BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

Drucksache 13/5478

13. Wahlperiode

02. 02. 90

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: Achter Tätigkeitsbericht
des Hamburgischen Datenschutzbeauftragten

Gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen achten Tätigkeitsbericht.*

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 46

Achter Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten

Zugleich
Tätigkeitsbericht der Aufsichtsbehörde
für den nicht-öffentlichen Bereich

vorgelegt zum 1. Januar 1990

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Claus Henning Schapper
Baumwall 7 · 2000 Hamburg 11 · Tel.: 35 04 20 44

Druck: Lütcke & Wulff, Hamburg 1

GLIEDERUNG

Seite

1. Die Fortentwicklung des Datenschutzrechts

Seit der Verabschiedung des Bundesdatenschutzgesetzes im Jahr 1977 sind die Novellierungsforderungen nicht abgerissen. Diejenigen, die die gesetzlichen Regelungen für unzureichend hielten, haben durch das Volkszählungsurteil des Bundesverfassungsgerichtes starken Auftrieb erhalten. Seitdem konzentriert sich die datenschutzrechtliche Diskussion darauf, die Umsetzung der vom BVerfG formulierten Grundsätze einzufordern. Der andere Strang der Kritik, die Forderung nach Anpassung des Datenschutzrechts an die stürmische Entwicklung auf dem Gebiet der Informationstechnik, ist dabei deutlich in den Hintergrund getreten.

1.1 Konsequenzen aus dem Volkszählungsurteil

Zunächst einmal möchte ich auf die Konsequenzen, die aus dem VZ-Urteil abzuleiten sind, aufmerksam machen. Verglichen mit den Erwartungen, die die Datenschutzbeauftragten vor fünf Jahren in einer Entschließung zusammengefaßt hatten, nehmen sich die seither erzielten (gesetzgeberischen) Erfolge bescheiden aus. Selbst dort, wo dem Gesetzgeber eine verhältnismäßig datenschutzfreundliche Einstellung bescheinigt werden kann, bleiben noch deutliche Defizite bestehen. Die novellierten Datenschutzgesetze von Hessen, NRW und Bremen und - ihnen folgend - der Entwurf zur Novellierung des Hamburgischen Datenschutzgesetzes bringen zwar Verbesserungen. Dennoch habe ich Zweifel, ob ihre im wesentlichen unverändert gebliebene Konzeption den verfassungsrechtlichen Anforderungen gerecht wird:

Die Erlaubnistatbestände auch dieser „modernen Datenschutzgesetze", wie sie von der Hamburger Justizbehörde genannt werden, sind weiterhin so allgemein gehalten und so weit gefaßt, daß sie die Datenverarbeitung nicht nur nicht einzuschränken vermögen, sondern ihre Ausdehnung - selbst wenn modernste Technik eingesetzt werden soll - eher fördern. Die Zulässigkeit von Speicherungen und Übermittlungen hängt nach wie vor allein davon ab, ob die Daten für die Aufgabenerfüllung der speichernden, der übermittelnden oder der empfangenden Behörde erforderlich sind. Nunmehr wird auch bei der Erhebung und bei jeglicher Verwendung von Daten an die Erforderlichkeit angeknüpft. Dies wäre hinnehmbar, wenn sich die Verwaltung bei der Anwendung der Datenschutzgesetze an der Rechtsprechung des BVerfG orientieren würde, das im Volkszählungsurteil noch einmal bekräftigt hat, die Grundrechte der Bürger dürften von der öffentlichen Gewalt jeweils nur insoweit beschränkt werden, als dies zum Schutz öffentlicher Interessen unerläßlich ist. Demgegenüber habe ich immer wieder feststellen müssen, daß nach Auffassung der Verwaltung die Datenverarbeitung nicht erst dann erforderlich ist, wenn kein anderes Mittel zur Aufgabenerfüllung zur Verfügung steht, sondern es genügt, daß anstelle der beabsichtigten Maßnahme ein größerer Aufwand, der dann als unangemessen bezeichnet werden kann, betrieben werden müßte. Dieses Anliegen der Verwaltung hat die Hamburger Justizbehörde in einem Vorentwurf zur Novellierung des HmbDSG aufgegriffen und die Erforderlichkeit wie folgt definiert: „Erforderlich ist jede zur Aufgabenerfüllung geeignete Maßnahme, die nach Aufwand oder Auswirkungen in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht." Diesen Versuch einer - wie ich meine - eindeutig verfassungswidrigen Legaldefinition hat die Justizbehörde auf massiven Protest des Datenschutzbeauftragten zwar aufgegeben, doch heißt es in der Begründung des jetzt der Bürgerschaft vorgelegten Gesetzentwurfs, daß eine Datenverarbeitung auch schon dann erforderlich sein könne, wenn eine Aufgabe sonst nur unter unverhältnismäßig großen Schwierigkeiten erfüllt werden könnte. Damit wird der Verhältnismäßigkeitsgrundsatz auf den Kopf gestellt; nicht das den Bürger, sondern das die Verwaltung am wenigsten belastende Verfahren erhält den Vorzug.

Nun könnte man mir entgegenhalten, daß die „modernen Gesetze" doch ein Korrektiv geschaffen haben, indem sie wenigstens die Zweckbindung abgesichert haben. Auch dem kann ich nicht zustimmen.

In Anlehnung an das nordrhein-westfälische Datenschutzgesetz soll in dem Entwurf für ein neues Hamburgisches Datenschutzgesetz der Grundsatz der Zweckbindung durch nicht weniger als acht Ausnahmetatbestände eingeschränkt werden.

Die Verarbeitung zu anderen Zwecken ist zulässig, wenn

— eine Rechtsvorschrift dies erlaubt oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung begründeten Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt,

— ein rechtliches Interesse an der Kenntnis der zu verarbeitenden Daten vorliegt und kein Grund zu der Annahme besteht, daß das Geheimhaltungsinteresse des Betroffenen überwiegt,

— Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte dafür bestehen, daß sie unrichtig sind,

— hierdurch erhebliche Nachteile für das Gemeinwohl oder schwerwiegende Beeinträchtigungen von gewichtigen Rechtspositionen einzelner verhindert oder beseitigt werden sollen,

— sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuches oder zur Erledigung eines gerichtlichen Auskunftsersuchens erforderlich ist und gesetzliche Regelungen nicht entgegenstehen,

— offensichtlich ist, daß sie im Interesse des Betroffenen liegt und keine Anhaltspunkte vorliegen, daß dieser in Kenntnis des anderen Zwecks seine Einwilligung nicht erteilen würde, oder

— die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen worden sind oder entnommen werden könnten oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß schutzwürdige Belange des Betroffenen offensichtlich entgegenstehen.

Hinzu kommt die im Gesetzesentwurf nicht ausdrücklich erwähnte - aber als selbstverständlich unterstellte - Zweckdurchbrechung mit Einwilligung der Betroffenen.

Schon die Vielzahl dieser Ausnahmen führt zu einer Umkehrung des Verhältnisses von Regel und Ausnahme: Der Gesetzentwurf versucht, jeder denkbaren Fallkonstellation einen eigenen Ausnahmetatbestand zu widmen, in dem er - um zwei Beispiele zu nennen, die bei der Gesetzesberatung in der Hamburger Bürgerschaft vorgetragen wurden - dem Verwaltungsangestellten den Blick in das Telefonbuch oder die Benachrichtigung von Angehörigen eines verunglückten Schülers durch den Schulleiter erlaubt, anstatt sich um eine praktikable Klausel für die „Trivialdatenverarbeitung" zu bemühen. Damit hat er aber das Zweckbindungsprinzip praktisch wieder aufgehoben; denn tatsächlich treffen die beschriebenen Tatbestände nicht nur auf die triviale Datenverarbeitung zu, sondern sie rechtfertigen auch sehr viel schwerwiegendere Eingriffe in das Persönlichkeitsrecht.

Völlig ausgehöhlt wird der Grundsatz der Zweckbindung jedoch durch weitere pauschale Ausnahmeregelungen, die sich an anderen Stellen des Gesetzentwurfs finden. So soll es nach § 13 Abs. 3 keine Zweckdurchbrechung darstellen, wenn die vorhandenen Daten zur Durchführung von Organisationsuntersuchungen benutzt werden. Darunter kann eine Vielzahl sehr unterschiedlicher Untersuchungsgegenstände und -ziele (z.B. Änderung von Behördenzuständigkeiten, Vorbereitung von Rationalisierungsmaßnahmen, Stellenzuschnitt und -bewertung) und Untersuchungsmethoden verstanden werden.

Daneben dürfen die Daten ohne Einwilligung der Betroffenen

— zu Forschungszwecken (§ 27 Abs. 1),

— zur Vorbereitung oder Überprüfung von Regelungen allgemeiner Art durch eine öffentliche Stelle (§ 27 Abs. 7),

— zur Durchführung organisatorischer Maßnahmen (§ 28 Abs. 1),

— zu Zwecken der Personalplanung und des Personaleinsatzes (§ 28 Abs. 1),

— für die Erstellung von Statistiken (§ 29) und

— für Zwecke der öffentlichen Planung (§ 30)

verarbeitet werden.

In der Gesamtschau wird deutlich: In Wahrheit geht es nicht darum, den Grundsatz der Zweckbindung zu verankern. Statt dessen soll die Verwaltung personenbezogene Daten zu nahezu jedem Zweck nutzen dürfen. Es muß nicht besonders betont werden, daß eine solche Absicht mit den Intentionen des Volkszählungsurteils nicht vereinbar ist. Ich habe deshalb von Anfang an und noch in der laufenden parlamentarischen Beratung vorgeschlagen, den Zweckdurchbrechungskatalog erheblich einzuschränken und die zusätzlichen Ausnahmevorschriften weitgehend zu streichen, ohne daß ich dadurch die Interessen der Verwaltung unzumutbar beeinträchtigt sähe.

Bemerkenswert ist, daß Hamburg sich in dem Bemühen, Zweckdurchbrechungen „flächendeckend" zuzulassen, offensichtlich von niemandem übertreffen lassen will. Keines der „modernen" Gesetze enthält ein derart engmaschiges Geflecht von Ausnahmeregelungen. Selbst die Bundesregierung, die sich in ihrem Entwurf zur Novellierung des BDSG für die Anliegen des Datenschutzes nicht gerade aufgeschlossen gezeigt hat, bleibt mit ihrem Zweckdurchbrechungskatalog für den öffentlichen Bereich hinter den Ausnahmetatbeständen im Hamburger Entwurf deutlich zurück.

Eine abschließende Bemerkung noch zum nicht-öffentlichen Bereich: Hier soll nach dem Willen der Bundesregierung der Zweckbindungsgrundsatz praktisch ebenfalls ausgehebelt werden. Zwar darf nach § 26 Abs. 4 Satz 1 E-BDSG der Empfänger übermittelte Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt wurden. Satz 2 jedoch hebt diesen Grundsatz praktisch wieder auf. Einmal gespeicherte Daten dürfen für jeden anderen Zweck verwendet werden, wenn die verarbeitende Stelle sie auch für diesen Zweck hätte speichern oder übermitteln dürfen.

1.2 Anschluß an die technische Entwicklung verpaßt

Einen weiteren strukturellen Mangel des BDSG- Regierungsentwurfes ebenso wie der bereits novellierten Landesdatenschutzgesetze und des Entwurfs für ein neues HmbDSG sehe ich darin, daß sie die technische Entwicklung nicht oder nur unzureichend einfangen: Die Vorgaben für technische und organisatorische Maßnahmen wurden nur redaktionell überarbeitet, datenschutzrechtliche Begriffe wie „speichernde Stelle" oder „Datei" nicht oder nur unzureichend weiterentwickelt, so daß die Regelungen schon der jetzt eingesetzten Technik nicht voll gerecht werden, keinesfalls aber geeignet sind, den sich abzeichnenden technischen Entwicklungen wirkungsvoll zu begegnen.

Der Vorsprung der Technikentwicklung vor der notwendigen rechtlichen Normierung hat sich schon in den letzten zehn Jahren vergrößert und angesichts der bereits vorliegenden Ergebnisse der jetzigen Novellierungsrunde läßt sich voraussagen, daß das Datenschutzrecht weiter zurückfallen wird. Dies läßt sich besonders gut am Technikeinsatz im nicht-öffentlichen Bereich belegen:

— Heute noch aktenmäßig erfaßte Datenbestände lassen sich mühelos automatisch erschließen und auswerten. Verfahren zur direkten Übernahme konventionell auf Papier aufgezeichneter Informationen auf automationsgerechte Medien bewirken einen reibungslosen Übergang von konventioneller Aktenführung zum papierlosen Büro.

— Die in der Anfangsphase der Datenverarbeitungstechnik fast immer vorhandene Zersplitterung der Informationen aufgrund inkompatibler Hard- bzw. Software weicht einer kräftigen Tendenz zur Integration und Verknüpfbarkeit. Das Zusammenwachsen von Nachrichten- und Datenverarbeitungstechnik zu einer umfassenden Informations- und Kommunikationstechnologie hat u.a. zur Folge, daß die Nutzung

von elektronisch gespeicherten Daten nicht mehr den bisherigen örtlichen Begrenzungen unterliegt.

— Bislang außerhalb der EDV angesiedelte Technikbereiche werden zunehmend digitalisiert, so z.B. die Bildverarbeitungs- und Spracherkennungstechnik. Dabei lasse ich völlig unberücksichtigt, daß neue Arbeitsgebiete der Informatik - zu denken ist etwa an die „Künstliche Intelligenz" - die Informationsverarbeitung möglicherweise nicht erst im nächsten Jahrtausend völlig umwälzen werden.

(1) Wo bleibt die „speichernde Stelle"?

Der Festlegung der speichernden Stelle kommt eine doppelte Funktion zu: Zum einen ist die speichernde Stelle Adressat der im Gesetz festgelegten Rechte des Betroffenen auf Auskunft, Berichtigung, Sperrung und Löschung. Zum anderen knüpft an den Begriff der speichernden Stelle auch der Übermittlungsbegriff an, der von großer datenschutzrechtlicher Bedeutung ist. Es wäre notwendig gewesen, im Rahmen der Novellierung der Entwicklung zu immer umfassenderen und komplexeren Systemen Rechnung zu tragen. Dieses Bemühen läßt der HmbDSG-Entwurf aber ebenso wie der BDSG-Entwurf leider vermissen.

Die Problematik läßt sich anhand verschiedener Aspekte verdeutlichen: Zur Zeit der Entstehung des BDSG war die automatisierte Datenverarbeitung eindeutig geprägt von der wenig flexiblen Stapelverarbeitung in Rechenzentren, die sich zudem auf wenige Groß-Verfahren konzentrierte. Die Bestimmung einer speichernden Stelle war vor diesem Hintergrund wenig problematisch.

Dies hat sich drastisch verändert:

Neben der Groß-ADV kommen zunehmend dezentrale Rechner zum Einsatz, deren Leistungsfähigkeit ständig wächst. Dies hat zur Folge, daß innerhalb einer Behörde bzw. eines Unternehmens faktisch eine Vielzahl datenverarbeitender Stellen entsteht, die in der Regel unabhängig voneinander agieren. Im öffentlichen Bereich wird diesem Trend zumindest insoweit Rechnung getragen, als die speichernde Stelle nicht institutionell-organisatorisch, sondern funkionell definiert wird. Selbstverständlich kann etwa die organisatorische Zuordnung des Krafttfahrzeug-Zulassungswesens zur Polizei keinen unbegrenzten polizeilichen Zugriff auf dessen Daten rechtfertigen.

Ich war davon ausgegangen, es sei mittlerweile unbestritten, daß hier die Übermittlungsbestimmungen der Landesdatenschutzgesetze anzuwenden sind. Es hätte also nahegelegen, diese Auslegung, die sich im Schrifttum und in der Verwaltungspraxis durchgesetzt hat, durch entsprechende Formulierungen in der Datenschutznovelle zu verankern. Stattdessen sorgt der Senatsentwurf für ein neues HmbDSG für zusätzliche Unklarheiten, wenn er (bei der Definition des „Dritten" in § 4 Abs.4) nicht mehr wie das geltende Recht von „speichernder Stelle" spricht, sondern von „öffentlicher Stelle", was sowohl eine Funktionseinheit innerhalb einer Behörde als auch die gesamte Hamburger Verwaltung bedeuten kann.

Für den privaten Bereich knüpft das Datenschutzrecht an die rechtliche Einheit an. Selbst wenn die Datenverarbeitung von ganz unterschiedlichen Unternehmensbereichen (z.B. Personalabteilung und Verkauf) zu verschiedenen Zwecken betrieben wird, muß nach dem geltenden Recht davon ausgegangen werden, daß sie innerhalb einer speichernden Stelle abgewickelt wird. Eine Datenweitergabe zwischen diesen Bereichen wird deshalb nicht als Übermittlung angesehen und unterliegt folglich keinen Beschränkungen, jedenfalls dann nicht, wenn es bei der Konzeption des Regierungsentwurfs bleibt, der für den nichtöffentlichen Bereich eine Zweckbindung innerhalb der speichernden Stelle nicht vorsieht.

Ein weiteres Problem: Unter Nutzung öffentlicher und privater Datennetze werden bislang getrennte Bereiche aufs engste miteinander verknüpft, ohne daß sich in jeder Phase mit Sicherheit feststellen ließe, wer jeweils speichernde Stelle ist. So werden bei den geplanten POS-Kassensystemen Kundendaten erhoben und in unterschiedlichen Systemen des Handels und der Kreditwirtschaft gespeichert und weiterverarbeitet.

Dabei wird zudem noch eine Zwischeninstanz mit datenschutzrechtlich ungeklärtem Status (Autorisierungszentralen) eingeschaltet, die zu prüfen hat, ob die beabsichtigte Transaktion ausgeführt werden darf.

International operierende Unternehmen und Gesellschaften bedienen sich für bestimmte Verarbeitungsschritte ausländischer Rechenzentren (z.B. Luftfahrtgesellschaften bei Buchungssystemen), ohne daß geklärt ist, ob und wie der Betroffene seine Rechte auch gegenüber den ausländischen Vertragspartnern deutscher Unternehmen durchsetzen kann.

(2) Technische und organisatorische Maßnahmen

In § 8 Abs. 1 E-BDSG - wie auch in die entsprechenden Vorschriften der bereits novellierten Landesdatenschutzgesetze und in § 8 Abs.2 E-HmbDSG - wurden die „zehn Gebote" des alten § 6 Abs. 1 BDSG nahezu unverändert übernommen. Auch wenn das Festhalten am Prinzip einer nicht an speziellen Informationstechniken ausgerichteten Datensicherungsvorschrift an sich zu begrüßen ist, reichen in Anbetracht der technischen Entwicklung seit der Formulierung dieser Vorschrift Mitte der 70er Jahre die vorgesehenen Maßnahmen nicht aus. Dies gilt insbesondere für die Regelung der Übermittlungskontrolle, in der gegenüber der alten Fassung lediglich die Wörter „Selbsttätige Einrichtungen" ersetzt wurden durch „Einrichtungen zur Datenübertragung".

Damit wird die Neufassung der Tendenz zu vernetzten Systemen nicht gerecht. Es genügt nicht, daß nur feststellbar ist, an welche Stellen personenbezogene Daten (hätten) übermittelt werden können. Geboten ist vielmehr, daß zum einen die speichernde Stelle die Übersicht über die Vernetzung ihrer Datenverarbeitungsanlage tatsächlich hat und daß zum anderen analog der Eingabekontrolle - bei den erfolgten Übermittlungen nachträglich deren nähere Umstände festgestellt werden können.

(3) Dateibegriff

Im BDSG-Entwurf ist - anders als bei den bisher novellierten Landesgesetzen - der Dateibegriff im wesentlichen unverändert beibehalten worden. Er hält in Anbetracht der technischen Entwicklung einer kritischen Überprüfung nicht stand. Es ist nicht akzeptabel, daß die Dateieigenschaft einer automatisierten Datensammlung weiterhin davon abhängig gemacht wird, ob die Sammlung nach bestimmten Merkmalen geordnet und umgeordnet werden kann. Die Beeinträchtigung von Persönlichkeitsrechten ist allein davon abhängig, ob Datensammlungen schnell erschlossen und ausgewertet werden können, also multifunktional verwendbar sind. Die Bindung der Dateieigenschaft an die Sortierfähigkeit geht von den Gegebenheiten bei der manuellen Datenverarbeitung aus. Manuelle Datensammlungen mögen mit vertretbarem Aufwand nur dann vielfältig ausgewertet werden können, wenn sie einheitlich nach bestimmten Merkmalen geordnet, also formatiert sind.

Anders bei automatisierten Datensammlungen: Die moderne DV-Technik gestattet detaillierte und schnelle Auswertungen auch bei unformatierten Daten. Zunehmend werden zudem formatierte und unformatierte Daten miteinander verknüpft.

Zumindest die im BDSG-Entwurf vorgenommene Dateidefinition läßt auch die Weiterentwicklung bei der optischen Speichertechnik außer Betracht. Die in zunehmendem Maße eingesetzten digitalen optischen Speicherverfahren zeichnen sich nicht nur durch eine enorme Steigerung des Speichervolumens sowohl verglichen mit der Mikroverfilmung als auch mit der magnetischen Speicherung aus; sie integrieren vielmehr Archivfunktionen (Speicherung und Rückgriff) mit einem umfassenden Informationsmanagement. Dadurch wird die Information verfügbar für die automatisierte Weiterverarbeitung. Ich gehe davon aus, daß solche optischen Verfahren nicht unter den engen Dateibegriff des BDSG-Entwurfs subsumiert werden können; denn mit ihrer Hilfe lassen sich zwar riesige Datenbestände sekundenschnell auswerten, die Daten sind jedoch nicht umzusortieren.

Vor dem Hintergrund einer derartig unzureichenden Dateidefinition ist es besonders bedenklich, daß der Schutzbereich des BDSG auf personenbezogene Daten in

Dateien beschränkt bleiben soll. Mir sind Fälle bekannt, in denen bewußt Speicherungsformen eingesetzt werden, die zwar einen schnellen Zugriff und umfassende Auswertungsmöglichkeiten, nicht aber eine Umsortierung der Daten ermöglichen, und dies allein zu dem Zweck, die Anwendung des Datenschutzgesetzes zu umgehen.

(4) Automatisierte Bildverarbeitung

Die Datenschutzgesetze - auch das HmbDSG - sollten auch für den zunehmend bedeutsamen Einsatz der Video-Technologie gelten, was nach den vorliegenden Formulierungen des Senatsentwurfs nicht sichergestellt wäre.

Die Speicherungs- und Auswertungsmöglichkeiten von Video- und sonstigen Bildaufzeichnungen haben ein Niveau erreicht, das eine Datenverarbeitung im automatisierten Verfahren ermöglicht. Bilder können nicht nur automatisiert aufgenommen und digitalisiert gespeichert werden; sie sind darüber hinaus sogar inhaltlich zu erschließen (Mustererkennung). Gerade weil die Datenerhebung mittels optischer Überwachungsanlagen in der Regel ohne Kenntnis und Zustimmung des Betroffenen geschieht und besonders tief in seine Persönlichkeitssphäre eingreifen kann, sind hier restriktive Regelungen bezüglich der Erhebung, Speicherung und Auswertung erforderlich.

Die bloße Videoaufnahme - ohne Speicherung auf Datenträger ist nicht als Erhebung i.S.v. § 4 Abs.2 S.2 Nr.1 E-HmbDSG anzusehen. Selbst wenn die Aufnahmen auf Videoband gespeichert werden, ist die Anwendbarkeit der Vorschriften des HmbDSG zweifelhaft, da Video-Aufzeichnungen möglicherweise weder unter den Dateibegriff des § 4 Abs. 5 noch unter den Aktenbegriff des § 4 Abs. 6 zu subsumieren sind.

(5) Nutzung von Telekommunikationsdiensten

Auch für den Nutzungsbereich der neuen Medien müssen - insbesondere nach der Deregulierung des Telekommunikationswesens durch das Poststrukturgesetz - gesetzliche Datenschutzregelungen erfolgen (sei es in den allgemeinen Datenschutzgesetzen oder im Rahmen eines Staatsvertrages). Die Regelungskompetenz für die Nutzung der Telekommunikation liegt bei den Ländern. Die Kompetenz des Bundes aus Art. 73 Nr. 7 GG für das (Post- und) Fernmeldewesen betrifft ausschließlich den Bereich der Fernmeldetechnik, d.h. der Übertragungs- und der Vermittlungseinrichtungen. Eine Bundeskompetenz zur inhaltlichen Regelung von Anwendungsformen der Telekommunikation, für die Fernmeldetechnik genutzt wird, läßt sich daraus nicht herleiten. Diese Rechtsauffassung wird m.W. von allen Bundesländern geteilt, sie hat z.B. zum Abschluß des Bildschirmtext-Staatsvertrages geführt und auch in die Landesmediengesetze Eingang gefunden.

Während der Ort der Regelung (HmbDSG, Hmb. Mediengesetz oder sonstige bereichsspezifische Regelung) von untergeordneter Bedeutung ist, muß gewährleistet werden, daß die Nutzungsregelungen unverzüglich und umfassend, d.h. sowohl für öffentliche als auch für private Telekommunikations-Anbieter und -Teilnehmer getroffen werden. Besonders dringend ist der Regelungsbedarf beim Fernwirken (TEMEX). Regelungen über das Fernmessen und Fernwirken sind in Hamburg bisher unterblieben, weil bei den Beratungen des Hamburgischen Mediengestzes angenommen worden war, daß derartige Dienste in absehbarer Zeit in Hamburg nicht angeboten würden.

Tatsächlich werden in Hamburg jedoch bereits seit Sommer 1988 Fernwirk- und Fernmeßdienste angeboten und betrieben. Hamburg ist nämlich einer der Orte, an denen die Deutsche Bundespost einen TEMEX-Betriebsversuch durchführt. An dem Betriebsversuch beteiligen sich sowohl öffentliche als auch private Stellen. Zum Teil sind bereits heute in Privatwohnungen Fernwirk- und Fernmeßeinrichtungen installiert, z.B. im Rahmen von Dienstleistungen des Wach- und Sicherungsgewerbes. Zumindest geplant war eine Anwendung der Baubehörde (Wasserverbrauchsmessung bei SAGA-Wohnungen).

Angesichts des aktuellen Regelungsbedarfs würde ich es begrüßen, wenn in Zusammenhang mit der Novellierung des HmbDSG eine Regelung über das Fernwirken

getroffen würde, wie sie bereits in eine Reihe von Ländergesetzen (z.B. Berliner Kabelpilotprojektgesetz, Bayerisches Medienerprobungs- und -entwicklungsgesetz und - allerdings nur für den öffentlichen Bereich - Hessisches und nordrhein-westfälisches Datenschutzgesetz) Eingang gefunden haben.

1.3 Bereichsspezifischer Datenschutz am Beispiel des Polizeirechts

Wenn sich die Gesetzgeber der technischen Entwicklung gegenüber bei der Formulierung der allgemeinen Datenschutzgesetze schon so neutral verhalten, wäre doch anzunehmen, daß sie jedenfalls in den Bereichen, in denen der Einsatz der Technik eine hervorgehobene Rolle spielt, entsprechende bereichsspezifische Regelungen vorsehen. Aber auch dies kann nicht festgestellt werden. Ein Beispiel dafür bietet die polizeiliche Datenverarbeitung.

Die Sicherheitsbehörden sind der Bereich der öffentlichen Verwaltung, in dem im größten Umfang z.T. besonders sensible Daten unter Einsatz technischer Mittel erhoben und verarbeitet werden.

Mit INPOL verfügen die Länderpolizeien und das BKA über ein umfangreiches, vielseitiges und schnelles Online-Informationssystem, in dem Personalien und andere Informationen über mehr als 2,6 Mio. Personen zum Abruf bereitgehalten werden. Dieses System weist Schnittstellen zum Zentralen Verkehrsinformationssystem ZEVIS in Flensburg mit 33,8 Mio. Kfz-Halterdaten und zum Ausländerzentralregister mit nahezu 10 Mio. Personendatensätzen auf.

Mit Projekten zur automatisierten Einsatzlenkung und zur computerunterstützten Vorgangsbearbeitung, wie sie an verschiedenen Orten parallel entwickelt werden, ist die Polizei dabei, ihre Datenverarbeitung auf eine neue Stufe zu heben und einen bisher nicht gekannten Integrationsgrad zu erreichen. Daten, die bisher manuell erhoben und allenfalls in Tagebüchern und Akten gespeichert wurden, werden durch den Einsatz von Datenbanksystemen jederzeit online verfügbar und lassen sich durch „flexible Abfragesprachen" miteinander verknüpfen. Davon werden nicht einmal die zu Dokumentationszwecken in „Langzeitspeicher" übernommenen Daten ausgenommen.

Gegenüber herkömmlichen polizeilichen Auskunftssystemen bieten die neuen Systeme einen deutlichen Gewinn an Flexibilität. Die Zweckentfremdung von Daten ist der dabei eingesetzten Technik praktisch immanent, da die Datennutzung - anders als bei dedizierten, also auf eine eng umschriebene Aufgabe zugeschnittenen Verfahren - nicht mehr in einem nachvollziehbaren Zusammenhang mit der Datenerhebung und Speicherung steht.

Die gegenseitige Verknüpfung von Datenverarbeitungssystemen führt zu einer ganz neuen Qualität der Mißbrauchsmöglichkeiten, insbesondere dann, wenn die Polizei auch auf Datenbestände anderer Behörden - Einwohnermeldeämter, Kraftfahrzeugzulassungsstellen, Ausländerbehörden usw. - zugreifen und die „eigenen" Daten mit den Dateien dieser Stellen abgleichen kann.

Neue Erhebungs- und Verarbeitungsmöglichkeiten, z.B. in der Video- und Bildauswertungstechnik führen dazu, daß in immer stärkerem Maße darüber hinaus verwertbare Informationen anfallen, die mit den sonstigen in Dateien gespeicherten Daten verknüpft werden können. Zu denken ist hier z.B. an die im Rahmen der Verkehrsüberwachung (aber auch bei Demonstrationen und verdeckten Ermittlungen) angefertigte Videoaufzeichnungen und Lichtbilder, die automatisiert abgelegt und ausgewertet werden können.

Lichtbild- und ED-Unterlagen bei den Sicherheitsbehörden werden bisher nur nach wenigen Merkmalen abgelegt und können auch nur über diese wenigen Merkmale durchsucht und ausgewertet werden. Die Verbindung von Video- und Datenbanksystemen erleichtert das Selektieren (Recherche) von Bildinformationen. Durch den Einsatz optischer Speichermedien sind die Restriktionen, die einer Massenverarbeitung von Bilddaten bisher entgegenstanden, zu überwinden. Eine effektive digitale Bildablage

und ein schneller Zugriff auf Bilddaten werden möglich. Mit Mitteln der digitalen Mustererkennung können Bilder automatisiert bzw. rechnerunterstützt ausgewertet und erschlossen werden. Über ISDN lassen sich digitalisiert gespeicherte Bilder online übertragen und von einer zentralen Bilddatei abrufen. Durch Kombination von dezentralen Digitalisierern und Bildauswerteeinrichtungen mit zentralen Datenbanken ließe sich ein Abgleich von vor Ort gewonnen Bildern mit zentralen Bilddateien vornehmen.

Darüber hinaus fallen durch die Digitalisierung des Telekommunikationsnetzes eine Vielzahl von Verbindungs- und Steuerungsdaten an, die bei der Überwachung der Kommunikation ausgewertet werden können. Auch bei der Analyse des gesprochenen Wortes werden die Auswertungsmöglichkeiten weiter verbessert. Es handelt sich dabei um die „Sprechererkennung" und die „Worterkennung". Die gewonnenen Erkenntnisse können - wie bei der Videotechnik - als Selektionsmerkmal für die Weiterverarbeitung (Aufzeichnung, Auswertung) benutzt werden.

Angesichts dieser technischen Möglichkeiten darf die Novellierung des Polizeirechtes nicht allein dem Zweck dienen, die polizeiliche Informationsverarbeitung im jetzigen Ausmaß abzusichern und darüber hinaus Spielräume für eine weitere Intensivierung polizeilicher Datenverarbeitungssysteme zu eröffnen. Dies wäre mit den vom BVerfG 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 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.

Es reicht nicht aus, in das Polizeigesetz eine Vorschrift aufzunehmen, die für jede automatisierte Datei lediglich eine Errichtungsanordnung vorschreibt und alles übrige der Errichtungsanordnung überläßt. Vielmehr muß auch hier der Gesetzgeber selbst die wichtigsten Vorgaben formulieren. Dazu gehört u.a. eine Regelung, die den Abruf von Daten auf die jeweils zuständigen Bediensteten zu beschränken. Ferner ist sicherzustellen, daß durch die automatisierte Verarbeitung keine unangemessenen Verkürzungen und Verzerrungen von Sachverhalten entstehen und daß die Herkunft und Richtigkeit von Informationen durch Akten oder andere Unterlagen nachweisbar sein muß. Von besonderer Bedeutung ist ferner die Regelung, daß zur Vorgangsverwaltung und zur Dokumentation geführte Dateien keine personengebundenen Hinweise enthalten dürfen. Es muß technisch sichergestellt werden, daß ein gleichzeitiger Zugriff auf solche Dateien und auf Daten, die der Bekämpfung von Verbrechen dienen, unterbleibt (s. für Hamburg auch 3.8.1).

1.4 Status und Aufgaben des Datenschutzbeauftragten

Man sollte nun meinen, daß den neuen Gefährdungen des informationellen Selbstbestimmungsrechts zumindest eine gestärkte Kontrollinstanz gegenübergestellt wird. Aber auch dies kann etwa dem Entwurf zur Novellierung des Hamburgischen Datenschutzgesetz nicht entnommen werden.

Weder soll der Datenschutzbeauftragte eine von der Exekutive unabhängigere Stellung - wie etwa der Rechnungshof - erhalten, noch soll die im geltenden Recht bestehende Kontrollücke beseitigt werden, nach der bei angeblich vorliegender „Gefährdung der Sicherheit des Bundes oder eines Landes" dem Datenschutzbeauftragten die Ausübung seiner Kontrollbefugnisse im Einzelfall untersagt werden kann.

Nicht einmal auf die zur Unabhängigkeit des Datenschutzbeauftragten im Widerspruch stehende Rechtsaufsicht, die doch nur den Sinn haben kann, in Konfliktfällen die Rechtsauffassung des Senats gegenüber dem Datenschutzbeauftragten durchzusetzen, mochte der Senat in seinem Gesetzesentwurf verzichten und dies, obwohl alle „modernen" Datenschutzgesetze auf dieses Relikt inzwischen verzichten, wenn es

ihnen nicht gar von Anfang an unbekannt war. Besonders befremdlich erscheint es, wenn der Senat im eigenen Gesetz die Rechtsaufsicht erhalten will, während er auf Bundesebene einen Entwurf zur Änderung des Bundesdatenschutzgesetzes unterstützt hat, der die Rechtsaufsicht der Bundesregierung über den Bundesdatenschutzbeauftragten beseitigen will.

Zusammenfassend muß ich nach fast acht Jahren Tätigkeit konstatieren, daß der Datenschutz es heute nicht leichter hat als zu Beginn meiner ersten Amtszeit.

2. Beobachtung der automatisierten Datenverarbeitung

2.1 Stand und Fortentwicklung der Regelungen für die automatisierte Datenverarbeitung

In der Vergangenheit habe ich wiederholt darauf hingewiesen, daß den ADV-Richtlinien des Senats eine große Bedeutung zukommt, weil sie als Gesamtkonzept zur Gewährleistung von Datenschutz, Datensicherheit und Ordnungsmäßigkeit der Datenverarbeitung in der Verwaltung zu verstehen sind (vergl. 5. TB 3.1.3 S. 10, 6.TB 3.4 S.19 ff, 7.TB 3.1 S.9 ff). Bei meinen Verfahrensprüfungen mußte ich wiederholt feststellen, daß die DS-Rahmenregelungen, die Freigaberichtlinie und die Dokumentationsrichtlinie nicht konsequent eingehalten werden (z.B. 6.TB 3.4.1 und 3.4.2 S.20 ff, 7.TB 3.1.1 S.9 f). Meiner Kritik wurde immer wieder mit dem Einwand begegnet, die Richtlinien seien unpraktikabel und - zumindest teilweise - überholt, die jeweils praktizierten von den Richtlinien abweichenden Vorgehensweisen gewährleisteten in gleicher Weise oder sogar besser als die Richtlinien die mit diesen angestrebten Ziele.

Mit immer neuen online-Verfahren und der zunehmenden Verbreitung von Personalcomputern und anderer dezentraler Technik wurde darüberhinaus weiterer Regelungsbedarf deutlich, da die bisher erlassenen ADV-Richtlinien diesen Bereich der Datenverarbeitung nur unzureichend abdecken (vergl. 6.TB 3.5 S.26 ff). Die jüngste Entwicklung schließlich, die beginnende Vernetzung dezentraler Rechner mit den Zentralrechnern der DVZ, also die Weiterentwicklung in Richtung auf eine immer komplexere technische Infrastruktur, stellt m.E. eine große Herausforderung dar: Es gilt nicht nur, diese Entwicklung technisch in den Griff zu bekommen, sondern es muß auch jederzeit sichergestellt sein, daß die rechtlichen Voraussetzungen für die Datenverarbeitung vorliegen, daß ein ausreichender Sicherheitsstandard vorhanden ist und daß den Anforderungen an die Wirtschaftlichkeit genügt wird. Dieses Ziel kann nur erreicht werden, wenn der Senat seine Organisationsgewalt wahrnimmt und ausreichende Regelungen zur Organisationskontrolle trifft und wenn die Einhaltung dieser Regelungen konsequent durchgesetzt wird.

2.1.1 Vorhandene Regelungen für die automatisierte Datenverarbeitung in der hamburgischen Verwaltung

Wie sieht nun das vorhandene Regelwerk für die automatisierte Datenverarbeitung der hamburgischen Verwaltung aus? Welches „Rüstzeug" findet der Bedienstete vor, dem die Aufgabe zugefallen ist, für die Erledigung einer Verwaltungsaufgabe ein automatisiertes Verfahren zu entwickeln, oder dem an seinem Arbeitsplatz IuK-Technik zur eigenverantwortlichen Nutzung zur Verfügung gestellt wird? Genau an diesem Punkt beginnt das Dilemma. Der Bedienstete kann sich nur mit Mühe und erheblichem Zeitaufwand einen einigermaßen vollständigen Überblick über die einschlägigen Vorschriften verschaffen, denn die Regelungen finden sich an den verschiedensten Stellen, z.T. auch dort, wo sie kaum zu erwarten wären. Ich will dies anhand der folgenden Auflistung aufzeigen:

— Automationsrichtlinien von 1965
(Fundstellen: MittVw 1965 Seite 151 und ADV-Handbuch Teil 1. Organisation S.7)

— DS-Richtlinie von 1977
(Fundstellen: MittVw 1977 Seite 205 und ADV-Handbuch Teil 4.1 Datenschutz/Datensicherung)

— DS-Rahmenregelungen von 1979
(Fundstellen: MittVw 1979 Seite 13 und ADV-Handbuch Teil 4.1 Datenschutz/Datensicherung)

— Freigaberichtlinie von 1982
(Fundstellen: MittVw 1982 Seite 70 und ADV-Handbuch Teil 4.1 Datenschutz/Datensicherung)

— Dokumentationsrichtlinie von 1982
(Fundstellen: MittVw 1982 Seite 76 und ADV-Handbuch Teil 4.1 Datenschutz/Datensicherung)

— Vorläufige Hinweise für die Verarbeitung personenbezogener Daten auf Personalcomputern (PC's) von 1987
(Fundstelle: MittVw 1988 Seite 61, dort als Anlage B beigefügt der „Neufassung der Hinweise zur Durchführung des Hamburgischen Datenschutzgesetzes und zu den datenschutzrechtlichen Regelungen des Sozialgesetzbuches (DS-Hinweise) vom 24. Februar 1982 in der Fassung vom 17. Februar 1988")

— Regelung zur Weiterentwicklung der IuK-Infrastruktur durch Verbindung von bisher autonom betriebenen Arbeitsplatz- und Abteilungsrechnern mit den Zentralrechnern der Datenverarbeitungszentrale
(Fundstelle: Rundschreiben des Organisationsamtes vom 23.12.88 an die Senatsämter, Fachbehörden, Bezirksämter unter dem Betreff „Nutzung und Förderung der Anwendung von Informations- und Kommunikationstechnik in der Hamburger Verwaltung")

— Regelung für den Test mit Originaldaten auf den Zentralrechnern der DVZ - bisher nur Entwurf -
(Fundstelle des Entwurfs: Anlage 3 zu dem Ergebnisvermerk über die Besprechung des Arbeitskreises der IuK-Beauftragten am 3.2.89)

— Grundsatzentscheidungen des Senats zur Neuorganisation der Nutzung von IuK-Technik auf der Grundlage der Senatsdrucksache 755/85
(Die o.g. Automationsrichtlinien wurden durch diese Grundsatzentscheidungen zwar hinfällig, sie sind jedoch nicht formell aufgehoben worden.)

— Leitlinien des Senats zur Weiterentwicklung der IuK- Infrastruktur
(Fundstelle: Senatsdrucksache 77/88)

— Rahmenvorgaben zur Weiterentwicklung der IuK-Infrastruktur von 1988
(Fundstelle: Rundschreiben des Senatsamtes für den Verwaltungsdienst vom 30.8.88)

— Weitere Ausgestaltungen der Grundsatzentscheidungen des Senats zur Drucksache 755/85 in dem neuen Instrument der IuK-Gesamtpläne, insbesondere in dem IuK-Gesamtplan 1990-1992
(Fundstelle: Senatsdrucksache 870/89)

Diese Aufzählung erhebt nicht den Anspruch auf Vollständigkeit, sie macht aber folgendes deutlich:

(1) Es gibt eine Vielzahl von Regelungen für die ADV, die zum Teil inaktuell sind.

