungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

- Personenbezogene Daten, die vor Abschluß des Arbeitsvertrages erhoben worden sind, sind unverzüglich zu löschen, sobald feststeht, daß ein Arbeitsvertrag nicht zustandekommt oder soweit sie im Falle eines Vertragsabschlusses für den Arbeitgeber nicht mehr erforderlich sind. Nach Beendigung des Arbeitsverhältnisses kann der Arbeitnehmer beantragen, daß diese Daten gelöscht werden, sobald feststeht, daß sie für die Abwicklung des Arbeitsverhältnisses nicht mehr benötigt werden und Rechtsvorschriften nicht entgegenstehen.

- Personenbezogene Daten, die im Rahmen der Durchführung von technischen und organisatorischen Maßnahmen gem. § 6 Abs. 1 Satz 1 BDSG und der Anlage dazu gespeichert werden, dürfen nicht zu anderen Zwecken verarbeitet oder sonst genutzt werden.

In einer weiteren Vorschrift, die die Rechte der Arbeitnehmer zu sichern hätte, ist der Auskunftsanspruch des Arbeitnehmers über § 26 Abs. 2 BDSG hinaus auszudehnen auf alle, nicht nur die regelmäßigen Datenempfänger, sowie auf die Auswertungsprogramme bzw. Einzelauswertungen, in die seine Daten einbezogen sind. Die Auskunftsbeschränkungen nach § 26 Abs. 4 Nrn. 4 und 5 BDSG (bei Daten aus allgemein zugänglichen Quellen und bei gesperrten Daten) müssen entfallen.

Über die bisherigen Regelungen hinaus und in Anlehnung an die neugefaßten Mitbestimmungsregelungen im hessischen und nordrheinwestfälischen Personalvertretungsgesetz müssen die Betriebs- und Personalräte ein eindeutiges Mitbestimmungsrecht haben bei der Einführung und Anwendung sowie bei wesentlicher Änderung und Erweiterung von Dateien mit personenbezogenen Daten der Arbeitnehmer und von Anlagen zur automatisierten Verarbeitung personenbezogener Daten der Beschäftigten und 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.

6.2.2.8 Handels- und Wirtschaftsauskunfteien

Häufig erheben die Auskunfteien Daten über Bürger, ohne daß diese unterrichtet werden und Gelegenheit erhalten, auf den Inhalt der über sie erteilten Auskunft Einfluß zu nehmen. Die Daten werden nicht nur für einen Auftraggeber gesammelt, sondern mehrere Jahre gespeichert, damit sie bei weiteren Anfragen wieder genutzt werden können. Nach erteilter Auskunft erhalten die Bürger über die Tatsache der Speicherung eine Benachrichtigung und – auf Anfrage – eine Auskunft darüber, welche Daten über sie gespeichert sind, und sonst nichts. Da die Tätigkeit der Auskunfteien sehr tief in das informationelle Selbstbestimmungsrecht des Bürgers eingreift, müssen dessen Rechte wesentlich verstärkt werden.

Gegenüber den Auskunfteien sind folgende unter Nr. 6.2.2.4 geforderten Erweiterungen der Rechte des Betroffenen von besonderer Bedeutung:

- Erstreckung der Auskunft auf Zweck der Speicherung, Herkunft der Daten und Empfänger der Auskunft
- Unentgeltlichkeit der Selbstauskunft
- Verpflichtung der Auskunftei, den Auskunftsempfänger zu unterrichten, wenn bereits übermittelte Daten berichtigt, gesperrt oder gelöscht werden
- Aufzeichnungspflicht des Auskunftsempfängers über sein berechtigtes Interesse.

Hinzu kommen folgende Forderungen, die speziell die Datenverarbeitung der Auskunfteien betreffen:

Es muß klargestellt werden, daß die von Auskunfteien erhobenen Daten nur zur Beurteilung von Bonität oder Vertrauenswürdigkeit der Betroffenen genutzt werden dürfen.

Nach § 32 Abs. 2 Satz 2 BDSG haben die Stellen, die bei Auskunfteien anfragen, ihr berechtigtes Interesse an der abgeforderten Auskunft begründet darzulegen. In der Praxis geschieht dies durch Ankreuzen eines vorgedruckten Textes auf dem sog. Anfrageschein. Fehlt das Kreuz, gilt die ebenfalls vorgedruckte Auffangbegründung (Bonitätsprüfung). Nach meiner Ansicht läßt sich damit das berechtigte Interesse nicht belegen. Die Aufsichtsbehörden sind im Falle einer Beschwerde wegen eines vorgetäuschten Interesses auf die Angaben angewiesen, die die Auskunftei aufgrund zivilrechtlicher Vereinbarungen von ihren Kunden verlangen kann. Eine eigene vollständige Sachverhaltsaufklärung ist den Aufsichtsbehörden nicht möglich. Deshalb muß die anfragende Stelle als Nutzer der Daten verpflichtet werden, ihr Interesse an jeder einzelnen Auskunft so zu dokumentieren, daß es bei einer Prüfung nachvollziehbar ist.