(2) Wegen der sehr unterschiedlichen Form der Regelungen (Richtlinien, Drucksachen, Rundschreiben, Anlagen zu Hinweisen usw.) kann Ungewißheit über den Grad der jeweiligen Verbindlichkeit entstehen.

(3) Angesichts der Verteilung der einzelnen Vorschriften auf derart viele Fundstellen muß bezweifelt werden, daß das Regelwerk im Verwaltungsalltag jederzeit „zur Hand" ist. Was nicht bekannt ist, kann nicht umgesetzt werden.

2.1.2 Konzept für eine zukünftige Form des Regelwerks

Unabhängig von der Frage, welchen Inhalt das Regelwerk im einzelnen in Zukunft haben wird, muß ein Konzept für dessen Form entwickelt werden. Ob nun ein neues ADV-Handbuch erstellt werden muß, mag dahinstehen. Es erscheint mir jedoch unabdingbar, daß den Bediensteten, denen die Umsetzung der Senatsentscheidungen und der Vorgaben letztlich obliegt, den Instanzen, die für die Umsetzung die Verantwortung tragen, und den Organen, die die Einhaltung der zur Organisationskontrolle getroffe-

nen Regelungen zu prüfen haben (Rechnungshof, HmbDSB, interne DVRevision), ein Regelwerk zur Verfügung gestellt wird, das handhabbar ist. So wie es z.B. eine hamburgische Sammlung von Zuständigkeitsanordnungen, eine Sammlung der Fachlichen Weisungen zum BSHG oder ein Verwaltungshandbuch für Schulen gibt, muß es auch möglich sein, alle geltenden Vorschriften zur automatisierten Datenverarbeitung mindestens als Loseblattsammlung herauszugeben und zu unterhalten.

2.1.3 Inhaltliche Fortschreibung von Regelungen

Die Nichteinhaltung der ADV-Richtlinien war nicht nur vom HmbDSB festgestellt worden, sondern auch vom Rechnungshof und dem DV-Revisor des Senatsamtes für den Verwaltungsdienst.Der Senat hatte durch einzelne Stellungnahmen zu dieser Kritik Zweifel daran aufkommen lassen, ob er die Regelungen für verbindlich ansah. Diese Zweifel sind inzwischen durch die eindeutige Erklärung des Senats in der Drucksache 13/3838 vom 6.6.89 (Stellungnahme des Senats zu einem Ersuchen der Bürgerschaft im Zusammenhang mit den Erörterungen zu meinem 6. und 7. Tätigkeitsbericht) beseitigt: Die Richtlinien seien für die Verwaltung verbindlich und an ihrer Fortschreibung werde gearbeitet.

2.1.3.1 Automationsrichtlinien

Den im Rahmen der Entscheidungen zur Drucksache 755/85 erteilten Auftrag des Senats zur Überarbeitung der Automationsrichtlinien hält der Arbeitskreis der IuK-Beauftragten durch die in der genannten Drucksache dargestellte Neuorganisation der Nutzung von IuK-Technik sowie durch die weitere Ausgestaltung der zur Drucksache ergangenen Grundsatzentscheidungen in dem neuen Instrument der IuK-Gesamtpläne (insbesondere im IuK-Gesamtplan 1990-1992, Drs. 870/89 vom Juli 1989) für erfüllt. Das mag vom Regelungsgehalt her zutreffen, aber es fehlt die Aufhebung der formal noch geltenden Automationsrichtlinien und es bestehen die unter 3.1.1 und 3.1.2 dargestellten Bedenken gegen die Form, in der die neuen Regelungen in Erscheinung treten.

2.1.3.2 Freigaberichtlinie, DS-Rahmenregelungen und Dokumentationsrichtlinie

Die Freigaberichtlinie von 1982 regelt „die abschließende Prüfung (Test) und die Einwilligung zur Anwendung in der jeweiligen Rechenstelle (Freigabe) von neuen Verfahren und Änderungen an bestehenden Verfahren, die

— in der Verwaltung der Freien und Hansestadt Hamburg oder in ihrem Auftrag von Stellen außerhalb der Verwaltung entwickelt oder verändert oder

— von Stellen außerhalb der Verwaltung der Freien und Hansestadt Hamburg übernommen werden."

Bei komplexen und zeitkritischen Verfahren bereitet die Umsetzung der Freigaberichtlinie in der bestehenden Form aus vielerlei Gründen zum Teil erhebliche Schwierigkeiten, die dazu geführt haben, daß die betroffenen Stellen nicht nach der Richtlinie verfahren, sondern eine selbst entwickelte abweichende Verfahrensweise anwenden (z.B. wendet das Personalamt für die Freigabe der Verfahren zur Berechnung und Zahlbarmachung der Dienst-und Versorgungsbezüge im automatisierten Verfahren der Freien und Hansestadt Hamburg ein von der Freigaberichtlinie abweichendes Verfahren an - vergl. 6. TB 3.4.2 S. 24 ff und in diesem TB 2.5). Wegen der besonderen Bedeutung der Freigabe für die Rechtmäßigkeit und die Ordnungsmäßigkeit der Datenverarbeitung habe ich die Nichteinhaltung der Freigaberichtlinie immer besonders kritisiert.

Die Bedeutung der Verfahrensfreigabe liegt darin, daß mit ihr die Übernahme der Verantwortung für die Anwendung eines Verfahrens durch die für eine bestimmte Verwaltungsaufgabe fachlich zuständige Stelle erklärt wird. Die Freigabe erfolgt aufgrund der Überzeugung, daß das vorgesehene Verfahren den rechtlichen, sonstigen fachlichen und organisatorischen Anforderungen dieser Aufgabe entspricht. Diese Überzeugung soll die fachlich zuständige Stelle sich durch eigene Tests verschaffen, denen Funktionstests der programmierenden Stelle vorausgegangen sind. Mit der Verfahrensfreigabe bescheinigt die fachlich zuständige Stelle die Richtigkeit aller zum Verfahren

gehörenden Programme, die Richtigkeit des Zusammenwirkens der Programme sowie die Angemessenheit der Organisation des Gesamtablaufs. Dem steht die Erkenntnis, daß es keine absolut fehlerfreien Programme gibt, nicht entgegen. Mit Richtigkeit ist in diesem Zusammenhang gemeint, daß bei Anwendung aller gebotenen Sorgfalt Fehler nicht mehr festgestellt wurden. Nach der Freigabe darf das Verfahren zur Produktion eingesetzt werden. Die Integrität der Programme ist Voraussetzung für die Fortgeltung der einmal erteilten Freigabe. Notwendige Änderungen an den Programmen oder dem Verfahrensablauf erfordern eine erneute Freigabe, und zwar des gesamten Verfahrens bzw. des betreffenden selbständigen Verfahrensteils.

Ein geordnetes Freigabeverfahren und die dazugehörige Dokumentation sind die Voraussetzung dafür, daß eine bestimmte Datenverarbeitung im nachhinein überprüfbar ist. Nur wenn feststeht, mit welcher Programmversion die Datenverarbeitung an einem bestimmten Tag erfolgt ist, ist eine nachträgliche Aufklärung von Fehlern oder Zweifeln möglich.

Soweit ich sehe, bestreitet inzwischen niemend mehr, daß an die Freigabe von ADV-Verfahren bestimmte materielle Anforderungen zu stellen sind, die unabdingbar sind. Die Art und Weise, wie diese Anforderungen erfüllt werden, kann jedoch unterschiedlich sein. Eine Freigaberichtlinie, die die betroffenen Stellen in der Praxis auch tatsächlich einhalten können, muß selbst bestimmte Anforderungen erfüllen: sie muß verbindliche Vorgaben auf den Umfang beschränken, der zu dem mit der Freigabe verfolgten Zweck erforderlich ist und sie muß den durch die rasante technische Entwicklung inzwischen möglichen vielfältigen Gestaltungsformen der ADV-Verfahren und den organisatorischen und personellen Gegebenheiten in der hamburgischen Verwaltung angemessen Rechnung tragen und in dieser Hinsicht für zukünftige Entwicklungen offen bleiben. Allerdings glaube ich nicht, daß eine neue Freigaberichtlinie - auch wenn eine flexible Regelung gelingt - das Problem „ein für alle Mal" lösen kann. Früher oder später wird sich erneut Anpassungsbedarf ergeben, der zu Änderungen führen muß, wenn es nicht erneut zu einem Verlust der Organisationskontrolle durch das Auseinanderdriften von Regelung und Praxis kommen soll.

Im Februar 1989 hat mich das Senatsamt für den Verwaltungsdienst - Organisationsamt - von seiner Absicht unterrichtet, die Freigaberichtlinie noch in diesem Jahr neu zu fassen. Im Rahmen dieses Vorhabens wollte es auch eine Regelung treffen für die Freigabe der vom Senatsamt zur Verfügung gestellten Allgemeinen Software (s.u. 2.1.3.3), und schließlich wollte es eine Regelung erarbeiten für solche Anwendungen, bei denen von den zuständigen Bearbeitern zur Erledigung von Verwaltungsaufgaben Arbeitsplatzrechner und konfektionierte Software (z.B.Datenbanksoftware, Tools) eingesetzt werden. Das Organisationsamt hat einen „Arbeitskreis Freigaberichtlinie" einberufen, der sich aus Vertretern des Organisationsamtes, der DVZ (Rechenstelle), der Kassenabteilung und der Steuerverwaltung (Anwender aus dem Bereich der Finanzbehörde), des Rechnungshofs und meiner Dienststelle zusammensetzt. Der Arbeitskreis arbeitet nach meinem Eindruck zügig, es hat sich jedoch als zu optimistisch erwiesen, eine Neufassung bis zum Sommer 1989 - wie vom Senatsamt angestrebt - vorlegen zu können: die zu regelnde Materie ist zugegebenermaßen schwierig.

Bei den Arbeiten hat sich herausgestellt, daß die vorgesehene Änderung der Freigaberichtlinie Auswirkungen auf andere Vorschriften hat und Änderungen der DS-Rahmenregelungen und der Dokumentationsrichtlinie folgen werden. Die dort erforderlichen Anpassungen sollen jedoch nicht zu einer weiteren Verzögerung bei der Einführung eines neuen Freigabeverfahrens führen.

In den DS-Rahmenregelungen z.B. werden insbesondere die Regelungen zum sogenannten DVZ-Test, d.h. dem Test mit Originaldaten, neu gefaßt werden müssen. Nach Nr. 2.7.2. der DS-Rahmenregelungen sind solche Tests nur in Ausnahmefällen und unter Einhaltung bestimmter Formvorschriften zulässig. Aufgrund der Kritik an dem in der Praxis festgestellten tatsächlichen Umgang mit dem Instrument DVZ-Test hat eine Arbeitsgruppe sich mit den verschiedenen Fallgestaltungen befaßt, bei denen bisher im Rahmen laufender Verfahren DVZ-Tests durchgeführt wurden. Weiter wurde kritisch

geprüft, in welchen Fällen die Durchführung eines Tests mit Originaldaten auch bei Anlegung eines strengen Maßstabs erforderlich oder geboten ist.

Als Ergebnis hat die Arbeitsgruppe ein Papier mit einer Neuregelung für Testarbeiten mit Origanaldaten vorgelegt, das meine Zustimmung hat. Ich habe dieses Papier bisher jedoch nur als Entwurf gesehen, mir ist nicht bekannt, aus welchem Grund die Regelung noch nicht in Kraft gesetzt worden ist. Die von der Arbeitsgruppe ausgearbeitete Regelung sollte bei der anstehenden Überarbeitung der DS-Rahmenregelungen in diese übernommen werden.

2.1.3.3 Dienstanweisung für die Beschäftigten mit systemtechnischen Aufgaben im Senatsamt für den Verwaltungsdienst -Organisationsamt - (Systemprogrammierung)

Im Rahmen meiner Prüfung des Sicherheitssystems der Datenverarbeitungszentrale hatte ich 1985 gefordert, Aufgaben und Befugnisse der Systemprogrammierung des Organisationsamtes zu definieren und darzustellen, wie in diesem für die Sicherheit der Datenverarbeitung der Freien und Hansestadt Hamburg besonders relevanten Bereich die Dienstaufsicht wahrgenommen wird. Der Dienstaufsicht hatte ich im Bereich der Systemprogrammierung eine besondere Bedeutung beigemessen, weil Systemprogrammierer Zugriff auf die Betriebssysteme und die Sicherheitssoftware in der DVZ haben (müssen).

Im März 1989 hat der Leiter des Organisationsamtes nun eine Dienstanweisung erlassen. Diese regelt die

— Aufstellung eines Verzeichnisses über die von der Systemprogrammierung bereitgestellten Produkte der Allgemeinen Software,

— Bestimmung von produktbezogenen Verantwortlichkeiten der Beschäftigten in der Systemprogrammierung,

— Berechtigungen zur Veränderung von Dateien, soweit diese mit der Nutzung von Allgemeiner Software in Beziehung stehen,

— Befugnisse, verändernde Zugriffe auf Produkte der Allgemeinen Software vorzunehmen, durch Bestimmung von Berechtigungsprofilen für technisch unterstützte Zugriffskontrollen,

— Vorgaben für die Protokollierung von verändernden Zugriffen auf Produkte der Allgemeinen Software,

— Festlegung von Mindestinhalten für die Dokumentation von Produkten der Allgemeinen Software,

— Bestimmung des Handlungsrahmens und der Verantwortlichkeiten für Abnahme und Freigabe von Produkten der Allgemeinen Software.

Die Dienstanweisung stellt meines Erachtens eine angemessene Regelung für die Systemprogrammierung und die Freigabe von Allgemeiner Software dar. Z.Z. wird geprüft, ob vergleichbare Regelungen für die Systemprogrammierung im Rechenzentren des Universitätskrankenhauses Eppendorf erlassen werden sollten.

2.2 Anschluß dezentraler Rechner an die DVZ

Bislang kamen bei der Datenfernverarbeitung in der Hamburger Verwaltung lediglich Terminals und Drucker ohne oder nur mit sehr eingeschränkter eigener Rechenkapazität als Datenendgeräte zum Einsatz. Parallel dazu wurden Personalcomputer oder Mehrplatzanlagen dezentral eingesetzt, die aber nicht mit den Rechnern in der Datenverarbeitungszentrale verbunden waren (autonome Anlagen).

Ende 1988 hat das Senatsamt für den Verwaltungsdienst - Organisationsamt - den Entwurf eines Rundschreibens über die Verbindung von Arbeitsplatz- und Abteilungsrechnern mit den Zentralrechnern der Datenverarbeitungszentrale vorgelegt (s.auch 2.1.1). Ich habe im Rahmen des Abstimmungsverfahrens auf folgende Probleme hingewiesen:

— Der Anschluß „intelligenter" Datenendgeräte an die Großrechner beeinflußt das Gesamtsystem der Datensicherung in der DVZ. Den mit der Einbindung derartiger Geräte verbundenen Risiken muß mit geeigneten Maßnahmen begegnet werden.

— Werden Daten durch Überspielung von ganzen Dateien oder Dateiabschnitten aus dem Sicherheitssystem der DVZ ausgelagert und dezentral verarbeitet, muß auch bei den dezentralen Geräten und Anlagen Vorsorge dafür getroffen werden, daß eine mißbräuchliche Kenntnisnahme, Veränderung oder sonstige nicht zulässige Verarbeitung dieser Daten unterbleibt. Dies setzt i.d.R zusätzliche - über die Normalausstattung dieser Geräte hinausgehende - Sicherheitsmaßnahmen voraus.

In der Endfassung der Richtlinie, gegen die ich keine Einwendungen erhoben habe, wird versucht, den beschriebenen Risiken durch ein formalisiertes Zulassungsverfahren, das den Anschluß von dezentralen Rechnern an die Gewährleistung eines technischen und organisatorischen Mindeststandards bindet, entgegenzuwirken. Anwendungen im DVZ-Verbundmodus werden im Grundsatz nur zugelassen, wenn

— hierbei keine personenbezogenen Daten verarbeitet werden,

— kein Bezug zum Haushalts-, sowie zum Anordnungs-, Kassen- und Rechnungswesen besteht,

— keine Verarbeitung von Daten erfolgt, die aufgrund bereichsspezifischer Vorschriften einer besonderen Geheimhaltung unterliegen (z.B. Steuer-, Statistik-, Meldegeheimnis).

Soweit - abweichend von diesen Grundsätzen - personenbezogene Daten im Verbund DVZ-PC verarbeitet werden sollen, sehen die Regelungen vor, daß der Hamburgische Datenschutzbeauftragte rechtzeitig vor Beginn der Verarbeitung zu informieren ist und ihm Gelegenheit zur Stellungnahme gegeben wird. Diese Stellungnahme sollen die planenden Stellen dem Senatsamt zusammen mit dem Antrag auf Anschlußrealisierung vorlegen.

Leider hat sich in der seitherigen Praxis gezeigt, daß in Einzelfällen die rechtzeitige Unterrichtung unterblieben ist. Gleichwohl bleibt festzuhalten, daß die beteiligten Stellen bemüht waren, durch geeignete Maßnahmen den angesprochenen Sicherheitsrisiken entgegenzuwirken.

Ein besonderes Problem stellt der Anschluß solcher dezentraler Rechner an die DVZ dar, die ihrerseits an Wählnetze (z.B. Datex-P) angeschlossen sind. Eine Komponente der Systemsicherheit in der DVZ besteht nämlich darin, die Datenfernverarbeitung über Standleitungen abzuwickeln und Wählverbindungen auf das unabdingbare Mindestmaß zu beschränken (vgl. auch 2.4). Durch strikte Abschottung der Anwendungen und zusätzliche Maßnahmen auf Betriebssystemebene der dezentralen Geräte muß sichergestellt werden, daß eine Durchschaltung von Wählverbindungen zu den Großrechnern in der DVZ unterbleibt und auf diese Weise das DVZ-Sicherheitssystem nicht unterlaufen werden kann.

2.3 Umstellung des Behördenfernsprechnetzes auf ISDN-Standard

Bereits seit vielen Jahrzehnten besteht in Hamburg ein vom Postnetz unabhängiges Behördenfernsprechnetz mit eigenen Knotenämtern und Vermittlungsstellen. Zur Zeit besteht dieses Netz aus insgesamt etwa 60.000 Sprechstellen, die durch mehr als 60 Vermittlungsstellen miteinander verknüpft sind.

Über das Netz wurden die Daten bislang analog übertragen. Die Verbindungen wurden mittels elektromechanischer Wähler und Relais geschaltet. Wie im Postnetz (vgl. 7. TB, 5.3.2, S. 18) wird auch im Behördenfernsprechnetz auf längere Sicht die herkömmliche analoge Übertragungs- und elektromechanische Vermittlungstechnik durch Digitaltechnik abgelöst werden. Angesichts der Größenordnung des Behördenfernsprechnetzes besteht ständig die Notwendigkeit zum Ersatz ausgesonderter bzw. nicht mehr funktionsfähiger Anlagen. Unabhängig davon, welche Technik bisher eingesetzt wurde, kommt bei der Ersatzinvestition seit einiger Zeit ausschließlich software-gesteuerte

Vermittlungstechnik zum Einsatz; in Zukunft sollen nur noch Kommunikationsanlagen mit ISDN-Kanalstruktur (2 Datenkanäle, 1 Signalisierungskanal) beschafft werden. Bis Mitte November waren ISDN-fähige Nebenstellenanlagen bereits in den Behörden Mitte (u.a. Bezirksamt Hamburg-Mitte, Umweltbehörde und Behörde für Inneres), Behörden Billstedt, AK-Bergedorf, Behörden Alter Steinweg (u.a. Behörde für Wirtschaft, Verkehr und Landwirtschaft, HmbDSB), Bernhardt-Nocht-Institut, TU-Harburg und Rathaus Hamburg (mit Senatskanzlei, Bürgerschaft und Senatsamt für den Verwaltungsdienst) installiert. Die baldige Inbetriebnahme weiterer ISDN-fähiger Telekommunikationsanlagen ist geplant.

2.3.1 Funktionsweise von ISDN-Nebenstellenanlagen

Die neue Technik ermöglicht, verglichen mit den alten Anlagen, ein erheblich größeres Leistungsspektrum. Sie bringt aber auch neuartige datenschutzrechtliche Probleme mit sich. Die auf dem Markt angebotenen ISDN-Anlagen sind grundsätzlich modularisiert: Neben einer Abstufung nach Größenklassen bieten die einzelnen Hersteller die Möglichkeit, zu den jeweils bereits vorhandenen Leistungsmerkmalen zusätzliche Leistungsmerkmale „nachzurüsten". Der Katalog von im Rahmen von Inhouse-ISDN-Anlagen möglichen Leistungsmerkmalen ist deutlich umfangreicher als der von der Post im öffentlichen Telekommunikationsnetz standardmäßig angebotene, wobei nur diejenigen ISDN-Anlagen eine Postzulassung erhalten, die mindestens die von der Post geforderten Leistungen erbringen können.

ISDN-Anlagen bieten umfassende Möglichkeiten zur Gebührenerfassung und Auswertung. Dabei ist sowohl ein (anonymisierter) Summennachweis als auch ein ausführlicher Einzelgebührennachweis mit den jeweils zugrundeliegenden Gesprächsdaten (gewählte Rufnummer, Dienstart, Zeitpunkt und Dauer der Verbindung) möglich. Gebührendaten können sowohl auf einem Drucker ausgegeben als auch mit einem Gebührencomputer weiterverarbeitet und mit anderen Daten verknüpft werden. Derartige komfortable Gebührendatenerfassungs- und Auswertungssysteme können auch dazu gebraucht werden, die Anwesenheit, die Leistung und das Verhalten der Beschäftigten zu kontrollieren. Mit der Speicherung der Zielnummern wird darüber hinaus in das informationelle Selbstbestimmungsrecht der Angerufenen eingegriffen.

Sofern in Behörden-Telekommunikationsanlagen eine Gebührendatenerfassung vorgesehen ist (dies ist nach meiner Kenntnis bisher nur bei der Anlage der TU Harburg der Fall), werden die auf Zusatzgeräten (sog. „Server") in Dateien gespeicherten Gesprächsdaten nach bestimmten Merkmalen (z.B. Dienst- und Privatgespräche) ausgewertet. Die Auswertungen umfassen nach Auskunft der Baubehörde lediglich Ferngespräche; die angerufenen Telefon-Zielnummern werden verstümmelt (ohne die letzten beiden Ziffern) ausgedruckt. Inwieweit mehr Daten gespeichert als programmgesteuert ausgegeben werden, habe ich noch nicht prüfen können.

2.3.2 Neue Qualität der Kommunikationsdatenverarbeitung

Die ISDN-Technologie ist Ausdruck des Zusammenwachsens von Informations- und Kommunikationstechnik, wobei die Prinzipien der Computertechnologie (digitale Schaltung und Datenübertragung) auf die Kommunikationssysteme übertragen werden. Vermittlungs- und Übertragungsvorgang werden einheitlich auf digitaler Basis abgewickelt, wodurch sich für das Gesamtsystem der technischen Kommunikation neue Möglichkeiten erschließen. ISDN-Anlagen sind Datenverarbeitungsanlagen, deren Aufgabe darin besteht, Kommunikationswege zu schalten und Informationen zu übertragen.

Das Konzept der ISDN-Nebenstellenanlagen geht - ebenso wie das ISDN-Konzept der Post - von einer Integration von Sprache, Text, Bild und Daten aus. Alle Kommunikationsdienste, die bisher über unterschiedliche Netze abgewickelt wurden, sollen in einem System zusammengefaßt werden und mit den Zusatzgeräten sollen zusätzliche, teils neue, teils wesentlich verbesserte Leistungen angeboten werden, ohne daß im Teilnehmerbereich neue Leitungen verlegt werden müssen (ISDN nutzt die bisherigen Telefondrähte als Anschlußleitungen).

An die ISDN-Anlagen können sowohl herkommliche analoge Telefone als auch neuartige digitale Endgeräte angeschlossen werden:

— Digitaltelefone,

— PC's und andere Datenendeinrichtungen,

— Multifunktionsterminals,

— Endgeräte für Teletex, Telefax und Bildschirmtext.

Für den einzelnen Kommunikationsteilnehmer hat die Digitalisierung der Vermittlungstechnik die negative Konsequenz, daß bei der Kommunikation die Anonymität weitgehend verloren geht. Die neue Technik macht es möglich, ohne größeren Aufwand jede einzelne Verbindung zu identifizieren und zu dokumentieren. Durch die Signalisierung der Verbindungsdaten erfolgt zwangsläufig eine Datenerhebung und eine (zumindest temporäre) Speicherung, und zwar auch dann, wenn diese Daten nicht für Zwecke der Weiterverarbeitung dauerhaft gespeichert werden. Es ist evident, daß sich hier eine Vielzahl neuer Überwachungsrisiken ergibt, die bislang nicht ausreichend rechtlich geregelt sind und die obendrein weiterer technischer Begrenzungen bedürfen.

Datenschutzrechtlich kritisch zu beurteilen sind alle Leistungsmerkmale, die zur Offenbarung oder Speicherung von Kommunikationsdaten führen. Eine solche Funktion ist - neben der Gebührendatenerfassung (vgl. 2.3.1) - die bei allen ISDN-Anlagen vorgesehene und zur Grundausstattung gehörende Anzeige der Telefonnummern des „A-Teilnehmers" (Anrufer) beim „B-Teilnehmer" (Angerufener). Dadurch kann der Angerufene den Anschluß identifizieren, von dem aus eine Verbindung aufgebaut wird, ohne daß dies von Anrufenden zu steuern wäre, es sei denn, er läßt die Signalisierung generell sperren, was technisch möglich ist (es ist bisher allerdings ungeklärt, ob z. B. der einzelne Verwaltungsmitarbeiter eine entsprechende Sperre bewirken kann, oder ob dies nur aufgrund von Anordnungen der Dienststellenleitungen erfolgt).

Sobald die ISDN-Nebenstellenanlagen an das ISDN-Netz der Post angeschlossen werden, wird die Signalisierung auch über das Postnetz verfügbar, was zusätzliche Probleme mit sich bringt, da nun auch die Nummern von anderen von der Post eingerichteten ISDN-Anschlüssen auf dem Display des Angerufenen signalisiert werden. Praktisch könnte mit jedem Anruf eine vom Anrufer ungewollte Datenerhebung vorgenommen werden. Eine derartige Datenerhebung halte ich ohne eine bereichsspezifische Rechtsgrundlage für unzulässig.

Mit Hilfe der Funktion „Fangen" kann die Rufnummer eines Anrufers automatisch auf einem Ausdruck oder manuell festgehalten werden; dies kann bei allen Anrufen oder auch gezielt bei einzelnen Anrufen geschehen. Auch wenn die Hersteller der TK-Anlagen bisher nur den automatisierten Ausdruck der „gefangenen" Anruferdaten anbieten, ist es ohne größere technische Schwierigkeiten möglich, die Ausgabe dieser Daten auf automatisiert auswertbare Speichermedien (Diskette, Festplatte, Band) umzuleiten. Diese Daten könnten mit den im Rahmen der Gebührendatenerfassung und auch mit anderweitig - z. B. in Personalinformationssystemen - gespeicherten Daten verknüpft und für die Erstellung von Kommunikations- und Verhaltensprofilen herangezogen werden.

Auch das Leistungsmerkmal „Freisprechen und Direktantworten" ist problematisch. Mit diesem Leistungsmerkmal kann der Anrufer in dem Gerät des Angerufenen ein Mikrophon aktivieren, das die Raumgeräusche auch ohne Abheben des Höres überträgt. Zwar wird die Aktivierung des in das Telefon eingebauten Mikrophons durch einen kurzen Ton signalisiert und das Leistungsmerkmal wird am Apparat durch ein Lämpchen angezeigt, doch gewährleisten diese Maßnahmen nur einen ungenügenden Schutz, wenn z.B. der Raum, in dem sich das Gerät befindet, zur Zeit der Aktivierung der Freisprecheinrichtung nicht besetzt war und die Personen, die sich im Raum aufhalten, keinen direkten Blickkontakt zum Telefon haben.

Schließlich sind auch die Teleserviceangebote Fernwartung und Fernverwaltung sind risikobehaftet. Bei der Fernwartung hat der Hersteller die Möglichkeit, über eine definierte Serviceschnittstelle Veränderungen einer TK-Anlage vorzunehmen. Dies bedeutet, daß sowohl einzelne Programme im Wege der Fernwartung verändert als auch völlig neue Programme oder Programmpakete in die Anlage eingegeben werden können, ohne daß sich dies seitens des Anwenders kontrollieren läßt. Mit Hilfe der Fernverwaltung kann der Leistungsumfang der Anlage verändert werden, z.B. durch Aktivieren

von Leistungsmerkmalen, Ändern von Rufnummern und Berechtigungen usw.. Sowohl bei der Fernverwaltung auch bei der Fernwartung erfolgt die Kommunikation zwischen der Servicestelle und der TK-Anlage über das Fernmeldenetz.

2.3.3 Prüfung der TK-Anlage des Rathauses

Im Oktober 1989 haben meine Mitarbeiter die Telekommunikationsanlage im Rathaus besichtigt und sich von Mitarbeitern des Herstellers und der Baubehörde - Abteilung Fernmeldetechnik - deren Funktion und Ausbaustand erläutern lassen. Die Prüfung hat Hinweise auf schwerwiegende Mängel ergeben, die sich sicherlich z.T. daraus erklären, daß die neue Telekommunikationsanlage zum Prüfungszeitpunkt erst provisorisch installiert war. Dies gilt insb. für die unzureichende Zugangssicherung. Einige Probleme sind jedoch von grundsätzlicher Bedeutung und ergeben sich aus der technischen Konzeption solcher Anlagen.

In der TK-Anlage des Rathauses wurden aufgrund der zum Prüfungszeitpunkt aktiven Leistungsmerkmale lediglich Bestandsdaten über die Konfiguration der Anlage einschließlich der angeschlossenen Endgeräte dauerhaft gespeichert. Verbindungsdaten (Daten über das Kommunikationsverhalten der Teilnehmer) wurden zum Prüfungszeitpunkt nicht auf externen Datenträgern gespeichert. Während des Verbindungsaufbaus und für die Dauer der Verbindung wurden der rufende Anschluß, die gewählte Rufnummer und der benutzte Dienst (Dienstekennung) im Arbeitsspeicher der Anlage gehalten. Diese Verbindungsdaten wurden sobald die Verbindung ausgelöst war und kein weiteres Leistungsmerkmal (z.B. automatischer Rückruf) aufgerufen wurde, zum Überschreiben durch das System freigegeben und konnten dann praktisch nicht mehr ausgewertet werden. Für Zwecke der Wahlwiederholung wurde die zuletzt gewählte Rufnummer für mindestens 45 Minuten festgehalten.

Neben dem Leistungsmerkmal „Gebührenerfassung am Platz" (GEP) war keine weitere Gebührenerfassung installiert. Bei der Gebührenerfassung am Platz werden bei über den zentralen Vermittlungsplatz hergestellten Amtsverbindungen auf dem Bildschirm der Vermittlungskraft die Verbindungsdaten und die aufgelaufenen Gebühreneinheiten angezeigt. Nach Auslösen der Verbindung kann die Vermittlungskraft die Anzeige löschen.

Sofern das Leistungsmerkmal automatischer Rückruf in Anspruch genommen wurde, wurden die Daten der gewünschten Verbindung in gesonderten internen Dateien im Arbeitsspeicher festgehalten. Die Funktion „automatische Anrufumleitung" führte ebenfalls zu einer zeitweiligen Zuspeicherung des Umleitungszieles.

Welche Leistungsmerkmale gerade aktiviert waren, ließ sich zwar durch eine Standardabfrage prüfen. Es war aber nicht lückenlos nachvollziehbar, welchen Zustand das System zu jedem früheren Zeitpunkt hatte, von wem und wann welche Leistungsmerkmale eingerichtet und aktiviert worden waren. Zwar reagierte das System auf Eingaben über das Betriebsterminal (z.B. Veränderung der aktivierten Leistungsmerkmale) mit Meldungen, die sowohl auf dem Bildschirm als auch über einen an das Terminal angeschlossenen Matrixdrucker ausgegeben wurden, doch ließ sich der Ausdruck durch Abschaltung des Druckers bzw. Herausziehen des Verbindungssteckers zum Terminal unterbinden. Ferner wurde festgestellt, daß am System - parallel zum Betriebsterminal - über eine V 24-Schnittstelle ein PC angeschlossen war, mit dem ein Siemens-Techniker den Systemzustand steuern und auch Leistungsmerkmale aktivieren oder deaktivieren konnte. Die über den PC abgewickelten Veränderungen wurden überhaupt nicht protokolliert. Der Papierausdruck gab also keinerlei verläßliche Informationen über Veränderungen des Systemzustands. Die Anlage war mithin nicht revisionssicher.

Die Aktivierung der und Deaktivierung von Leistungsmerkmalen setzte den Zugang zum Betriebsterminal, die Kenntnis des Paßwortes und des Systems voraus. Diese Voraussetzungen hatten nur Mitarbeiter der Herstellerfirma. Mitarbeiter der Baubehörde kannten das entsprechende Paßwort nicht und konnten somit die Aktivierung von Leistungsmerkmalen nicht beeinflussen (wohl aber die für den einzelnen Anschluß festgelegten Parameter).

Jedenfalls in der Phase der Einrichtung der Anlage und der damit verbundenen Hektik konnten Unbefugte ohne weiteres in die Räume der Vermittlungsstelle gelangen, wie meine Mitarbeiter bei einem unangekündigten Besuch feststellen konnten. Die unzureichende Zugangssicherung ist vor allem deshalb als schwerwiegender Mangel anzusehen, weil sich auch bei der neuen Anlage Gespräche abhören ließen, ohne daß hierzu größerer technischer Aufwand hätte getrieben werden müssen.

Die Anzeige der Telefonnummer des Anrufenen auf dem Display des Angerufenen war auf der Rathaus-Anlage installiert und aktiviert. Auch die Rufnummern analoger Anschlüsse wurden signalisiert. Die Signalisierung setzte lediglich voraus, daß der angerufene Apparat über ein entsprechendes Display verfügt. Dies war bei etwa 100 von insges. über 1000 Geräten der Fall. Durch eine entsprechende Konfiguration der Anschlüsse konnte die Anzeige von Rufnummern unterdrückt werden.

Obwohl die GAL-Fraktion wiederholt darauf hingewiesen hatte, daß sie mit der Anzeige ihrer Rufnummern nicht einverstanden war, wurden zum Prüfungszeitpunkt (knapp eine Woche nach Inbetriebnahme der Anlage) auch die Anrufe von Apparaten der GAL-Fraktion signalisiert. Dieser Mangel ist inzwischen jedoch abgestellt.

Die Betroffenen waren nur mangelhaft informiert worden. Insbesondere fehlte jeder Hinweis auf die vorgenommene Rufnummernsignalisierung auf dem Display des Angerufenen und der Hinweis auf die Möglichkeit, diese Funktion in der Anlage zu unterdrücken.

Wenn, wie geplant, voraussichtlich im Frühjahr 1990 die Rathaus-Anlage an das öffentliche ISDN angeschlossen wird, ergeben sich - die weiter oben (2.3.2) bereits erwähnten - Probleme. Bevor die TK-Anlage des Rathauses mit ISDN-Verbindungen an das Post-ISDN angeschlossen wird, ist eine Klärung der damit verbundenen - auch datenschutzrechtlichen - Fragen erforderlich.

Im Hinblick auf die neuen Möglichkeiten der ISDN-fähigen Nebenstellenanlagen, halte ich verbindliche Regelungen über zugelassene Leistungsmerkmale, Sicherung der Anlage gegen Manipulation und Abhören, Gebäude- und Betriebssicherung für erforderlich. Da ein großer Teil der Betroffenen Mitarbeiter der FHH sind, könnte eine Regelung - wie auch von der Bundespost ausdrücklich vorgeschlagen - durch Dienstvereinbarung oder durch eine behördenübergreifende Vereinbarung nach § 94 HmbPersVG erfolgen. Auch bezüglich der anderen Teilnehmer, insb. der Bürgerschaftsfraktionen, müßten verbindliche Regelungen getroffen werden, die einen Mißbrauch von Daten ausschließen.

Damit kontrolliert werden kann, welche Leistungsmerkmale aktiviert und welche gesperrt sind, müssen technische Veränderungen an der Anlage vorgenommen werden, insb. eine lückenlose, manipulationssichere Protokollierung von Veränderungen der Systemkonfiguration und der Leistungsmerkmale. Das Einspielen neuer Software und die Aktivierung von Leistungsmerkmalen darf nicht unkontrolliert durch den Hersteller erfolgen. Hier muß das aus der Datenverarbeitung bekannte „Vier-Augen-Prinzip" greifen, wobei Veränderungen nur vorgenommen werden können, wenn sowohl der Hersteller als auch der Betreiber (hier: Baubehörde) damit einverstanden sind. Dies wäre z.B. durch Abforderung von zwei Paßworten der höchsten Stufe zu gewährleisten.

2.3.4 Pilotprojekt Telekommunikationssystem als Kommunikationsdrehscheibe

Bereits heute wird über eine ISDN-fähigen Vermittlungsstelle des Behördennetzes probeweise Datenfernverarbeitung betrieben (TU-Harburg). Die Nutzungsmöglichkeiten von ISDN-Anlagen im non-voice-Bereich sollen aufgrund eines Senatsauftrages auch im Rahmen des Projektes „Telekommunikationssystem als Kommunikationsdrehscheibe" untersucht werden.

Im Juni 1989 hat sich unter Federführung der Baubehörde eine entsprechende Projektgruppe konstituiert. Aufgabe dieser Projektgruppe soll es sein, die sich durch den Einsatz einer ISDN-fähigen Kommunikationsanlage bietenden Möglichkeiten der technischen Kommunikation hinsichtlich

— Akzeptanz,
— Arbeitsorganisation,
— Datenschutz,
— Mitbestimmung,
— Schulung,
— technische Realisation

zu untersuchen und Vorgaben für die Einführung dieser Technik in der Verwaltung zu erarbeiten. An der Projektgruppe sind Vertreter des Senatsamtes für den Verwaltungsdienst, des des Hamburgischen Datenschutzbeauftragten und Personalrats der Baubehörde beteiligt.

Schwerpunktmäßig soll geprüft werden, welche Möglichkeiten ISDN-fähige Kommunikationsanlagen neben dem komfortablen Telefonieren bieten, vor allem im Bereich der Text- und Datenkommunikation. Zu diesem Zweck sollen „Kommunikationsmodellgruppen" (KMG) gebildet werden, die bestimmte Anwendererfordernisse beispielhaft abdecken sollen. Bei Redaktionsschluß für diesen Tätigkeitsbericht war die Bildung der KMG noch nicht abgeschlossen. Es zeichnet sich aber ab, daß folgende Anwendungsbereiche getestet werden sollen:

— Datenfernverarbeitung in der Datenverarbeitungszentrale (Dialogbetrieb),
— schnelle Übertragung großer Datenmengen (graphische Datenverarbeitung) bei der digitalisierten Stadtgrundkarte,
— Bürokommunikationssysteme (insbesondere Eignung des Behördentelefonnetzes zum direkten Anschluß von Terminels an dezentrale Mehrplatzanlagen),
— Verbundbetrieb von dezentralen Rechnern verschiedenen Hersteller,
— behördenübergreifende Dokumentenbearbeitung (Edifakt),
— Nutzung multifunktioneller Endgeräte (z.B. Btx/Telefonieren/ PC).

Der Schwerpunkt des Pilotprojektes wird bei der noch auf ISDN-Standard umzustellenden TK-Anlage der Baubehörde liegen; es sind jedoch auch Übergänge zu anderen Nebenstellenanlagen vorgesehen. Mit der praktischen Umsetzung des Pilotvorhabens ist bereits im ersten Halbjahr 1990 zu rechnen.

2.4 Datenvermittlungssystem der Statistischen Ämter

Bereits seit Mitte der 80er Jahre wickelt die nordrhein-westfälische Verwaltung einen großen Teil ihrer Datenkommunikation über ein eigenes Verwaltungsnetz, das „Datenvermittlungssystem Nordrhein-Westfalen" (DVS) ab. Dabei werden sowohl eigene Leitungswege als auch das Datex-P-Netz der Post genutzt. Heute sind bereits mehrere hundert Datenverarbeitungssysteme unterschiedlicher Größenordnung, darunter auch etliche Großrechner in Universitäts- und Verwaltungsrechenzentren, an das DVS angeschlossen.

Auch das Statistische Bundesamt und die meisten Statistischen Landesämter bedienen sich des DVS, um im Rahmen der Verbundprogrammierung erstellte Quellprogramme und Dateien mit aggregierten Daten auszutauschen, was zuvor per Magnetbandaustausch geschah. Im Mai 1989 teilte mir das Statistische Landesamt mit, daß nun auch das StL Hamburg über Datex-P an das DVS angeschlossen werden solle.

Datenschutzrechtlich bedeutsam ist dies Projekt deshalb, weil mit der Anbindung an das DVS erstmalig die Datenverarbeitungszentrale (DVZ), auf deren Rechnern eine Vielzahl personenbezogener Daten verarbeitet wird, an ein Wählnetz angeschlossen werden soll. Damit könnten sich Konsequenzen für das dortige Datensicherungskonzept ergeben.

Meine Erkundigungen haben ergeben, daß auch vor diesem Hintergrund gegen den geplanten Anschluß keine Bedenken bestehen, sofern die im DVS und in der DVZ vorgesehenen Sicherungsmaßnahmen ergriffen werden und von dem fachlich zuständigen Statistischen Landesamt gewährleistet wird, daß sich die Übermittlungen im zulässigen Rahmen halten. Ich werde dies zu gegebenem Zeitpunkt überprüfen.

2.5 Prüfung der Personalamtsverfahren

Über den Beginn der Prüfung der automatisierten Verfahren zur Berechnung und Zahlbarmachung der Dienst- und Versorgungsbezüge in der Freien und Hansestadt Hamburg (im folgenden als Personalamtsverfahren bezeichnet) und die ersten bei der Prüfung gewonnenen Erkenntnisse habe ich bereits in meinem 6. TB (3.4.2 S.24 ff) berichtet. Die Prüfung wurde 1988 und 1989 fortgesetzt. Die Sachverhaltsermittlungen wurden Ende Juli 1989 beendet und der abschließende Prüfbericht den Beteiligten am 2. November 1989 zur Stellungnahme übersandt.

Als wesentliches Ergebnis der Prüfung ist festzustellen, daß bei den Personalamtsverfahren, die als Gesamtsystem eines der bedeutendsten Verfahren der Freien und Hansestadt Hamburg darstellen, verbindliche Richtlinien des Senats über etliche Jahre nicht eingehalten wurden und dies - obwohl allen Verantwortlichen bekannt - nicht in angemessener Zeit zu Konsequenzen führte.

2.5.1 Nichteinhaltung der Freigaberichtlinie

Welchen Sinn die Verfahrensfreigabe hat und welche Bedeutung ihr für die Rechtmäßigkeit und Ordnungsmäßigkeit der Datenverarbeitung zukommt, habe ich im Zusammenhang mit meinen grundsätzlichen Ausführungen zu dem Datenverarbeitungs-Regelwerk für die Freie und Hansestadt Hamburg (s.o. 2.1.3.2) dargestellt.

Insbesondere an den Personalamtsverfahren (aber z.B. auch an dem Verfahren INFES der Finanzbehörde) hat sich der Streit darüber entzündet, ob es bei komplexen und zeitkritischen Verfahren in der Praxis überhaupt möglich ist, die Freigaberichtlinie einzuhalten, die mit ihren detaillierten Regelungen als zu starr und zu sehr an überholten Formen der automatisierten Datenverarbeitung ausgerichtet kritisiert wird. Zweifel wurden vor allem daran geäußert, daß die Kapazitäten der DVZ ausreichten, wenn tatsächlich für alle Verfahren vor der Freigabe ein Abnahmetest in der Form durchgeführt werden würde, wie es in der Freigaberichtlinie vorgeschrieben ist. Das Personalamt vertritt bis heute die Meinung, jedenfalls bei den Personalamtsverfahren sei die Einhaltung der Freigaberichtlinie nicht möglich. Es hat ein eigenes Verfahren für die Freigabe entwickelt, das ich im wesentlichen für geeignet halte, die aus datenschutzrechtlicher Sicht an die Freigabe von ADV-Verfahren zu stellenden Anforderungen zu erfüllen. Ob das Verfahren auch alle auf dem Haushalts-, Kassen- und Rechnungswesen beruhenden Anforderungen, insbesondere das „VierAugen-Prinzip" erfüllt, unterliegt nicht meiner abschließenden Beurteilung, sondern der der Finanzbehörde und des Rechnungshofes.

Von einer Darstellung des vom Personalamt entwickelten Freigabeverfahrens an dieser Stelle sehe ich ab wegen der inzwischen aufgenommenen Aktivitäten zur Neufassung der Freigaberichtlinie (s.o. 2.1.3). Ich gehe davon aus, daß im Rahmen der Neuregelung sowohl die Mängel der bisherigen Regelung beseitigt als auch die Erfahrungen und Vorschläge der betroffenen Stellen berücksichtigt werden.

Im Rahmen der Freigabeproblematik habe ich weiter bemängelt, daß die Personalamtsverfahren, deren Entwicklung vor dem Inkrafttreten der ADV-Richtlinien begann, auch nach dem Inkrafttreten der Freigaberichtlinie nicht als Ganzes freigegeben worden sind. Ich vertrete die Ansicht, die für die Wahrnehmung einer Verwaltungsaufgabe zuständige Stelle hat bei Einführung eines neuen ADV-Verfahrens und bei Änderungen eines solchen Verfahrens in einem formalen Akt, der „Freigabe", zum Ausdruck zu bringen, daß sie die Verantwortung für das gesamte Verfahren übernimmt. Es genügt m.E. nicht, jeweils bei Hinzukommen eines neuen Programms oder nach Programmänderungen nur das einzelne Programm freizugeben. Das Personalamt stellt bisher in Abrede, daß eine Freigabe des Gesamtverfahrens möglich sei. Auch mit dieser Problematik befaßt sich der 1989 einberufene „Arbeitskreis Freigaberichtlinie".

2.5.2 Defizite bei der Umsetzung der Dokumentationsrichtlinie

Ich habe kritisiert, daß auch nach dem Inkrafttreten der Dokumentationsrichtlinie keine allgemeine Verfahrensbeschreibung erstellt worden ist und daß zum Zeitpunkt der Prüfung Teile der Dokumentation (Verzeichnis der Auftragsberechtigungen, Stammbandsatzbeschreibung) nicht auf einem aktuellen Stand waren.

Die allgemeine Verfahrensbeschreibung ist wesentliche Voraussetzung für die Prüfbarkeit des Verfahrens, d.h. dafür, daß es einem sachverständigen Dritten möglich ist, sich in angemessener Zeit einen Überblick über die Wirkungsweisen, Kontrollen und Ergebnisse zu verschaffen. In dem Fehlen einer allgemeinen Verfahrensbeschreibung sehe ich nicht bloß einen Mangel der Dokumentation. Ich führe das Fehlen auch auf gravierende Organisationsmängel zurück, nämlich darauf, daß die Zwecke des Verfahrens, also die Aufgaben, die das Verfahren erfüllen soll, die an dem Verfahren beteiligten Stellen und ihre Funktionen sowie die von dem Verfahren zu erfüllenden Anforderungen nicht - zumindest nicht rechtzeitig und nicht umfassend - festgelegt worden sind. Diese Festlegungen hätten am Anfang der Verfahrensentwicklung erfolgen müssen. Ich habe bei meiner Prüfung nicht feststellen können, daß außer dem Zweck „Berechnung und Zahlbarmachung der Bezüge" weitere Zwecke festgelegt worden sind. Tatsächlich dienen die Verfahren aber auch anderen Zwecken wie z.B. der Personalverwaltung und -planung. Ich habe auch nicht feststellen können, wer eigentlich „Herr der Daten", also speichernde Stelle im Sinne des Datenschutzrechts ist. Es bestehen Zweifel, ob dies die einzelnen Behörden jeweils für einen Teil des Datenbestandes sind oder die BVSt oder das Personalamt. Bei Einrichtung der BVSt ist dieser nur die Aufgabe „Berechnung und Zahlung der Bezüge" übertragen worden.

2.5.3 Nutzung von Originaldaten für Testzwecke

Bei der Prüfung habe ich festgestellt, daß die Programme, die der Aufgabenerfüllung nach dem Schwerbehindertengesetz dienen, nicht mit speziellen Testdaten ausgetestet werden, sondern es werden immer, wenn ein Test nötig ist, die Produktionsdaten in eine Testdatei überspielt, auf die die für die Schwerbehinderten-Programmroutinen zuständigen Programmierer zugreifen können. In der Dokumentation fand sich keine Unterlage, aus der eine entsprechende Entscheidung der fachlich zuständigen Stelle hervorgeht und in der die Notwendigkeit zum Test mit Originaldaten begründet wird. Auch gibt es keine Beschreibung der dabei einzuhaltenden Vorgehensweise. Die Kopieraufträge zur Übertragung der Daten aus der Produktionsdatei in eine Testdatei werden allerdings von der fachlich zuständigen Stelle mit unterzeichnet. Eine Anzeige über Tests mit Originaldaten an das Senatsamt für den Verwaltungsdienst nach Nr.2.7.1 und 2.7.2 der DS-Rahmenregelungen ist nicht erfolgt.

Ich habe grundsätzlich Bedenken gegen eine Teststrategie, die von vornherein auf einen Test mit Originaldaten abgestellt ist. Der Test mit Originaldaten soll nur auf besondere Ausnahmefälle beschränkt sein (s.o. 2.1.3.2). Wenn im Falle der Programme für die Schwerbehinderten das festgestellte Testverfahren aber tatsächlich erforderlich sein sollte und beibehalten werden muß, dann muß es so gestaltet werden, daß Mißbrauch ausgeschlossen werden kann, und das Verfahren muß in der Dokumentation so beschrieben werden, daß es nachvollziehbar und kontrollierbar ist. Mindestens müßte

- die Entscheidung der fachlich zuständigen Stelle, daß die die Schwerbehinderten betreffenden Verfahrensteile nur mit Originaldaten getestet werden sollen, sich aus der Dokumentation ergeben
- die entsprechende Teststrategie im einzelnen beschrieben sein, so daß Kontrollen im Nachhinein möglich sind,
- schriftlich geregelt werden, wer auf die personenbezogenen Daten, die in die Testdatei kopiert werden, zugreifen darf,
- sichergestellt werden, daß die Daten sofort nach Erfüllung des Testzwecks gelöscht werden,

— das Testergebnis dokumentiert werden, wobei das Problem zu lösen ist, daß die einzelnen Testfälle personenbezogene Daten sind und nicht wie erfundene Testdaten ohne weiteres zur Dokumentation genommen werden können.

2.5.4 Mängel bei der Organisation und Überwachung der Schriftgutvernichtung

Bei meiner Prüfung der Verfahren des Personalamtes habe ich festgestellt, daß auch die BVSt sich für die Vernichtung des ausgesonderten Schriftgutes eines Auftragnehmers bedient hat. Bei der Auswahl des Auftragnehmers hat sie nicht die gebotene Sorgfalt aufgewendet, sie hat z.B. nicht geprüft, ob der Auftragnehmer geeignete technische und organisatorische Maßnahmen getroffen hat, um die datenschutzrechtlich einwandfreie Vernichtung des Schriftgutes zu gewährleisten. Sie hat dem Auftragnehmer keine genauen Weisungen zur Behandlung des ihm übergebenen Materials erteilt, wozu sie im Hinblick auf die gesetzliche Bestimmung, Auftragsdatenverarbeitung ist nur im Rahmen der Weisungen des Auftraggebers zulässig (§ 3 Abs. 2 HmbDSG und § 37 BDSG), verpflichtet war. Sie hat erstmals am 16.5.1988 einen schriftlichen Vertrag mit dem Auftragnehmer geschlossen, jedoch nicht geprüft, ob der Auftragnehmer die in dem Vertrag zugesicherte Behandlung des Materials (vor allem die unverzügliche Zerkleinerung in einem eigenen Shredder) überhaupt leisten konnte. Tatsächlich hat der betreffende Auftragnehmer bis heute keinen eigenen Shredder, sondern bedient sich eines Unterauftragnehmers (s.u. 2.6).

Ich habe die BVSt aufgefordert, ein Entsorgungskonzept für eine datenschutzrechtlich einwandfreie Schriftgutvernichtung zu entwickeln.

2.5.5 Bewertung

In meiner Bewertung der Prüfungsfeststellungen habe ich mich im wesentlichen auf die Kritik an den vorstehend dargestellten grundsätzlichen Mängeln beschränkt. Von einer formellen Beanstandung der Verstöße gegen die verbindlichen ADV-Richtlinien gem. 21 HmbDSG habe ich abgesehen, weil ich dieses Mittel zum jetzigen Zeitpunkt nicht für geboten halte, um die Verwaltung zu bewegen, die aufgezeigten Mängel abzustellen. Wie oben (2.1) dargestellt, hat der Senat den Auftrag zur Überarbeitung der Richtlinien erteilt, und das Senatsamt für den Verwaltungsdienst hat mit der Umsetzung dieses Auftrages begonnen. Ich erwarte, daß das Personalamt meine in dem Bericht aufgestellten Forderungen, soweit sie von dem neuen Regelwerk unabhängig sind, umgehend erfüllt, daß das Senatsamt für den Verwaltungsdienst ein überarbeitetes, praktikables Regelwerk (in handhabbarer Form - s. 2.1.2) zügig erstellt und daß, sobald eine neue Freigaberichtlinie erlassen ist, auch die Personalamtsverfahren in Übereinstimmung mit der Richtlinie freigegeben werden. (Diese Erwartung schließt die Möglichkeit ein, daß das Personalamt sein derzeitiges Freigabeverfahren im wesentlichen beibehalten kann, dieses Verfahren also - unter Berücksichtigung der Forderung nach Freigabe von ADV-Verfahren als Ganzes - mit der neuen Freigaberichtlinie zugelassen wird.)

Stellungnahmen der Beteiligten (Personalamt, BVSt, DVZ und - wegen der grundsätzlichen Kritik daran, daß die Nichtanwendung der verbindlichen ADV-Richtlinien des Senats jahrelang geduldet wurde - Organisationsamt) zu meinem Prüfungsbericht lagen mir bis zum Redaktionsschluß für diesen Bericht (1.12.89) noch nicht vor.

2.6 Schriftgutvernichtung

Die Probleme der Verwaltung bei der Organisation und Überwachung der Schriftgutvernichtung habe ich bereits in meinen beiden letzten Tätigkeitsberichten (6.TB 3.3 S.18f und 7.TB 3.4 S.14f) dargestellt. Daran anknüpfend kann ich nunmehr berichten, daß das Senatsamt für den Verwaltungsdienst und die Finanzbehörde im Februar in den MittVw 1989 Seite 10ff die

> „Bekanntmachung über die Entsorgung von Altpapier und anderen verbrauchten Datenträgern"

und im Anhang dazu die

> „Erläuterungen und Hinweise zur praktischen Umsetzung der Bekanntmachung über die Entsorgung von Altpapier und anderen verbrauchten Datenträgern vom 1.2.1989"

veröffentlicht haben. Als Anlage zum Anhang ist auch der im 7. TB erwähnte Mustervertrag für die Vergabe von Arbeiten zur Schriftgutvernichtung an gewerbliche Auftragnehmer abgedruckt. Meine Forderung nach einer Aufbereitung des Problems an zentraler Stelle ist damit erfüllt. Die veröffentlichten Regelungen und Erläuterungen sind geeignet, bei den für die Organisation der Schriftgutvernichtung verantwortlichen Stellen das notwendige Problembewußtsein herzustellen und sie bei der Entwicklung eines angemessenen Entsorgungskonzeptes für ihren Bereich zu unterstützen.

Gleichwohl kann ich immer noch nicht feststellen, daß die Probleme bei der Schriftgutvernichtung in der hamburgischen Verwaltung behoben sind. Dies will ich mit einem Beispiel belegen.

Wie meine Umfrage vom April 1987 bei allen Hamburger Behörden gezeigt hatte, bedienten sich seinerzeit 27 öffentliche Stellen zur Schriftgutvernichtung eines Auftragnehmers, der - obwohl als juristische Person privaten Rechts organisiert - gem. § 3 Abs. 3 HmbDSG meiner Kontrolle als Datenschutzbeauftragter unterlag, weil er zu 100% im Eigentum der FHH stand und für Auftraggeber tätig war, die als öffentliche Stellen der FHH den Bestimmungen der §§ 16-23 HmbDSG unterliegen. Seinerzeit firmierte dieser Auftragnehmer mit „Hamburger Arbeit Beschäftigungsgesellschaft mbH (HAB)". Zwischen den Auftraggebern und dem Auftragnehmer waren keine schriftlichen Verträge geschlossen worden, und die Auftraggeber hatten dem Auftragnehmer auch keine Weisungen hinsichtlich der Behandlung des Schriftgutes und der zu treffenden Sicherheitsvorkehrungen erteilt, wozu sie gem. § 3 Abs. 2 und 3 HmbDSG verpflichtet sind. Es hatte sich auch kein Auftraggeber bei der HAB über die dortigen Gegebenheiten und Betriebsabläufe informiert.

Inzwischen sind im Zuge einer Umorganisation bei der HAB einige Betriebsteile, darunter die Schriftgutvernichtung, ausgegliedert und von einer neu gegründeten Firma, der „HamburgWest Beschäftigungsgesellschaft mbH (HWB)", übernommen worden. Auch die HWB gehört zu 100% der FHH. Die öffentlichen Stellen, die ihr zu vernichtendes Schriftgut bis dahin der HAB überlassen hatten, haben ohne besondere Umstände ihr Schriftgut nun der HWB anvertraut.

Im Dezember 1988 habe ich geprüft, welche technische Ausstattung der HWB für die Schriftgutvernichtung zur Verfügung stand und wie der Transport, die Lagerung, die Bearbeitung und schließlich die Vernichtung des Materials organisiert waren. Dabei habe ich festgestellt, daß die HWB ihre Auftragnehmer nicht informiert hatte, als sie wegen Stillegung ihres Shredders zur Vernichtung von Schriftgut selbst gar nicht mehr in der Lage war, und daß sie deshalb - ohne Kenntnis der Auftraggeber - das Material an einen gewerblichen Altpapiervernichter als Subunternehmer weitergab, mit dem sie ebensowenig einen schriftlichen Vertrag geschlossen hatte wie mit den Auftraggebern. Das habe ich als schwerwiegenden Verstoß gegen datenschutzrechtliche Grundsätze gewertet. Für diesem Vertoß sind jedoch auch die Auftraggeber verantwortlich, worauf ich weiter unten zurückkommen werde.

Ich will an dieser Stelle auf meine Prüfungsfeststellungen bei der HWB nicht weiter eingehen, weil ich den Eindruck gewonnen habe, daß die HWB nunmehr bemüht ist, die ordnungsgemäße Durchführung der Schriftgutvernichtung sicherzustellen. Jedenfalls ist sie meinen zur Beseitigung der gravierenden Mängel erhobenen Forderungen nachgekommen, soweit deren Erfüllung von ihr abhing. So hat sie insbesondere Geldmittel für die Anschaffung eines neuen leistungsfähigen Shredders eingeworben, und diese Mittel sind bewilligt worden. Sie hat sämtliche Auftraggeber mit Rundschreiben vom 25.7.89 über die bei ihr vorhandene technische Ausstattung und die Tatsache, daß ein Subunternehmer eingeschaltet wird, informiert, und sie hat mit einem dem Rundschreiben beigefügten Vertragsmuster den Ablauf bei der Vernichtung zutreffend

beschrieben. Gleichzeitig hat sie den Auftraggebern ein Angebot zum Abschluß eines Vertrages nach dem übersandten Muster unterbreitet. An dem Entwurf dieses Vertrages war ich beteiligt. Er entspricht den aus datenschutzrechtlicher Sicht zu stellenden Anforderungen.

Der von der HWB angebotene Vertrag ist nicht identisch mit dem in den MittVw veröffentlichten Mustervertrag, er stellt aber eine zulässige Variante dar. Die Abweichungen sind dadurch begründet, daß die HWB wegen ihrer besonderen sozialpolitischen Ziele (Schaffung von Arbeitsgelegenheiten für Personen mit besonderen Schwierigkeiten auf dem Arbeitsmarkt) nicht bloß die unverzügliche Vernichtung des Schriftgutes betreiben, sondern das zur Vernichtung bestimmte Material vorher noch bearbeiten will, um es dem Recycling zuführen zu können und damit auch einen Beitrag zum Umweltschutz zu leisten. Wenn das ausgesonderte Schriftgut der Behörden nicht wegen eventueller besonderer Sensibilität oder Geheimhaltungsbedürftigkeit der gespeicherten Daten von vornherein für eine Vernichtung durch die HWB ausscheidet, was jede Behörde eigenverantwortlich zu prüfen hat, dann ist - bei Einhaltung der von der HWB zugesicherten Abläufe und Vorkehrungen - eine datenschutzrechtlich einwandfreie Schriftgutvernichtung auch dort möglich. Diese Aussage entbindet die Behörden jedoch nicht von ihrer Verpflichtung, selbst in angemessenen Abständen die Auftragsdurchführung bei dem Auftragnehmer und ggf. dem Subunternehmer zu kontrollieren.

Ich hätte nach der Veröffentlichung in den MittVw und nach dem Rundschreiben der HWB erwartet, daß bei allen öffentlichen Stellen, die Schriftgut durch Auftragnehmer vernichten lassen, nun vollständige Klarheit über ihre Pflichten besteht und daß sie die Auftragsverhältnisse unverzüglich angemessen und schriftlich regeln würden. Umso bedenklicher finde ich die Tatsache, daß nach einer mir von der HWB übersandten Liste mit Stand vom 13.10.89 immerhin neun ihrer Auftraggeber immer noch keinen schriftlichen Vertrag mit ihr geschlossen und auch nicht in anderer Form Weisungen zur Behandlung des Schriftgutes erteilt haben. Mir ist nicht bekannt, ob sich schon eine der auftraggebenden Stellen einmal vor Ort darüber informiert hat, wie die Gegebenheiten und Arbeitsabläufe bei der HWB aussehen.

Abschließend will ich folgendes noch einmal klarstellen:

Die Verantwortung für die ordnungsgemäße Vernichtung nicht mehr benötigten Schriftgutes trägt bis zuletzt die speichernde Stelle. Sie hat die Vernichtung zu organisieren. Bedient sie sich dabei eines Auftragnehmers, so hat sie gem. § 3 Abs. 1 HmbDSG bei der Auswahl des Auftragnehmers besondere Sorgfaltspflichten. Sie muß vor Auftragserteilung die von dem potentiellen Auftragnehmer in seinem Betrieb getroffenen technischen und organisatorischen Maßnahmen hinsichtlich ihrer Eignung zur Datensicherung (s. § 8 Abs. 1 HmbDSG) prüfen.

Sie muß gem. § 3 Abs. 2 HmbDSG dem Auftragnehmer Weisungen zur Behandlung des Schriftgutes erteilen, denn ein Auftragnehmer darf Datenverarbeitung nur getreu ihm erteilter Weisungen betreiben (§ 3 Abs. 2 Satz 2 HmbDSG, § 37 BDSG). Deshalb muß die Initiative zur Gestaltung des Auftragsverhältnisses vom Auftraggeber ausgehen, er darf nicht abwarten und darauf hoffen, daß der Auftragnehmer das Verfahren schon angemessen und sicher organisieren wird. Und schließlich hat er durch Kontrollen die Einhaltung seiner Weisungen zu überwachen.

3. Einzelne Probleme des Datenschutzes im öffentlichen Bereich

3.1 Sozialwesen

3.1.1 Der Modellversuch ist tot, aber die Datenverarbeitung geht weiter

Schwerpunkt meiner Beratungstätigkeit im Bereich der Sozialversicherung war im abgelaufenen Berichtsjahr immer noch das Projekt der Krankenkassen, Daten von

Krankenhauspatienten zu speichern und auszuwerten, das als „Hamburger Modellversuch Krankenhäuser" bekannt geworden ist und zu dem ich bereits in meinem 7. TB (4.1.2, S. 33) Stellung genommen habe.

Ziel des Modellversuchs, an dem sich die gesetzlichen Krankenkassen aller Kassenarten für 3 Jahre beteiligen wollten, war die Schaffung von mehr Transparenz über die Struktur des Leistungsangebots und über die Merkmale der Patienten als Nachfrager der Leistung. Beim Vertrauensärztlichen Dienst, der seit September zum Medizinischen Dienst der Krankenkassen umgestaltet ist, sollte eine Datensammlung geschaffen werden, auf deren Grundlage Notwendigkeit und Dauer der stationären Behandlung überprüft werden konnten, in der Erwartung, Verweildauer und Kosten senken zu können. Darüber hinaus erhoffte man sich Erkenntnisse für die Beratung der Krankenkassen bei Pflegesatzverhandlungen, Krankenhausbedarfsplanungen und Großgeräteplanungen.

Die erforderlichen Versichertendaten sollten dem Medizinischen Dienst durch Umleitung des Datenflusses zwischen Krankenhäusern und Krankenkassen über ein eigens für den Modellversuch eingerichtetes Krankenhausdezernat zukommen, das mit Ärzten und Datenerfassungskräften ausgestattet wurde. Für jeden Behandlungsfall sollten sich die Krankenhäuser vertraglich verpflichten, Aufnahme- und Entlassungsanzeigen über den Medizinischen Dienst an die Krankenkassen zu liefern. Darüber hinaus war die Vereinbarung eines Verweildaueranhaltszahlenkatalogs geplant, wobei für jeden Patienten, der die seiner Diagnose zugeordnete Standardverweildauer zu überschreiten drohte, eine Verlängerungsanzeige mit Begründung für die Notwendigkeit des längeren Aufenthalts fällig werden sollte.

Nach dem ursprünglichen Konzept des Modellversuchs war vorgesehen, daß sich der Medizinische Dienst aus dieser zentralen Datensammlung für stationär behandelte Versicherte aller beteiligten gesetzlichen Krankenkassen noch während des Aufenthalts der Patienten im Krankenhaus Einzelfälle aussucht, um Notwendigkeit und Dauer der Krankenhausbehandlung zu prüfen und so den Krankenkassen zu ermöglichen, auf die Verweildauer im konkreten Einzelfall Einfluß zu nehmen. Neben der Einzelfallprüfung sollten die Daten klinik- und abteilungsvergleichend ausgewertet werden, z.B. um überdurchschnittliche Verweildauern und Fehlbelegungen aufzuspüren.

Als Modellversuch auf vertraglicher Grundlage ist das Projekt inzwischen gescheitert, da die Krankenkassenverbände und die Krankenhausträger bei ihren Verhandlungen über das Konzept des Vorhabens keine Einigung erzielen konnten, wofür neben datenschutzrechtlichen Fragen vor allem fachliche und berufsrechtlicher Einwände ausschlaggebend waren. Das Scheitern des Modellversuchs, noch ehe er richtig begonnen hatte, bedeutet aber nicht, daß sich damit die datenschutzrechtliche Problematik erledigt hat. Die Krankenkassen verfolgen vielmehr das Projekt in seinen wesentlichen Grundzügen weiter. Daß als Rechtsgrundlage anstelle der ursprünglich geplanten vertraglichen Vereinbarung das SGB V direkt Anwendung findet, ist für die datenschutzrechtliche Beurteilung irrelevant. Vertragliche Regelungen, wie sie im Rahmen der Selbstverwaltung im Recht der gesetzlichen Krankenversicherung einen breiten Raum einnehmen, können erforderliche gesetzliche Eingriffsgrundlagen weder ersetzen noch außer Kraft setzen. Eine gesetzliche Regelung zumindest der wesentlichen Eingriffsvoraussetzungen ist immer dann notwendig, wenn Grundrechtspositionen Dritter tangiert sind.

Durch die Offenbarung von Patientendaten einschließlich Diagnose und Dauer des Krankenhausaufenthalts wird das informationelle Selbstbestimmungsrecht des Patienten eingeschränkt. Das SGB V erlaubt den Krankenhäusern die Weitergabe bestimmter Daten an die Krankenkassen, nicht aber an den Medizinischen Dienst. Deshalb mußte das Konzept des Modellversuchs so geändert werden, daß die zuständigen Krankenkassen Empfänger der Entlassungsanzeigen bleiben. Die Auswahl der Einzelfälle, die mit dem Ziel der Überprüfung der Leistungspflicht dem Medizinischen Dienst zu Begutachtung vorgelegt werden sollen, muß von der Krankenkasse getroffen wer-

den. Beim Medizinischen Dienst darf keine kassenübergreifende Zentraldatei mit medizinischen Daten entstehen.

Diese rechtlichen Vorgaben für die Datenverarbeitung werden durch das Scheitern des Modellversuchs nicht berührt. Es kann deshalb auf den Lösungsansätzen aufgebaut werden, die für den Modellversuch entwickelt wurden. So haben die Krankenkassen auf Grund meiner datenschutzrechtlichen Bedenken eine gemeinsame Datenverarbeitungsstelle der Krankenversicherungen in Form einer Arbeitsgemeinschaft gegründet. Sie betreibt Auftragsdatenverarbeitung für die einzelnen Krankenkassen. Bis zur Abstimmung eines Datensicherungskonzepts speichert sie aus den Entlassungsanzeigen lediglich einen reduzierten Datensatz ohne Namen, Geburtsdatum und Anschrift des Patienten zum Zwecke statistischer Auswertungen für Pflegesatzverhandlungen und Bedarfsplanung. Zukünftig ist eine zeitlich befristete Speicherung personenbezogener Daten in Einzeldateien der jeweils zuständigen Krankenkassen vorgesehen, die der Auswahl geeigneter Einzelfälle für eine Beteiligung des Medizinischen Dienstes dienen soll. Nach Ablauf von maximal 3 Monaten wird der Personenbezug der Daten gelöscht und der Datensatz in eine anonymisierte Gesamtdatei übernommen, die für statistische Auswertungen zu Verfügung steht.

Über Rechtsgrundlagen und Verfahren der Übermittlung von Verlängerungsbegründungen, die gegenüber Aufnahme- und Entlassungsanzeigen noch sensiblere und detailliertere Informationen über den Gesundheitszustand des Patienten enthalten, müssen noch Gespräche mit den Krankenkassen, den Krankenhausträgern und der Ärztekammer geführt werden. Aus datenschutzrechtlicher Sicht ist die rechtliche Grundlage im SGB V für die Offenbarung dieser Daten problematisch, da zwar den Krankenkassen die Erhebung der erforderlichen Informationen zur Prüfung der Leistungspflicht und zur Beteiligung des Medizinischen Dienstes erlaubt ist, aber für die Krankenhäuser eine korrespondierende Befugnis zur Offenbarung der Daten fehlt. Ausdrücklich erlaubt ist den Krankenhäuser nach der Regelung des § 301 SGB V lediglich die Übermittlung von Aufnahme- und Entlassungsdiagnose, Aufnahme- und Entlassungsgrund sowie Aufnahme- und Entlassungstag des Patienten.

Ich neige der Auffassung zu, daß dieser Datenkatalog die Datenübermittlung zwischen Krankenhäusern und Krankenkassen abschließend regelt. Dagegen wollen die Krankenkassen aus ihrer Verpflichtung zur wirtschaftlichen Leistungserbringung und aus ihrer Befugnis zur Datenerhebung eine Verpflichtung der Krankenhäuser zur Offenbarung weiterer Patientendaten herleiten, zumindest wenn sich im Einzelfall Zweifel an der Leistungspflicht ergeben. Daß im Einzelfall zusätzliche Informationen zur Aufgabenerfüllung benötigt werden, ist ohne weiteres nachvollziehbar, eine normenklare Regelung fehlt aber im SGB V. Was die Übermittlungsregelungen für Patientendaten angeht, hat der Gesetzgeber die ihm gestellte Aufgabe nur mangelhaft erfüllt, was angesichts des hektischen Gesetzgebungsverfahrens nicht verwundern kann. Konsequenterweise ist eine Novellierung des SGB V zu fordern, mit der die Übermittlungsbefugnisse der Leistungserbringer klar geregelt werden.

3.1.2 Projekt Sozialhilfe-Automation (PROSA)

Ich habe im letzten Tätigkeitsbericht über das geplante Verfahren berichtet und die damit verbundenen Risiken für das informationelle Selbstbestimmungsrecht der Hilfeempfänger/innen dargestellt (7. TB, 4.1.6, S. 36).

Der vom Senat der Projektgruppe vorgegebene Zielrahmen ist inzwischen konkretisiert worden. Folgende Aufgabenbereiche sollen technisch unterstützt werden:

— Sozialhilfe nach dem Bundessozialhilfegesetz

— Kriegsopferfürsorge

— Verwandte Leistungen (Blindengeld, Garantiefonds usw.)

— Heranziehung Unterhaltspflichtiger

— Geltendmachung und Überwachung von Forderungen

— Nutzung und Verwaltung von Plätzen in Gemeinschaftsunterkünften und Hotels
— Nutzung und Verwaltung von orthopädischen Hilfsmitteln
— Darstellung des Regelwerks (z.B. Fachliche Weisungen, Gerichtsurteile)
— Kontrollfunktionen für Rechnungshof und Vorprüfungsstelle
— Abrechnung von Heimkosten mit nichtstaatlichen Alten- und Pflegeheimen
— Abrechnung von Krankenhilfekosten mit Kassenärztlichen Vereinigungen.

Über Schnittstellen sollen folgende Aufgabenbereiche mit PROSA verbunden werden:

— Erstellen des Regelwerks durch die BAGS
— Abwicklung des Kassen- und Rechnungswesens durch die Landeshauptkasse
— Verfahren bei der Geltendmachung von Wohngeldansprüchen für Sozialhilfeempfänger
— Aufbereitung der Daten für die Bundessozialhilfestatistik durch das Statistische Landesamt
— Durchführung von Rechtsmittelverfahren in Sozialhilfeangelegenheiten durch die Rechtsämter der Bezirksämter und die Rechtsabteilung der BAGS
— Rentenauskunftsverfahren der Deutschen Bundespost

An der Ausgestaltung dieser Kommunikationsbeziehungen wird von der Projektgruppe im Rahmen des Fachkonzeptes zur Zeit noch gearbeitet.

Die vom Senat eingesetzte Lenkungsgruppe hat inzwischen ein Konzept zur technischen Durchführung von PROSA beschlossen. Dieses Konzept sieht die Entwicklung eines Bildschirm-Dialogverfahrens vor, das zentral durch die Datenverarbeitungszentrale der Finanzbehörde (DVZ) zur Verfügung gestellt werden soll.

Diese Entscheidung für eine „zentrale Lösung" ist vom Senat u.a. damit begründet worden, daß zwar keine Form der Verarbeitung von Daten ohne Risiko sei, jedoch in der DVZ alle jene Sicherheitsmaßnahmen konzentriert seien, die dieses Risiko am ehesten beherrschbar machten. Der dort vorhandene Sicherheitsstandard sei vergleichbar und zu vertretbaren Preisen in dezentralen Rechenstellen zur Zeit nicht herstellbar. Ich hatte im Verlauf der Diskussion darauf hingewiesen, daß gegen keine der beiden in Frage kommenden Lösungen prinzipielle datenschutzrechtliche Bedenken bestehen, sofern der erforderliche Sicherheitsstandard gewährleistet wird. Da die Verwaltung aber bisher kein vergleichbares Projekt mit verteilter Rechnerleistung realisiert hat, kann nicht beurteilt werden, ob es ihr gelingen würde, die damit verbundenen technischen und organisatorischen Probleme zu bewältigen.

Eine weitergehende Beurteilung des Projektes ist mir erst möglich, wenn das Fachkonzept vorliegt, in dem u.a. festgelegt wird, welche Daten künftig automatisiert gespeichert werden und in welchem Umfang Dritte Zugriff auf diese Daten haben sollen.

3.1.3 Richtlinien zum Bewilligungsverfahren bei medikamentengestützten Drogentherapien

Ich habe in der Vergangenheit wiederholt gefordert, die Aktenführung in Sozialdienststellen zu ändern, und zwar in der Weise, daß Gesundheitsangelegenheiten in einer gesonderten Akte geführt werden, damit insbesondere bei Aktenvorlage an andere Dienststellen oder bei Aktenübersendungen an Gerichte - mit Einsichtsmöglichkeiten durch die Verfahrensbeteiligten - Gesundheitsdaten entfernt werden können, wenn ihre Kenntnis im konkreten Zusammenhang nicht erforderlich ist. Ich habe die Behörde für Arbeit, Gesundheit und Soziales (BAGS) nunmehr aufgefordert, die Trennung der Akten bis spätestens Ende Februar 1990 vorzunehmen.

In Gesundheitsangelegenheiten öffentlich Bediensteter (Beihilfe) ist die Notwendigkeit einer Trennung von der Personalakte längst anerkannt und entsprechend umgesetzt worden.

Meine Forderung, einen vergleichbaren Schutz von Gesundheitsdaten auch Sozialhilfeempfängern zu gewähren, hat im Berichtszeitraum besondere Aktualität bekommen. Durch eine Presseveröffentlichung erfuhr ich von der sog. „Richtlinie zum Bewilligungsverfahren bei medikamentengestützten Drogentherapien". Diese Richtlinie sieht im Zusammenhang mit einer Fachlichen Weisung der BAGS u.a. folgendes vor:

Nicht krankenversicherte Drogenabhängige bekommen - wie andere Hilfeempfänger auch - gem. § 37 Bundessozialhilfegesetz (Krankenhilfe) einen Behandlungsschein, der dokumentiert, daß das Sozialamt die Kosten übernimmt. Der behandelnde Arzt reicht diesen Behandlungsschein der Kassenärztlichen Vereinigung (KV) ein, die dann wiederum mit der BAGS (Landessozialamt - Rechnungsstelle -) abrechnet. Die KV stellt den Gesamtbetrag der erbrachten Leistungen in Rechnung, rechnet also nicht personenbezogen ab. Die Behandlungsscheine werden der BAGS übersandt und dort archiviert. Eine einzelfallbezogene Prüfung findet in der Regel nicht statt. Dieses Verfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Problematisch wird das Abrechnungsverfahren dann, wenn Drogenabhängige (was regelmäßig der Fall ist oder jedenfalls sein sollte) begleitend zur ärztlichen Behandlung psychosozial betreut werden. Die Stellen, die diese Betreuung übernehmen, haben ihre Kosten einzelfallbezogen direkt mit der BAGS abzurechnen. Die zitierte Richtlinie der BAGS sieht nun vor, daß das Landessozialamt die Rechnungen bezahlt und sie danach zu den einzelnen Sozialamtsakten weiterreicht, damit (erst) dort die sachliche und rechnerische Richtigkeit geprüft wird. Die Abrechnungen sollen in der Akte verbleiben.

Es ist offensichtlich, daß bei diesem Verfahren die gesetzlich vorgeschriebene Geheimhaltung nicht gewährleistet werden kann: Nach § 203 Abs. 1 StGB werden u.a.

— Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,

— Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist und

— staatlich anerkannte Sozialarbeiter und staatlich anerkannte Sozialpädagogen

bestraft, wenn sie unbefugt ihnen anvertraute Geheimnisse offenbaren. Geheimnis im Sinne dieser Vorschrift ist regelmäßig schon die Tatsache, daß sich eine bestimmte Person mit der Bitte um Beratung/Behandlung an sie gewandt hat.

Unzweifelhaft unterliegen deshalb die hier in Rede stehenden Abrechnungen von Drogenberatern dem Schutz von § 203 StGB. Diese Abrechnungen enthalten personenbezogene Daten der behandelten Drogenabhängigen, die von den Beratern nur mit Einwilligung der Betroffenen weitergegeben werden dürfen, da es für Drogenberater eine gesetzliche Offenbarungsbefugnis zu Abrechnungszwecken nicht gibt.

Da die Schweigepflicht der Berater sich auf den Sozialleistungsträger, der die Daten zu Abrechnungszwecken übermittelt bekommt, erstreckt (§ 76 Sozialgesetzbuch X), dürfen diese Daten ausschließlich im Rahmen der erteilten Einwilligung verarbeitet werden. Anfang August war ich mit der BAGS noch darüber einig, daß bei dem derzeitigen Verfahren nicht gewährleistet ist, daß Unbefugte (z.B. Polizei, Gerichte) keinen Zugriff auf diese Daten nehmen. Die BAGS hatte deshalb zugesagt, bis zur 2. Septemberhälfte eine Entscheidung für ein datenschutzkonformes Verfahren zu treffen. Diese Entscheidung steht leider immer noch aus. Die BAGS prüft zur Zeit, ob der sozialhilferechtliche Vollzug bei der Drogenberatungsstelle der BAGS (RE) angesiedelt werden kann. Ich würde dies begrüßen.

3.1.4 Mitteilung des Sozialhilfebezuges an unterhaltspflichtige Dritte

Es beschweren sich immer wieder Sozialhilfeempfänger darüber, daß Sozialämter unterhaltspflichtigen Dritten (Verwandte, Geschiedene oder getrennt lebende Ehepartner) die Höhe der ihnen gewährten Sozialhilfe mitteilen.

So belastend dies auch für die betroffenen Hilfeempfänger ist, die u.a. befürchten müssen, daß damit ihre finanzielle Bedürftigkeit einem unüberschaubar großen Personenkreis bekannt wird, kann ich in diesen Fällen leider nicht helfen.

Die Rechtslage ist eindeutig:

Eine Durchbrechung des in § 35 SGB I (Sozialgesetzbuch) normierten Sozialgeheimnisses, das die Sozialämter grundsätzlich zur Verschwiegenheit verpflichtet, ist u.a. gem. § 69 Abs. 1 Nr. 1 SGB X zulässig, soweit dies erforderlich ist für die Erfüllung gesetzlicher Aufgaben nach dem Bundessozialhilfegesetz (BSHG).

Eine solche gesetzliche Aufgabe des Sozialamtes ist es, Unterhaltsansprüche, die Hilfeempfänger gegen Dritte haben, auf den Träger der Sozialhilfe, die Freie und Hansestadt Hamburg, überzuleiten (§ 90 BSHG). Die „Überleitungsanzeige", die den Unterhaltspflichtigen zugeht, bewirkt den Übergang des Unterhaltsanspruches bis zur Höhe der Aufwendungen des Sozialamtes.

Diese Rechtslage macht es erforderlich, den Unterhaltspflichtigen die Höhe des Sozialhilfebezuges mitzuteilen. Auf die Unterhaltsfähigkeit kommt es dabei zunächst nicht an.

Nach Auskunft von Sozialämtern kommt es im übrigen relativ häufig vor, daß Unterhaltspflichtige sich nach Erhalt der Überleitungsanzeige zur Zahlung in Höhe des mitgeteilten Sozialhilfebezuges verpflichten. In diesen Fällen müssen sie selbst ihre Einkommens- und Vermögensverhältnisse dem Sozialamt nicht offenbaren, weil eine Prüfung ihrer Unterhaltsfähigkeit durch das Sozialamt entfällt.

3.1.5 Schweigepflichtentbindung im Verfahren nach dem Schwerbehindertengesetz

Im 6. Tätigkeitsbericht (6. TB, 4.16.4, S. 115) hatte ich über Verhandlungen mit dem Versorgungsamt zum Thema Schweigepflichtentbindungserklärung im Verfahren nach dem Schwerbehindertengesetz berichtet. Als Ergebnis dieser Gespräche wurde in die Antragsvordrucke für den Erstantrag und den Neufeststellungsantrag nach dem Schwerbehindertengesetz eine neue Fassung der Schweigepflichtentbindung aufgenommen, mit der deutlich wurde, daß das Versorgungsamt nur die zur Aufgabenerfüllung wirklich benötigten Informationen bei dritten Stellen anfordern darf.