Daten bei Auskunfteien müssen nach drei Jahren gelöscht und nicht mehr – wie jetzt – nach fünf Jahren gesperrt werden.

Trifft der Empfänger nach einer Übermittlung durch Auskunfteien oder vergleichbaren Einrichtungen eine die Interessen des Betroffenen beeinträchtigende Maßnahme, so hat er dem Betroffenen die übermittelten Daten und die übermittelnde Stelle mitzuteilen. Darüber hinaus muß sichergestellt werden, daß alle Auskunftsdienste – unabhängig von der Art der Verfahren und dem Kreis der Betroffenen – in den Anwendungsbereich des 4. Abschnitts des BDSG aufgenommen werden.

6.2.2.9 Direktwerbung

Unter dem Begriff Direktwerbung sind – entsprechend dem Entwurf einer Empfehlung des Ministerkomitees des Europarats an die Mitgliedsstaaten zum Schutz personenbezogener Daten bei der Verwendung für Zwecke der Direktwerbung – alle Aktivitäten zu verstehen, die darauf abzielen, einem Teil der Bevölkerung durch Post, Telefon oder andere Direktmedien Waren oder Dienstleistungen anzubieten oder sonstige Werbemittel zu übersenden, die den Betroffenen informieren oder eine Reaktion bei ihm hervorrufen sollen, ebenso wie jede Hilfstätigkeit hierzu.

Unter Nr. 5.2 habe ich noch einmal (vgl. 1. TB, 7.3; 2. TB, 4.1.3; 3. TB, 4.1.2) dargestellt, welche Probleme bei der Direktwerbung durch das geltende Recht nicht gelöst wer-

den. Um die Rechtsstellung des Betroffenen zu stärken, mache ich die nachfolgenden Vorschläge:

Die in den Europaratsleitlinien festgehaltenen Empfehlungen müssen teilweise konkretisiert und in das BDSG übernommen werden.

Das Erheben bei anderen Stellen als dem Betroffenen setzt angemessene Vorkehrungen voraus; dazu zählt, daß die Herkunft der Daten dokumentiert wird. Werden die Daten beim Betroffenen zu einem anderen Ziel erhoben und sollen die Daten dennoch zu Werbezwecken genutzt werden, ist der Betroffene bei der Erhebung ausdrücklich darauf hinzuweisen. Das Erheben unter irreführender Zweckangabe (Preisausschreiben) darf nicht erlaubt sein.

Vor Weitergabe muß der Betroffene Gelegenheit haben, der Nutzung seiner Daten zu Werbezwecken zu widersprechen. Die Weitergabe von besonders sensitiven Daten (z.B. Daten über gesundheitliche Verhältnisse und über religiöse und politische Anschauungen), sollte von einer ausdrücklichen Einwilligung abhängig gemacht werden. Die Weitergabe und die Bedingungen für die Nutzung sind vertraglich – und zwar in Schriftform – festzulegen. Wer Adressen weitergibt, muß alle Empfänger aufzeichnen.

Jeder muß das Recht haben, die Aufnahme von Daten zu seiner Person in Marketinglisten oder die Übermittlung von Daten auf solchen Listen an Dritte zu untersagen. Das heißt, es muß eine „Robinson-Liste" geben, in der alle Personen zu vermerken sind, die nicht direkt umworben werden wollen.

Jeder muß in der Lage sein, Daten zu seiner Person, die für Werbezwecke genutzt werden, zu erfahren und zu berichtigen. Dazu gehört auch seine Zugehörigkeit zu einer bestimmten Personengruppe.