Auch die Anschreiben, mit denen das Versorgungsamt Unterlagen bei Ärzten, Krankenhäusern und sonstigen Einrichtungen unter Hinweis auf die vorliegende Einwilligung anfordert, sollten überarbeitet werden. Durch eine Eingabe wurde mir bekannt, daß das Versorgungsamt die mir damals gemachten Zusagen nur zum Teil umgesetzt hat:

Das Formschreiben, mit dem Unterlagen bei anderen Stellen als Krankenhäusern und niedergelassenen Ärzten angefordert wurden, wurde nicht - wie vereinbart - an den neuen Text der Einwilligungsklausel angepaßt, und auch die Klausel wurde nicht abgedruckt. So wurde die Hamburger Werkstatt für Behinderte GmbH vom Versorgungsamt aufgefordert, die bei ihr vorhandenen „Versicherungs-, Betreuungs-, Gesundheits-, Personal- und Heilverfahrensakten" von behinderten Arbeitnehmern zu übersenden. Es wurde versichert, daß eine entsprechende Einverständniserklärung des jeweiligen Antragstellers vorliege.

Die Werkstatt hatte - zu Recht - Zweifel, daß die Übersendung der angeforderten Akten zur Aufgabenerfüllung des Versorgungsamtes erforderlich sei und bat deshalb in einem Fall darum, die dem Auskunftsersuchen zugrundeliegende Einverständniserklärung des Behinderten zu übersenden.

Das Versorgungsamt teilte der Werkstatt daraufhin mit, daß die Erklärung drucktechnisch Bestandteil des Antragsvordrucks sei und deshalb nicht übersandt werden könne (der Gedanke, eine Kopie zu übersenden, kam dem Versorgungsamt ganz offensichtlich nicht). Im übrigen, so das Versorgungsamt weiter, werde im Schrifttum zum Verwaltungsverfahrensrecht einhellig die Auffassung vertreten, daß bei Auskunftsersuchen

von Behörden deren Erklärung genüge, daß ihnen eine Einverständniserklärung vorliege. Die Werkstatt wurde - ohne daß das Auskunftsersuchen auf die Unterlagen beschränkt wurde, für deren Anforderung der Antragsteller tatsächlich seine Zustimmung erklärt hatte - gebeten, die Übersendung der Unterlagen nunmehr baldmöglichst zu veranlassen.

Erst nachdem sich die Werkstatt weiterhin hartnäckig weigerte, die angeforderten Akten zu übersenden, wurden ihr vom Versorgungsamt die Unterlagen genannt, die zur Aufgabenerfüllung erforderlich waren.

Die BAGS erklärte das Vorgehen des Versorgungsamtes damit, daß seinerzeit versehentlich versäumt worden sei, das Formblatt zu ändern. Dieses Versäumnis werde umgehend nachgeholt. Ich gehe davon aus, daß der neue Vordruck die Schweigepflichtentbindungserklärung, wie sie von den Antragstellern unterschrieben wird, enthalten wird.

Nur so haben die angeschriebenen Stellen die Möglichkeit zu prüfen, ob und in welchem Umfang die Übermittlung medizinischer Daten auf der Grundlage dieser Erklärung zulässig ist.

Der Fall hat u.a. deutlich gemacht, daß es offenbar nicht ausreicht, datenschutzkonforme Lösungen mit der Verwaltung zu erarbeiten. Mehrfach hat es sich leider als erforderlich erwiesen, die praktische Umsetzung zu kontrollieren.

3.1.6 ODIN

Die Unfallversicherungsträger planen die Einrichtung eines Organisationsdienstes für nachgehende Untersuchungen (ODIN) für die zentrale Erfassung von Versicherten, die bei ihrer beruflichen Tätigkeit krebserzeugenden Gefahrstoffen ausgesetzt sind bzw. waren.

Die Landesunfallkasse hat mich um Stellungnahme gebeten, ob gegen einen Beitritt zum ODIN-Verfahren datenschutzrechtliche Bedenken bestehen. Meine Prüfungen führten zu dem Ergebnis, daß für die Datenverarbeitung eine ausreichende gesetzliche Grundlage fehlt.

Im Rahmen des ODIN-Verfahrens soll eine Vielzahl sensibler personenbezogener Daten durch den Arbeitgeber, die Landesunfallkasse und die Berufsgenossenschaft Chemie verarbeitet werden. Mit der Erhebung, Speicherung und Übermittlung dieser Daten wird in das informationelle Selbstbestimmungsrecht des Arbeitnehmers eingegriffen, wofür nach der Rechtsprechung des Bundesverfassungsgerichts eine bereichsspezifische gesetzliche Grundlage erforderlich ist, aus der sich die Voraussetzungen und der Umfang des Eingriffs für den Bürger klar erkennbar ergeben müssen. Diese Anforderungen erfüllen weder die §§ 28 ff. Gefahrstoffverordnung mit den Regelungen über die Vorsorgeuntersuchung noch § 21 Chemikaliengesetz mit der darin normierten Auskunftspflicht. Beide lassen eine Übermittlung der für das ODIN-Verfahren benötigten Daten an die Berufsgenossenschaft nicht zu. Auch auf die aufgrund von § 708 RVO erlassenen Unfall-Verhütungs-Vorschriften kann die Datenverarbeitung nicht gestützt werden. Eingriffe in das informationelle Selbstbestimmungsrecht müssen in den Grundzügen gesetzlich geregelt sein, Satzungen reichen als Rechtsgrundlage allein nicht aus. Sie beziehen sich zudem nur auf die Mitglieder der Unfallversicherung, während im ODIN-Verfahren auch Daten früherer Mitglieder verarbeitet werden sollen.

Schließlich bietet auch die Änderung des § 96 Abs. 3 SGB X im Rahmen des Gesundheitsreformgesetzes keine inhaltliche Rechtsgrundlage für die geplante Datenverarbeitung. Zwar wird den Unfallversicherungsträgern ausnahmsweise zugestanden, eine Zentraldatei für Daten ärztlich untersuchter Leistungsempfänger zu bilden, diese bedarf jedoch inhaltlich einer spezialgesetzlichen Rechtsgrundlage.

Wegen der fehlenden rechtlichen Grundlagen halte ich das ODIN-Verfahren für datenschutzrechtlich unzulässig und habe deshalb der Landesunfallkasse empfohlen, dem Verfahren nicht beizutreten.

3.2 Personalwesen

3.2.1 IuK-Projekte in der Personalverwaltung

Seit meinem letzten Bericht wurde die Voruntersuchung zum „Projekt Personalwesen" abgeschlossen und die Umsetzung der Zentralisierung der Beihilfefestsetzung begonnen.

— die Voruntersuchung zur Reorganisation der Hamburgischen Personalverwaltung - Projekt Personalwesen - enthält eine ausführliche Bestandsaufnahme der gegenwärtigen Arbeitsabläufe in Personalabteilungen und der Besoldungs- und Versorgungsstelle. In einer Schwachstellenanalyse offenbart sie auch Mängel im Datenschutz und fordert z.B. die Abkoppelung der Kindergeldbearbeitung von der übrigen Personalverwaltung. Ferner wird darauf hingewiesen, daß bei der Versendung von Vordruck-Durchschriften an andere Dienststellen zuweilen mehr übermittelt wird, als für die Aufgabenerfüllung des Empfängers erforderlich ist - z.B. in Ernennungsverfahren. Auch die Ablage vollständiger Pfändungs- und Abtretungsvorgänge in den Personalabteilungen wird zu Recht als nicht notwendig bezeichnet. Ich begrüße die selbstkritische Sicht und hoffe, daß sie auch bei der anstehenden Detailplanung und zukünftigen Umsetzung der Reorganisation anhält. Meine Anmerkungen im 6. TB (4.2.3, S. 38) zur Personalstrukturdatei wurden im entsprechenden Kapitel des Voruntersuchungsberichts noch nicht aufgegriffen.

  Für die weitere Projektdurchführung schlägt das Personalamt die Einrichtung eines Projektausschusses vor, dem auch ein Mitarbeiter des Hamburgischen Datenschutzbeauftragten angehören soll. Besondere Aufmerksamkeit werde ich etwa auf die angekündigte Erweiterung der Datenbasis, auf die Zugriffsregelungen und die Möglichkeit zentraler Datenauswertungen richten. Nach meinem Eindruck sind z.B. personalplanerische und personalpolitische Aufgaben auch mit anonymisierten, aggregierten Daten zur erfüllen. In jedem Falle muß eine Bildung von Persönlichkeitsprofilen durch Verknüpfung aller dann zentral verfügbaren Personaldaten eines Bediensteten vermieden werden. Die Gefahren und Risiken von umfassenden Personalinformationssystemen habe ich in meiner Funktion als Aufsichtsbehörde über den nicht-öffentlichen Bereich erfahren und beschrieben.

— Die Zentralisierung der Beihilfefestsetzung in der Besoldungs- und Versorgungsstelle ist im Berichtsjahr weiter fortgeschritten. Das Personalamt hat mir die umfangreiche Arbeitsanleitung für die EDV-Unterstützung der Beihilfesachbearbeiter, das Konzept der Zugriffsregelungen und eine Übersicht über die genutzten Dateien und Daten übersandt. Weitere Unterlagen wurden angekündigt. Das Angebot, die zentralisierte Beihilfefestsetzung im Rahmen einer Demonstrationsveranstaltung auch in der Praxis kennenzulernen, werde ich zur gegebener Zeit gerne annehmen. Auch wenn ich gegenwärtig keine Anhaltspunkte für Verstöße gegen Datenschutzbestimmungen habe, schließe ich nicht aus, das neue Verfahren zu einem späteren Zeitpunkt einer gesonderten Überprüfung zu unterziehen, wie ich es in diesem Jahr mit dem sogenannten Personalamtsverfahren getan habe.

  Der Senatsbeschluß zur Einführung der zentralen Beihilfefestsetzung stellt es dem Landesbetrieb Krankenhäuser frei, sich dem Verfahren bei der Besoldungs- und Versorgungsstelle anzuschließen. Tut er dies nicht, hat er die mit der Zentralisierung bezweckte Abschottung von Beihilfe-Sachbearbeitung und sonstiger Personalverwaltung auf andere Weise zu gewährleisten. In einem Gespräch mit dem Landesbetrieb habe ich für eine dezentrale Beihilfesachbearbeitung in den einzelnen Krankenhäusern folgende Anforderungen formuliert:

— Die Personalleiter als Beteiligte an Personalentscheidungen dürfen am Vorgang der Beihilfefestsetzung nicht mehr teilhaben. Sie dürfen insbesondere keine Kenntnise von den in den Rechnungen der Mitarbeiter enthaltenen Diagnosen erhalten.

— Die Beihilfesachbearbeiter dürfen nicht die Beihilfen von Mitarbeitern berechnen, deren Personalakten sie führen.

— Beihilfeanträge der Mitarbeiter müssen den Beihilfesachbearbeitern in verschlossenen, gekennzeichneten Umschlägen zugehen. Die Einblicknahme anderer, nicht an der Beihilfefestsetzung Beteiligter muß ausgeschlossen sein.

Als Alternative kommt eine Beihilfefestsetzung in der Zentrale des Landesbetriebs in Betracht, sofern die beteiligten Sachbearbeiter ausschließlich Beihilfen bearbeiten und nicht einem Vorgesetzten unterstellt sind, der zugleich Zugriff auf die Personalakten der Beihilfeantragsteller hat. Hier die Wahl zu treffen, ist nun Aufgabe des Landesbetriebes. Ich habe deutlich gemacht, daß eine Fortsetzung der gegenwärtigen Praxis, die jedenfalls zum Teil Beihilfe-Sachbearbeitung und Personalverwaltung nicht trennt, datenschutzrechtlich nicht mehr hinnehmbar ist. Nach einer telefonischen Auskunft kurz vor Redaktionsschluß dieses Berichts haben die Krankenhäuser den Personalabteilungsleitern die Einsicht in Beihilfeunterlagen inzwischen untersagt. Als endgültige Lösung wird jetzt doch der Anschluß an das zentrale BVSt-Verfahren erwogen.

3.2.2 PC-Anwendung im Personalwesen

Von einzelnen Personalräten und Dienststellenvertretern aus Bezirksämtern wurde ich darauf aufmerksam gemacht, daß die jeweilige Verwaltungsabteilung die Einführung von PC's in der Aus- und Fortbildungsabteilung und in der allgemeinen Verwaltung betreibt. Ich wurde gebeten, in das Mitbestimmungsverfahren datenschutzrechtliche Aspekte einzubringen. In Besprechungen mit der Verwaltungsabteilung von Bezirksämtern, Sachbearbeitern für das Aus- und Fortbildungswesen sowie mit den Personalräten der meisten Bezirksämter habe ich unter anderem auf folgende Grundsätze bei der Verarbeitung personenbezogener Daten auf PC's hingewiesen (vgl. auch 6. TB, 3.5, S. 26 ff): Inhaltlich ist zunächst der Zweck der Datenverarbeitung, d.h. die zu erfüllende gesetzliche Aufgabe möglichst genau festzulegen. Dem muß der Umfang der erhobenen und verarbeiteten Daten entsprechen. Zur Ausübung des Mitbestimmungsrechts muß sich der Personalrat nicht mit der Auskunft über die Art der Daten zufrieden geben, sondern kann den vollständigen Datensatz verlangen. Auch die Frage nach den konkreten Auswertungsmöglichkeiten ist mit dem Hinweis auf den Namen einer Standard-Software noch nicht beantwortet. Gerade die Anwendung moderner Datenbankverwaltungssysteme wirft hier Probleme auf: Um eine - technisch mögliche - zweckwidrige Nutzung wie die Verknüpfung gespeicherter Daten zu Persönlichkeits-Profilen zu verhindern, sollten die Sachbearbeiter jedenfalls dann keinen Durchgriff auf das Betriebssystem haben und sich die Auswertungsprogramme nicht selbst schaffen können, wenn mit demselben PC verschiedene Aufgaben von verschiedenen Personen erfüllt werden sollen. Nur bei Verwendung von compilierten Programmen in Verbindung mit einer strikten Menü-Steuerung lassen sich in diesen Fällen die Auswertungen so festlegen und begrenzen, daß auch der Personalrat eine ausreichende Grundlage für seine Mitbestimmungsentscheidung hat. Auch die Frage, wann die gespeicherten Daten wieder zu löschen sind und wie die Auskunfts -, Berichtigungs- und Sperrungsrechte des Betroffenen gewährleistet werden können, müssen geklärt werden. Ein weiterer wichtiger Bereich ist die technische und organisatorische Datensicherung besonders dann, wenn mehrere Personen womöglich mit verschiedenen Fachaufgaben denselben PC bedienen sollen. Hier sind durch Kennung und Passwort Zugriffskontrollen einzubauen, die jeden Sachbearbeiter auf „seinen" Daten-Pool beschränken. Ferner ist zu prüfen, ob nicht die Verwendung einer Festplatte die Risiken eines kaum kontrollierbaren Disketten-Verkehrs ausschließen kann. Angesichts der Sensibilität der Daten etwa im Aus- und Fortbildungsbereich (z.B. die Anwärter-Personalien einschließlich Krankheitsdaten) kann auch nicht jeder über die PC-Grundausstattung hinausgehende Sicherungsaufwand als unverhältnismäßig abgewehrt werden.

Insgesamt habe ich auf Grund meiner Kontakte zu Personalräten und Dienststellenvertretern aus der Praxis den Eindruck gewonnen, daß gerade die dezentrale PC-Einführung nicht selten vorschnell ohne das notwendige anwendungstechnische Know-how, vor allem aber ohne das erforderliche datenschutzrechtliche Wissen erfolgt. Ich zweifle auch daran, daß wirklich alle in Behörden und Ämtern auf PC geführten Dateien zum Register des Hamburgischen Datenschutzbeauftragten angemeldet wurden.

3.2.3 Ausfallzeiten-Statistik im Landesbetrieb Krankenhäuser

Der Landesbetrieb Krankenhäuser plant eine detaillierte EDV-Auswertung der Abwesenheits- und Ausfallzeiten aller Krankenhausmitarbeiter. Mit diesen Statistiken will der Landesbetrieb einerseits der Forderung der Krankenkassen nachkommen, Unterlagen für die Refinanzierung der Personalbedarfe bereitzustellen, und andererseits Grundlagen für eine zukünftige Personalbudgetierung schaffen. Jeder Mitarbeiter hat dazu einen Dienstzeitnachweis auszufüllen, der neben Namen, Kennziffer, Kostenstelle und Dienstart die tägliche Abwesenheitszeit wiedergibt, aufgeschlüsselt nach sechs vorgegebenen Abwesenheitsgründen (Urlaub, Krankheit, Fortbildung, Ausgleich für Schichtdienstler, Mutterschutz und sonstige Ausfallzeit). Dieser Nachweis geht beispielsweise beim Pflegedienstpersonal über die Stationsleitung und die Pflegedienstleitung des Krankenhauses an die Personalabteilung, die ihn einer Datenerfassungskraft weiterreicht. Diese nimmt Plausibilitätsprüfungen vor und veranlaßt die folgenden Auswertungen: Jahres- und Monatsübersichten über die Ausfallzeiten, aufgeschlüsselt 1. nach Krankenhaus/Abteilung/Kostenstelle, 2. nach den verschiedenen Dienstarten (Ärztlicher Dienst, Pflegedienst, Funktionsdienst usw.) und 3. nach den sechs Abwesenheitsgründen. So kann z.B. festgestellt werden, daß im Dezember 1989 im Krankenhaus X, Abteilung Y, im Ärztlichen Dienst wegen Fortbildung Z Stunden nicht für die Patientenbetreuung zur Verfügung standen. Angesichts des Detaillierungsgrades der Auswertungen werden nicht selten Einzelwerte auftauchen, die den Rückschluß auf bestimmte Personen zulassen.

In meiner Stellungnahme und einem Gespräch mit dem Landesbetrieb ging es zum einen um die datenschutzrechtliche Zulässigkeit, zum anderen um die Mitbestimmungspflichtigkeit dieses Verfahrens. Die krankenhausinterne Weitergabe des Dienstzeitnachweises offenbart nach der Zusicherung des Landesbetriebes den beteiligten Stellen keine Beschäftigtendaten, die nicht schon durch die Dienstplanaufstellung bzw. die Personalverwaltung bekannt sind. Die Plausibilitätskontrollen durch die Datenerfassungskraft dienen in erster Linie der Aufklärung logischer Widersprüche bei der Ausfüllung des Dienstzeitnachweises. Inwieweit die Plausibilitätskontrolle „Abweichung der gemeldeten Stundenzahl um mehr als 10% von der Soll-Stundenzahl" auch Elemente der Verhaltens- und Leistungskontrolle enthält, bedarf noch weiterer Klärung. In einem ersten Zwischenergebnis konnte Einigkeit darüber erzielt werden, daß zunächst nur die für die Krankenkassen-Anforderung notwendige Datenverarbeitung in Angriff genommen wird. Hierfür reicht die Jahresstatistik für das gesamte Krankenhaus aus, aufgeschlüsselt nach Dienstarten und Abwesenheitsgründen, wobei Daten, die Angaben von weniger als drei Personen zusammenfassen, nicht übermittelt werden sollen. Damit ist der Personenbezug ausgeschlossen, die Statistik anonym. Insoweit dürfte auch ein Mitbestimmungsrecht des Personalrats jedenfalls wegen der Einführung einer technischen Überwachungseinrichtung zur Verhaltens- und Leistungskontrolle nicht gegeben sein. Soweit die Statistiken einer Personalbudgetierung durch die Krankenhäuser dienen und dafür auch Einzeldaten enthalten sollen, wird die Auswertung zurückgestellt und zu gegebener Zeit das Gespräch mit dem Personalrat aufgenommen werden.

3.2.4 Bewerberfragebogen

In den Mitteilungen für die Verwaltung vom 11.8.89 (Seite 208) veröffentlichte das Personalamt die Musterformblätter „Fragebogen für Bewerberinnen und Bewerber" und „ergänzende Angaben zur Person der/des Einzustellenden". Sie entsprechen dem im 7. TB

(4.2.3, S. 46 ff) beschriebenen Diskussionsstand. Nach schwebenden Straf- oder Disziplinarverfahren sowie nach einem Führungszeugnis werden alle Beamten-Bewerber und „ausgewählte Bewerber" auf Angestellten-Positionen der Vergütungsgruppen Vb bis I BAT bzw. übertariflich beschäftigte Angestellte gefragt. Die vom Bundeszentralregister abgeleitete Einschränkung, daß nur Verfahren anzugeben sind, die „voraussichtlich zu einer Geldstrafe von 90 Tagessätzen oder einer Freiheitsstrafe von mehr als 3 Monaten führen", stößt bei den Personalverwaltungen der Behörden weitgehend auf Unverständnis. Wegen der nahezu unmöglichen Prognosen durch den eventuellen Täter selbst wird diese Regelung als unpraktikabel empfunden. 1987 hatte ich dem Personalamt objektive Maßstäbe zur notwendigen Einschränkung der Auskunftspflicht vorgeschlagen (6. TB, 4.2.2, S. 37): Beschränkung auf gerichtliche Verfahren und Vorsatztaten, bei Arbeitnehmern Begrenzung auf relevante Deliktstypen. Andere geeignete Kriterien wurden mir aus den Personalverwaltungen bisher nicht mitgeteilt.

Dennoch halte ich die nun veröffentlichten Bewerber - und Einzustellenden - Fragebögen für einen wirklichen Fortschritt gegenüber den bislang verwendeten behördenspezifischen Fragebögen. Das zweistufige Verfahren vermeidet die Abfrage sensibler Daten, wenn eine Einstellung nicht in Betracht kommt. Der Umfang der Fragen ist insgesamt stark reduziert worden. Es kommt nun darauf an, die Personalabteilungen der Behörden und Ämter zur Einleitung des Mitbestimmungsverfahrens nach § 87 Abs. 1 Hamburgisches Personalvertretungsgesetz zu bewegen, um die neuen Fragebögen auch tatsächtlich einzuführen. Ich beabsichtige, im nächsten Jahr alle Behörden nach dem Sachstand zu fragen und alle von den Musterformblättern abweichende Fragebögen datenschutzrechtlich zu überprüfen.

Bei der Anwendung der Muster-Fragebögen ist durchaus Raum für behördenspezifische Fragen, die besonderen Anforderungen bestimmter Arbeitsplätze Rechnung tragen (vgl. 7. TB, 4.2.3, S. 46 für das Heimpersonal). So habe ich mit Vertretern der Feuerwehr und der Innenbehörde Einigkeit über die von Bewerbern für den Feuerwehrdienst zu beantwortenden Fragen erzielt, die zum Teil von den Mustern des Personalamtes abweichen.

Auch mit der Polizei wurde eine derartige Diskussion aufgenommen. Als ein notwendiger Erörterungsgegenstand hat sich dort z.B. der handgeschriebene Lebenslauf herausgestellt. Ich meine, daß die für eine Bewerberauswahl notwendigen Daten bereits im Fragebogen enthalten sind (Schul- und Berufsausbildung), und sonstige - vom Bewerber selbst ausgewählte - Angaben grundsätzlich nicht relevant sind. Die Form des Lebenslaufes (Länge, Schreibstil, Auswahl, Schriftbild, Rechtschreibung) mag zwar weitere Aufschlüsse über die Persönlichkeit des Bewerbers offenbaren, ihre Deutung durch psychologisch nicht geschultes Personal ist hier jedoch kaum objektivierbar, kann weitgehend auf Vorurteilen beruhen und ist in ihrer Aussagekraft äußerst unsicher. Vor allem der Umstand, daß Lebensläufe von 16-20jährigen derzeit das ganze Berufsleben hindurch in der Personalakte verbleiben und in dieser Zeit von vielen Personen eingesehen werden, weckt erhebliche datenschutzrechtliche Bedenken. Sollte für die Bewerbung nicht grundsätzlich auf die Vorlage eines ausführlichen handgeschriebenen Lebenslaufes verzichtet werden, wäre zumindest eine Rückgabe nach der Auswahlentscheidung geboten.

3.2.5 Beihilfe bei Psychotherapien

Beihilfeleistungen für Psychotherapien erhält ein Bediensteter nur, wenn zuvor die Beihilfefähigkeit der Behandlung durch ein Gutachten festgestellt wurde. Anders als in den anderen Bundesländern erstellt in Hamburg ein Fachmediziner des personalärztlichen Dienstes dieses Gutachten aufgrund eines ausführlichen Berichts des Psychotherapeuten des Bediensteten. Derselbe Arzt des personalärztlichen Dienstes ist auch für vom Dienstherrn geforderte Untersuchungen in diesem Bereich (Nervenkrankheiten, Psychopathien) zuständig. In beiden Fällen bleibt der Bedienstete/Patient nicht anonym. Die Beihilfe- und die Untersuchungsakten führt der betreffende Arzt seit 1976, ohne daß die Frage der Löschung geklärt ist.

Ich habe gegenüber dem Personalamt Bedenken gegen dieses Verfahren deutlich gemacht: Es ist nicht auszuschließen, daß Erkenntnisse aus der Beihilfebearbeitung - bewußt oder unbewußt - auch in dienstärztliche Untersuchungen einfließen oder bei personalrechtlichen Auseinandersetzungen zwischen Personalamt und Betroffenen eine Rolle spielen.

Im Juli 1989 teilte mir das Personalamt mit, daß nach dem Anlaufen der Zentralisierung der Beihilfe (s.o. 3.2.1) auch das Beihilfeverfahren bei Psychotherapien geändert und wahrscheinlich der Bundespraxis angeglichen wird. Das bedeutet, daß die Beihilfefähigkeit von einem externen Arzt festgestellt wird, wobei Grundlage - wie in Schleswig-Holstein - ein anonymisierter Bericht des Psychotherapeuten des Bediensteten sein sollte.

3.2.6 Neuregelung des Personalaktenrechts

Nachdem im letzten Jahr eine interministerielle Arbeitsgruppe in Bonn ihren „Bericht zur strukturellen Fortentwicklung des Personalaktenrechts im öffentlichen Dienst" vorgelegt hatte, erarbeitete das Bundesinnenministerium in diesem Jahr einen entsprechenden Gesetzentwurf, der eine - nahezu gleichlautende - Änderung des Bundesbeamtengesetzes und für die Landesbeamten des Beamtenrechtsrahmengesetzes vorsieht. Der Referenten-Entwurf befindet sich derzeit sowohl in den Bundesministerien als auch in den Landesbehörden in der Diskussion. Die geplante gesetzliche Regelung wird in Hamburg die im 6. TB (4.2.1, S. 36) behandelte Verwaltungs- „Anordnung über die Führung und Verwaltung der Personalakten" von 1971 (Mitteilung für die Verwaltung, Seite 280) weitgehend ersetzen.

Der Gesetzentwurf des Bundesinnenministeriums läßt folgende Schwerpunkte erkennen:

— In die Personalakte ist nur aufzunehmen, was einen unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis hat.

— Teil- und Nebenakten werden zugelassen; die Grundakte muß aber ein vollständiges Verzeichnis enthalten.

— Die Beihilfeunterlagen sind in gesonderten Teilakten aufzubewahren und organisatorisch getrennt von der übrigen Personalverwaltung zu bearbeiten.

— Die Rechte des Betroffenen werden folgendermaßen festgelegt: der Bedienstete ist vor Aufnahme von potentiell nachteiligen Eintragungen in die Personalakte anzuhören; Unzutreffendes ist aus der Personalakte zu entfernen und nicht nur richtigzustellen; Mißbilligungen und nachteilige Behauptungen - außer in Beurteilungen - müssen grundsätzlich nach 2 Jahren aus der Personalakte herausgenommen werden, ebenso ein Führungszeugnis nach Eintritt der Tilgungsreife entsprechend dem Bundeszentralregistergesetz.

— Die Weitergabe der Personalakte an andere Dienstherren bzw. Behörden anderer Geschäftsbereiche ist grundsätzlich an die Einwilligung des Betroffenen gebunden, wobei relativ weite und unbestimmte Ausnahmen zugelassen werden. Auskünfte aus der Personalakte an Dritte werden beschränkt und sind dem Betroffenen mitzuteilen.

— Die automatisierte Personaldatenverarbeitung, insbesondere die von medizinischen und psychologischen Daten wird einer Zweckbindung unterworfen; sie darf beamtenrechtliche Entscheidungen unterstützen, aber nicht ersetzen.

Zusammen mit anderen Datenschutzbeauftragten habe ich diesen Entwurf beraten und dem Personalamt gegenüber dazu Stellung genommen. Ich begrüße, daß das tief in das informationelle Selbstbestimmungsrecht eingreifende Personalaktenrecht nun endlich - 6 Jahre nach dem Volkszählungsurteil - gesetzlich geregelt werden soll. Inhaltlich weist der Gesetzentwurf die erfreuliche Tendenz auf, das bisher vorherrschende Prinzip der Vollständigkeit der Personalakte vorsichtig durch den datenschutzrechtlichen Grundsatz der Erforderlichkeit von Datenspeicherungen und -über-

mittlungen zur ersetzen. Die Gesetzesbegründung enthält allerdings noch den nicht mehr zeitgemäßen Satz: „Der Zweck der Personalakte besteht darin, ein möglichst vollständiges Bild über den beruflichen Werdegang und insoweit über die Persönlichkeit der Beamten zu geben, ...".

Eine Reihe von datenschutzrechtlichen Detail-Anregungen hat das Bundesinnenministerium in die nunmehr vorliegende zweite Fassung (Stand September 1989) übernommen. Es bleiben aber vor allem folgende Kritikpunkte:

— Der Zugang zur Personalakte wird im Gesetzentwurf den „mit der Bearbeitung von Personalangelegenheiten beauftragten" Beschäftigten eingeräumt. Das in Hamburg aufgetauchte Problem (vgl. 7. TB, 4.2.2, S. 45), ob und gegebenenfalls welche Vorgesetzte (Dienst-/Fach-Vorgesetzte) Einsicht in die Personalakten nehmen dürfen, bleibt offen. Hier sollte eine Einschränkung auf Dienstvorgesetzte festgelegt werden.

— Bei der Weitergabe von Beihilfe-Unterlagen, bei der Vorlage der Personalakte bei Behörden eines anderen Geschäftsbereiches sowie bei Auskünften an Dritte fordert der Gesetzentwurf die Einwilligung des Betroffenen grundsätzlich. Die Ausnahmen, die durch unbestimmte Rechtsbegriffe wie „berechtigte" bzw. „schützenswerte Interessen" gekennzeichnet sind, lassen sich kaum eingrenzen und sind nicht hinreichend normenklar.

— Diese unklare Ausnahmeregelung wird im Gesetzentwurf durch eine Verweisung auch auf Datei-Verarbeitungen und automatisierte Abrufverfahren erstreckt.

— Nachgetragen werden sollte ein Verbot, Bediener-Daten (etwa maschinelle Protokolle der Tätigkeiten an einem Bildschirm-Arbeitsplatz) in die Personalakten aufzunehmen bzw. zu Verhaltens- und Leistungskontrollen zu nutzen.

— Schließlich sollte auch festgelegt werden, welche Daten für die Personalakte erhoben werden müssen. Die Datenerhebung ist zwar dem „Personalaktenrecht" vorgelagert, hätte aber als dessen Grundlage durchaus mitgeregelt werden können. Der Umfang des Fragerechts des Dienstherren, wie er in den Bewerber- und Einzustellenden-Fragebögen zum Ausdruck kommt (siehe oben) bleibt sonst weiterhin ohne gesetzliche Ermächtigung.

Angesichts der intensiven Diskussion in den Ministerien und Behörden habe ich Zweifel, ob die notwendigen Änderungen des Beamten- und des Beamtenrechtsrahmen-Gesetzes noch in dieser Legislaturperiode verabschiedet werden, wie es geplant war. Ich würde eine schnelle einer späteren „perfekten" Lösung vorziehen.

3.2.7 Entfernung von Vorgängen aus der Personalakte

Aus der Hamburger Verwaltungspraxis hatte ich mich in diesem Zusammenhang mit folgender Eingabe zu beschäftigen: Ein Petent wandte sich dagegen, daß ein einige Jahre altes personalärztliches Zeugnis weiterhin offen in der Personalakte verbleibt, obwohl es inzwischen völlig obsolet sei, einen falschen Eindruck über den Gesundheitszustand des Petenten erwecken und diesen so in seinem beruflichen Fortkommen hindern könne. Abgesehen davon, daß das ärztliche Zeugnis nur in einem verschlossenen Umschlag zur Akte genommen werden durfte, stellt sich hier die Frage, welcher Grundsatz Vorrang hat: das Prinzip der Vollständigkeit der Personalakte (Zeugnis als Beleg dafür, daß der Beamte zu einem bestimmten Zeitpunkt personalärztlich untersucht wurde, mit dem Befund X) oder das Prinzip der Erforderlichkeit (ist das ärztliche Zeugnis noch für die aktuelle oder zukünftige Beurteilung des Betroffenen erforderlich?). Nach meiner Auffassung verbietet es das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung, die historische Wahrheit und Vollständigkeit der Personalakte über das Interesse des Betroffenen an einer Geheimhaltung und an den eigenen aktuellen Entwicklungsmöglichkeiten zu stellen. Legitim ist ausschließlich die Frage, ob die vor Jahren diagnostizierte Krankheit heute wirklich ausgeheilt ist, so daß der Betroffene mit allen anderen Beamten, die sich z.B. mit ihm auf eine neue Stelle

bewerben, gleichbehandelt werden muß. Dies ist jedoch eine medizinische, keine personalaktenrechtliche Frage.

3.2.8 Gleichstellungsgesetz

Die Leitstelle Gleichstellung der Frau hatte den Behörden den Entwurf eines Gleichstellungsgesetzes zur Abstimmung vorgelegt.

In meiner Stellungnahme habe ich vor allem auf zwei datenschutzrechtlich wichtige Punkte aufmerksam gemacht:

— Soll bei der Bewerber/innen/auswahl berücksichtigt werden, daß berufsrelevante Fähigkeiten und Erfahrungen zum Teil auch durch Haushaltsführung und Kindererziehung erworben werden können, so fragt sich, wie dies im Einzelfall belegt und womöglich kontrolliert werden soll. Es muß sichergestellt werden, daß über diesen Auswahlgesichtspunkt keine tiefgreifenden Einblicke in die Privatsphäre der Bewerberin bzw. des Bewerbers gerechtferigt und keine detaillierte Offenbarung von Familienverhältnissen gefordert werden darf.

— Der Gesetzentwurf gestattet der Frauenbeauftragten die Einsicht in die Bewerbungsunterlagen, macht die Einsicht in die Personalakte der Bewerber aber - zu Recht - von der Zustimmung der/des Betroffenen abhängig. Verwaltungsinterne Bewerber können sich in den „Bewerbungsunterlagen" mit einem knappen Hinweis auf die Personalakte begnügen und die Einsichtnahme in diese durch die Frauenbeauftragte ablehnen. Verwaltungsexterne Bewerber müssen ausführliche Unterlagen einreichen, in die die Frauenbeauftragte auch ohne Einwilligung Einsicht nehmen kann.

  Vorzuziehen sind demgegenüber Bewerbungsverfahren, die generell ohne die Vorlage der Personalakte auskommen. Wenn sowohl verwaltungsexterne wie verwaltungsinterne Bewerber für die Auswahl ausreichende Unterlagen beibringen müssen (ohne Rückgriff auf die Personalakte), werden beide Bewerber-Arten gleich behandelt, bleiben all die vielen, für die Auswahl unerheblichen Daten aus der Personalakte dem Zugriff der Einstellungsbehörde verschlossen und ist auch die Frauenbeauftragte bei der Erfüllung ihre Aufgaben nicht mehr auf den good will der Bewerber angewiesen.

3.2.9 Sicherheitsrichtlinien

Das Landesamt für Verfassungsschutz bat mich, zum Entwurf seiner Sicherheitsrichtlinien Stellung zu nehmen. Sie orientieren sich an entsprechenden Bundesvorschriften. Zunächst ist festzustellen, daß Sicherheitsrichtlinien die erforderliche gesetzliche Ermächtigung für Sicherheitsüberprüfungen nicht ersetzen können. Ich begrüße aber, daß das Landesamt anders als das Bundesamt für Verfassungsschutz die Sicherheitsüberprüfungen nicht nur von der Kenntnis, sondern von der Zustimmung des Betroffenen und seines Lebenspartners abhängig machen will. Auch sehen die Hamburger Richtlinien - anders als die des Bundes - vor, daß die Daten des Lebenspartners im Rahmen der untersten Sicherheitsstufe nicht gespeichert werden. Es bleibt allerdings das generelle Problem, daß nach den Erfahrungen der letzen Jahre auch die Lebenspartner der betroffenen Bediensteten in die Sicherheitsüberprüfungen mit einbezogen werden. Die Erforderlichkeit dieser Maßnahme haben spektakuläre Spionagefälle der jüngeren Vergangenheit plausibel gemacht. Ich bin allerdings der Auffassung, daß die Partner-Einbeziehung erst bei den relativ wenigen Sicherheitsüberprüfungen der beiden obersten Stufen angemessen und erforderlich ist. Im übrigen habe ich in meiner Stellungnahme z.B. eine generelle statt einer nur „grundsätzlichen" Trennung von Geheimschutzbeauftragten-Funktion und Personalverwaltungsfunktion gefordert, eine klarere Kompetenzregelung für die Sicherheitsüberprüfungen (Geheimschutzbeauftragter oder Landesamt für Verfassungsschutz?) empfohlen und eine ausführlichere Aufklärung des Betroffenen auch über die sonstige Erkenntnisquellen des Landesamtes angeregt.

3.3 Statistik

3.3.1 Entwurf eines Landesstatistikgesetzes

Im Oktober hat die Behörde für Inneres einen Referentenentwurf für ein Hamburger Landesstatistikgesetz vorgelegt, der indes noch verbesserungsbedürftig erscheint. Im einzelnen ist folgendes anzumerken:

Die Aufgaben des Statistischen Landesamtes sollten - wie in anderen Landesstatistikgesetzen - im Gesetz präzise bestimmt werden. Dabei sollte festgeschrieben werden, daß das Statistische Landesamt neben seinen statistischen Aufgaben keine weiteren Verwaltungsaufgaben wahrnimmt. Nur so kann m.E. die konsequente Abschottung von Statistik und Verwaltung letztlich gewährleistet werden. Die im Entwurf vorgesehenen Formulierungen gewährleisten dies nicht. Danach ist die Wahrnehmung der statistischen Aufgaben organisatorisch und personell von der Erfüllung anderer Aufgaben des Verwaltungsvollzugs zu trennen, soweit dies zur Wahrung des Statistikgeheimnisses erforderlich ist. Diese Regelung muß im Kontext des Erforderlichkeitsbegriffes gesehen werden, der in § 8 Abs. 1 HmbDSG enthalten ist: „Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." Dies bedeutet, daß die Abschottung der statistischen Daten von Wirtschaftlichkeitsbetrachtungen abhängig gemacht wird; die Vorschrift ist deshalb unakzeptabel.

Nach dem Entwurf sollen Landesstatistiken, bei denen Angaben ausschließlich aus öffentlichen Registern verwendet werden und eine Rechtsvorschrift der für die Durchführung der Statistik zuständigen Behörde ein besonderes Zugangsrecht zu diesen Registern gewährt, keiner Anordnung durch Gesetz bedürfen. Aus der Begründung geht hervor, daß der Begriff weit gefaßt ist und auch nicht allgemein zugängliche Register umfaßt. Diese Vorschrift ist mit der verfassungsrechtlich gebotenen Normenklarheit unvereinbar. Die Begriffe „besonderes Zugangsrecht" und „öffentliche Register" werden nicht klar definiert. Besonders kritisch wäre es, wenn hier ein - möglicherweise an eine andere Aufgabe gebundenes - „besonderes Zugangsrecht" unzulässig als Rechtsgrundlage für die Datenübermittlung für statistische Aufbereitungen verstanden wird.

Eine derartige Eingriffsbefugnis wäre zudem auch nicht mit dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz zu vereinbaren. Auch die Nutzung von Registerdaten für statistische Zwecke kann in erheblichem Umfang in das informationelle Selbstbestimmungsrecht der Betroffenen eingreifen. Deshalb bedarf es auch hier der Anordnung durch Landesgesetz, wo im einzelnen geregelt werden müßte, welche Daten für statistsiche Auswertungen übermittelt werden dürfen.

Da die Vorschrift des § 8 des Entwurfs die im allgemeinen Datenschutzrecht enthaltene Norm zur Auftragsdatenverarbeitung verdrängen soll, muß angesichts der besonderen Sensibilität der Statistikdaten mindestens der Datenschutzstandard der Auffangnorm gewährleistet sein. Verglichen mit dem § 3 E-HmbDSG (Drs. 13/3282) ist die vorgesehene Regelung im Landesstatistikgesetz aber weniger konkret und bindet die für die statistische Datenverarbeitung zuständigen Stellen in geringerem Maße. Deshalb sollte - in Ergänzung zu den in § 3 Abs.1 E-HmbDSG enthaltenen Vorschriften - vorgesehen werden, daß statistische Arbeiten nur an solche Personen und Stellen vergeben werden dürfen, bei denen Interessenkonflikte zwischen den ihnen übertragenen statistischen Arbeiten mit beruflichen oder sonstigen Interessen nicht zu befürchten sind. Es sollte ausgeschlossen werden, daß die mit statistischen Arbeiten beauftragten Stellen ihrerseits Arbeiten in Form von Unterauftragsverhältnissen delegieren.

Die Regelungen zur Geschäftsstatistik (§ 9) erscheinen mir ebenfalls als noch verbesserungsbedürftig. Es müßte zudem geklärt werden, in welchem Verhältnis diese Vorschrift zur in § 29 E-HmbDSG vorgesehenen Regelung über die Nutzung von Verwaltungsdaten für die Erstellung von Statistiken steht.

Es sollte klargestellt werden, daß die Weisungsbefugnis für die Verarbeitung von Daten der Geschäftsstatistik auch dann bei den Behörden liegt, bei denen die Daten angefallen sind, wenn die Verarbeitung durch das Statistische Landesamt erfolgt.

Einer Klarstellung bedarf auch, daß Statistiken, die überregional koordiniert und länderübergreifend zusammengefaßt werden (sog. „koordinierte Länderstatistiken") keine Geschäftsstatistiken i.S.v. § 9 sind. Der überregionale Charakter dieser Statistiken hat, verglichen mit für Zwecke der Dokumentation des eigenen Dienstbetriebs erstellten Statistiken, eine höhere Eingriffsqualität zur Folge, zumindest dann, wenn für deren Erstellung - wie bei den Justizstatistiken - den Betroffenen über Aktenzeichen oder sonstige Identifikatoren zurechenbare Einzelangaben verarbeitet werden, es sich mithin auch bei den Statistikdaten um personenbezogene Daten handelt.

In der Begründung wird ausgeführt, daß Geschäftsstatistiken einer Anordnung durch spezialgesetzliche Regelung deshalb nicht bedürften, weil eine Auswertung personenbezogener Merkmale vielfach lediglich mittels Strichliste erfolge. Im Umkehrschluß muß daraus gefolgert werden, daß Statistiken, bei denen zuordnungsfähige Einzeldatensätze verwendet werden, einer spezialgesetzlichen Anordnung bedürfen. Die Vorschrift ist jedoch so gestaltet, daß Daten, die im Geschäftsgang anfallen, generell für Geschäftsstatistiken genutzt werden dürfen. Sofern Einzelangaben über längere Zeiträume für Zwecke der Geschäftsstatistik gespeichert werden oder für die Erstellung dieser Statistiken mit anderen Einzelangaben über denselben oder auch Betroffene verknüpft werden, erhält der Statistikdatenbestand eine neue Qualität. Dies gilt z.B. dann, wenn - wie in der Personalstrukturdatei des Personalamtes - Daten aus der Gehaltsabrechnung über viele Jahre in einer gesonderten Datei personenbezogen gespeichert werden (Personalstrukturdatei, vgl. 6. TB, 4.2.3, S. 38), obwohl sie für die Verwaltungsaufgabe, in deren Rahmen sie angefallen sind, überhaupt nicht mehr erforderlich sind und deshalb eigentlich gelöscht werden müßten.

Um den in der Begründung vorgebrachten Gedanken zur Geltung zu bringen, müßte der Begriff der Geschäftsstatistik im Gesetz so definiert werden, daß nur solche Statistiken als Geschäftsstatistiken anzusehen sind, bei denen ein Rückschluß auf einzelne Fälle nicht möglich ist. Ferner sollte ausgeschlossen werden, daß für Geschäftsstatistiken mehrere Vorgänge derselben Betroffenen zusammengeführt werden, wenn dies aus Gründen der Vorgangsbearbeitung im Rahmen der Verwaltungsaufgabe nicht erforderlich ist.

Sollte der Begriff der Geschäftsstatistik nicht in der von mir vorgeschlagenen Form eingeschränkt werden, bedarf es zumindest zusätzlicher Regelungen über Trennung, Löschung und Zweckbindung der Daten.

3.3.2 Wohnungsstichprobe

Ende August 1989 hatte ich durch Presseveröffentlichungen erfahren, daß die Bundesregierung den Entwurf eines Gesetzes über die Durchführung einer Repräsentativstatistik auf dem Gebiet des Wohnungswesens (Gebäude- und Wohnungsstichprobengesetz) vorgelegt hatte. Durch Wohnungsstichproben wollte die Bundesregierung in regelmäßigen zeitlichen Abständen (alle fünf Jahre, beginnend 1990) bei 1 v.H. der Wohnungen wohnungspolitisch erforderliche Informationen erheben. Neben Daten zu den Wohnungen sollten dabei auch in erheblichem Umfang Informationen über die „Wohnsituation der Haushalte" abgefragt werden (u.a. Familienzusammenhang, Staatsangehörigkeit und Höhe des monatlichen Nettoeinkommens, Form des Zusammenlebens).

Die grundsätzliche Frage, warum die Daten, die aus der Volkszählung und dem Mikrozensus vorhanden sind, nicht ausreichen, um die mit dem vorliegenden Gesetzentwurf angestrebten Ziele zu erfüllen, wird weder im Entwurf selbst noch in der Begründung überzeugend beantwortet. Ich habe insb. im Hinblick auf Fragen, die sich auf den Intimbereich beziehen, Zweifel, ob das Interesse der Allgemeinheit an der Statistik gegenüber dem Recht des Einzelnen auf informationelle Selbstbestimmung überwiegt. Bereits in seinem „Mikrozensusbeschluß" von 1969 bezog sich das Bundesver-

fassungsgericht auf das Menschenbild des Grundgesetzes, das dem einzelnen Bürger „einen unantastbaren Bereich privater Lebensgestaltung" gewährt, „der der Einwirkung der öffentlichen Gewalt entzogen ist". Ein überwiegendes Allgemeininteresse, das Voraussetzung für die Datenerhebung ist, bestehe regelmäßig nur an Daten mit Sozialbezug unter Ausschluß unzumutbarer intimer Angaben und von Selbstbezichtigungen.

So berührt z.B. die Frage nach der „Form des Zusammenlebens und -wohnens" (§ 4 Nr. 3) unzweifelhaft den unantastbaren Bereich privater Lebensgestaltung. Da nach dem Familienstand gesondert gefragt wird, sollte hier offensichtlich etwas anderes (was?) abgefragt werden. Wie detailliert muß die Antwort sein, um hier der Auskunftspflicht Genüge zu tun? Bei der Frage nach dem Familienzusammenhang könnte es zu einer unzulässigen Ausforschung von Adoptions- und Adoptionspflegeverhältnissen kommen (§ 1758 BGB).

Der Gesetzentwurf sagte nichts darüber aus, wie z.B. damit umgegangen werden soll, wenn besonders sensible Bereiche (wie z.B. Frauenhäuser, Sammelunterkünfte für Asylbewerber, Behinderteneinrichtungen) in die Zufallsauswahl geraten. Aus den Erfahrungen bei der Volkszählung waren insoweit offensichtlich keine Lehren gezogen worden.

Auch unter dem Gesichtspunkt der Normenklarheit wies der Entwurf erhebliche Mängel auf:

Die Bezeichnung des Gesetzes und die Bezeichnung der Erhebung in § 1 des Entwurfs erweckten den Eindruck, es handele sich um eine Erhebung von Angaben ausschließlich über Gebäude, Wohnungen und die „Wohnsituation" (was immer das sein mag) von Haushalten. Tatsächlich werden mit den in § 4 Nr. 3 genannten Erhebungsmerkmalen sehr sensible personenbezogene Daten erfragt, wodurch die Erhebung einen starken bevölkerungsstatistischen Einschlag erhält. Dies müßte bereits im Namen des Gesetzes und in der allgemeinen Beschreibung der Erhebung (§ 1) zum Ausdruck kommen.

Die Erhebungsmerkmale waren zum Teil unklar. Bei der Konkretisierung der Fragen wird darauf zu achten sein, daß jeder Auskunftspflichtige auch ohne Hilfe eines Erhebungsbeauftragten in der Lage ist, die Fragen ordnungsgemäß und nur in erforderlichem Umfang zu beantworten. Es wäre nicht hinnehmbar, wenn die Auskunftspflichtigen auf die Konkretisierung der Fragen durch die Interviewer angewiesen wären und es damit im Ermessen der Interviewer stünde, wie detailliert die Fragen beantwortet werden.

Der Gesetzentwurf regelte nicht, welche Anstrengungen die Betroffenen machen müssen, um ihrer Auskunftspflicht nachzukommen. Die Verpflichtung zur Auskunftserteilung kann sich m.E. nur auf die Angaben erstrecken, die die Auskunftspflichtigen nach bestem Wissen und Gewissen aus dem Gedächtnis erteilen können. Aber wer hat schon den „durchschnittlichen Jahresenergieverbrauch eines Gebäudes", das „Alter und Volumen seines Öltanks", das „Baujahr des Heizkessels" und die „Emissionsbelastung" seiner Wohnung im Kopf. Ist der Auskunftspflichtige, um Auskunft geben zu können, auch verpflichtet, Bücher, Aufzeichnungen, Geschäftspapiere und andere Urkunden einzusehen? Ist er gar gezwungen, rechtzeitig Aufzeichnungen zu machen, für den Fall, daß er auskunftspflichtig wird? Was wäre hier mit dem Verhältnismäßigkeitsgrundsatz noch vereinbar? Zu diesen Fragen finden sich auch im Bundesstatistikgesetz keine Antworten.

Der Senat hat meine Bedenken nur zum Teil aufgegriffen. Er hat im Bundesrat einer Entschließung zugestimmt, die die Zielrichtung des Gesetzentwurfes ausdrücklich begrüßt, zugleich aber darum bittet, im weiteren Erhebungsverfahren die Erhebungsmerkmale, die die Privatsphäre auskunftspflichtiger Personen in besonderer Weise berühren, entsprechend dem Grundsatz der Verhältnismäßigkeit auf das für die Zielsetzungen des Gesetzes notwendige Maß zu begrenzen und die unverzichtbaren

Merkmale in einer Weise gesetzlich zu regeln, die dem Grundsatz der Normenklarheit entspricht. Die erste Wohnungsstichprobe soll nach der Entschließung des Bundesrates erst im Jahr 1992 stattfinden.

3.3.3 Übermittlung statistischer Daten an die EG

Die Bundesregierung hat am 30. März 1989 dem Bundesrat den Entwurf einer Verordnung (EWG/Euratom) des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften (SEAG) zugeleitet.

Die Verordnung bezweckt, die zuständigen nationalen Stellen dazu zu ermächtigen, dem Statistischen Amt der EG vertrauliche statistische Daten zu übermitteln, die dem Statistikgeheimnis unterliegen (§ 16 BStatG). Sofern es sich dabei um personenbezogene Daten handelt, bedeutet die Übermittlungsbefugnis eine Einschränkung des Rechts auf informationelle Selbstbestimmung.

Die in dem Verordnungsentwurf enthaltenen Sicherungsvorschriften gegen eine unzulässige Datenverarbeitung bleiben hinter den Regelungen des BStatG zurück:

— Zweckbindung nur bezogen auf „statistische Zwecke" (Art. 5 Nr. 2), nicht an die Erforderlichkeit für die Erstellung der einzelnen Statistik (§ 16 Abs. 2 BStatG),

— Zugang zu den vertraulichen Informationen - in Ausnahmefällen - auch für die „sonstigen auf Vertragsbasis tätigen natürlichen Personen",

— keine Unterscheidung zwischen Erhebungs- und Hilfsmerkmalen (§ 10 Abs. 1 BStatG) mit daran anknüpfenden Trennungs- und Löschungsgeboten (§ 12 BStatG),

— keine strafrechtliche Ahndung von Verletzungen der Geheimhaltungsverpflichtungen durch Mitarbeiter des SAEG oder sonstiger beauftragter Personen, die dem Standard des § 203 StGB genügt,

— keine unabhängige Datenschutzkontrolle, sondern lediglich Einsetzung eines „Beratenden Ausschusses für die Statistische Geheimhaltung" unter Vorsitz des Generaldirektors des SAEG.

Von grundsätzlicher Bedeutung ist die Frage, inwieweit der Betroffene das ihm in der Bundesrepublik zustehende Recht auf informationelle Selbstbestimmung auch gegenüber europäischen Institutionen durchsetzen kann. Nach der Rechtsprechung der Bundesverfassungsgerichts (BVerfGE 73, S. 339) obliegt die gerichtliche Überprüfung der Verfassungsmäßigkeit von Rechtsakten der EG dem Europäischen Gerichtshof. Dieser rechnet zwar die Grundrechte zu den allgemeinen Rechtsgrundsätzen, deren Wahrung er zu sichern hat, doch bezieht er sich dabei ausdrücklich auf die gemeinsamen Verfassungsüberlieferungen der Mitgliedsstaaten. Ob und inwieweit auch das vom BVerfG in seinem VZ-Urteil entwickelte Recht auf informationelle Selbstbestimmung zu den vom EuGH zu gewährleistenden überlieferten Grundrechten gehört, ist zweifelhaft.

Solange es auf Ebene der Europäischen Gemeinschaften kein wirksames Datenschutzrecht und keine effektive Datenschutzkontrolle gibt, ist es besonders wichtig, daß die europarechtlichen Vorschriften, die Eingriffe in das Recht auf informationelle Selbstbestimmung zulassen, den verfassungsrechtlichen Anforderungen des Grundgesetzes entsprechen. Das bedeutet im konkreten Fall, daß der im BStatG erreichte Standard in der EG-Verordnung gewährleistet werden muß.

Diese durch einen Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigte Kritik hat den Bundesrat veranlaßt, die Bundesregierung zu bitten, darauf hinzuwirken, daß der gesetzliche verankerte Standard des nationalen Geheimhaltungsschutzes gewährleistet wird.

3.3.4 Volkszählungsnachlese

Auch zwei Jahre nach dem Erhebungsstichtag bestand Veranlassung, sich mit der Abwicklung der letzten Volkszählung auseinanderzusetzen. Mit Schreiben vom 24.

April 1989 hat mir die Innenbehörde mitgeteilt, daß am 21. April die amtliche Bevölkerungszahl festgestellt worden sei. Gem. § 15 VZG sind die Erhebungsvordrucke zum frühestmöglichen Zeitpunkt, spätestens 2 Wochen nach Feststellung der amtlichen Bevölkerungszahl zu vernichten. Die laufenden Nummern und Ordnungsnummern sind zu löschen, sobald die Zusammenhänge zwischen Personen, Haushalten, Wohnungen und Gebäuden festgehalten worden sind, spätestens zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl. Die genauen Adreßangaben (Straße und Hausnummer) sind zu löschen, wenn ihre Zugehörigkeit zur Blockseite (kleinste zulässige räumliche Gliederung) festgelegt ist. Da die Zuordnung zur kleinräumigen Gliederung verarbeitungstechnisch vor der Festlegung der amtlichen Bevölkerungszahl liegt, dürfen die genauen Adreßangaben ebenfalls nicht länger gespeichert bleiben, als dies für die übrigen zu löschenden Hilfsangaben erlaubt ist. Die Löschungen hätten bis zum 5. Mai vorgenommen werden müssen.

Es hat mich deshalb sehr überrascht, als mir die Innenbehörde am 30. Mai mitteilte, daß - weil sich die Einwohnerzahl Hamburgs um 14 (!) Personen verschoben habe - die amtliche Feststellung der Einwohnerzahl noch einmal, diesmal am 5. Mai, stattgefunden habe. Die Innenbehörde hat daraus offensichtlich abgeleitet, daß die gesetzliche 2-Wochen-Frist damit noch einmal zu laufen beginnt, denn auf Rückfragen hin teilte mir die Innenbehörde mit, daß die Ordnungsnummern, laufenden Nummern und die Hilfsmerkmale Straße und Hausnummer erst am 19. Mai 1989 im Zuge der Erstellung des für Zwecke der statistischen Auswertung vorgesehenen Datensatzes („Satzart 30") gelöscht worden seien.

Während die Vernichtung der schriftlichen Erhebungsunterlagen bis zum 5. Mai 1989 abgeschlossen war und somit vor Ablauf der gesetzlichen „Ausschlußfrist" erfolgte, wurde die Löschung der laufenden Nummern und Ordnungsnummern um zwei Wochen verspätet vorgenommen. Die gesetzlich vorgeschriebenen Löschungsfristen wurden also überschritten.

Die langwierigen, sich über fast zwei Jahre hinziehenden Kontrollen der Vollzähligkeit, Vollständigkeit und Plausibilität der Angaben haben mich in meinen Bedenken gegen Großzählungen wie die Volkszählung noch einmal bestätigt. Ich hoffe, daß in Zukunft intensiv über Alternativen zu derartigen Totalerhebungen nachgedacht wird. Nur so kann die Statistik den bei großen Teilen der Bevölkerung verlorenen Kredit zurückgewinnen.

3.4 Berichte über Kinder in Vorschulklassen

Im letzten Tätigkeitsbericht (7. TB, 4.5.1, S. 60) hatte ich über einen nach Persönlichkeits- und Verhaltensmerkmalen gegliederten Vordruck berichtet, den Klassenleiter für die Beurteilung von Vorschulkindern benutzen mußten (sogen. Beurteilungsbogen zur Feststellung der Lernausgangslage von Schulanfängern). Die Beurteilung wurde bei Einschulung der Kinder zur Schülerakte genommen und dort für eine nicht festgelegte Zeit verwahrt. Eine Kopie wurde den Eltern nicht ausgehändigt, viele Eltern kannten diese Beurteilung nicht einmal.

Abgesehen davon, daß dieses Verfahren schon aus formalen Gründen rechtswidrig war (fehlende Rechtsgrundlage), war es geeignet, Schulanfängern einen unbelasteten Start erheblich zu erschweren. Hinzu kam eine problematische Ungleichbehandlung gegenüber solchen Kindern, die keine Vorschule besuchen und für die lediglich das Ergebnis der „Schulreife-Untersuchung" in der Schülerakte vermerkt wird.

Die Schulbehörde ist nun meiner Forderung, diese Vordrucke abzuschaffen, nachgekommen. Das bisherige Verfahren wird auch nicht - wie zunächst von der Schulbehörde angedacht - durch einen individuell konzipierten Berichtstext ersetzt. In der Schülerakte wird nur noch vermerkt, ob ein Kind am Ende des Besuches der Vorschulklasse schulreif ist.

3.5 Auskunftsanspruch über Umweltdaten

Mit einem Auskunftsanspruch der Bürger über Umweltdaten hatte ich mich im Rahmen einer Stellungnahme zum Entwurf eines 6. Gesetzes zur Änderung des Hmb. Wassergesetzes zu befassen. Ich habe mich in der Vergangenheit wiederholt, zuletzt im Zusammenhang mit der Diskussion um die Gesetzentwürfe für ein Akteneinsichtsrecht in Umweltakten und für ein Umweltdatenauskunftsgesetz, für eine bessere Information der Bürger über Umweltbeeinträchtigungen eingesetzt (siehe dazu auch 6. Tätigkeitsbericht, Ziff. 4.7).

Transparenz des Verwaltungshandelns und seiner Entscheidungsgrundlagen und Schutz personenbezogener Daten stehen als Aspekte demokratischer Informationsregelungen in einem Spannungsverhältnis, das aufgrund einer Rechtsgüterabwägung zu lösen ist. Voraussetzung für den Schutz und den Erhalt der natürlichen Lebensgrundlagen ist eine breite Information über bestehende und geplante Umweltbeeinträchtigungen, sei es um individuelle Schutzvorkehrungen treffen oder weiteren Schäden vorbeugen zu können. Diesem Informationsinteresse der Allgemeinheit steht das Individualrecht auf Schutz von personenbezogenen Daten und von Betriebs- und Geschäftsgeheimnissen gegenüber. Soweit die Preisgabe geschützter Daten zur Zuordnung der Verursachung oder der Verantwortlichkeit für eine Umweltbeeinträchtigung erforderlich ist, gebührt dem Informationsinteresse der Vorrang, denn von Umweltbeeinträchtigungen sind alle betroffen.

Für die inhaltliche Ausgestaltung des Informationsrechts gebe ich unter dem Gesichtspunkt der Verbesserung der Transparenz nach wie vor dem Akteneinsichtsrecht den Vorzug vor einem bloßen Auskunftsrecht, das stets mit einer Selektion der Daten einhergeht und die Gefahr einer Verkürzung des Informationszusammenhangs in sich birgt.

Der Entwurf der Umweltbehörde für einen Auskunftsanspruch im Wassergesetz ist nach dem Scheitern eines umfassenden Informationsrechts über Umweltdaten nur ein recht kleiner Schritt in die richtige Richtung einer Verbesserung der Informationsgrundlagen der Öffentlichkeit über Umweltbeeinträchtigungen.

Aus datenschutzrechtlicher Sicht muß in der Regelung des Auskunftsrechts zum Ausdruck kommen, über welche Daten zu informieren ist und daß die in der Offenbarung an jederman liegende Zweckentfremdung der Daten, die ja zur Erfüllung bestimmter Aufgaben der zuständigen Behörden erhoben wurden, aus übergeordneten Interessen der Allgemeinheit zulässig ist. Die Güterabwägung zwischen den Belangen des Gewässerbenutzers und den Informationsinteressen der Allgemeinheit sollte aus dem Gesetz in den Grundzügen erkennbar sein, indem konkret definiert wird, welche Angaben zur Person des Betroffenen zulässigerweise offenbart werden dürfen. Der Schwerpunkt bei dem geplanten Auskunftsrecht liegt bei anlagebezogenen Daten. Erlaubnisse und Bewilligungen beziehen sich in der Regel auf eine Wasserbenutzungsanlage oder ein Grundstück, jedoch sind diese zumindest im Einzelfall natürlichen Personen zuzuordnen.

Im Wege einer generellen Rechtsgüterabwägung könnte festgelegt werden, daß der Schutz der Information, daß eine natürliche Person Inhaber einer wasserechtlichen Erlaubnis oder Bewilligung ist oder daß ihr eine erlaubte oder unerlaubte Gewässerbenutzung zuzurechnen ist, hinter dem Informationsbedürfnis der Öffentlichkeit zurückzutreten hat. Soweit es für die Bestimmung, Unterscheidung oder Zuordnung von Umweltdaten erforderlich ist, würde sich diese Einschätzung neben dem Namen auch auf den Beruf, die Branchen- oder Geschäftsbezeichnung, die innerbetriebliche Funktionsbezeichnung und die Anschrift des Grundstücks, von dem die Gewässerbenutzung ausgeht, erstrecken.

Im Interesse einer normenklaren und transparenten Regelung habe ich vorgeschlagen, im Gesetz konkret die Daten zu benennen, die außer den anlagebezogenen Informationen offenbart werden dürfen.

Der Schutz von Betriebs- und Geschäftsgeheimnissen könnte für das Auskunftsrecht in ähnlicher Weise geregelt werden wie für das Einsichtsrecht in das Wasserbuch, das Einblicke in geheimzuhaltende Unterlagen nur mit Zustimmung des berechtigt an der Geheimhaltung Interessierten zuläßt. Vorab wäre allerdings die Frage zu stellen, ob die Bekanntgabe von Emissionswerten überhaupt Betriebs - bzw. Geschäftsgeheimnisse tangiert. In der Begründung zum Entwurf des Umweltdatenauskunftsgesetzes waren Zweifel daran geäußert worden, ob Genehmigungsdaten als zum Schutz der Allgemeinheit festgesetzte Soll-Werte geeignet sind, Geschäfts- und Betriebsgeheimnisse zu offenbaren. Für die ermittelten Ist - Werte wurde nach Anhörung von Experten darauf hingewiesen, daß Betriebs- und Geschäftsgeheimnisse nur berührt sein können, wenn durch diese Informationen konkrete Rückschlüsse auf anlagebezogene Daten ermöglicht würden. Die Kenntnis von Emissionen allein ermögliche wegen der Breite und Differenziertheit der Produktionsverfahren und ohne Kenntnis der Vermeidungs- und Reinigungstechniken keine Rückschlüsse auf Produktionsverfahren.

Unter diesen Voraussetzungen dürfte der Schutz von Betriebs- und Geschäftsgeheimnissen durch Einzelfallprüfungen sichergestellt werden können, wenn im konkreten Fall die Verletzung schutzwürdiger Belange zu befürchten ist. Bereits bei Durchführung der wasserrechtlichen Verfahren müßte der Antragsteller geltend machen, daß bestimmte Informationen unter das Betriebs- bzw. Geschäftsgeheimnis fallen. Eine Prüfung der Darlegung des Betroffenen müßte gleichermaßen für die zugelassenen wie für die tatsächlichen Gewässerbenutzungen erfolgen. Für unzulässige Gewässerbeeinträchtigungen durch einen Schadensfall oder eine Betriebsstörung könnte generell festgelegt werden, daß das Informationsinteresse der Allgemeinheit im Schadensfall dem Geheimhaltungsinteresse des Gewässerbenutzers vorgeht.

Nach dem Entwurf ist die Auskunft auf das Informationsersuchen innerhalb einer angemessenen Zeit zu erteilen. Ich befürworte stattdessen die Festschreibung einer konkreten Frist zur Sicherstellung des Informationsbedürfnisses der Betroffenen.

3.6 Steuerwesen

3.6.1 Voraussetzungen für die Einleitung eines Verfahrens nach § 208 Abs. 1 Nr. 3 AO

Aufgrund einer Eingabe sah ich mich veranlaßt, der Frage nachzugehen, unter welchen Voraussetzungen die Aufnahme von Ermittlungen durch die Steuerfahndung zulässig ist.

Der Eingabe lag folgender Sachverhalt zugrunde:

Im Landeskriminalblatt war eine Meldung erschienen über einen Einbruch in eine Etagenwohnung. Neben der knappen Schilderung des Tathergangs enthielt sie eine Auflistung des Diebesgutes, das aus diversen Schmuckstücken, Euroschecks und mehreren Sparbüchern bestand. Es war eine Meldung unter etlichen gleichartigen.

Während die Polizei ihre Ermittlungen gegen die unbekannten Täter alsbald ergebnislos einstellte, nahm die Steuerfahndung ihre Ermittlungen gegen die Geschädigten auf. Sie erfragte beim mit der Sache befaßten Kriminalkommissariat den Namen und die Adresse der Bestohlenen, stellte anhand der Adresse das zuständige Finanzamt fest und ließ sich die Lohnsteuerjahresausgleichsanträge der Betroffenen aus den letzten Jahren übermitteln, woraus sie entnehmen konnte, daß Zinseinnahmen, die aus den Sparguthaben geflossen sein mußten, nicht deklariert waren. Daraufhin wurde ein Steuerstrafverfahren gegen die Bestohlenen eingeleitet und durchgeführt, das schließlich - wie üblich? - gem. § 153a StPO eingestellt wurde, nachdem die Beschuldigten die hinterzogenen Steuern nachgezahlt und einen etwa gleich hohen Betrag zugunsten einer gemeinnützigen Einrichtung entrichtet hatten.

Kernfrage bei der Beurteilung der Rechtmäßigkeit des Vorgehens der Steuerfahndung ist, ob im konkreten Fall die Voraussetzungen für die Einleitung eines Verwaltungsverfahrens gegen die Eigentümer der gestohlenen Sparbücher aufgrund von § 208 Abs. 1 Nr. 3 AO vorlagen oder nicht, d.h. hier:

> Ist die Veröffentlichung einer polizeilichen Meldung über einen Einbruchdiebstahl im Landeskriminalblatt ein ausreichender Anlaß für Ermittlungen der Steuerfahndung gegen die ihr unbekannten Geschädigten?

In Literatur und Rechtsprechung ist - soweit ersichtlich - unstreitig, daß § 208 AO keine allgemeine Ermächtigung zu beliebigen Eingriffen, zur Anwendung beliebiger Mittel darstellt. Ebenso wie das Strafverfahren kennt auch das Steuerverwaltungsverfahren keine Wahrheitsfindung um jeden Preis. Unstreitig ist weiter, daß die Anforderungen an die Voraussetzungen zur Einleitung eines (Verwaltungs-) Verfahrens nach § 208 Abs. 1 Nr. 3 AO geringer sind als die für die Einleitung eines Straf- oder Bußgeldverfahrens. Für die letzteren muß bekanntlich ein Anfangsverdacht vorliegen, d.h. es müssen konkrete Anhaltspunkte vorhanden sein, die nicht bloß auf die Möglichkeit, sondern auf eine gewisse, wenn auch zweifelhafte Wahrscheinlichkeit einer Tatbestandsverwirklichung schließen lassen.

Nicht einheitlich ist jedoch die Meinung darüber, um wieviel geringer die Anforderungen im Hinblick auf eine mögliche Tatbestandsverwirklichung sein dürfen, damit die Einleitung eines Verfahrens nach § 208 Abs. 1 Nr. 3 AO sich nicht als eine willkürliche Maßnahme, als eine „ins Blaue hinein" getroffene und damit als unzulässige Maßnahme erweist. Am niedrigsten ist die Schwelle bei den Verfechtern der Ansicht, daß, weil nach dem Wortlaut des § 208 Abs. 1 Nr. 3 AO kein begründeter Anhalt oder Verdacht für die Notwendigkeit von Fahndungsmaßnahmen vorauszusetzen ist, es ausreicht, wenn nach einem gegebenen Sachverhalt die Möglichkeit einer objektiven Steuerverkürzung besteht. Danach soll die Einleitung eines Verfahrens durch die Steuerfahndung nur dann unzulässiges Übermaß sein, wenn es für die Möglichkeit einer Steuerverkürzung gar keine Anhaltspunkte gibt oder diese Möglichkeit sogar ausgeschlossen ist (so Tipke/Kruse Tz. 5 zu § 208).

Demgegenüber vertreten andere die - restriktivere - Ansicht, es müßten mindestens „konkrete Anhaltspunkte im Einzelfall" vorliegen (z.B. Hensel und K. Vogel, zitiert bei Tipke/Kruse a.a.O.).

In der Begründung des Finanzausschusses zu dem Entwurf der Abgabenordnung 1977 (Bundestags-Drs. 7/4292 S. 36) heißt es: „... dies gilt insbesondere in solchen Fällen, in denen noch keine hinreichenden Anhaltspunkte für das Vorliegen einer Steuerstraftat oder Steuerordnungswidrigkeit vorliegen, andererseits jedoch ein dahingehender Verdacht nach den gegebenen Umständen naheliegt."

Der BFH hat (in der Entscheidung BStBl. 68, 365, 369) ausgeführt, es genüge insbesondere, daß unter Berücksichtigung der allgemeinen Erfahrung der Finanzbehörde die Vermutung begründet ist, daß ein steuergesetzlicher Tatbestand verwirklicht worden ist („... wenn aufgrund konkreter Momente oder aufgrund allgemeiner Erfahrung ... die Möglichkeit ... in Betracht kommt").

In einem Fall, der das Ersuchen an eine Zeitung um Auskunft über Name und Adresse der Auftraggeber einzelner Chiffreanzeigen über den Verkauf ausländischer Immobilien von beträchtlichem Wert betrifft (BFHE 148, 108), hat es der BFH genügen lassen, daß aufgrund allgemeiner Erfahrung die Möglichkeit objektiver Steuerverkürzung bestand.

In einem Fall, in dem es um ein Sammelauskunftsersuchen der Steuerfahndung an ein Kreditinstitut über dessen Provisionszahlungen an alle in einer bestimmten Zeit für das Kreditinstitut tätig gewordenen Kreditvermittler ging, hat der BFH das Auskunftsersu-

chen für zulässig erachtet, vorausgesetzt, daß nach allgemeiner Erfahrung verhältnismäßig viele Kreditvermittler ihre Provisionen nicht versteuern und die Ausführung des Ersuchens keine unverhältnismäßige (unzumutbare) Belastung bedeutet (BFH BStBl. 87, 484).

Das Finanzgericht Hamburg (EFG 87, 9) hat die allgemeine Erfahrung genügen lassen, daß Zahnärzte, die Goldgeschäfte mit Scheideanstalten machen, die Einkünfte daraus nicht selten nicht versteuert haben.

In einem anderen Fall hat das Finanzgericht Hamburg (EFG 87, 275) die Steuerfahndung für berechtigt erklärt, die in den Verkauf von kostspieligen Segel- und Motoryachten eingeschalteten Makler zur Angabe von Namen und Anschriften ihrer Auftraggeber aufzufordern, weil es eine Erfahrung dahingehend gebe, daß solche Vermögensgegenstände oft nicht steuerrechtlich erfaßt würden.

Allen zitierten Entscheidungen liegt die Konstellation zugrunde, daß die von der Steuerfahndung aufgrund von § 208 Abs. 1 Nr. 3 AO zur Auskunftserteilung nach § 93 Abs. 1 Satz 1 herangezogenen Dritten sich gegen die Auskunftsverpflichtung zur Wehr setzten. Sie beriefen sich im einzelnen auf das Grundrecht der Pressefreiheit, auf das Bankgeheimnis, auf die Beachtung des Verhältnismäßigkeitsgebotes, auf Auskunftsverweigerungsrechte nach §§ 102 ff. AO 1977. In seinem Beschluß vom 6.4.1989 (1 BvR 33/87) setzt sich das Bundesverfassungsgericht mit der Frage der Verfassungsmäßigkeit der Vorschriften der §§ 93 Abs. 1 Satz 1, 208 Abs. 1 Nr. 3 AO auseinander und bejaht diese. Das Gericht führt in seinem Beschluß zu § 208 AO weiter aus, daß die Vorschrift einerseits dem besonderen Charakter der „Vorfeldermittlungen" der Steuerfahndung Rechnung trage und andererseits nicht unberücksichtigt lasse, daß auch derartige Ermittlungsmaßnahmen im Einzelfall geeignet, erforderlich und angemessen sein müssen. Das BVerfG bestätigt auch die Auffassung des BFH, daß es in Fällen der vorliegenden Art zwar keines strafprozessual erheblichen Tatverdachts, wohl aber eines hinlänglich begründeten Anlasses bedürfe und daß letzterer dann gegeben sei, wenn aufgrund konkreter Momente oder aufgrund allgemeiner Erfahrungen im Einzelfall die Heranziehung eines Auskunftspflichtigen geboten sei. Daraus folgt, daß auch das BVerfG es für erforderlich hält, die genannten Vorschriften in der dargelegten Weise unter Beachtung des Verhältnismäßigkeitsgrundsatzes auszulegen und anzuwenden.

In dem Fall, den der HmbDSB zu beurteilen hatte, geht es zwar nicht um Einwände eines nach § 93 Abs. 1 Satz 1 zur Auskunft herangezogenen Dritten, sondern um Einwendungen der Betroffenen gegen die Aufnahme der Ermittlungstätigkeit durch die Steuerfahndung. Dieser Unterschied im Sachverhalt steht der Heranziehung der vorstehend aufgeführten Entscheidungen des BFH, des FG Hamburg und des BVerfG zur Beurteilung des hier untersuchten Falles jedoch nicht entgegen. Eine Analyse der zitierten Entscheidungen führt zu dem Ergebnis, daß der BFH - ohne daß dies beim BVerfG auf Bedenken stößt - als Mindestvoraussetzung für die Aufnahme von Ermittlungen durch die Steuerfahndung fordert:

— In Anbetracht konkreter Momente (des Einzelfalls) oder

— im Hinblick auf eine bestimmte, klar zu definierende Personengruppe und bestimmte, mit dieser Personengruppe zusammenhängende allgemeine Erfahrungen der Finanzämter

muß die Möglichkeit objektiver Steuerverkürzung in Betracht kommen.

Beide Alternativen sind in dem hier zu beurteilenden Fall nicht erfüllt:

(1) Es ist nicht erkennbar, worin gerade in diesem Einzelfall

— bei einem Wohnungseinbruch in einem Mehrfamilienhaus wurden mehrere Sparbücher, Euroschecks und diverser Schmuck gestohlen

die „konkreten Merkmale" bestehen sollen, die die „Möglichkeit objektiver Steuerverkürzung in Betracht kommen" lassen. Das Vorhandensein der Sparbücher per se ist keine Besonderheit. Es kann heutzutage unterstellt werden, daß praktisch jeder Bürger, in welcher Form auch immer, Konten bei einem Kreditinstitut unterhält. Wäre dies bereits ein Anlaß zum Tätigwerden, so könnten die Kreditinstitute in der Tat wahllos schon nach bestehendem Abgabenrecht von den Finanzbehörden aufgefordert werden, listenmäßig Kontenstände und Erträge mitzuteilen. Dies wären aber dann wohl Maßnahmen nach Art einer „Rasterfahndung", die der BFH gerade als unzulässig verworfen hat und die mit Sicherheit auch nicht mit der Rechtsprechung des Bundesverfassungsgerichts in Einklang stünden. Auch der Umstand, daß die Sparbücher bei einem Einbruch gestohlen worden sind, kann sicher nicht als konkretes Merkmal für die Möglichkeit herhalten, daß gerade die zu diesen Sparguthaben geflossenen Zinseinnahmen nicht versteuert worden sind.

(2) Es ist auch nicht erkennbar, zu welcher besonderen Personengruppe, über die die Finanzbehörde spezielle, im Hinblick auf Steuerhinterziehung relevante allgemeine Erfahrungen hat, die Geschädigten gehören sollten. Sie gehören zu der „Personengruppe" derjenigen, die Sparguthaben besitzen. Da heutzutage die meisten Bürger in der Bundesrepublik ein Sparbuch haben, gehören sie keiner „besonderen" Personengruppe an. Es dürfte problematisch sein, wollte die Finanzbehörde bzw. die Steuerfahndung sich darauf berufen, erfahrungsgemäß versteuerten Sparkonteninhaber ihre Zinseinnahmen nicht. Bestünde ein solcher Erfahrungswert, müßten die Finanzämter wegen des Gebots der gleichmäßigen Besteuerung bei jeder Einkommensteuererklärung und allen Lohnsteuerjahresausgleichsanträgen, in denen keine Zinseinkünfte angegeben worden sind, entsprechende Nachfragen zur Ermittlung des Sachverhalts halten, da - wie ausgeführt - heute fast jeder ein Sparguthaben hat. Dies geschieht in der täglichen Praxis der Finanzämter jedoch nicht. Erst recht wird sich die Steuerfahndung nicht darauf berufen wollen, es sei eine allgemeine Erfahrung, daß gerade die Eigentümer solcher Sparbücher, die irgendwann gestohlen werden, ihre Zinseinnahmen nicht deklarieren.

Die verfassungsrechtliche Ermittlungsschranke - ein „hinreichender Anlaß" - darf nicht dadurch ihrer praktischen Wirksamkeit beraubt werden, daß man den Inhalt des hinreichenden Anlasses sich in ein Nichts auflösen läßt. Nach allem war das Erfordernis eines hinreichenden Anlasses für die Aufnahme von Ermittlungen im vorliegenden Fall nicht erfüllt. Denn die Meldung im Landeskriminalblatt über den Einbruch im hier erörterten Fall enthielt nichts, was als „hinreichender Anlaß" zu steuerlichen Ermittlungen gegen die Geschädigten hätte herhalten können.

Die vorstehend herausgearbeitete verfassungsrechtliche Ermittlungsschranke steht auch nicht im Widerspruch zu dem im Besteuerungsverfahren und im Steuerstrafverfahren geltenden Legalitätsprinzip. Zwar haben die Finanzbehörden von Amts wegen die notwendigen Ermittlungen anzustellen, um eine gleichmäßige Besteuerung zu gewährleisten. Daraus folgt jedoch nicht die Zulässigkeit einer Sachaufklärung um jeden Preis. Das der Sachaufklärung dienende Beweisverfahren ist nicht nur an Form- und Ordnungsvorschriften gebunden, es muß auch die rechtliche und sittliche Wertordnung des Grundgesetzes beachtet werden. Mit dem Übermaßverbot und dem Grundsatz der Verhältnismäßigkeit wäre eine Verpflichtung zur Sachaufklärung ohne hinreichenden Anlaß, also ins Blaue hinein, unvereinbar.

Auch im Strafrecht gibt es keine unbeschränkte Ermittlungsbefugnis. Abgesehen davon, daß nach § 152 StPO das Vorliegen eines Anfangsverdachts Voraussetzung für die Einleitung eines Ermittlungsverfahrens ist, haben ausgehend von § 136a StPO Rechtsprechung und Lehre das Institut des Beweisverbotes und des Beweisverwertungsverbotes entwickelt. Danach dürfen Beweise, die unter Verstoß gegen ein Beweisverbot erhoben worden sind, nicht verwertet werden. In der steuerrechtlichen Literatur ist vor allem unterschieden worden zwischen der Verletzung bloßer Form- und Ord-

nungsvorschriften und der Verletzung von solchen Beweis- und Ermittlungsverboten, die der Ermittlung um jeden Preis Grenzen setzen. Nur letztere werden als echte Beweisverbote bezeichnet. Der Verstoß gegen solche Beweisverbote löst ein Verwertungsverbot aus. Danach dürfen insbesondere Ermittlungshandlungen, mit denen gegen Grundrechte, insbesondere gegen Art. 1 und 2 GG verstoßen wird, nicht verwertet werden. Das Verbot der Aufnahme von Ermittlungen ohne hinreichenden Anlaß dient dem Schutz des aus Art. 1, 2 GG abgeleiteten Persönlichkeitsrechts. Für die ohne hinreichenden Anlaß ermittelten Erkenntnisse im hier erörterten konkreten Fall kann daher von einem Verwertungsverbot für die durch die Steuerfahndung ermittelten Tatsachen ausgegangen werden.

Ich habe der Finanzbehörde meine Rechtsauffassung mitgeteilt und sie um Stellungnahme gebeten. Außerdem habe ich die Finanzbehörde um Auskunft darüber gebeten, nach welchen Kriterien die Steuerfahndung bisher entschieden hat, ob sie Ermittlungen einleitet oder nicht.

3.6.2 Kontrollmitteilungsverordnung

Wer meine bisherigen Tätigkeitsberichte kennt, weiß vermutlich, wie alt inzwischen die Forderung der Datenschutzbeauftragten nach einer tragfähigen Rechtsgrundlage für den Austausch von Kontrollmitteilungen im Besteuerungsverfahren ist (zuletzt 7. TB 4.9.1, S. 72).