Darüber hinaus muß jeder uneingeschränkt in der Lage sein, die Löschung oder sonstige Entfernung solcher Daten aus einigen oder allen bei Benutzern geführten Listen zu veranlassen. Das setzt voraus, daß der Betroffene bei jeder ihm zugehenden Werbezuschrift die Möglichkeit haben muß, zu erfahren, aus welcher Quelle die Daten stammen, die im konkreten Zusammenhang verwendet wurden. Die Praxis hat gezeigt, daß manches werbende Unternehmen diese Angaben nicht machen will und viele wegen eines zwischengeschalteten Adreßmittlers dazu auch gar nicht in der Lage sind. Der Umworbene muß jedoch wissen, welche Daten über ihn durch wen weitergegeben worden sind, damit er weiß, gegen wen er seine Rechte geltend machen kann. Ein solcher Auskunftsanspruch setzt jedoch eine Pflicht voraus, die Herkunft und den Umfang der erhaltenen Daten aufzuzeichnen.

Zu den in der Leitlinie des Europarats geforderten Maßnahmen, die die Einhaltung dieser Empfehlungen sicherstellen sollen, zählt vor allem, daß alle an der Direktwerbung beteiligten Stellen regelmäßig von einer Aufsichtsbehörde überwacht werden. Der Anwendungsbereich des 4. Abschnitts des BDSG ist deshalb auf alle Beteiligten auszudehnen.

6.2.2.10 Medienarchive

Unternehmen und Hilfsunternehmen der Presse unterhalten Archive, in denen personenbezogene und nicht personenbezogene Informationen gesammelt werden. In den Archiven werden über bestimmte Personen aus dem Zeitgeschehen fast ausschließlich veröffentlichte Artikel aus Zeitungen, Zeitschriften und Meldungen von Nachrichtenagenturen gesammelt. Dieses Material wird entweder durch die systematische Ordnung der Ablage (z.T. mehrfach) oder über Suchkarteien erschlossen, die z.T. automatisiert sind.

Wenn das Material über die systematische Ordnung der Ablage erschlossen wird, handelt es sich nicht um Dateien, so daß das BDSG formal nicht anzuwenden ist. Auch wenn die Daten in Dateien archiviert wurden, sind die Archive durch das sog. Medienprivileg des § 1 Abs. 3 BDSG von der Geltung des BDSG weitgehend ausgenommen,

sofern sie personenbezogene Daten ausschließlich zu eigenen publizistischen Zwekken verarbeiten.

An der Grundentscheidung, die Presse von der Geltung des BDSG auszunehmen, sollte festgehalten werden. Ich halte es aber für erforderlich, die Rechte des Betroffenen zu verstärken und Klarheit über die Grenzen des Medienprivilegs zu schaffen; die dafür erforderlichen Ergänzungen und Änderungen tangieren aber die Pressefreiheit nicht.

Wenn Pressearchive sich automatisierter Verfahren bedienen, veranlassen die hohen Kosten die betreffenden Unternehmen nicht selten dazu, nach anderen Abnehmern für die Dienstleistungen ihrer Archive zu suchen. Wenn die Abnehmer nicht ihrerseits Presseunternehmen sind, wird die Grenze des Medienprivilegs gem. § 1 Abs. 3 BDSG mit der Folge überschritten, daß das Pressearchiv unter den 4. Abschnitt des BDSG fällt.

Ich werde mich zunächst mit den datenschutzrechtlichen Problemen innerhalb des Medienprivilegs und dann mit den Problemen befassen, die bei Anwendung des 4. Abschnitts des BDSG entstehen.

1. Stärkung der Rechte des Betroffenen

   Die Archive sammeln nahezu ausschließlich Daten, die aus allgemein zugänglichen Quellen (weit überwiegend Medien) stammen. Dennoch können für den Betroffenen Gefährdungen entstehen, weil

   - über die Richtigkeit des aus allgemein zugänglichen Quellen stammenden Materials Meinungsverschiedenheiten bestehen können und
   - durch die Zusammenstellung von Material aus verschiedenen Quellen und über eine längere Zeit hinweg ein Persönlichkeitsbild entstehen kann, das der Zeitungsleser aus seinen im allgemeinen punktuellen Eindrücken nicht gewinnen kann.

   Aus diesen Gründen sollten dem Betroffenen folgende Rechte gegenüber Medienarchiven eingeräumt werden:

   - Ein Auskunftsrecht, soweit er durch eine Berichterstattung in seinen schutzwürdigen Belangen beeinträchtigt wird, jedenfalls dann, wenn die Daten in Dateien oder in personenbezogen erschließbaren Akten gespeichert werden,
   - ein Berichtigungsrecht, wenn sich bei der Auskunft herausstellt, daß die verwendeten Daten unrichtig sind,
   - eine Verpflichtung der Medien, eine Gegendarstellung nach dem Presserecht zu den entsprechenden Daten zu nehmen und dort so lange aufzubewahren, wie auch die dazugehörigen Daten gespeichert werden.