Seit dem Inkrafttreten des § 93a AO, der Grundlage für die Kontrollmitteilungsverordnung ist, sind vier Jahre vergangen (Inkrafttreten: 25.12.85), ohne daß die Verordnung verabschiedet worden ist. In Erwartung der Verordnung zu § 93a AO habe ich mich in den zurückliegenden vier Jahren in Bezug auf Kontrollmitteilungen im Bereich der Steuerverwaltung mit wenigen Ausnahmen abwartend verhalten. Ich habe der Finanzbehörde allerdings mit Schreiben vom 24.4.1989 und 27.9.1989 erklärt, daß ich nunmehr alle Kontrollmitteilungen, die ohne ausreichende Rechtsgrundlage ausgetauscht werden, beanstanden werde.

Ich will meinen Standpunkt zu Kontrollmitteilungen noch einmal verdeutlichen:

— Kontrollmitteilungen bedürfen einer tragfähigen Rechtsgrundlage.

— § 93a AO allein ist noch keine ausreichende Rechtsgrundlage. Erst eine Verordnung zu § 93a AO kann für die in § 93a AO genannten Arten von Kontrollmitteilungen eine solche Grundlage schaffen.

— Alle Kontrollmitteilungen, die in einer Verordnung zu § 93a AO nicht angeordnet werden können, weil eine entsprechende Ermächtigung in dieser Vorschrift nicht ausgesprochen ist, und für die keine spezielle Rechtsgrundlage in einem anderen Gesetz (wie z. B. § 29 Abs. 3 Bewertungsgesetz) existiert, sind unzulässig.

— Kontrollmitteilungen, die in der Verordnung zu § 93a AO zwar angeordnet werden könnten, weil § 93a AO eine entsprechende Ermächtigung enthält, begegnen inzwischen immer stärkeren Bedenken, weil die sie tragende rechtliche Grundlage tatsächlich eben noch nicht existiert. Nach der Rechtsprechung des Bundesverfassungsgerichts darf die Verwaltung „für eine Übergangszeit bis zur Schaffung ausreichender gesetzlicher Grundlagen" mit einer bisher geübten in verfassungsrechtlich geschützte Positionen des Bürgers eingreifenden Praxis nur in dem Umfang fortfahren, der im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Betriebes unerläßlich ist (BVerfGE Band 41 Seite 251/266 ff.; Band 51 Seite 268/287 ff). Dabei hat sie nicht nur zu prüfen, was in der jeweiligen Situation unerläßlich ist. Sie hat auch zu prüfen, ob nicht unter Berücksichtigung der gegebenen Verhältnisse eine schonendere Maßnahme als die bisher geübte Praxis ausreicht, dies insbesondere dann, wenn eine bereits vorliegende rechtliche Rahmenregelung solche schonendere Regelung trifft. Dies ist in Bezug auf Kontrollmitteilungen im Bereich der Abgabenordnung insofern der Fall, als in § 93a Abs. 3 AO bestimmt

worden ist, daß die Betroffenen über gefertigte Kontrollmitteilungen zu unterrichten sind. Eine solche Unterrichtung der Betroffenen war bisher nicht vorgeschrieben und wurde auch nicht praktiziert.

Ich vermag nicht zu übersehen, welche Kontrollmitteilungen zur Zeit an die Finanzbehörden übermittelt werden. Deshalb vermag ich auch nicht zu beurteilen, ob in meinem Zuständigkeitsbereich noch unzulässige Kontrollmitteilungen ausgetauscht werden. Ich habe die Finanzbehörde gebeten, mir bis Ende Oktober 1989 mitzuteilen,

— ob und gegebenenfalls welche Kontrollmitteilungen ohne ausreichende Rechtsgrundlage von öffentlichen Stellen außerhalb des Finanzbereichs und von privaten Stellen bei den Finanzämtern eingehen,

— auf Grund welcher allgemeinen Weisungen, Ersuchen oder Anordnungen die absendenden Stellen die Kontrollmitteilungen fertigen,

— ob die Betroffenen über die Kontrollmitteilungen unterrichtet werden,

— was mit solchen bei den Finanzämtern eingehenden Kontrollmitteilungen geschieht, die nach meinen obigen Ausführungen zweifellos unzulässig sind.

Dieser Bitte ist die Finanzbehörde bisher noch nicht nachgekommen.

3.7 Einwohnerwesen

3.7.1 Ausländerzentralregister

In meinem 7. Tätigkeitsbericht (4.10.1, S. 78) habe ich mich zu dem Referentenentwurf eines Gesetzes über das Ausländerzentralregister (AZR), den der Bundesminister des Innern im Juli 1988 vorgelegt hatte, ausführlich geäußert. Am 6.6.1989 hat die Bundesregierung einen neugefaßten Entwurf beschlossen und dem Bundesrat zur Stellungnahme zugeleitet. Diese Gelegenheit habe ich genutzt, um einige grundsätzliche Anmerkungen zum AZR zu machen, die ich an dieser Stelle noch einmal wiedergeben möchte:

— Nach der Rechtsprechung des Bundesverfassungsgerichts ist das Recht auf informationelle Selbstbestimmung Teil des in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankerten allgemeinen Persönlichkeitsrechts. Dieser Grundrechtsschutz steht uneingeschränkt auch den in der Bundesrepublik Deutschland und Berlin lebenden Ausländern zu. Auch sie müssen Eingriffe und Einschränkungen ihrer Rechte nur im überwiegenden Allgemeininteresse hinnehmen. Deshalb dürfen die gesetzlichen Regelungen zum AZR nicht zu einer allgemeinen Diskriminierung der Ausländer führen. Ein mit dem AZR vergleichbares zentrales Kommunikationssystem existiert für deutsche Staatsangehörige nicht. Schon aus diesem Grund muß sich das AZR auf die notwendigsten Funktionen beschränken, um sicherzustellen, daß nur die unerläßlichen Eingriffe in das informationelle Selbstbestimmungsrecht von Ausländern vorgenommen werden.

— Gegen die vorgesehene Verwendung des AZR als Indexregister zum Zweck der Feststellung, ob eine - und wenn ja, welche - Ausländerbehörde Unterlagen über einen bestimmten Ausländer besitzt, habe ich keine Bedenken, weil damit lediglich der Zugang zu den Akten der Ausländerbehörden erleichtert werden soll. Das System darf jedoch den Rückgriff auf die bei den örtlichen Behörden gesammelten Informationen nicht ersetzen. Keinesfalls darf das AZR zu einem bundesweiten zentralen Informations- und Kommunikationssystem über Ausländer ausgebaut werden, in welches nicht nur Hinweise zur Identität des Ausländers und zur aktenführenden Ausländerbehörde, sondern Daten über die verschiedensten Lebenssachverhalte, die für irgendeine der mit dem AZR kommunizierenden Behörden von Interesse sein könnten, eingespeichert werden. Genau dies ist jedoch geplant. So sollen etwa auch subjektiv gefärbte „Einreisebedenken", Angaben aus den verschiedensten Verwaltungsverfahren anderer Behörden (Verfahren zur Feststellung der Eigenschaft als Deutscher, Einbürgerungsverfahren, Asylverfahren), bestehende

strafrechtliche Verdachtsmomente, Suchvermerke und sogar der gesamte INPOL-Fahndungsbestand im AZR gespeichert werden - und dies, um dem Register eine sogenannte „Substitutionsfunktion" zu übertragen, d.h. Entscheidungen der verschiedensten Dienststellen nur aufgrund von Registerauskünften zu ermöglichen, ohne daß mit der sachbearbeitenden Ausländerbehörde Kontakt aufgenommen werden müßte.

— Nach der Gesetzesbegründung soll die Substitutionsfunktion „insbesondere die für Eilentscheidungen relevanten Erkenntnisse" ermöglichen. Aus dem Gesetzestext ergibt sich dies jedoch nicht. Vielmehr läßt das Gesetz zu, daß nicht nur die mit ausländerrechtlichen Entscheidungen betrauten Behörden, sondern sämtliche Polizeivollzugsbehörden, Staatsanwaltschaften, Zollbehörden, Arbeitsämter, ja selbst sämtliche Geheimdienste das AZR als allgemeines Auskunftssystem benutzen können - und wie vorauszusehen ist, auch benutzen werden. Diese - zumindest bewußt in Kauf genommene - Möglichkeit der Registernutzung wird noch dadurch erleichtert, daß sämtlichen genannten Behörden ein on-line-Zugriff auf die gespeicherten Daten ermöglicht werden soll. Damit wird das AZR - trotz aller schon bei anderer Gelegenheit vorgebrachten verfassungsrechtlichen Bedenken - zu einem „Bundesmelderegister" für Ausländer ausgebaut, noch dazu angereichert mit den verschiedensten Sozial- und Intimdaten und somit für Ausländer das informationelle Selbstbestimmungsrecht ausgehöhlt, denn sie werden durch die Zusammenführung sämtlicher Daten der beteiligten Behörden tatsächlich zu „gläsernen Menschen".

— Hinzu kommt, daß eine Vielzahl der mit dem Register kommunizierenden Behörden die Übermittlungen an das Register im Wege der Datenfernübertragung vornehmen soll, so daß das AZR - trotz der in § 6 Abs. 1 vorgeschriebenen Nachberichtspflicht - weder für die Richtigkeit noch für die Aktualität der gespeicherten Daten Verantwortung übernehmen kann. Gleichzeitig werden mit dieser Konstruktion die Rechte der Betroffenen in unzumutbarem Maße beschränkt. Ihnen wird zugemutet, einer Behörde gegenüberzustehen, die eine unübersehbare Anzahl von Datenempfängern bedient, selbst aber nicht garantieren kann, korrekte Daten geliefert zu haben, und vielleicht nicht einmal weiß, von wem die Daten in das Register eingestellt worden sind. Damit wird die Realisierung von Berichtigungsansprüchen faktisch unmöglich gemacht, weil die Betroffenen gerade nicht erfahren werden, wer was wann und bei welcher Gelegenheit über sie erfahren und ggf. als Erkenntnis in eigene Akten oder Dateien übernommen hat. Dies gilt umso mehr, als viele der Betroffenen ihre Rechte auch noch aus dem Ausland verfolgen müssen, weil Eintragungen im Register eine (Wieder-) Einreise von vornherein verhindern.

  Völlig aussichtslos wird ein solches Unterfangen schließlich, wenn das Hindernis auf überhaupt nicht mehr faßbaren, auf subjektiver Einschätzung von Sachbearbeitern beruhenden „Einreisebedenken" oder verkürzten und damit meist den tatsächlichen Sachverhalt verzerrenden Textzusätzen beruhen.

Nach allem komme ich deshalb zu dem Ergebnis, daß der Entwurf einer verfassungsrechtlichen Prüfung nicht standhalten kann und entscheidender Veränderung bedarf.

So muß - wenn nicht ein völliger Verzicht auf die Substitutionsfunktion des Registers geboten ist - zumindest gesetzlich festgeschrieben werden, daß das Register neben seiner Identifizierungs- und Nachweisfunktion nur für Eilentscheidungen genutzt werden darf. Entsprechend ist der Datenbestand auf die Daten zu beschränken, die für Eilentscheidungen unerläßlich sind. Sonstige Entscheidungen zuungunsten der Betroffenen allein aufgrund von Registerauskünften sollten ausdrücklich verboten werden. Der on-line-Zugriff auf diese Daten ist auf solche Behörden zu beschränken, die ausländerrechtliche Eilentscheidungen zu treffen haben. Im übrigen ist im Register festzuhalten, wer welche Daten eingestellt oder abgerufen hat.

Obwohl die Stellungnahme des Bundesrats bereits seit Mitte September vorliegt, hat die Bundesregierung ihren Entwurf noch nicht im Bundestag eingebracht.

3.7.2 Projekt Automation Standesämter (PASTA)

Im Berichtsjahr bin ich darüber unterrichtet worden, daß der Senat ein Automationsvorhaben im Personenstandswesen plant. Das Projekt befindet sich derzeit unter Federführung des Bezirksamtes Harburg in einer ersten Erprobungsphase im Standesamt Eimsbüttel. Die Projektleitung strebt an, im Laufe des Jahres 1990 das automatisierte Verfahren in allen hamburgischen Standesämtern aufzunehmen.

Nach dem gegenwärtigen Projektstand soll hierfür das PC-Netzwerk „AUTISTA" eingesetzt werden. Dieses spezielle, für standesamtliche Zwecke entwickelte PC-Verfahren ermöglicht die weitgehend automatisierte Erledigung der umfangreichen Schreibarbeiten für die Herstellung der Urkunden und Einträge sowie der sonstigen im Zusammenhang mit den Beurkundungen stehenden Nebenarbeiten. Der Standesbeamte erhebt die bislang im herkömmlichen Schreibverfahren erfaßten Daten nunmehr mittels eines PC und speichert sie vorübergehend für die Beurkundung und die mit ihr zusammenhängenden Nebenarbeiten, insbesondere den umfangreichen standesamtlichen Mitteilungsverkehr. Außer auf technische Fragen, die aus datenschutzrechtlicher Sicht bei der weiteren Umsetzung des Vorhabens von besonderer Bedeutung sind, habe ich in einer ersten Stellungnahme darauf hingewiesen, daß bei der Durchführung des Projekts auch rechtliche Probleme auftreten. So besteht mit der Behörde für Inneres Einvernehmen darüber, daß die derzeitigen Erlaubnisvorschriften für die personenbezogene Datenverarbeitung, insbesondere die Übermittlungsvorgänge, im Standesamtsbereich unzureichend sind. Spätestens seit dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 reichen Verwaltungsvorschriften - wie z.B. die Dienstanweisung für Standesbeamte - als Befugnisnorm nicht mehr aus. Ohne Änderung der Rechtsgrundlagen kann die Datenverarbeitung der Standesämter in der gegenwärtigen Form lediglich noch während einer Übergangszeit geduldet werden. Es ist derzeit völlig ungewiß, wann mit einer entsprechenden Änderung der personenstandsrechtlichen Vorschriften gerechnet werden kann.

In Anbetracht dieser Situation habe ich Bedenken, bereits bestehende Datenverarbeitungsabläufe durch die Ausschöpfung neuer technischer Möglichkeiten qualitativ zu verändern. Auch die Behörde für Inneres hat zum Ausdruck gebracht, daß nach der gegenwärtigen Rechtslage eine Automation im Personenstandswesen nur als Arbeitshilfe bei den standesamtlichen Beurkundungen und den damit in unmittelbarem Zusammenhang stehenden Nebenarbeiten zulässig sein darf.

Die Projektplanung sieht übrigens in einer späteren Projektausbaustufe vor, einen online-Anschluß oder einen Datenträgeraustausch zu bzw. mit anderen automatisierten Verfahren, wie z.B. Einwohnerwesen, zu realisieren. Da es gegenwärtig hierfür keine Rechtsgrundlage gibt, müßte vor einer Umsetzung dieses Vorhabens zunächst eine entsprechende Änderung des Hamburgischen Meldegesetzes in Angriff genommen werden.

3.8 Polizei

In die Diskussion um die polizeiliche Datenverarbeitung ist Bewegung geraten. Nicht nur, daß die Datenverarbeitungssysteme konzeptionell überdacht und dynamisch ausgebaut werden; endlich hat die Behörde für Inneres im Berichtsjahr auch einen Entwurf für ein neues Polizeirecht vorgelegt, mit dem die verfassungsrechtlich gebotenen gesetzlichen Grundlagen für diese Datenverarbeitung geschaffen werden sollen.

3.8.1 Entwurf für ein neues Polizeirecht in Hamburg

Nachdem bereits einige Verwaltungsgerichte dem Begehren von Bürgern auf Löschung ihrer bei der Polizei gespeicherten personenbezogenen Daten entsprochen haben, ist in diesem Berichtszeitraum eine im Ergebnis übereinstimmende Entscheidung des Verwaltungsgerichts Hamburg ergangen. Das Verwaltungsgericht hat dem Kläger gegenüber der Innenbehörde einen uneingeschränkten Auskunftsanspruch mit

der Begründung zuerkannt, daß die Speicherung seiner personenbezogenen Daten bei der Staatsschutzabteilung der Polizei mangels gesetzlicher Grundlage rechtswidrig sei. Es bleibt abzuwarten, ob diese Entscheidung, gegen die von der Behörde Berufung eingelegt worden ist, vom Oberverwaltungsgericht bestätigt wird.

Um die dringend benötigten Rechtsgrundlagen für die polizeiliche Datenverarbeitung zu schaffen, sind in den letzten Jahren in Berlin, Niedersachsen, Hessen, Bayern, Nordrhein-Westfalen und im Saarland Entwürfe für die Novellierung der Polizeigesetze erarbeitet worden. Im Januar 1990 will nun auch der Hamburger Senat den Entwurf eines Gesetzes zur Änderung des SOG und zur Sicherung des Datenschutzes bei der Polizei beschließen. Das Gesetz soll noch in dieser Legislaturperiode verabschiedet werden.

3.8.1.1 Konzeption der Novellierung

Von einer umfassenden Novellierung des SOG, das seit seinem Inkrafttreten 1966 im wesentlichen unverändert geblieben ist, wurde wegen der in dieser Legislaturperiode nur noch begrenzt zur Verfügung stehenden Zeit Abstand genommen. Statt dessen ist ein aus zwei Artikeln bestehender Gesetzentwurf erarbeitet worden, der das Ziel verfolgt, zum einen offenkundige Regelungsdefizite im geltenden SOG zu beseitigen und zum anderen dringend erforderliche Regelungen über die Datenverarbeitung der Polizei zu schaffen. Diese Konzeption begegnet folgenden Bedenken:

Da der Gesetzentwurf bereichsspezifische Regelungen nur für die Datenverarbeitung der Polizei enthält, läßt er weiterhin eine Regelungslücke in den Fällen offen, in denen eine andere Verwaltungsbehörde Maßnahmen zur Abwehr einer Gefahr ergreift und die damit im Zusammenhang stehende Erhebung und Verarbeitung personenbezogene Daten (noch) nicht bereichspezifisch geregelt ist. Solche speziellen Regelungen fehlen z. B. weitgehend im Bauordnungsrecht, im Gewerberecht und im Bereich des technischen Umweltschutzes. Sind im Spezialgesetz entsprechende Regelungen (noch) nicht enthalten, so müssen die Bestimmungen des allgemeinen Polizei- und Ordnungsrechts herangezogen werden. Für einen Rückgriff auf das noch allgemeinere Datenschutzgesetz ist daneben aus Gründen der Gesetzessystematik kein Raum. Es bleibt festzuhalten, daß der hamburgische Gesetzgeber, um diese Regelungslücke zu schließen, so bald wie möglich eine eigene Regelung für die Datenverarbeitung der Ordnungsbehörden treffen muß.

3.8.1.2 Wichtige Kritikpunkte

Zu dem Entwurf habe ich gegenüber der Innenbehörde eine umfangreiche Stellungnahme abgegeben. Da ich an dieser Stelle nicht auf alle Einzelheiten eingehen kann, „beschränke" ich meine Ausführungen auf einige besonders wichtige Kritikpunkte:

3.8.1.2.1 Abkehr von den Grundsätzen des traditionellen Polizeirechts

Ziel des Entwurfes ist nicht nur die Beseitigung von Regelungsdefiziten und die Schaffung der gebotenen bereichsspezifischen Regelungen für die Datenverarbeitung der Polizei. Es geht vielmehr auch darum, die polizeiliche Tätigkeit weit in das Vorfeld konkreter Gefahren zu verlagern und jeden Bürger in polizeiliche Maßnahmen einzubeziehen.

Nach herkömmlicher Rechtslage hat die Polizei generell zwei Aufgaben zu erfüllen: zum einen Straftaten (§ 163 Abs. 1 StPO) sowie Ordnungswidrigkeiten (§ 53 Abs. 1 OWiG) zu erforschen; zum anderen im Einzelfall bestehende konkrete Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren, soweit andere Verwaltungsbehörden nicht rechtzeitig eingreifen können. Ein polizeilicher Eingriff in die Rechte des Bürgers setzt also nach bisherigem Recht im Bereich der Gefahrenabwehr das Vorliegen einer konkreten Gefahr voraus. Außerdem dürfen sich polizeiliche Maßnahmen nur gegen

Störer, also die Verursacher der Gefahr, sowie unter bestimmten engen Voraussetzungen gegen Notstandspflichtige richten.

Von diesen traditionellen Grundsätzen soll nun - der langjährigen Praxis folgend - in zweifacher Hinsicht abgewichen werden:

Zum einen soll die Polizei für die Verfolgung künftiger Straftaten vorsorgen und drohende Gefahren verhüten (vorbeugende Bekämpfung von Straftaten) sowie die erforderlichen Vorbereitungen für die Hilfeleistung in Gefahrenfällen treffen. Diese neuen Aufgaben knüpfen gerade nicht mehr an das Vorliegen einer konkreten Gefahr an, sondern bewegen sich im Vorfeld der herkömmlichen Gefahrenabwehr. Deshalb handelt es sich nicht lediglich um eine Klarstellung der Aufgaben der Polizei, sondern um eine Aufgabenerweiterung, zu deren Erfüllung der Polizei erstmals zahlreiche Eingriffsbefugnisse im Bereich der Informationsbeschaffung und -verarbeitung eingeräumt werden. Die Vorverlagerung polizeilicher Maßnahmen zur „vorbeugenden Bekämpfung von Straftaten" hat zur Folge, daß der traditionelle Anknüpfungspunkt der „Gefahr" künftig nicht mehr die Regel, sondern „die mehr und mehr zur Polizeirechtsgeschichte degenerierende Ausnahme" ist.

Zum anderen sollen die polizeilichen Befugnisse auf „andere Personen" ausgedehnt werden, die nach herkömmlichem Recht weder Störer noch Notstandspflichtige sind. Damit wird auch hier das Regel-Ausnahme-Verhältnis der traditionellen polizeilichen Eingriffslehre zuungunsten des Bürgers verändert: Die Differenzierung zwischen Störer und Nichtstörer verliert ihre Bedeutung, was den Zugriff auf jedermann immer mehr zur Regel macht. Auf diese Weise wird die Freiheit des einzelnen, „vom Staat in Ruhe gelassen zu werden" (BVerfGE 27,1), solange er nicht in die Rechte anderer eingreift, in verfassungsrechtlich bedenklicher Weise eingeschränkt.

3.8.1.2.2 Gefahrenabwehr oder Strafverfolgung?

Von der Beantwortung der Frage, ob die „vorbeugende Bekämpfung von Straftaten" dem Bereich der Strafverfolgung oder der Gefahrenabwehr zuzuordnen ist, hängt die Gesetzgebungskompetenz des hamburgischen Gesetzgebers ab. Unterfällt diese Aufgabe dem Bereich der Strafverfolgung, so steht den Ländern gemäß Art. 72 Abs. 1 i. V. m. Art. 74 Nr. 1 GG die Regelungskompetenz nur zu, solange und soweit der Bund von seinem Gesetzgebungsrecht keinen Gebrauch gemacht hat. Bisher steht eine Regelung durch den Bundesgesetzgeber noch aus; der Bundesjustizminister beabsichtigt aber - wie dem Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts - StVÄG 1989 (Stand: 26. Juni 1989) zu entnehmen ist-, die Datenverarbeitung der Strafverfolgungsbehörden „für Zwecke künftiger Strafverfolgung" zu regeln. Sobald der Bund die vorgesehenen Regelungen in Gesetzesform verabschiedet, würden die landesrechtlichen Vorschriften gegenstandslos. Für eine befriedigende Lösung dieser Streitfrage ist es unumgänglich, den seit Jahren zwischen Innen- und Justizministern bestehenden Kompetenzkonflikt endlich durch einen Konsens zu beenden.

Nach meiner Auffassung kann lediglich die Verhütung von Straftaten dem Bereich der Gefahrenabwehr zugerechnet werden. Dabei gehe ich davon aus, daß eine Verhinderung von Stratataten mit polizeilichen Mitteln nur in Betracht kommt, wenn deren Begehung im konkreten Einzelfall hinreichend wahrscheinlich ist. Hierfür stehen der Polizei nach herkömmlichem Polizeirecht aber ausreichend Befugnisse zur Verfügung. Um Straftaten zu verhüten, für deren beabsichtigte Begehung es keinerlei Anhaltspunkte gibt, die vielleicht noch gar nicht geplant sind, dafür ist die Erhebung und Speicherung von Daten durch die Polizei ungeeignet und es liegt auch gar nicht in ihrer Absicht, ihre Datensammlungen hierfür zu nutzen.

Wie die Praxis zeigt, geht es der Polizei vielmehr schwerpunktmäßig darum, zur Aufklärung von Straftaten auf ihre Datensammlungen zurückgreifen zu können. Wird eine Straftat begangen, so sollen aus den polizeilichen Datenbeständen mit Hilfe automati-

sierter Aktenerschließungs- und Verknüpfungsverfahren Verdächtige ermittelt werden. Damit weist die Vorsorge für die Verfolgung künftiger Straftaten eine größere Sachnähe zur Strafverfolgung als zur Gefahrenabwehr auf. Sie läßt sich auch nicht allein deshalb dem Bereich der Gefahrenabwehr zuordnen, weil sie zukunftsgerichtet ist und weil es im Zeitpunkt der Speicherung an einem gemäß § 152 StPO erforderlichen konkreten Tatverdacht fehlt. Denn der Sache nach handelt es sich um „antizipierte" Strafverfolgung. Dies spricht dafür, die Voraussetzungen der Sammlung und Speicherung von Daten zum Zwecke der Vorsorge für künftige Strafverfolgung im Strafverfahrensrecht zu regeln.

Eine Regelung in der StPO würde nicht zwangsläufig zum Verbot polizeilicher Datenverarbeitung zu diesem Zweck führen. Sie muß allerdings - dem Grundgedanken des Strafprozeßrechts entsprechend - der Leitung und Kontrolle der Staatsanwaltschaft unterstellt werden. Außerdem dürfte auf die Datensammlungen im Einzelfall nur dann zurückgegriffen werden, wenn der im Strafverfahrensrecht geforderte Anfangsverdachteine unverzichtbare rechtsstaatliche Voraussetzung für die Aufnahme von Ermittlungen gegeben wäre. Auf diese Weise würde sichergestellt werden, daß der Bürger erst dann zum Gegenstand polizeilicher Ermittlungen wird, wenn konkrete Anhaltspunkte dafür vorliegen, daß er eine Straftat begangen haben könnte.

Sollte es in Ausnahmefällen wirklich einmal erforderlich sein, die zur Vorsorge für die künftige Strafverfolgung angelegten Datensammlungen zum Zwecke der Gefahrenabwehr zu nutzen, so stellt diese Nutzung eine Zweckänderung dar. Sie darf nur unter Voraussetzungen zugelassen werden, die im Gesetz - nach meiner Auffassung ebenfalls im Strafverfahrensrecht - genau festgelegt werden müssen.

Trotz meiner Bedenken gegen eine Regelung der polizeilichen Datenverarbeitung zur Vorsorge für künftige Strafverfolgung in den Landespolizeigesetzen kann ich mich den von der Innenbehörde angeführten Argumenten für eine solche Regelung nicht verschließen. Angesichts der Ungewißheit, wann eine bundesgesetzliche Regelung zu erwarten ist, würde ein Regelungsverzicht des hamburgischen Gesetzgebers dazu führen, den verfassungsrechtlich bedenklichen Zustand fehlender gesetzlicher Grundlagen für die polizeiliche Informationsverarbeitung noch länger aufrecht zu erhalten. Allerdings müßte er wenn er von seiner konkurrierenden Kompetenz Gebrauch macht die im Strafverfahrensrecht geltende Voraussetzung des Anfangsverdachts sowohl bei der Erhebung als auch bei der Nutzung auf personenbezogene Daten berücksichtigen und die Datenverarbeitung der Polizei im Vergleich zur bisherigen Praxis erheblich einschränken.

3.8.1.2.3 Besondere Gefährdungen des Persönlichkeitsrechts durch den Einsatz neuer Informationstechnologien

In der Einleitung (1.3) hatte ich darauf hingewiesen, daß großräumige Verbundsysteme, völlig neue Formen der Massendatenverarbeitung, hochleistungsfähige Verknüpfungsverfahren, eine ständig zunehmende Zahl von on-line-Verbindungen, der Einsatz selbsttätiger Aufzeichnungsgeräte sowie die Entwicklung von Mustererkennungstechniken und der Aufbau von Bilddatenbanken neuartige Gefährdungen des Rechts auf informationelle Selbstbestimmung mit sich bringen, die in ihren Auswirkungen auf das Persönlichkeitsrecht teilweise noch gar nicht abzuschätzen sind.

Angesichts dieser technischen Möglichkeiten und des zunehmenden Einsatzes von PCs in der polizeilichen Praxis besteht die Gefahr, daß die Verarbeitung und Übermittlung einer Vielzahl personenbezogener Daten nicht mehr überschaubar und wirksam zu kontrollieren ist. Um diesen Gefahren für den Freiheitsbereich des einzelnen zu begegnen, bedarf es präzise formulierter Eingriffsermächtigungen, der Beschränkung des Einsatzes neuer Informationstechnologien auf das unbedingt erforderliche Maß, der strikten Beachtung des Zweckbindungsgebotes und ausreichender verfahrensrechtlicher Sicherungen. Diesen Anforderungen wird der Gesetzentwurf weitgehend nicht gerecht.

3.8.1.2.4 Straftaten mit erheblicher Bedeutung

Fast alle wesentlichen Befugnisse zur Datenverarbeitung, auch so gravierende Erhebungsmethoden wie die verdeckte Anwendung technischer Mittel oder der Einsatz von V-Leuten und verdeckt ermittelnden Polizeibeamten knüpfen nach dem Entwurf an den Begriff der „Straftaten mit erheblicher Bedeutung" an. Da dieser Begriff keinen feststehenden Inhalt hat, wird im Gesetzentwurf der Versuch einer - restriktiven - Legaldefinition unternommen. Dies ist grundsätzlich zu begrüßen. Gleichwohl muß der Versuch als gescheitert angesehen werden. Darüber hinaus ist der so definierte Begriff nicht geeignet, die Voraussetzung für die schwerwiegensten Informationseingriffe zu bieten.

Nach § 1 Abs. 4 GDPol-E sind Straftaten mit erheblicher Bedeutung insbesondere Verbrechen sowie die in §§ 129, 138 StGB genannten Straftaten und katalogmäßig aufgeführte sonstige Straftaten, wenn diese gewerbsmäßig oder bandenmäßig begangen wurden. Diese Definition enthält nach zwei Seiten Öffnungen, durch die jede weitere Straftat mit einbezogen werden kann. Selbst Bagatellstraftaten sind nicht ausgeschlossen.

Eines der beiden Einfallstore ist das Wort „insbesondere", das von vornherein die Möglichkeit eröffnet, jeder beliebigen Straftat erhebliche Bedeutung zuzumessen, und damit die angestrebte Beschränkung wieder zunichte macht. Es muß deshalb gestrichen werden. Die andere Öffnung ergibt sich aus der Nennung des § 129, nach der die Mitgliedschaft in einer Vereinigung strafbar ist, deren Zweck oder Tätigkeit auf die Begehung von Straftaten - gleich welcher Qualität - gerichtet ist. Auch diese Vorschrift muß deshalb aus der Definition gestrichen werden.

Erst aufgrund dieser beiden Änderungen wäre eine gewisse Einengung erreicht und bekäme der Begriff der „Straftaten mit erheblicher Bedeutung" normenklare Konturen, auf deren Grundlage polizeiliche Datenverarbeitungsmaßnahmen gestützt werden könnten.

Aber auch eine solche Definition hätte den Nachteil fehlender Differenzierungsmöglichkeiten. So sind nach der bisherigen Konzeption des Entwurfes der Einsatz verdeckter Ermittler oder längerfristige Observationen an die gleiche Voraussetzung geknüpft wie etwa Identitätsfeststellungen an „gefährlichen Orten". Dies dürfte gegen den Grundsatz der Verhältnismäßigkeit verstoßen. Deshalb ist zu fordern, daß für die besonders tiefen Grundrechtseingriffe unabhängig von der Definition der „Straftaten mit erheblicher Bedeutung" eigenständige Straftatenkataloge geschaffen werden, die wesentlich enger sein müssen als der sehr weite Begriff der Straftaten mit erheblicher Bedeutung.

3.8.1.2.5 Das Zweckbindungsgebot

Das Bundesverfassungsgericht hat im Volkszählungsurteil ausgeführt, daß die Verwendung personenbezogener Daten nur zu dem Zweck erfolgen darf, zu dem sie erhoben worden sind. Der Verwendungszweck ist bereichsspezifisch und präzise zu bestimmen. Um die Zweckbindung sicherzustellen, hält das Gericht außerdem einen amtshilfefesten Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote für erforderlich. Aus diesen Grundsätzen zum Zweckbindungsgebot folgt, daß Zweckänderungen bzw. Zweckdurchbrechungen einen weiteren, über die zweckgebundene Erhebung und Verwendung hinaus gehenden Eingriff in das Recht auf informationelle Selbstbestimmung beinhalten, der seinerseits einer präzisen Regelung bedarf. Nur so kann der Bürger - wenn er überhaupt in der Lage ist, den komplizierten und sehr abstrakten Gesetzestext in seinen praktischen Auswirkungen zu verstehen - abschätzen, wer was wann und bei welcher Gelegenheit über ihn weiß. Diesen Anforderungen wird der Gesetzentwurf in mehrfacher Hinsicht nicht gerecht:

— Die allgemeinen Vorschriften zur Datenspeicherung, -veränderung und -nutzung und zur Datenübermittlung sehen zwar eine Zweckbindung vor. Diese wird aber

durch sehr allgemein gehaltene Voraussetzungen für eine Zweckänderung weitgehend wieder aufgehoben. Einmal rechtmäßig erhobene Daten dürfen zu jedem anderen polizeilichen Zweck verwendet werden, soweit die Polizei die Daten auch zu diesem Zweck hätte erheben dürfen. Da die Tatbestände für eine polizeiliche Datenerhebung derartig weit gefaßt sind, daß kaum eine Situation vorstellbar ist, in der die Polizei Daten nicht erheben dürfte, hat die Zweckbindung für die Polizei praktisch keine Bedeutung. Dies steht in krassem Widerspruch zu der von mir seit langem erhobenen Forderung nach Abschottung von für bestimmte Zwecke angelegten Datensammlungen innerhalb der Polizei.

— Auch bei der Übermittlung von Daten sind Zweckänderungen in großem Umfang zulässig. So kann die Polizei z. B. von sich aus personenbezogene Daten an alle besonderen Ordnungsbehörden übermitteln, wenn diese die Daten aus polizeilicher Sicht zur Erfüllung ihrer Aufgabe benötigen könnten. Auf Ersuchen jeglicher Behörde oder öffentlichen Stelle darf sie Daten weitergeben, wenn dies (1) zur Abwehr einer bevorstehenden Gefahr durch den Empfänger, (2) in besonders gelagerten Einzelfällen zur Feststelllung der gesetzlichen Voraussetzungen für den Erlaß eines Verwaltungsaktes durch eine andere für Aufgaben der Gefahrenabwehr zuständigen öffentlichen Stelle oder (3) zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder schwerwiegende Beeinträchtigungen von gewichtigen Rechtspositionen einzelner erforderlich ist. Diese weit gefaßten Formulierungen ermöglichen es, daß jede von den Behörden für zweckmäßig erachtete Datenübermittlung vorgenommen werden kann.

3.8.1.2.6 Beschränkung des Löschungs- bzw. Vernichtungsgebotes auf „suchfähig gespeicherte personenbezogene Daten"

Die Beschränkung des Löschungs- bzw. Vernichtungsgebotes auf „in Dateien suchfähig gespeicherte personenbezogene Daten" und „zu einer Person suchfähig angelegte Akten" ist sachlich nicht gerechtfertigt. Sie ist meines Erachtens geeignet, das Vernichtungsgebot leerlaufen zu lassen. Denn nach meiner Erfahrung sind personenbezogene Angaben nicht nur - wie es in der Begründung irreführend heißt - „Beiwerk" in einem Sachvorgang oder in einer zu einer anderen Person angelegten Akte. Vielmehr ist es einem mit bestimmten Vorgängen vertrauten Sachbearbeiter in der Regel möglich, beispielsweise auf dem Umweg über eine Sachakte - z.B. zu einem „Fan-Club" - oder bestimmte andere Personenakten gezielt auf darin enthaltene personenbezogene Angaben zurückzugreifen. Um die Löschung bzw. Vernichtung der zu einer bestimmten Person gespeicherten Daten und angelegten Akten sicherzustellen und einen Rückgriff auf dieses Material über Sachakten zu verhindern, muß die Beschränkung auf „suchfähig" gespeicherte Angaben entfallen.

3.8.1.2.7 Verdeckte Datenerhebung

Der Novellierungsentwurf schafft erstmals Befugnisse für die Polizei, Informationen mit verdeckten Mitteln zu erheben. Zu den verdeckten Mitteln zählen die längerfristige Observation, der Einsatz technischer Mittel sowie der Einsatz von Vertrauenspersonen und verdeckten Ermittlern. Ihr Einsatz war nach der bisherigen Gesetzeslage dem nur beobachtenden, nicht mit exekutiven Befugnissen ausgestatteten Verfassungsschutz vorbehalten. Die Übertragung heimlicher Erhebungsbefugnisse auf die mit weitreichenden Eingriffsbefugnissen ausgestattete Polizei ist verfassungsrechtlich bedenklich, weil in einem demokratischen Rechtsstaat staatliche Maßnahmen grundsätzlich offen, d. h. für den Bürger als solche erkennbar und gerichtlich überprüfbar, vorgenommen werden müssen. Nur wenn der Staat dem Bürger „mit offenem Visier" gegenübertritt, ist dieser in der Lage, sein Recht auf informationelle Selbstbestimmung wahrzunehmen und sich gegen vermeintlich rechtswidrige Eingriffe in seine Rechtssphäre mit rechtsstaatlichen Mitteln zur Wehr zu setzen.

Problematisch ist weiterhin, daß beim Einsatz verdeckter Mittel - ebenso wie bei der Speicherung personenbezogener Daten zur vorbeugenden Straftatenbekämpfung - nicht genau genug zwischen dem Zweck der Gefahrenabwehr und dem Zweck der Strafverfolgung unterschieden wird. Soweit sich der Einsatz verdeckter Mittel zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person - etwa im Falle einer Geiselnahme - als notwendig erweist, ist die Regelung im Polizeigesetz nicht zu beanstanden. Allerdings muß bei jeder der besonderen Ermittlungsmethoden sorgfältig geprüft werden, ob sie im Bereich der Gefahrenabwehr wirklich erforderlich ist. An der Erforderlichkeit hege ich insbesondere beim Einsatz verdeckter Ermittler Zweifel. Soweit verdeckte Mittel im Bereich der vorbeugenden Verbrechensbekämpfung eingesetzt werden, geht es der Polizei in erster Linie um die Erforschung und Aufklärung von Straftaten in bestimmten Kriminalitätsbereichen. Sie unterfallen damit dem Bereich der Strafverfolgung und müssen - wie dies im Referententwurf des Bundesministers der Justiz zum Strafverfahrensänderungsgesetz (StVÄG 1989) vorgesehen ist - in der StPO geregelt werden. Aus Gründen der Rechtsstaatlichkeit halte ich es grundsätzlich für erforderlich, so gravierende Eingriffe in das Persönlichkeitsrecht des Betroffenen zumindest an das Vorliegen eines Anfangsverdachts zu knüpfen. Der Zugriff auf Personen jenseits dieser Schwelle - also im Vorfeld strafbarer Handlungen - ist verfassungsrechtlich bedenklich, weil er das Recht des Bürgers, ohne Anfangsverdacht nicht mit Ermittlungshandlungen überzogen und ausgeforscht zu werden, in Frage stellt.

Hält man den Einsatz besonderer Mittel der Datenerhebung dennoch schon im Vorfeld eines Anfangsverdachts für notwendig, so können diese Maßnahmen wegen der damit verbundenen schwerwiegenden Eingriffe in das Recht auf informationelle Selbstbestimmung jedenfalls nur bei der Bekämpfung besonders gravierender oder sozialschädlicher Delikte in Betracht kommen. Nach meinen Erfahrungen ist der Einsatz dieser Mittel nur in Kriminalitätsbereichen erforderlich, 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 durch den Einsatz verdeckter Mittel Informationen zu verschaffen, um überhaupt Straftaten aufdecken und aufklären zu können. Demgegenüber will der Gesetzentwurf den Einsatz verdeckter Mittel zum Zwecke der vorbeugenden Straftatenbekämpfung bereits dann zulassen, wenn Tatsachen die Annahme rechtfertigen, „daß diese Personen Straftaten mit erheblicher Bedeutung begehen werden". Aber nicht jedes Verbrechen, jedes „gewerbs- oder bandenmäßig" begangene Vergehen und schon gar nicht jede sonstige Straftat mit erheblicher Bedeutung ist dem Bereich der organisierten Kriminalität zuzurechnen, für deren Bekämpfung die Polizei nach eigenem Bekunden die verdeckten Erhebungsmethoden braucht. Im Interesse der Normenklarheit sollten die in Betracht kommenden Straftaten in abschließenden Katalogen aufgeführt werden. Keinesfalls dürfen die Befugnisnormen so weit gefaßt werden, daß heimliche Maßnahmen der Polizei - von Bagatellfällen abgesehen - sozusagen routinemäßig zur Verfügung stehen.

Besonders bedenklich ist der Einsatz besonderer Ermittlungsmethoden gegenüber Kontakt- und Begleitpersonen, soweit diese nicht nur als unvermeidbar Betroffene mit

einbezogen werden. Ich halte einen gezielten Einsatz besonderer Mittel nach dem Grundsatz der Verhältnismäßigkeit nicht für zulässig.

Schließlich bedarf es gerade bei der Regelung des Einsatzes besonderer Erhebungsmethoden einer Harmonisierung mit den geplanten Regelungen im Strafverfahrensrecht. Der Polizei dürfen im Bereich der Vorfeldermittlungen keinesfalls weitreichendere Befugnisse eingeräumt werden als bei strafrechtlichen Ermittlungsverfahren, die immerhin einen Anfangsverdacht voraussetzen. Außerdem ist durch Angleichung der Vorschriften sicherzustellen, daß die geplanten Regelungen in der StPO, die z.T. enger und mit wirksameren Verwertungsbeschränkungen versehen sind, nicht durch ein Ausweichen auf parallele Befugnisse im präventiven Bereich umgangen werden.