2. Wahrung der Grenzen des Medienprivilegs

   § 1 Abs. 3 BDSG nimmt die Medien von der Geltung des BDSG aus, wenn personenbezogene Daten „ausschließlich zu eigenen publizistischen Zwecken" verarbeitet werden. Aufgrund der bisherigen Erfahrungen hat sich gezeigt, daß diese Formulierung nicht alle Fragen klärt, wie folgende beispielhafte Aufzählung zeigt:

   - Ist die (kollegiale) Hilfe von Medienarchiven untereinander noch Verarbeitung zu eigenen publizistischen Zwecken?
   - Ist der sog. Leserservice (Erfüllung von Wünschen der – eigenen – Leser, die Auszüge aus eigenen oder auch anderen Erzeugnissen erhalten wollen) noch Verarbeitung zu publizistischen Zwecken?
   - Sind Verträge mit anderen Medien, die keine eigenen Archive unterhalten, über Belieferung mit Archivmaterial auch eigene publizistische Zwecke?

   Hieraus ergibt sich die Notwendigkeit, das Medienprivileg so zu formulieren, daß die o.g. Fälle eindeutig darunter fallen und so die bisherige Auslegung bestätigt wird.

3. Ergänzung von Bestimmungen im 4. Abschnitt des BDSG

Soweit Medienarchive auch kommerziell genutzt werden, fallen sie unter den 4. Abschnitt des BDSG. Für diese Fälle müssen einige Bestimmungen des 4. Abschnitts so modifiziert werden, daß einerseits ein angemessener Datenschutz gewährleistet ist, andererseits aber die Arbeit der Archive nicht unmöglich gemacht wird.

- Von der Pflicht zur Benachrichtigung nach der erstmaligen Übermittlung müssen die Medienarchive ausgenommen werden, soweit die Anschrift des Betroffenen mit vertretbarem Aufwand nicht ermittelt werden kann und die Daten sich auf denjenigen beziehen, der sie veröffentlicht hat (in erster Linie der Autor).
- Die Medienarchive müssen von der Verpflichtung ausgenommen werden, die personenbezogenen Daten 5 Jahre nach der Einspeicherung zu sperren.
- Die Medienarchive müssen verpflichtet werden, Gegendarstellungen des Betroffenen zu den gespeicherten Daten zu nehmen.

6.2.2.11 Kritik der Koalitionsvorschläge zum nicht-öffentlichen Bereich

Es ist zu begrüßen,

- daß der Entwurf der CDU-FDP-Koalition einen verschuldensunabhängigen Schadensersatzanspruch einführen will,
- daß die Auskunft über gespeicherte Daten auch im nicht-öffentlichen Bereich grundsätzlich unentgeltlich sein soll. Die Regelung der Voraussetzungen, unter denen für die Auskunft ausnahmsweise ein Entgelt verlangt werden kann, ist allerdings unbefriedigend.
- daß der Betroffene die Möglichkeit haben soll, der Verwendung übermittelter personenbezogener Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung zu widersprechen. Wünschenswert wäre allerdings, daß bereits der Übermittlung der Daten für diese Zwecke widersprochen werden könnte, und schließlich
- daß die Befugnisse der Aufsichtbehörde erweitert werden sollen.

Schwerer ins Gewicht fallen allerdings die Regelungsdefizite, die nach dem Entwurf verbleiben würden, so daß insgesamt die für den nicht-öffentlichen Bereich vorgeschlagenen Änderungen als unbefriedigend angesehen werden müssen.

Zu bemängeln ist insbesondere, daß der Anwendungsbereich des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen nicht ausgeweitet werden soll. Es soll beim Dateibezug bleiben; die Erhebung von Daten wird nicht mit aufgenommen.

Die Regelung der Rechte der Betroffenen bleibt hinter dem Notwendigen zurück, und es bleibt dabei, daß der Bürger vor Benachteiligungen bei Verweigerungen der Einwilligung nicht geschützt wird.

Ich hatte schon deutlich gemacht, daß ich die Vorstellungen der Bundesregierung zur Verbesserung des Arbeitnehmerdatenschutzes in ihrer Zielrichtung teile. Anders als sie bin ich aber der Auffassung, daß der Auftrag des Volkszählungsurteils es gebietet, diese Regelungen unverzüglich zu schaffen.