Die im Gesetzentwurf vorgesehene Regelung erscheint auch deshalb nicht sachgerecht, weil weitgehend gemeinsame Voraussetzungen für den Einsatz der verschiedenen Erhebungsmethoden aufgestellt werden. Die Maßnahmen greifen unterschiedlich stark in das Persönlichkeitsrecht des Betroffenen ein, so daß bezüglich der Voraussetzungen und auch der Anordnungsbefugnisse stärker differenziert werden müßte. Wegen der Eingriffsqualität des Einsatzes technischer Mittel in und aus Wohnungen sowie des Einsatzes von V-Leuten und verdeckten Ermittlern müssen die Voraussetzungen hierfür besonders restriktiv ausgestattet werden. Zu den einzelnen Erhebungsmethoden ist folgendes anzumerken:

3.8.1.2.7.1 Längerfristige Observation

Nur die „längerfristige Observation", d. h. die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder an mehr als 2 Tagen durchgeführt werden soll, unterfällt einschränkenden Voraussetzungen. Meines Erachtens ist die Schwelle zur längerfristigen Observation zu hoch angesetzt. Auch eine Observation von bis zu 24 Stunden Dauer greift so tief in das Persönlichkeitsrecht des Betroffenen ein, daß sie nur unter besonderen Voraussetzungen zulässig sein kann. Deshalb schlage ich vor, Observationen von mehr als 6 Stunden Dauer in den Anwendungsbereich der Sonderregelung einzubeziehen.

3.8.1.2.7.2 Einsatz technischer Mittel

Die Vielzahl der bereits heute verwendeten technischen Mittel von der „Lauschwanze" bis zur „Nadelöhrkamera" sind für den Bürger nicht mehr überschaubar. Deshalb sollten die in Frage kommenden Mittel dem Gebot der Normenklarheit entsprechend im Gesetz abschließend - zumindest aber beispielhaft - aufgezählt werden. Folgt man diesem Vorschlag nicht, so sollte wenigstens aufgrund einer Verwaltungsvorschrift eine detaillierte Liste der von der hamburgischen Polizei verwendeten Mittel aufgestellt und jährlich aktualisiert werden. Diese Liste sollte dem Innenausschuß der Bürgerschaft und dem Hamburgischen Datenschutzbeauftragten zur Kenntnis gegeben werden, um eine Kontrolle des Einsatzes technischer Mittel zu ermöglichen.

3.8.1.2.7.3 Einsatz von Vertrauenspersonen

Der Einsatz von „Vertrauenspersonen" ist besonders problematisch, weil diese schwer zu steuern und zu überwachen sind. Um rechtswidrigen Praktiken vorzubeugen, muß zum einen der Begriff der „V-Person" genau definiert werden. Zum anderen müssen die Grenzen ihres Einsatzes verbindlich festgelegt werden. Außerdem sollte im Gesetz selbst klargestellt werden, daß V-Personen ebenso wie verdeckte Ermittler bei der Erfüllung ihres Auftrages keine Straftaten begehen dürfen. Wegen der Eingriffsintensität des Einsatzes von „V-Leuten" und dem damit verbundenen Risiko der Beteiligung an strafbaren Handlungen sollte diese Erhebungsmethode nur im Bereich der Schwerstkriminalität angewandt werden dürfen.

3.8.1.2.7.4 Einsatz verdeckter Ermittler

Der Einsatz verdeckter Ermittler begegnet ebenfalls schwerwiegenden Bedenken. Ein Problem sehe ich darin, daß der verdeckte Ermittler im „Milieu" stets vor der Frage stehen wird, sich um einer erfolgreichen Durchführung seiner Ermittlungen willen an Straftaten zu beteiligen bzw. diese zumindest nicht zu verhindern oder seinen Einsatz abzubrechen. Häufig wird sich eine Beteiligung an strafbaren Handlungen nur um den Preis des Ermittlungserfolges vermeiden lassen. Dieses stellt einerseits den betroffenen Beamten vor erhebliche Probleme und macht andererseits deutlich, wie fragwürdig ein solcher Einsatz unter rechtsstaatlichen Gesichtspunkten ist. Ferner ist zu bedenken, daß die Durchführung von Ermittlungen mit Hilfe von aktiven Täuschungen aufgrund einer mit falschen Papieren abgesicherten Legende besonders tief in das Persönlichkeitsrecht des Betroffenen eingreift, was allenfalls hinnehmbar wäre, wenn zumindest ein Anfangsverdacht i.S.v. § 152 StPO gegeben wäre. Die Vornahme einer so einschneidenden Maßnahme ohne konkrete Verdachtsmomente verletzt meines Erachtens das Recht des unverdächtigen Bürgers, vom Staat in Ruhe gelassen zu werden. Deshalb halte ich den Einsatz verdeckter Ermittler allenfalls im Bereich der Strafverfolgung für zulässig. Für eine Regelung ausschließlich zu Zwecken der Strafverfolgung spricht außerdem, daß der Einsatz verdeckter Ermittler in erster Linie der Aufklärung von Straftaten dient. Es geht gerade im Bereich der organisierten Kriminalität um die Erlangung qualifizierter Sachbeweise, da ein Zeugenbeweis in diesem Bereich selten geführt werden kann. Schließlich haben nach meiner Kenntnis auch die Verfechter des Einsatzes verdeckter Ermittler im polizeilichen Bereich bisher nicht dargelegt, inwieweit die in der Praxis erzielten Erfolge dem repressiven und dem präventiven Bereich zuzurechnen sind.

3.8.1.2.8 Polizeiliche Beobachtung

Die polizeiliche Beobachtung erfolgt ebenfalls ohne Kenntnis der Betroffenen. Im Gegensatz zu den vorstehend genannten Maßnahmen verschafft sich aber die Polizei nicht aktiv Informationen, sondern registriert lediglich das Auftreten der Betroffenen an bestimmten Orten, z. B. anläßlich einer Identitätsfeststellung an einer Kontrollstelle oder beim Grenzübertritt. Auf diese Weise kann sie ein Bewegungsbild der betreffenden Personen gewinnen.

Die Voraussetzungen für die polizeiliche Beobachtung bedürfen der Einschränkung. Es sollte klargestellt werden, daß personenbezogene Daten nur anläßlich einer zu anderen Zwecken rechtmäßig durchgeführten Polizeikontrolle oder einer grenzpolizeilichen Kontrolle erhoben werden dürfen. Art und Umfang der zu meldenden Daten sollten abschließend im Gesetz festgelegt werden.

Wegen der besonderen Eingriffstiefe der Maßnahme halte ich die Ausschreibung zur polizeilichen Beobachtung ebenfalls nur zur vorbeugenden Bekämpfung besonders schwerwiegender oder sozialschädlicher Straftaten für zulässig. Insoweit verweise ich auf meine Ausführungen zum Einsatz verdeckter Mittel. Die Erhebung von Daten etwaiger Begleitpersonen muß an noch engere Voraussetzungen geknüpft werden. An die Erforderlichkeit ist ein strenger Maßstab anzulegen.

Die Befristung der Anordnung auf maximal ein Jahr sowie die Verpflichtung, die Fortdauer der Ausschreibung zu überprüfen und das Ergebnis der Überprüfung aktenkundig zu machen, begrüße ich, halte aber eine Überprüfungsfrist von drei - statt sechs - Monaten für sachgerecht.

3.8.1.2.9 Datenabgleich

Die im Gesetzentwurf vorgesehene Regelung zum Datenabgleich bezweckt, die bisherige Praxis des Datenabgleichs gesetzlich festzuschreiben. Diese Praxis habe ich bereits in meinen früheren Tätigkeitsberichten (3. TB, 3.8.5.6; 4. TB, 4.9.2.8) als viel zu weitreichend kritisiert.

Im Gegensatz zur ständigen Praxis ist zu fordern, daß neu erhobene Daten mit bereits vorhandenen Datenbeständen der Polizei nur abgeglichen werden dürfen, wenn dies sowohl vom Zweck der Erhebung als auch vom Zweck der Speicherung erfaßt wird. Ein Abgleich von Daten eines Störers kann danach nur insoweit zulässig sein, als dies zur Abwehr der Gefahr, die er verursacht, erforderlich ist. Deshalb ist die vorgesehene Regelung, wonach ein Abgleich der Daten von Störern und sog. Vorverdächtigen mit jedweder polizeilichen Datei ohne weiteres zulässig sein soll, viel zu weit.

Noch bedenklicher ist die Regelung des Datenabgleichs mit Daten „anderer Personen". Es muß sichergestellt werden, daß ein Abgleich von Daten unverdächtiger Dritter unter strikter Wahrung des Verhältnismäßigkeitsgrundsatzes auf die Fälle beschränkt wird, in denen diese auf gesetzlicher Grundlage in Anspruch genommen werden dürfen. In den genannten Vorschriften wird nicht deutlich, wann und zu welchem Zweck ein Datenabgleich vorgenommen werden darf.

Auch die Regelung zum Abgleich personenbezogener Daten mit dem Fahndungsbestand halte ich für unverhältnismäßig. Die bisher schon geübte Praxis, bei beliebigen Anlässen - wie z.B. dem routinemäßigen Abfragen der Personalien bei Verkehrsunfällen, Verkehrskontrollen, Aufnahme von Anzeigen etc. - erlangte Daten mit dem Fahndungsbestand abzugleichen, soll festgeschrieben werden. Dies führt dazu, daß jeder Bürger unabhängig vom Vorliegen eines Verdachtes routinemäßig anhand des Fahndungsbestandes überprüft werden kann. Demgegenüber kann der Abgleich personenbezogener Daten mit dem Fahndungsbestand nur zulässig sein, wenn die gesetzlichen Voraussetzungen für eine Personenkontrolle vorliegen. In diesem Fall dienen Erhebung und Speicherung der Daten dem gleichen Zweck, da die Identitätsfeststellung u.a. die Prüfung beinhaltet, ob eine bekannte Person mit einer polizeilich gesuchten identisch ist. In allen anderen Fällen führt der Abgleich mit dem Fahndungsbestand zu einer unzulässigen Zweckdurchbrechung.

Außerdem sollte eine Höchstfrist festgelegt werden, nach deren Ende der Betroffene zum Zwecke der Überprüfung seiner Personalien nicht mehr länger festgehalten werden darf. Zu denken wäre an ein oder maximal zwei Stunden.

Weiterhin ist der routinemäßige automatisierte Abgleich des Veränderungsbestandes des Melderegisters mit dem Inhalt polizeilicher Dateien (insbesondere dem Fahndungsbestand in POLAS und INPOL), der ebenfalls ständiger Praxis entspricht, aus folgenden Gründen abzulehnen:

Die Regelung entspricht der den örtlichen Meldebehörden auf der Grundlage von § 31 Abs. 5 HmbMG in § 15 MeldDÜV (Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister) auferlegten Verpflichtung, der Polizei den Veränderungsbestand des Melderegisters regelmäßig „zur Aktualisierung kriminalpolizeilicher personenbezogener Sammlungen" und „zur Durchführung von Fahndungsmaßnahmen und zur Aufklärung des Schicksals von Vermißten" in der Form des automatisierten Datenabgleichs zu übermitteln. Gegen die Zulässigkeit eines solchen Datenabgleichs spricht, daß eine Vielzahl unbeteiligter Bürger von einer Maßnahme betroffen werden, deren Erfolgsaussichten gering einzuschätzen sein dürften. Sie entspricht daher nicht dem Grundsatz der Verhältnismäßigkeit. Überdies führt der Abgleich dazu, daß die Polizei ihre Bestände mit Hilfe von Daten aktualisieren kann, die sie selbst nicht erheben dürfte. Genauso wenig wie die Polizei zum Zwecke der Aktualisierung von KpS-Unterlagen unverdächtige Bürger anhalten und ihre Personalien feststellen darf, ist ein solcher Eingriff sozusagen im Wege der Ersatzvornahme durch die Nutzung von Meldedaten zulässig.

3.8.1.2.10 Rasterfahndung

Die Rasterfahndung dient im Gegensatz zum o.a Datenabgleich nicht dazu, namentlich bekannte gesuchte Personen festzustellen. Anhand bestimmter Merkmale sollen vielmehr unbekannte Störer (oder Tatverdächtige) identifiziert werden, indem Datenbe-

stände anderer öffentlicher oder privater Stellen nach vorgegebenen Kriterien ausgewertet werden. So soll schrittweise ein immer enger werdender Personenkreis herausgefiltert werden, auf den immer mehr, für die gesuchte Person charakteristische Merkmale zutreffen. Gegen den auf diese Weise eingegrenzten Personenkreis wird dann mit herkömmlichen Methoden weiter ermittelt (vgl. 3. TB, 3.8.5.6, 4. TB, 4.9.2.9).

Es ist bisher von polizeilicher Seite nicht dargelegt worden, aus welchen Gründen und in welchen Fällen die Rasterfahndung zum Zwecke der Gefahrenabwehr überhaupt benötigt wird. Auch die Begründung zu dem Gesetzentwurf gibt hierüber keinen Aufschluß. Solange die Notwendigkeit des Einsatzes der Rasterfahndung im präventiven Bereich nicht überzeugend begründet worden ist, halte ich es für ausreichend, sie unter engen Voraussetzungen allein zum Zwecke der Strafverfolgung zuzulassen. Eine entsprechende Regelung ist im Referentenentwurf des BMJ zum Strafverfahrensänderungsgesetz vorgesehen. Sollte sich die Rasterfahndung auch zum Zwecke der Gefahrenabwehr als unbedingt erforderlich erweisen, so müßte wenigstens klargestellt werden, daß eine über die Abwehr der konkreten Gefahr hinausgehende Nutzung von Daten in „Trefferfällen" nur zulässig ist, wenn gegen den Betroffenen wegen des Vorfalles ein Ermittlungsverfahren eingeleitet wird. Können nach weiteren konventionellen Ermittlungen keine zusätzlichen Verdachtsmomente festgestellt werden, so sind die durch den Abgleich erhaltenen Daten und Unterlagen unverzüglich zu löschen bzw. zu vernichten. Eine Aufbewahrung zu Zwecken der vorbeugenden Straftatenbekämpfung ist auszuschließen.

3.8.2 Entwicklung der polizeilichen Datenverarbeitung

Ich habe bereits vor fünf Jahren versucht, einen Überblick über die polizeilichen Informationssysteme zu geben (3. TB, 3.8.1, S. 65 ff.). Auch wenn die Grundstruktur der polizeilichen Datenverarbeitung beibehalten wurde, haben sich seither doch wichtige Änderungen ergeben, die mir eine erneute Gesamtdarstellung als sinnvoll erscheinen lassen.

3.8.2.1 Das INPOL-Konzept

Bei INPOL handelt es sich um ein vom Bund (BKA) und den Ländern im Verbund betriebenes Informationssystem der Polizei. Dabei werden DV-technisch in einer zentralen Datenbank verbundene, rechtlich aber selbständige Dateien geführt:

— Personen- und Sachfahndung,

— Haftdatei,

— Kriminalaktennachweis (KAN),

— ED-Datei,

— Falldateien,

— Spurendokumentationssysteme (SPUDOKs),

— PIOS-Dateien.

Mit Ausnahme der PIOS-Anwendungen greifen die verschiedenen Dateien auf nur einmalig gespeicherte Personendaten zu.

INPOL ist das wichtigste länderübergreifende Informationssystem der deutschen Polizei, die einen wesentlichen Teil ihrer informationellen Zusammenarbeit über dieses System abwickelt, wobei das Bundeskriminalamt meist als Zentralstelle fungiert. Die derzeitige Konzeption und Aufgabenstellung von INPOL ergibt sich aus dem von der Innenministerkonferenz beschlossenen „Konzept zur Fortentwicklung des polizeilichen Informationssystems INPOL" vom 12. Juni 1981. Danach dient INPOL der Verbrechensbekämpfung. „Unter dieser Zielsetzung und nach Maßgabe der für den jeweiligen Sachbereich getroffenen Einzelregelungen enthält es alle bei den zuständigen Polizei-

dienststellen des Bundes und der Länder angefallenen einschlägigen Informationen (Daten) und macht sie für weitere Ermittlungen verfügbar".

Das gegenwärtige INPOL-System besteht aus zwei Ebenen:

— INPOL-Bund als zentrale Anwendung mit Zugriffsmöglichkeit für das BKA und für die Länder-Polizeien,

— Länder-INPOLs, die mehr und z.T. weitergehende Informationen enthalten (Modus-operandi-Daten zu Personen und Fällen, Folgedaten zu in INPOL-Bund gespeicherten Personen, Folgedaten zu Fällen mit unbekanntem Täter), aber bislang nur der jeweiligen Länderpolizei zugänglich sind.

3.8.2.2 INPOL-Bund

3.8.2.2.1 „Rechtmäßige Personalien"

Im Prinzip sollen im gesamten INPOL-Systeme alle zu einer Person gespeicherten Daten in einem gemeinsamen Datensatz geführt werden („rechtmäßige Personalien" bzw. P-Gruppe). Damit soll vermieden werden, daß Redundanzen und Ungenauigkeiten bei der Speicherung entstehen und so zu einer verminderten Datenintegrität führen. Die Erreichung der redundanzfreien Personendatenspeicherung wird durch „programmierte Regeln" sichergestellt.

Lediglich die PIOS-Anwendungen weichen von dem Grundsatz des gemeinsamen Zugriffs auf einen Personendatensatz ab. Die in diesen Dateien geführten Personalien sind getrennt von den sonstigen INPOL-Personalien. Dies kann zu einer Mehrfachführung von Personalien führen.

Neben den eigentlichen Identifikationsdaten (Name, Vorname, akademischer Grad), Spitzname, Geburtsdatum und Ort, Geschlecht, Staatsang., Volkszugehörigkeit enthält der Personendatensatz auch sog. personengebundene Hinweise (PHW's). Die PHW's beschreiben bestimmte Eigenschaften der gespeicherten Personen, z.B. Hinweise auf Prostitution, Ansteckungsgefahr, Rauschgiftkonsum, Bewaffnung. Die früher ebenfalls gespeicherten Merkmale „geistesschwach", „entmündigt" und „internationaler Rechtsbrecher" sind aufgrund entsprechender Forderungen der Datenschutzbeauftragten gelöscht worden.

3.8.2.2.2 Datei Personenfahndung

Die Datei Personenfahndung im INPOL-System wird beim BKA und bei den Länderkriminalämtern mit parallelem Bestand geführt. Das BKA synchronisiert und aktualisiert die bei Bund und Ländern parallel geführten Dateien. Das Fahndungssystem umfaßt ca. 200.000 Personen mit etwa 250.000 Notierungen.

Die Datei Personenfahndung enthält im wesentlichen Daten von

— zur Festnahme oder Ingewahrsamsnahme ausgeschriebenen Personen,

— Ausländern, gegen die eine unanfechtbare Ausweisungs- bzw. Abschiebungsverfügung vorliegt,

— Personen, die aufgrund von Ersuchen ausländischer Polizei- und Justizbehörden festgenommen werden sollen,

— Personen, die zur polizeilichen Beobachtung ausgeschrieben sind,

— Personen, denen die Fahrerlaubnis entzogen wurde und die den Führerschein nicht abgegeben haben.

Der Datensatz besteht aus den Datengruppen „Rechtmäßige Personalien" und ggf. „andere Personalien" sowie aus einer oder mehreren Datengruppen „Fahndungsnotierung".

Die Daten werden von den sachbearbeitenden Dienststellen der Länder, des BKA, der Grenzschutzämter und vom Zollkriminalinstitut, die auch jeweils für diese Daten ver-

antwortlich sind, online geliefert und können nicht nur von den datenliefernden Stellen abgerufen werden; sondern auch von allen Grenzdienststellen, der Bahnpolizei und dem Fahndungsdienst der Deutschen Bundesbahn, der Generalbundesanwaltschaft und einigen anderen Staatsanwaltschaften (nur im Rahmen der Erprobung) und von der Hausinspektion des Deutschen Bundestages. Der Zugriff erfolgt mit Namen, Vornamen und Geburtsdatum vollständig oder fragmentarisch, alphabetisch oder phonetisch. Die Zugriffsrechte der einzelnen Dienststellen sind differenziert.

Die Löschung der Fahndungsnotierungen erfolgt entweder manuell nach polizeilicher Erledigung oder automatisch nach Erreichen des Laufzeitendes durch Programm. Die Regellaufzeiten liegen zwischen 3 Monaten (vorläufige Fahndungsnotierungen) bis zu 10 Jahren (Ausweisungs- und Abschiebungsverfügungen). Die übrigen Fahndungsnotierungen haben eine Regellaufzeit von einem Jahr.

3.8.2.2.3 Datei Sachfahndung

Die Datei Sachfahndung wird parallel beim BKA und bei den LKÄ geführt. Sie dient der Erfassung von alphanumerisch gekennzeichneten Gegenständen zur Beweissicherung, Einziehung, Eigentumssicherung, Beobachtung, Insassenfeststellung, Zwangsentstempelung, Besitzer- Eigentümerermittlung, Identitätsprüfung und zollrechtlichen Überwachung. In die Datei werden Daten von Eigentümern, Besitzern oder Geschädigten, Beschuldigten, Tatverdächtigen oder vermißten Personen im Zusammenhang mit den ausgeschriebenen Sachen gespeichert: z.Z. etwa 2.200.000 Fälle mit ca. 3.300.000 Gegenständen.

Die Daten werden von den sachbearbeitenden Länderdienststellen, vom BKA, den Grenzschutzstellen und dem Zollkriminalinstitut online angeliefert. Die liefernde Stelle ist für die Datenpflege verantwortlich. Die Löschung erfolgt - in Abhängigkeit von der Art der Sachen - nach 2 Jahren (Gegenstände allgemein), 5 Jahren (KFZ, Dokumente, Schmuck, Uhren, Pelze), 10 Jahren (Pässe), 20 Jahren (Reisepaßvordrucke) und 30 Jahren (Waffen). Nach Erledigung der Fahndungsnotierungen werden die Daten weitere 5 Jahre im Sachfahndungsarchiv des BKA vorgehalten.

3.8.2.2.4 Kriminalaktennachweis

Der Kriminalaktennachweis (KAN) wird vom Bund als Zentralstelle für den elektronischen Datenverbund geführt. Er umfaßt einen Bestand von etwa 630.000 Personen mit insgesamt etwa 800.000 Fundstellen. Der KAN, an dem Hamburg bisher nicht beteiligt ist, dient dem Nachweis von Kriminalakten, die beim Bund und bei den Ländern in Fällen schwerer oder überregional bedeutsamer Straftaten über Beschuldigte oder sonst tatverdächtige Personen angelegt sind.

Der Datenkatalog im KAN umfaßt:

— die rechtmäßigen Personalien

— andere Personalien und

— Unterlagen (kriminalaktenführende PolDienststelle, KANr., Aussonderungsprüfung, Sondervermerk (Freitext).

Der KAN kann über Name, Vorname, Geburtsdatum in jeder Verbindung, die den Namen enthält, erschlossen werden. Auskünfte aus dem KAN dürfen nur an sachbearbeitende, d.h. mit der Bearbeitung von Ermittlungsvorgängen befaßte Polizeidienststellen erteilt werden.

Die Anlieferung der Daten erfolgt durch die sachbearbeitenden Polizeidienststellen der Länder, das BKA und die Grenzschutzdirektion. Die Verantwortung für die Speicherung liegt bei der Dienststelle, die die Daten einspeichert. Das BKA hat darüber hinaus als Zentralstelle nach dem BKA-Gesetz zu prüfen, ob die Speicherungen plausibel sind

und daß keine Zweifel in bezug auf das Vorliegen der Speicherungsvoraussetzungen bestehen.

3.8.2.2.5 Haftdatei

Die Haftdatei dient dem Nachweis von Personen, die sich aufgrund richterlicher Anordnung in behördlichem Gewahrsam befinden (aktuelle Haftnotierung) oder befanden (inaktuelle Haftnotierung). Inaktuelle Notierungen sollen deshalb gespeichert werden, um auf Fahndungsnotierungen von bereits in Haft befindlichen Personen aufmerksam zu machen und die Überprüfung von Alibis zu erleichtern. Die Haftdatei umfaßt etwa 255.000 Personen mit 66.000 aktuellen und 410.000 inaktuellen Notierungen.

Inaktuelle Haftnotierungen werden zwei Jahre gespeichert und dann gelöscht, „es sei denn, daß zum Löschungszeitpunkt die betroffene Person KAN-Relevanz besitzt." In diesem Fall werden inaktuelle Haftnotierungen fünf Jahre gespeichert.

3.8.2.2.6 ED-Datei

Die Datei Erkennungsdienst (ED-Datei) wird innerhalb des INPOL-Verbundes als logisch eigenständige Datei geführt. Sie wird von den Polizeien der Länder und des Bundes gespeist und ist das Gesamtverzeichnis von Verwaltungsdaten über ED-Maßnahmen. Sie enthält neben den Identifikationsangaben zur Person die Angaben über Ort, Datum und Art der durchgeführten ED-Maßnahmen.

Die ED-Datei umfaßt einen Bestand von ca. 410.000 Personen mit etwa 515.000 Notierungen. Sie soll dazu dienen,

— Personen, insbesondere solche, die unter falschem Namen auftreten oder Personalienangaben verweigern, zu identifizieren,

— namensgleiche Personen zu unterscheiden,

— Ergebnisse aus ED-Behandlungen zusammenzufassen,

— den Stand von Personenfeststellungsverfahren zu erkennen,

— daktyloskopische Sofortvergleiche vorzunehmen.

Mit dem Zugang der Daten beim Rechner des BKA gehen diese in den Besitz des BKA über, das damit für die Pflege der angelieferten und gespeicherten Informationen verantwortlich wird. Die Lieferländer werden automatisiert vermerkt und erlangen einen Mitbesitz an den Daten. Das BKA informiert die LKÄ über den Bearbeitungsstand der jeweiligen ED-Maßnahme (z.B. über das Vorliegen identischer Fingerabdrücke, die in einer besonderen Fingerabdruckdatei gespeichert sind).

3.8.2.2.7 Falldateien

Die Falldateien dienen dem Ziel, „Führungsinformationen" zu gewinnen, Straftäter-Auskünfte zu erhalten und die modus-operandi-Recherche zu erleichtern.

Gespeichert werden fallbezogene Informationen. Bekannte Straftaten sollen (noch) unbekannten Tätern zugeordnet werden können. Dies setzt voraus, daß aus bekannten Verhaltensweisen von Tätern auf ihre spätere Vorgehensweise geschlossen werden kann. Die Speicherung eines Betroffenen in einer FD kann nur erfolgen, wenn über ihn ein INPOL-Personendatensatz gespeichert ist.

3.8.2.2.8 Spurendokumentationssysteme

Bei dem Spurendokumentationssystem handelt es sich um vom BKA zur Verfügung gestellte Verfahrenshülsen zur Dokumentation von Spuren bei umfangreichen Ermittlungsverfahren. SPUDOK's bieten die Möglichkeit zum Abgleich nahezu aller Textteile, da im Prinzip alle Wörter, die nicht eingeklammert sind, als Suchbegriffe benutzt werden können.

3.8.2.2.9 PIOS-Dateien

Die PIOS (Personen, Institutionen, Objekte, Sachen)-Dateien sind Verbunddateien, bei denen - anders als sonst im INPOL-System - das BKA und sämtliche LKÄ für die jeweils von ihnen eingegebenen Daten gleichwertige Datenbesitzer sind. Sie werden für bestimmte Kriminalitätsbereiche eingerichtet. So gibt es u.a. die Arbeitsdatei „PIOS Innere Sicherheit (APIS)", die „Arbeitsdatei PIOS Organisierte Kriminalität (APOK)", die „Arbeitsdatei PIOS Landesverrat (APLV)" und etwa die „Arbeitsdatei PIOS Rauschgift (APRG)".

Diese Dateien sollen für ihren jeweiligen Anwendungsbereich ermöglichen

— relevante Personen, Institutionen, Objekte, Sachen und Ereignisse sowie Zusammenhänge zwischen ihnen zu erkennen,

— Erkenntnisse für polizei- und ermittlungstaktisches Vorgehen zu gewinnen und

— unbedeutende Informationen und Erkenntnisse auszuscheiden.

3.8.2.3 INPOL-Land

Neben dem INPOL-Bund bestehen die INPOL-Anwendungen der Länder (INPOL-Land); in Hamburg das polizeiliche Auskunftssystem POLAS, das sich in Datei- und Satzstruktur von INPOL deutlich unterscheidet, ohne daß darauf hier vertiefend eingegangen werden muß, weil erhebliche Änderungen mit dem INPOL-Ausbau geplant sind.

Die für INPOL-Land erforderliche Datenverarbeitungsanlage wird bisher von dem jeweiligen Land geplant, beschafft, programmiert, betrieben und unterhalten. Die für den Verbund erforderlichen Programme werden zwischen Bund und Ländern abgestimmt.

3.8.2.4 Bewertung

Versucht man die Entwicklung der polizeilichen Datenverarbeitung aus datenschutzrechtlicher Sicht zu kommentieren, so ist zu differenzieren. Zwar betreiben die Polizeien ihre Informationsverarbeitung unter der Sammelbezeichnung INPOL, in Wirklichkeit handelt es sich aber um eine Zusammenfassung qualitativ höchst unterschiedlicher Anwendungen. Das INPOL-System besteht einerseits aus Teilen, bei denen es im wesentlichen um die Beschleunigung, Vereinfachung und mengenmäßige Bewältigung traditioneller kriminalpolizeilicher Arbeitsformen geht. Hier wird insbesondere die Überlegenheit des Computers an Schnelligkeit und an Kapazität zum Einsatz gebracht. Daneben kommen auch Verfahren zur Anwendung, die wesentliche qualitative Veränderungen gegenüber der bisherigen polizeilichen Tätigkeit mit sich bringen, die die bloße „Registraturfunktion" der Datenverarbeitung durch zusätzliche Komponenten ergänzen, wie Freitextverarbeitung, Verknüpfungen und bessere Recherchiermöglichkeiten.

Diese Neuentwicklungen bergen aus datenschutzrechtlicher Sicht auch neue Gefahren in sich. Die Freitextverarbeitung, d.h. die inhaltliche Erschließung nicht formatierter Angaben, kann die Neigung fördern, nicht mehr nach Sachlage, sondern nach „Computerlage" Entscheidungen zu treffen. Verknüpfungen können die gespeicherten Daten in einen mehrdimensionalen Zusammenhang bringen. Damit wächst die Gefahr, daß Verbindungen zwischen Daten und damit letztlich Aussagen über Personen formalisiert, d.h. nach festen Regeln und im Einzelfall möglicherweise falsch zustande kommen. Neue Recherchiermöglichkeiten bringen die gespeicherten Daten in einen permanenten Auswertungszusammenhang, vervielfachen also ihre Nutzbarkeit, ohne daß die Aktualität und die Zuverlässigkeit der Aussagen diesen Bedeutungszuwachs immer rechtfertigen.

(1) Die unter der Bezeichnung INPOL-Bund betriebenen Anwendungen sind datenverarbeitungstechnisch eng miteinander verbunden. Rechtlich handelt es sich zwar um unterschiedliche und selbständige Dateien. Für sie gelten auch jeweils unterschiedli-

che Errichtungsanordnungen. Technisch ist die Verarbeitung dieser Daten aber so organisiert, daß die unterschiedlichen Dateien lediglich Abschnitte einer großen zentralen Datenbank sind, in der die Personalien (sog. P-Datensatz) nur einmal geführt werden, unabhängig davon, in wievielen unterschiedlichen Dateien Daten zu der jeweiligen Person gespeichert sind.

Zum Inhalt des Personendatensatzes gehören nicht nur die Angaben, die zur Identifikation einer Person erforderlich sind, sondern auch personengebundene Hinweise (PHW's), die eine kanppe erste Einschätzung der Person ermöglichen sollen (wie z.B. gewalttätig, bewaffnet oder Ausbrecher, aber auch Freitodgefahr oder Ansteckungsgefahr).

Derartige Merkmale bergen stets die Gefahr einer negativen sozialen Abstempelung. Diese Bedenken müssen dann zurückstehen, wenn es um die Abwehr von Gefahren für Polizeibeamte wie auch u.U. für den Betroffenen selbst geht. Deshalb kann die Verwendung einiger PHW's bei der Fahndungsdatei im Grundsatz hingenommen werden, nicht aber auch dann, wenn auf Dateien zugegriffen wird, deren Daten nicht für ein unmittelbares polizeiliches Handeln gegen den Betroffenen bestimmt sind. Typisch hierfür ist der Kriminalaktennachweis (KAN).

Diese Struktur der Datenverarbeitung bedeutet, daß im Grunde ein zentraler Personenindex betrieben wird, der aus den Personalien all derer gebildet ist, die in irgendeiner INPOL-Datei gespeichert sind. Eine derartige Struktur ermöglicht dateiübergreifende Recherchen und sonstige Nutzungen der Daten, die über den jeweils konkreten Zweck der einzelnen Datei hinausgehen. Die Grundsätze der Zweckbindung, die für jede Datei in der betreffenden Errichtungsanordnung spezifisch festgelegt sind, sind bei einer solchen Datenverarbeitungsstruktur nicht einzuhalten.

(2) Nach wie vor fehlt es an einer einwandfreien gesetzlichen Regelung der Frage, nach wem unter welchen Voraussetzungen wie gefahndet werden darf und wer wann unter welchen Voraussetzungen fahndungsmäßig überprüft werden darf. Statt dessen ist immer noch ein Beschluß in Kraft, der von der Innenministerkonferenz im September 1977 im Zusammenhang mit der Terroristenbekämpfung gefaßt wurde. Hiernach sind alle Personen, deren Personalien der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden (z.B. bei Verkehrskontrollen, Unfällen, Vernehmungen etc.) in INPOL abzufragen. Von diesem Beschluß wird nach Aussagen der Polizei zwar nur mit gebotener Zurückhaltung Gebrauch gemacht. Dies ändert jedoch nichts daran, daß für eine so weitgehende Anweisung jegliche Rechtfertigung fehlt.

(3) Ein weiteres Problem der Datei Personenfahndung besteht darin, daß sie auch dem Nachweis von Personen dient, die der polizeilichen Beobachtung - PB - unterliegen. Die polizeiliche Beobachtung erstreckt sich auch auf Personen, gegen die kein substantieller Tatverdacht besteht und von denen auch keine konkrete Gefahr ausgeht. Die polizeiliche Beobachtung soll vorbeugend klären, ob ein Tatverdacht überhaupt besteht und gegen welche Personen er sich richtet bzw. ob eine konkrete Gefahr vorliegt und von wem sie ausgeht.

Die einschlägige Polizeidienstvorschrift grenzt zwar den zu erfassenden Personenkreis und den Anlaß der Beobachtung ein; so dürfen andere Personen nur ausgeschrieben werden, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung des Sachverhalts oder zur Ergreifung des Täters führen kann. Diese wenig präzisen Eingrenzungen können jedoch eine gesetzliche Regelung nicht ersetzen.

(4) Das Konzept für einen bundeseinheitlichen Kriminalaktennachweis geht davon aus, daß im KAN, auf den alle Polizeibehörden mit kriminalpolizeilichen Aufgaben Zugriff haben, nur Kriminalakten gespeichert werden, die schwere oder überregional bedeutsame Straftaten betreffen. Bei der Definition dessen, was überregional bedeutsam ist, und insbesondere bei der Erarbeitung konkreter Straftatenverzeichnisse, die für die Praxis von der Polizei angelegt worden sind, wurde indes ein äußerst großzügiger Maßstab angelegt.

Im übrigen laufen die Beschlüsse zum KAN weitgehend leer, weil nach Auffassung der Polizei die regionale Abschichtung nicht durchgängig gelten soll. Ein Beispiel hierfür ist die zentrale Speicherung von erkennungsdienstlichen Unterlagen beim BKA. Sie führt auch dann zur Speicherung von Personalien beim BKA, wenn die vorgeworfene Straftat keine überregionale Bedeutung hat. Fragt in solchen Fällen eine Polizeidienststelle zu einer Person an, die wegen einer nicht unter die KAN-Kriterien fallenden Straftat ed-behandelt wurde, so erhält sie zwar keinen KAN-Bestand. Dennoch bekommt sie aber die Personendaten, weil über die angefragte Person ed-Unterlagen vorliegen.

Gleiches gilt für alle Kriminalitätsbereiche, in denen Falldateien betrieben werden.

(5) Für die Errichtung der Haftdatei gibt es ausnahmsweise eine Rechtsgrundlage. Sie findet sich in § 4 Abs. 1 BKA-G. Dort heißt es jedoch lediglich: „Die Landeskriminalämter unterrichten das Bundeskriminalamt unverzüglich über den Beginn, die Unterbrechung und die Beendigung von richterlich angeordneten Freiheitsentziehungen."

Nicht von § 4 BKA-G gedeckt ist somit die Registrierung von inaktuellen Haftmeldungen für fünf bzw. zwei Jahre über das Haftende hinaus. Diese dient der Polizei vornehmlich zur Erleichterung ihrer Ermittlungsarbeit, etwa um Alibis verdächtiger Personen leichter nachprüfen zu können. Die Speicherung der inaktuellen Haftnotierungen ist überdies deswegen besonders fraglich, weil hier im besonderen Maße die Gefahr einer sozialen Abstempelung, einer Stigmatisierung des Betroffenen besteht, die der Resozialisierung der Betroffenen entgegenstehen kann.

(6) Ein Wesensmerkmal der PIOS- und SPUDOK-Anwendungen ist die Erfassung der Personen, die nicht Verdächtige oder Beschuldigte sind, bei denen aber „zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies (die Speicherung) zur Aufklärung oder vorbeugenden Bekämpfung schwerwiegender Straftaten, zur Ergreifung von zur Festnahme gesuchten Personen oder zur Abwehr einer im einzelnen Fall bestehenden erheblichen Gefahr erforderlich ist" (Ziffer 4.2.11 der Dateirichtlinien).

Eine Erfassung von „anderen Personen", deren Beteiligung an der Tat noch ungeklärt ist, betrifft notwendigerweise auch Personen, die - im nachhinein betrachtet - völlig unschuldig sind. Darüber hinaus besteht bei einem „Verdachtsverdichtungsinstrument" wie PIOS oder SPUDOK immer die Gefahr, daß quantitative Gesichtspunkte zu sehr in den Vordergrund treten. Wenn etwa ein Name zum dritten Mal auftaucht, liegt für viele der Schluß nahe, diese Person sei „auffällig".

Aus der Sicht des Datenschutzes kann diesen Gefahren am ehesten durch ein differenziertes und kurz bemessenes Fristensystem und durch eine bessere Beachtung des Zweckbindungsprinzips begegnet werden.

Der Einhaltung der Nr. 4.5 der Dateienrichtlinien, wonach diese sogenannten „anderen Personen" von der Sepicherung zu unterrichten sind, sofern diese ein Jahr überschreitet, kommt deswegen besondere Bedeutung zu. Die Bestrebungen der Polizei gehen leider in die entgegengesetzte Richtung. Während die Erfassung „anderer Personen" weiter zunimmt, werden die besonderen Schutzvorkehrungen, die für diese Personengruppe gelten, kontinuierlich vernachlässigt.

Bei mehreren Errichtungsanordnungen neueren Datums fällt auf, daß die „verdächtigen Personen" zu umfassend definiert werden, daß kaum noch feststellbar ist, was diesen Personenkreis von den „anderen Personen" unterscheiden soll. So bleibt beispielsweise unklar, ob eine Perosn, die im Notizbuch eines Verdächtigen verzeichnet ist, nun ihrerseits bereits verdächtigt ist oder ob es sich lediglich um eine „andere Person" handelt, deren Daten bis zur Klärung des Verdachts gegen den Notizbuchinhaber gespeichert werden müssen.

(7) Datenschutzrechtlich wirft besonders die vielfältige Verwendbarkeit der SPUDOK's Probleme auf. Die Eigenschaft der SPUDOK's, nahezu alle erfaßten Textteile abgleichen zu können, eröffnet die Möglichkeit, mit Hilfe der Verfahrenshülle SPUDOK beliebige Sonderdateien einzurichten, die nicht unbedingt der Aufklärung großer Ermitt-

lungskomplexe dienen müssen, wofür sie ursprünglich entwickelt wurden, sondern - wie es zunehmend geschieht - auch zur Bewältigung polizeilicher „Großlagen", zur Gefahrenabwehr oder auch zur Fahndung nach ausgebrochenen Straftätern.

3.8.2.5 Weiterer Ausbau

Am 1./2. Dezember 1986 hat der AK II der Innenministerkonferenz eine Arbeitsgruppe eingesetzt, die den Auftrag erhielt, eine Bestandsaufnahme über den Stand der polizeilichen DV zu erstellen und zu prüfen, ob und inwieweit das INPOL-Fortentwicklungskonzept einer klarstellenden Interpretation oder ggf. Fortschreibung bedarf. Diese Arbeitsgruppe hat am 1. August 1988 einen 1. Bericht zu Stand und Entwicklung der polizeilichen Datenverarbeitung vorgelegt.

Datenschutzrechtlich bedeutsam sind dabei folgende Komplexe:

— Indexdatenführung im Verbund

— Beseitigung von Strukturunterschieden

— Öffnung der internen Falldateien des BKA

— Veränderungen der Personalienführung

— Veränderungen der Haftdatei.