M.E. können wir uns nicht damit begnügen,

- daß bereits nach geltendem Recht Arbeitnehmerdaten in gewissem Umfang geschützt sind
- und daß künftige arbeitsgerichtliche Entscheidungen die Grundsätze des grundlegenden Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz vom 15.12.1983 beachten und im Wege der verfassungskonformen Auslegung arbeits- und datenschutzrechtlicher Normen dem Datenschutz im Arbeitsrecht einen höheren Rang als bisher verschaffen werden.

Sicherlich macht ein wirksamer Persönlichkeitsschutz des Arbeitnehmers präzise, konkrete Regelungen erforderlich. Mir scheinen aber aber in einem Bereich, in dem

detaillierte Regelungen –auf der Grundlage verbesserter Mitbestimmungsmöglichkeiten– ohnehin in Betriebsvereinbarungen geschaffen werden müssen, die Vorschläge in dem Entwurf der SPD-Fraktion als Ansätze für gesetzliche Grundsatzregelungen durchaus geeignet. Dabei halte ich es für eine Frage von sekundärer Bedeutung, in welches Gesetz Regelungen zur Verbesserung des Arbeitnehmerdatenschutzes aufgenommen werden. Angesichts des Fehlens eines Arbeitsgesetzbuches erscheint es mir aber nicht als sachfremd, wenn

- individualrechtliche Regelungen ins BDSG (oder dienstrechtliche Regelungen ins Beamtenrecht) und
- kollektivrechtliche Regelungen ins Betriebsverfassungsgesetz und die Personalvertretungsgesetze

übernommen werden.

Schließlich bleiben auch die Vorschläge der Bundesregierung für Regelungen im 4. Abschnitt des BDSG für Auskunfteien und Adreßhandel hinter dem Notwendigen zurück.

HmbBG	=	Hamburgisches Beamtengesetz
HmbDSB	=	Hamburgischer Datenschutzbeauftragter
HmbDSG	=	Hamburgisches Datenschutzgesetz
HmbPersVG	=	Hamburgisches Personalvertretungsgesetz
HmbSOG	=	Hamburgisches Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
HmbVerfSchG	=	Hamburgisches Verfassungsschutzgesetz
HUK-Verband	=	Verband der Haftpflicht-, Unfall-, Auto- und Rechtsschutzversicherer e.V.
IMK	=	Konferenz der Innenminister
IuK	=	Information und Kommunikation
JVA	=	Justizvollzugsanstalt
KAN	=	Kriminalaktennachweis
KBA	=	Kraftfahrtbundesamt
KGSt	=	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KpS	=	Kriminalpolizeiliche personenbezogene Sammlung
LDSG	=	Landesdatenschutzgesetz
LID	=	Lehrerindividualdatei
MAD	=	Militärischer Abschirmdienst
ME	=	Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder
MiStra	=	Mitteilungen in Strafsachen
MittVw	=	Mitteilungen für die hamburgische Verwaltung
MiZi	=	Mitteilungen in Zivilsachen
NADIS	=	Nachrichtendienstliches Informationssystem
NJW	=	Neue Juristische Wochenschrift
NRW	=	Nordrhein-Westfalen
OFD	=	Oberfinanzdirektion
OWiG	=	Ordnungswidrigkeitengesetz
PB	=	Polizeiliche Beobachtung
PC	=	Personal Computer
PIN	=	Identifizierungsnummer
PIOS	=	Inpol-Anwendungen Personen, Institutionen, Objekte und Sachen
PIS	=	Personalinformationssystem
POLAS	=	Polizeiliches Auskunftssystem
POS	=	Point of Sale

RVO	=	Reichsversicherungsordnung
RZ	=	Rechenzentrum
Schufa	=	Schutzgemeinschaft für allgemeine Kreditsicherung
SGB	=	Sozialgesetzbuch
SOG	=	s. HmbSOG
SPUDOK	=	Spurendokumentation
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StV-Btx	=	Staatsvertrag über Bildschirmtext
StVG	=	Straßenverkehrsgesetz
StVollzG	=	Strafvollzugsgesetz
TB	=	Tätigkeitsbericht
TEMEX	=	Telemetry Exchange
UKE	=	Universitätskrankenhaus Eppendorf
VE	=	Vorentwurf
VV	=	Verwaltungsvorschift
VZ-Urteil	=	Volkszählungsurteil
WoBindG	=	Wohnungsbindungsgesetz
ZAG	=	Gesetz über die Zusammenarbeit der Dienste und der Polizei
ZAW	=	Zentralausschuß der Werbewirtschaft e.V.
ZEVIS	=	Zentrales Verkehrsinformations-System
ZPO	=	Zivilprozeßordnung