(1) Es wird zwischen Volldaten und Indexdaten unterschieden. Indexdaten enthalten lediglich einen Verweis, wo die gesamten (und inhaltlich bedeutsamen) Daten gespeichert sind. In Zukunft sollen Volldaten nur noch in der zuständigen LDVA und der ZDVA (im BKA) gespeichert werden. Die Ländersysteme sollen nur noch Indexdaten enthalten. Bei Anfragen wird automatisch auf die volldatenführende Stelle durchgeschaltet. Man verspricht sich dadurch die Vermeidung doppelter Speicherung und die Verhinderung von Inkonsistenzen im Datenbestand. Auch bei PIOS-Anwendungen soll auf den INPOL-Personalienbestand zurückgegriffen werden.

(2) Die Länder-INPOL's haben sich hinsichtlich ihrer technischen Realisierung und ihrer Strukturen auseinanderentwickelt. Diese Strukturunterschiede sollen beseitigt werden, damit die Systeme reibungslos miteinander kommunizieren können. Ein Durchreichen von Daten aus INPOL-Land in das INPOL-Bund soll jederzeit möglich sein. In PIOS sollen Querverweise eingebaut und erweiterte Zugriffsmöglichkeiten unterhalb der LKÄ eröffnet werden.

(3) Bisher vom BKA geführte interne Falldateien sollen für den Länderzugriff geöffnet werden. Die Arbeiten zur Weiterentwicklung der Falldateien soll mit dem Ziel wiederaufgenommen werden, den Kriminalpolizeilichen Meldedienst einschließlich der Sondermeldedienste in einer Falldatei für „Straftaten mit länderübergreifender Bedeutung" zusammenzufassen.

(4) Die verschiedenen Gruppen sollen überprüft werden. Eine neue W-Gruppe mit wertenden Informationen über Personen (z.B. Spitz- und Gruppennamen) soll eingeführt werden. Die W-Gruppe soll an die Stelle der PHW's treten.

(5) Die Haftdatei soll aktualisiert werden. Es wird geprüft, ob weitere Datenfelder eingerichtet werden sollen. Auf eine Datenreduzierung bei Inaktualität der Haftdaten soll verzichtet werden.

Fazit: Diese geplanten Veränderungen zeigen, daß keines der datenschutzrechtlichen Bedenken konstruktiv aufgegriffen werden soll. Statt dessen wird unter Effektivi-

tätsgesichtspunkten das INPOL-System im Sinne möglichst reibungsloser Kommunikation und Datenflüsse verfeinert werden. Darüber hinaus muß bei der dargestellten Entwicklung die Sorge bestehen, daß die zunehmende Dateienvielfalt bei der Polizei die Durchsetzung datenschutzrechtlicher Regeln noch weiter erschwert. Die polizeilichen Informationssysteme haben jetzt schon eine Komplexität erreicht, die sie nur noch für einige Experten überschaubar sein läßt. So wird es insbesondere für die Betroffenen immer schwieriger, ihre ihnen nach den Datenschutzgesetzen zustehenden Rechte auf Auskunft über gespeicherte Daten sowie auf Sperrung, Berichtigung und Löschung von Daten durchzusetzen.

3.8.3 Internationaler Datenaustausch (Schengener Informationssystem)

Am 14. Juni 1985 unterzeichneten die Regierungen Frankreichs, der Bundesrepublik Deutschland und der Beneluxstaaten in Schengen/Luxemburg ein Abkommen über den schrittweisen Abbau der Grenzen zwischen ihren Ländern. Dabei knüpften sie den Wegfall der Grenzkontrollen an eine Reihe von Maßnahmen, die die befürchteten Sicherheitsdefizite ausgleichen sollen. Die Maßnahmen sollen in einem Zusatzübereinkommen festgehalten werden. Hierzu gehört die Errichtung eines gemeinsamen automatisierten Informationssystems für den Bereich der Fahndung (Schengener Informationssystem - SIS). Dieses System soll vor allem der Ausschreibung zur Festnahme und zur Zurückweisung an der Grenze, der verdeckten Registrierung und der Ermittlung des Aufenthalts von Zeugen im Strafverfahren dienen. Überdies sollen der Informationsaustausch zum Zwecke der Bekämpfung bestimmter Formen der Kriminalität verstärkt, die ausländer- und asylrechtlichen Entscheidungen vereinheitlicht und ein gemeinsames Verfahren für intensivierte Kontrollen an den Außengrenzen festgelegt werden.

Das Zusatzabkommen verfolgt den Zweck, die aus dem vorgesehenen Abbau von Grenzkontrollen „resultierenden Sicherheitsdefizite" zu kompensieren. Ich habe dagegen Sorge, daß der Umweg über ein internationales Abkommen zur Überkompensation genutzt werden soll.

So ist für den grenzüberschreitenden Verkehr vorgesehen, daß ein Drittausländer - also ein Reisender, der nicht Bürger eines der Vertragsstaaten ist - von jedem Vertragsland an der Grenze zurückzuweisen ist, wenn seine Anwesenheit eine Gefahr für die öffentliche Ordnung, die nationale Sicherheit oder die internationalen Beziehungen einer der Vertragsparteien darstellt. Entsprechend muß er von jedem Vertragsland abgeschoben werden, wenn er die Bedingungen einer der Vertragsparteien für einen kurzen Aufenthalt nicht oder nicht mehr einhält, über keine gültige Aufenthaltserlaubnis einer anderen Vertragspartei verfügt und seine freiwillige Ausreise nicht angenommen werden kann. Danach ist zu befürchten, daß das ausländerunfreundlichste Recht eines der Vertragsstaaten zum allgemein verbindlichen Standard erhoben wird.

Aber selbst Bürger der Vertragsparteien haben mit stärkeren Kontrollen als bisher zu rechnen, wenn sie aus Drittländern in das Vertragsgebiet zurückkehren, denn das Abkommen sieht vor, daß alle Personen einer solchen Kontrolle zu unterziehen sind, die die Feststellung der Identität anhand der Reisepapieren ermöglicht. Dies kann zu schweren Beeinträchtigungen des Urlaubsverkehrs z.B. an den Grenzen zu Österreich und der Schweiz führen.

3.8.3.1 Die nationale Kommission für die Informatik und die Freiheiten (CNIL) der französischen Republik, der Bundesbeauftragte für den Datenschutz der Bundesrepublik Deutschland und die beratende Kommission nach dem Datenschutzgesetz des Großherzogtums Luxemburg vom 31. März 1979 haben über das SIS beraten und in ihrer Erklärung vom 16. März 1989 gefordert, daß zugleich mit der Planung dieses Systems ein wirksamer Datenschutz sichergestellt wird. Folgende Mindestbedingungen müssen nach ihrer Auffassung erfüllt sein, bevor das SIS in Betrieb genommen wird:

— Der Inhalt gemeinsamer Dateien, ihr Zweck und ihre Verwendung müssen präzise und abschließend rechtsverbindlich definiert werden.

— Der Einzelne muß in jedem Vertragsstaat ein Recht auf Zugang zu den ihn betreffenden gespeicherten Daten haben - wobei Einschränkungen aus Gründen der polizeilichen Aufgabenerfüllung in Betracht kommen - und ein Recht auf Berichtigung unzutreffender sowie auf Löschung nicht stichhaltiger Daten haben.

— Die Verarbeitung und Nutzung der gespeicherten personenbezogenen Daten muß in allen Vertragsstaaten einer Kontrolle durch unabhängige Organe unterliegen.

— Es ist Aufgabe eines gemeinsamen Organs, das aus Vertretern der nationalen Kontrollorgane der Vertragsstaaten zusammenzusetzen ist, gemeinsame Kontrollaufgaben wahrzunehmen und insbesondere die Probleme zu erörtern und einer harmonisierten Lösung zuzuführen, die sich aus der Praxis der nationalen Kontrollorgane ergeben können.

— Ohne der Einrichtung dieses noch zu schaffenden gemeinsamen Organs vorzugreifen, sollten die nationalen Datenschutzkontrollorgane schon jetzt an der Ausarbeitung des SIS beteiligt werden.

— Die Bestimmungen des Datenschutzübereinkommens des Europarates sind als verbindliche Mindestanforderungen zu betrachten.

— Darüber hinaus haben die Datenschutzbehörden angekündigt, daß sie auch auf den Gebieten des Ausländer- und Asylrechts darüber wachen werden, daß neue grenzüberschreitende Datenflüsse und internationale Informationssysteme nur eingerichtet werden, wenn die Mindestanforderungen des Datenschutzes in allen Vertragsstaaten erfüllt sind.

Die neueste Fassung des Entwurfs eines Zusatzübereinkommens trägt diesen Forderungen im wesentlichen Rechnung. Die Vertragsstaaten wollen sich darüber hinaus verpflichten, Datenschutzvorschriften für das Schengener Informationssystem entsprechend den Grundsätzen der Datenschutzkonvention des Europarates und auch der Empfehlung des Ministerkomitees des Europarats an die Mitgliedsstaaten über die Nutzung personenbezogener Daten im Polizeibereich als Mindeststandard zu erlassen. Dies ist zu begrüßen.

3.8.3.2 In ihrer Entschließung vom 26./27.10.1989 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz weitere Forderungen erhoben. In der Entschließung heißt es:

Die Datenschutzbeauftragten fordern für das SIS insbesondere die

— Festlegung der Voraussetzungen, nach denen unter Berücksichtigung der Verhältnismäßigkeit (zum Beispiel nach der Schwere der Straftaten) Informationen aus dem nationalen in den internationalen Fahndungsbestand übernommen werden sollen,

— Festlegung, unter welchen Voraussetzungen und in welchem Umfang die verschiedenen Inlandsbehörden auf die Daten zugreifen dürfen,

— konkrete Beschreibung der Voraussetzungen, unter denen verdeckte Registrierungen erlaubt werden sollen (Straftatenkatalog),

— präzisere Beschreibung der Kriterien, nach denen Zweckdurchbrechungen zur Verhütung einer Straftat mit erheblicher Bedeutung sowie aus schwerwiegenden Gründen der Staatssicherheit erlaubt werden sollen und

— Aufnahme einer Verpflichtung, Zweckänderungen zu Kontrollzwecken zu dokumentieren.

— Die Regelungen über den Datenschutz - insbesondere die Rechte der Betroffenen und die Datenschutzkontrolle - müssen auf die im Zusatzübereinkommen vorgesehene konventionelle Verarbeitung personenbezogener Daten ausgedehnt werden. Dies gilt vor allem für den Informationsaustausch in den Bereichen des Ausländerrechts und des Asylverfahrens.

Der Entwurf des Zusatzübereinkommens enthält eine pauschale Verpflichtung der Vertragsparteien, daß ihre nationalen Sicherheitsdienste sich untereinander unter Berück-

sichtigung des nationalen Rechts und nach Maßgabe ihrer jeweiligen Zuständigkeit bei der Abwehr von Nachteilen für die Staatssicherheit Hilfe leisten. Die Datenschutzbeauftragten weisen vorsorglich darauf hin, daß eine solche Bestimmung nach deutschem Verfassungsrecht keine tragfähige Grundlage für einen umfassenden Datenaustausch der Geheimdienste darstellt.

Der Vertragsentwurf verpflichtet jeden Vertragsstaat, Ausländer aus dritten Staaten an der Grenze zurückzuweisen, wenn ein anderer Vertragsstaat ihn „zur Einreiseverweigerung" ausgeschrieben hat. Es ist nicht vorgesehen, daß der vollziehende Staat die Gründe der Ausschreibung zur Kenntnis nimmt und rechtlich überprüft. Die Datenschutzbeauftragten fordern die verbindliche Festlegung der sachlichen Voraussetzungen solcher Ausschreibungen und die Ermöglichung einer Überprüfung.

Die Datenschutzbeauftragten machen darauf aufmerksam, daß das Zusatzübereinkommen den deutschen Gesetzgeber nicht von der dringenden Notwendigkeit enthebt, vor Inkrafttreten des Zusatzübereinkommens für die polizeiliche Datenverarbeitung verfassungskonforme Rechtsgrundlagen zu schaffen.

Im übrigen gilt: Bevor die einzelnen Vertragsstaaten ihre im Entwurf des Zusatzübereinkommens vorgesehene Verpflichtung, spezielle nationale Regelungen für das Erheben und Nutzen von Daten zu erlassen, nicht erfüllt haben, dürfen Daten an diese Staaten auf der Grundlage des Zusatzübereinkommens nicht übermittelt werden.

Eine Stellungnahme der Bundesregierung zu der Entschließung lag bei Redaktionsschluß zu diesem Bericht noch nicht vor.

3.8.4 Einsatz von Personalcomputern

Die Tendenz, PC's für kriminalpolizeiliche Zwecke verstärkt einzusetzen, hat sich im Berichtsjahr weiter verstärkt. Trotz der mit dem Einsatz von PC's verbundenen Sicherheitsrisiken habe ich dem in der Vergangenheit gleichwohl zugestimmt, weil die Behörde für Inneres und die Polizei darauf hingewiesen haben, daß dies nur für einen Übergangszeitraum bis zur Umstellung der Großrechneranlage auf ein neues Betriebssystem erforderlich sei, und gleichzeitig zugesichert haben, ein den besonderen Risiken entsprechendes Sicherungskonzept in Abstimmung mit dem Datenschutzbeauftragten in die Praxis umzusetzen. Das inzwischen entwickelte Konzept ist seit Januar 1988 durch eine Verfügung des Polizeipräsidenten in Kraft gesetzt. Ein wichtiger Punkt in dem Sicherungskonzept besteht darin, daß den anwendenden Stellen ausschließlich Laufzeitverfahren mit einer geschlossenen Benutzeroberfläche (Bedienerführung) ohne Entwicklungswerkzeuge zu übergeben sind. Damit soll die Funktionstrennung zwischen programmierender Stelle und fachlich zuständiger Stelle - ein fundamentales Datenschutzprinzip - sichergestellt werden, da dann ein Datenmißbrauch die Zusammenarbeit von zwei verschiedenen Stellen voraussetzen würde.

Im September des Berichtsjahres habe ich den PC-Einsatz bei zwei Kriminalpolizeidienststellen, die Daten untereinander auf Disketten austauschen, geprüft. Dabei konnte ich feststellen, daß das allgemeine Sicherungskonzept und die Verfahrensvorgaben weitgehend beachtet und eingehalten werden. Allerdings mußte ich die Polizei auf zwei Schwachstellen aufmerksam machen. Die eine liegt beim Transport der Disketten zwischen den Dienststellen. Die getroffenen Maßnahmen entsprechen nicht vollständig den Anforderungen nach Nr. 9 der Anlage zu § 8 Abs. 1 Satz 1 HmbDSG. Dazu gehört nach allgemeiner Auffassung, daß bewegliche Datenträger in geeigneten Behältern auf dokumentierten Wegen zu transportieren sind. Entsprechend hatte ich schon früher gefordert, daß bei jeder Dienststelle eine manuell geführte Übersicht (etwa in Form eines Oktavheftes) anzulegen ist, aus der ersichtlich sein muß, wann welche Datenträger mit welchem Datenbestand an andere Dienststellen abgesandt wurden und wann sie dort eingingen. Eine solche Übersicht wird jedoch nicht geführt, obwohl sie erforderlich ist, um überprüfen zu können, ob die gewählten Transportwege sicher sind und an welche Dienststelle welche Daten geliefert werden.

Als gravierender ist die Schwachstelle im technischen System anzusehen. So war es möglich, entgegen den Anforderungen des Sicherungskonzeptes die vorgegebene Benutzeroberfläche zu verlassen und auf die Befehlspunktebene zu gelangen. Auf dieser Ebene können wesentliche Sicherungen des eingesetzten ADV-Verfahrens unterlaufen werden. Darüber hinaus besteht die Möglichkeit, die Datenbankstruktur zu verändern, neue Dateien und Datenbanken anzulegen, weitere Felder als Suchbegriffe zu definieren, unberechtigte Kopien der Datenbestände anzufertigen und Befehlsdateien anzuzeigen, zu verändern oder zu löschen. Allerdings ergaben sich keine Anhaltspunkte dafür, daß dies in der Praxis bereits geschehen ist.

Die Dokumentation der Transportwege für die Disketten hat die Behörde für Inneres abgelehnt, weil dies zu aufwendig sei. Stattdessen würden die übermittelten Daten protokolliert und die Protokolle bei der empfangenen Dienststelle abgelegt. Gegen die Protokollierung habe ich nichts einzuwenden, die Ablehnung der Dokumentation kann ich dagegen nicht akzeptieren. Ich habe schon häufiger darauf hingewiesen, daß auf Disketten große Datenbestände gespeichert und in kürzester Zeit manipuliert oder kopiert werden können. Es müßte deshalb auch im Interesse der Polizei zumindest die Transportdauer nachprüfbar festgehalten werden.

Zu der von mir aufgezeigten Schwachstelle in der Technik hat die Behörde für Inneres darauf hingewiesen, daß die Polizei nicht in der Lage sei, diese zu beseitigen, da Geräte installiert worden seien, die dem Sicherheitskonzept nicht genügen könnten. Damit zeigt sich, daß auch bei der zweiten PC-Anwendung für kriminalpolizeiliche Zwecke die auch aus Sicht der Polizei notwendigen Sicherheitsstandards nicht eingehalten werden können, so wie ich es schon bei dem PC-Verfahren im Rahmen der Telefonüberwachung feststellen mußte, das ich im Jahre 1988 geprüft hatte (7. TB, 4.13.3).

Bei dieser Sachlage, die aus der Sicht des Datenschutzbeauftragten unakzeptabel ist, muß sich die Behörde für Inneres fragen lassen, wer die Verantwortung dafür übernimmt, daß die Datensicherheit für diese höchst sensiblen Daten nicht im erforderlichen Umfang gewährleistet ist und daß offensichtlich erhebliche Haushaltsmittel für DV-Verfahren ausgegeben werden, die für den vorgesehenen Verarbeitungszweck nicht in jeder Hinsicht geeignet sind.

3.8.5 Anschluß der Landespolizeischule an die Zentralrechner der Datenverarbeitungszentrale (DVZ)

Ich habe stets darauf hingewiesen, daß die Sicherung personenbezogener Daten auf den Zentralrechnern der DVZ ungleich besser vorgenommen werden kann als auf dezentralen Datenverarbeitungsanlagen. Diese Sicherungsmöglichkeiten werden jedoch zum Teil zunichte gemacht, wenn dezentrale Anlagen an die Zentralrechner angeschlossen werden. Deshalb sind nach einem - mit mir abgestimmten - Rundschreiben des Senatsamtes für den Verwaltungsdienst vom 23.12.1988 über die Weiterentwicklung der IuK-Infrastruktur durch Verbindung von bisher autonom betriebenen Arbeitsplatz- und Abteilungsrechnern mit den Zentralrechnern der Datenverarbeitungszentrale Anwendungen im DVZ-Verbundmodus nur zugelassen, wenn hierbei keine personenbezogenen Daten verarbeitet werden. Ausnahmen können nur aus zwingenden Gründen zugelassen werden. Dies ist von den Anwendern eingehend zu begründen und zugleich darzulegen, durch welche Maßnahmen sichergestellt wird, daß eine unbefugte Datenverarbeitung, insbesondere ein Abruf von gesicherten Daten auf Zentralrechnern zur weiteren dezentralen Speicherung und Nutzung, ausgeschlossen ist. Soweit personenbezogene Daten verarbeitet werden sollen, ist der Hamburgische Datenschutzbeauftragte rechtzeitig vor Beginn der Verarbeitung zu informieren. Ihm ist Gelegenheit zur Stellungnahme zu geben. Eine vorliegende Stellungnahme ist dem Senatsamt zusammen mit dem Antrag auf Anschlußrealisierung vorzulegen.

Vor diesem Hintergrund war ich völlig überrascht, als mir das Senatsamt für den Verwaltungsdienst im Juli 1989 mitteilte, daß es den Anschluß eines autonom betriebenen dezentralen Rechners der Landespolizeischule an die Zentralrechner der DVZ, auf

dem personenbezogene Daten zu Schulungszwecken verarbeitet werden sollen, genehmigt habe. Zu diesem Zeitpunkt war ich von dem Vorhaben weder informiert noch war mir eine Gelegenheit zur Stellungnahme gegeben worden. Ich kam nicht umhin festzustellen, daß Regelungen, die ausdrücklich zur verfahrensmäßigen Absicherung des Rechts auf informationelle Selbstbestimmung geschaffen wurden, auf diese Weise bewußt unterlaufen worden waren, und forderte die beteiligten Stellen auf, den Anschluß zunächst nicht zu realisieren. Dies wurde zugesichert. Nach einer anschließenden Prüfung des geplanten Verfahrens habe ich eine Reihe von Forderungen erhoben und Vorschläge unterbreitet, die weitestgehend berücksichtigt wurden, so daß ich gegen den Anschluß in diesem Einzelfall keine Bedenken mehr erheben mußte. Ich muß allerdings dringend davor warnen, von dieser Möglichkeit vermehrt Gebrauch zu machen. Es besteht unter datenschutzrechtlichen Aspekten ein sehr großes Interesse daran, das geschlossene System der DVZ zu erhalten. Der Anschluß von dezentralen Rechnern muß deshalb unabweisbaren Ausnahmen vorbehalten bleiben.

3.8.6 Datenverarbeitung beim polizeilichen Staatsschutz

3.8.6.1 APIS

Schon 1987 hatte ich die Datenverarbeitung beim polizeilichen Staatsschutz überprüft (6.TB, 4.11.3). Die Prüfung hat insbesondere bei der Speicherpraxis in die als bundesweit betriebene „Arbeitsdatei PIOS-Innere Sicherheit (APIS)" erhebliche Mängel deutlich gemacht. Statt einer Stellungnahme zu meinem Prüfbericht hatte der Polizeipräsident im September 1989 im Rechtsausschuß der Bürgerschaft mitgeteilt, daß der gesamte von Hamburg eingegebene Datenbestand in APIS überprüft werde und zum damaligen Zeitpunkt schon zu etwa 35 % der Löschung von Datensätzen über Beschuldigte und Verdächtige geführt habe. Seit dieser Zeit vertröstet mich die Innenbehörde mit Zwischenbescheiden, in denen mir eine baldige Stellungnahme zu meinem Prüfbericht angekündigt wird.

Zum Redaktionsschluß für diesen Bericht wurde ich telefonisch wiederum nur darauf hingewiesen, daß mit einer Stellungnahme nun in Kürze gerechnet werden könne. Es muß festgehalten werden, daß es die Behörde für Inneres und die Polizei in über zwei Jahren nicht geschafft haben, sich zu einer begrenzten Prüfung verbindlich zu äußern. Da diese Verfahrensweise mir gegenüber mit § 20 Abs. 4 HmbDSG nicht zu vereinbaren ist, werde ich gezwungen sein, sie gegenüber dem Senat Anfang des kommenden Jahres förmlich zu beanstanden.

3.8.6.2 Nichtautomatisierte Datenverarbeitung

Bei meiner im Jahre 1987 durchgeführten Prüfung bei der polizeilichen Staatsschutzabteilung habe ich erhebliche Mängel bei der Führung von zwei manuellen Dateien festgestellt (6. TB, 4.11.3.1). Dabei handelt es sich zum einen um die sog. Indexkartei und zum anderen um die Personen- und Fallkartei bei der Fachdirektion 7 (jetzt LKA 3). Am Beispiel der Indexkartei soll die generelle datenschutzrechtliche Problematik deutlich gemacht werden, die mit der Führung manueller „Vorgangs-Suchkarteien" verbunden ist. Auch die Ausführungen zur Personen- und Fallkartei sind beispielhaft für die Kritik, die ich an polizeilichen Errichtungs- oder Feststellungsanordnungen immer wieder anzubringen habe.

3.8.6.2.1 Indexkartei

Die Indexkartei dient als sog. „Vorgangs-Suchkartei" dem Wiederauffinden von Vorgängen im Tagebuch und in den vom zuständigen Sachbearbeiter angelegten Handakten. Für alle Personen, die im Zusammenhang mit Meldungen über Ereignisse, Anzeigen, Anfragen etc. mit dem Staatsschutz in Berührung kommen, wird eine Karteikarte angelegt. Auf dieser werden Name, Vorname, Geburtsdatum und Anschrift der betreffenden Person sowie die Tagebuchnummer und der Sachbearbeiter vermerkt. Kommen neue Vorgänge zu derselben Person hinzu, so werden sie mit den entsprechenden Tage-

buchnummern in chronologischer Reihenfolge auf der Karteikarte eingetragen. Die Kartei ist alphabetisch geordnet. Die Karteikarten werden nach Ablauf von 5 Jahren - von der letzten Eintragung an gerechnet - aussortiert. Eine Überprüfung der Aussonderungsfristen findet nunmehr einmal jährlich statt.

Nach meiner Auffassung handelt es sich bei der Indexkartei um eine Datei, die der Erfüllung polizeilicher Aufgaben (Gefahrenabwehr und Strafverfolgung) dient und deshalb nach den Bestimmungen der Hamburgischen Dateirichtlinien von 1985 einer Feststellungsanordnung bedarf. Die Innenbehörde vertritt demgegenüber die Ansicht, daß für die Indexkartei als reine „Vorgangsuchkartei" eine Feststellungsanordnung nicht erforderlich sei. Es ist zwar richtig, daß die Kartei vorrangig zum Zwecke der Vorgangsverwaltung geführt wird. Die Vorgangsverwaltung ist aber nicht Selbstzweck, sondern ermöglicht u.a. den Zugriff auf bei der Polizei vorhandene Vorgänge, wenn diese zum Zwecke der Gefahrenabwehr oder der Strafverfolgung benötigt werden.

Am Beispiel einer Eingabe will ich deutlich machen, wie sich die Eintragung in der Indexkartei für den Betroffenen auswirken kann. Ein Student hatte während eines Spaziergangs durch die „City Nord" ein Gebäude fotografiert, in dem - was für Außenstehende nicht erkennbar war - die Pläne für die neue Nato-Fregatte „NFR 90" entwickelt werden. Das Gebäude ist deshalb in polizeiliche Schutzmaßnahmen einbezogen. Der Petent wurde von der Besatzung eines Streifenwagens angehalten und nach seinen Personalien befragt. Der hierüber gefertigte Bericht wurde an die Staatsschutzabteilung weitergeleitet. Die Durchschrift des Berichtes wird bei der Polizeirevierwache 1 Jahr und das Original bei der Fachdirektion 5 Jahre verwahrt.

Die Ermittlungen der FD 7 und des Landesamtes für Verfassungsschutz, dem die Personalien übermittelt worden waren, ergaben keine Anhaltspunkte für ein strafbares Verhalten, so daß ein strafrechtliches Ermittlungsverfahren nicht eingeleitet wurde. Trotzdem verbleiben die Daten des Petenten, für den eine Karteikarte in der Indexkartei angelegt worden ist, 5 Jahre lang im direkten Zugriff der Polizei. Über die Karteikarte kann jederzeit auf die vom Sachbearbeiter angelegte Handakte zurückgegriffen werden, in der sich der Bericht und der übrige Schriftwechsel zu dem Vorgang befinden. Taucht der Name des Petenten in dieser Zeit in irgendeinem „staatsschutzrelevanten" Zusammenhang - z.B. anläßlich einer Demonstration - auf, so wird der Vorgang entsprechend ergänzt und weitergeführt. Dies kann zu einem völlig falschen Bild des Petenten führen. Um dieser Gefahr vorzubeugen, müssen nach meiner Auffassung auch für die Indexkartei zumindest die differenzierten Aufbewahrungsfristen der KpS-Richtlinien (Richtlinien zur Führung Kriminalpolizeilicher personenbezogener Sammlungen) gelten. Im Falle des Petenten habe ich die Aussonderung der Karteikarte aus der Indexkartei gefordert. Eine weitere Aufbewahrung ist unzulässig, da die Ermittlungen ergeben haben, daß die Gründe, die zur Aufnahme in die Kartei geführt haben, nicht zutreffen (Ziff. 5.4 (3) KpS-Richtlinien). Eine weitere Aufbewahrung wäre allenfalls dann zulässig, wenn sie reinen Dokumentationszwecken dienen würde. Dann müßten die Daten aber aus dem aktuellen Datenbestand ausgesondert werden. Sie dürften also nicht für andere Zwecke verwendet oder gar an andere Stellen übermittelt werden.

Besonders problematisch ist in diesem Zusammenhang die Tatsache, daß dem Betroffenen auf Anfrage mitgeteilt werden würde, daß er nicht in kriminalpolizeilichen personenbezogenen Sammlungen (KpS) der Polizei gespeichert ist. Da nach Auffassung der Innenbehörde die Indexkartei der FD 7 nicht zu den KpS zählt, entspricht diese Aussage ihrem Rechtsverständnis. Nach meiner Auffassung zeigt gerade dieses Ergebnis, daß der Rechtsstandpunkt der Behörde nicht akzeptabel ist. Die Auskunft ist für den Betroffenen irreführend, weil sie nicht erkennen läßt, daß die Polizei 5 Jahre lang anhand der Indexkartei gezielt auf seine Daten und die vorhandenen Unterlagen zurückgreifen kann.

3.8.6.2.2 Personen- und Fallkartei

In der Personen- und Fallkartei werden zu einer großen Anzahl von Personen und zu bestimmten Sachkomplexen (wie z.B. Flora-Theater, Hafenstraße o.ä) Karteikarten

geführt, die durch Auflistung von Aktenzeichen auf entsprechende Personen- oder Fallakten verweisen. Sie wird für die Sachbearbeitung, die Vorgangsverwaltung und für die Erteilung von Auskünften benutzt. Für die Personen- und Fallkartei ist mir der Entwurf einer Feststellungsanordnung übersandt worden, der vor allem folgenden Bedenken begegnet:

— In vielen Fällen kommt es zu Parallelspeicherungen in der Personen- und Fallkartei und in APIS. Um solche unnötigen Doppelspeicherungen zu vermeiden, müßte auf die zusätzliche Eintragung von Daten, die im APIS-Bestand vorhanden sind, in die Personen- und Fallkartei verzichtet werden. Die Personen- und Fallkartei sollte auf die Fälle von regionaler Bedeutung beschränkt werden, während die Fälle von überregionaler Bedeutung nur noch in APIS eingestellt werden sollten.

— Der Anwendungsbereich der Datei ist viel zu weit gefaßt. Sie dient praktisch der Erfüllung sämtlicher Aufgaben, die in den Zuständigkeitsbereich der Staatsschutzabteilung fallen. Zur Beschreibung des Anwendungsbereichs wird in dem Entwurf der Feststellungsanordnung einfach auf den Organisationplan der Fachdirektion verwiesen. Statt dessen halte ich eine klare Festlegung derjenigen Straftatbestände in einem abschließenden Katalog für erforderlich, die in den einzelnen Zuständigkeitsbereichen des Staatsschutzes - z.B. Terrorbekämpfung, Waffen- und Sprengstoffdelikte oder Landesverrat und nationalsozialistische Gewaltverbrechen - typischerweise einschlägig sind. Sollte eine abschließende Aufzählung nicht möglich sein, so muß zumindest anhand konkreter, restriktiv anzuwendender Kriterien festgelegt werden, wann und unter welchen Voraussetzungen personenbezogene Daten in der Datei gespeichert werden dürfen. Ein allgemeines politisches Motiv reicht - ebenso wie bei APIS - keinesfalls aus, um eine Aufnahme in die Kartei zu rechtfertigen.

  Um eine wirksame Überprüfung zu gewährleisten und unzulässige Speicherungen von vornherein zu vermeiden, sollten außerdem die Gründe für die Einstellung in die Datei bzw. für die Aufrechterhaltung der Speicherung nach Abschluß des Ermittlungsverfahrens schriftlich in der entsprechenden Handakte vermerkt werden. Eine solche Begründung sollte spätestens nach der Mitteilung der Staatsanwaltschaft über den Ausgang des Ermittlungsverfahrens erfolgen.

3.8.7 Auskunft über gespeicherte Daten

Wenn Bürger über ihre bei der Polizei gespeicherten Daten Auskunft verlangen, bekommen sie unter den Einschränkungen, die ich vorstehend bei 3.8.6.2.1 beschrieben habe, in den meisten Fällen die gewünschten Informationen. Nur selten macht die Polizei von der Möglichkeit Gebrauch, die Auskunft gem. § 14 Abs. 2 oder 3 HmbDSG zu verweigern, etwa weil die Erfüllung polizeilicher Aufgaben durch die Auskunft erschwert oder gefährdet würde. In solchen Fällen ist sie nach einhelliger Auffassung gehalten, ihr Geheimhaltungsinteresse mit dem Auskunftsinteresse der Betroffenen abzuwägen. Dies gelingt nicht immer.

Im Fall einer Petentin, die sich schon im November 1987 an mich gewendet hatte, weil sie in einer Presseveröffentlichung unter Berufung auf polizeiliche Informationssysteme der RAF-Szene zugeordnet worden war, konnte sich die hamburgische Polizei bis heute nicht durchringen, die nach meiner Auffassung gebotene Auskunft zu erteilen. Es dürfte unbestreitbar sein, daß eine solche Veröffentlichung ein gesteigertes Auskunftsinteresse der Betroffenen begründet. Dementsprechend hatte das Bundeskriminalamt, das ebenfalls um Auskunft ersucht worden war, schon im Januar 1988 umfassend Auskunft erteilt. Dies läßt den Schluß zu, daß jedenfalls diese Dienststelle ein Geheimhaltungsinteresse der Polizei, das das Auskunftsinteresse der Betroffenen überwiegen könnte, nicht sah. Gleichwohl hält die Hamburger Polizei seit nunmehr fast zwei Jahren an ihrer ursprünglichen Entscheidung, keine Auskunft zu erteilen, fest. Bis mir gegenüber ein sachlich begründbares Geheimhaltungsinteresse, das sich nicht in Leerformeln erschöpft, darlegt wurde oder die begehrte Auskunft erteilt ist, werde ich das Anliegen der Petentin mit den mir zur Verfügung stehenden Möglichkeiten unterstützen.

3.9 Verfassungsschutz

3.9.1 Stand der Gesetzgebung

Im April 1989 hat die Bundesregierung den Entwurf eines Artikelgesetzes (BT-Drs. 11/4306), das auch eine Neufassung des Bundesverfassungsschutzgesetzes (BVerfSchG-E) enthält, eingebracht. Der Gesetzentwurf soll nach dem Willen der Bundesregierung Rechtsgrundlagen und Tätigkeiten des Bundesamtes für Verfassungsschutz klarer beschreiben und insbesondere näher bestimmen, unter welchen Voraussetzungen es personenbezogene Informationen erheben, verarbeiten und nutzen darf. Mit ihm sollen die nach dem Volkszählungsurteil des Bundesverfassungsgerichts erforderlichen Rechtsgrundlagen für die Befugnisse der Verfassungsschutzbehörden geschaffen werden. Dieses Ziel wird nach meiner Auffassung in weiten Bereichen verfehlt. Im übrigen wird es immer wahrscheinlicher, daß das Gesetzesvorhaben in dieser Legislaturperiode nicht verwirklicht werden kann - und dies, obwohl schon seit 1983 klar ist, daß die Verfassungsschutzbehörden dringend auf die erforderlichen Rechtsgrundlagen für ihre Arbeit angewiesen sind.

Bei dieser Sachlage ist die Position des Senats, mit einem eigenen Verfassungsschutzgesetz zu warten, bis ein Bundesverfassungsschutzgesetz in Kraft getreten ist, unhaltbar geworden. Hamburg muß sich von der Rechtsentwicklung des Bundes abkoppeln, um zügig einen rechtsstaatlichen Zustand herzustellen. Im folgenden will ich anhand des vorliegenden Entwurfes einige Vorschläge zur Novellierung des Verfassungsschutzrechts unterbreiten.

3.9.1.1 Auftrag des Verfassungsschutzes

Der Verfassungsschutz ist nach dem Willen der „Väter des Grundgesetzes" Bestandteil der wehrhaften Demokratie. In Art. 87 Abs. 1 Satz 2 GG wird der Bund ermächtigt, eine Zentralstelle „zur Sammlung von Unterlagen für Zwecke des Verfassungsschutzes und des Schutzes gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden", einzurichten. In § 3 Abs. 1 Nr. 1 BVerfSchG-E wird die Aufgabe des Verfassungsschutzes - aufbauend auf einer Begriffsbestimmung in Art. 73 Ziff. 10b GG definiert als Sammlung und Auswertung von Informationen über „Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern der Verfassungsorgane des Bundes oder eines Landes zum Ziele haben".

Zentraler Begriff bei der Bestimmung der Aufgaben der Verfassungsschutzbehörden ist die „freiheitliche demokratische Grundordnung". Dieser muß, um das Aufgabenfeld des Verfassungsschutzes deutlich zu machen und zugleich im Hinblick auf die freie politische Betätigung der Bürger zu begrenzen, näher erläutert werden - und zwar im Gesetz selbst. Dazu können einschlägige Entscheidungen des Bundesverfassungsgerichts - etwa die grundlegende Entscheidung zum SRP-Verbot (BVerfGE Bd. 2, S. 1/3) - und die in § 92 StGB enthaltenen Begriffsbestimmungen mit herangezogen werden. Ein bloßer Verweis hierauf in der Begründung des Entwurfs genügt allerdings nicht. Bei der Inhaltsbestimmung des Begriffs „freiheitliche demokratische Grundordnung" ist vom Demokratieprinzip auszugehen: wesensnotwendig ist die ständige Chance zum demokratischen Wechsel, zur Veränderung der politischen und sozialen Verhältnisse. Geschützt wird der demokratische Prozeß einschließlich seiner Voraussetzungen für die politische Betätigung des einzelnen sowie von Zusammenschlüssen bis hin zur Bildung einer Opposition, nicht aber die jeweilige Regierungsmeinung. Nicht das Ziel einer Veränderung der politischen Verhältnisse richtet sich gegen die freiheitliche demokratische Grundordnung, sondern die Beseitigung der Chance der Veränderung. Nicht Gegnerschaft zur jeweiligen Regierung oder zu bestimmten Parteien kennzeichnet also den Verstoß gegen die freiheitliche demokratische Grundordnung, sondern

der Kampf um die Beseitigung der demokratischen Struktur. Nur in diesem Rahmen haben die Verfassungsschutzbehörden ihre Aufgaben zu erfüllen.

3.9.1.2 Beschreibung der Aufgaben

Diese aus der Verfassung abgeleitete Beschränkung der Aufgaben des Verfassungsschutzes kommt in der im BVerfSchG-E vorgenommenen Aufgabenbeschreibung nicht mit der gebotenen Normenklarheit zum Ausdruck. Da andererseits Befugnisse mit Eingriffscharakter an die verschwommenen Aufgabenzuweisungen anknüpfen, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung der Aufgaben des Verfassungsschutzes.

Dabei ist folgendes zu berücksichtigen:

— Der Verwendungszweck von Datensammlungen muß im Gesetz präzise bestimmt werden. Die vorgesehene Formulierung, wonach es Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist, Informationen zu sammeln über „Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziele haben", läßt den eigentlichen Zweck der Sammlungen und ihre Auswertung jedoch offen. Sammlung und Auswertung durch das BfV sind aber kein Selbstzweck. Deshalb muß - und zwar im Gesetz - festgelegt werden, welchen unterschiedlichen Zwecken die einzelnen Informationssammlungen des BfV dienen.

— Um eine ausufernde Beobachtungspraxis politisch aktiver Zusammenschlüsse oder gar einzelner Personen zu verhindern, muß klargestellt werden,

  * daß der Begriff der Bestrebungen das Handeln einer Mehrzahl von Personen voraussetzt, daß deren gemeinsame Aktivität einen gewissen Grad von organisatorischer Verfestigung erreicht hat, und daß die Beobachtung und Registrierung einzelner Personen nur dann erfolgen darf, wenn ein Bezug zu einer extremistischen Bestrebung in der Person des Betroffenen konkret erfüllt ist;
  * daß es nicht zulässig ist, Informationen auch über solche Bestrebungen zu sammeln und zu speichern, die erkennbar nicht gegen die freiheitliche demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen extremistischen Bestrebungen mitwirken;
  * daß Informationen über nicht extremistische Organisationen, die Gegenstand extremistischer Beeinflussung (-sversuche) sind, nur insoweit gesammelt und gespeichert werden dürfen, als konkrete Anhaltspunkte für eine solche (versuchte) „Unterwanderung" vorliegen und dies für die Feststellung der Unterwanderung erforderlich ist;
  * daß sich bei der Beobachtung extremistischer Organisationen die Tätigkeit des Verfassungsschutzes auf deren Träger, d.h. die führenden und aktiv mitarbeitenden Personen, beschränken muß und nicht routinemäßig auf einfache Mitglieder erstrecken darf.

3.9.1.3 Erhebung personenbezogener Daten und Einsatz nachrichtendienstlicher Mittel

Die Befugnisse des Verfassungsschutzes zur Erhebung personenbezogener Daten müssen im Hinblick auf die grundlegende Bedeutung der Grundrechtsausübung im Bereich der politischen Betätigung des Bürgers stärker als im Entwurf vorgesehen eingegrenzt werden.

Es muß 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.

Insbesondere für den Einsatz nachrichtendienstlicher Mittel muß gelten, daß sie sich nur gegen denjenigen richten dürfern, der selbst verdächtig ist, die in § 7 Abs. 1

genannten Tätigkeiten auszuüben. Der gezielte Einsatz gegen unverdächtige bzw. unbeteiligte Dritte ist auszuschließen.

Die zulässigen nachrichtendienstlichen Mittel sollten im Gesetz abschließend genannt werden. Es 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 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, 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.

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.

Soweit Handlungen erlaubt sein sollen, die eigentlich strafbar wären (z.B. Herstellung und Verwendung falscher Ausweispapiere), müssen deren Voraussetzungen im Bundesverfassungsschutzgesetz genau geregelt werden.

Ferner sollten zum Schutze des Betroffenen beim Einsatz nachrichtendienstlicher Mittel die im Gesetz zu Artikel 10 Grundgesetz (G-10) vorgesehenen Verfahrenssicherungen in die vorliegenden Entwürfe übernommen werden. Dieser Gedanke findet sich bereits ansatzweise in dem Entwurf, sollte aber konsequent weitergeführt werden:

— Eingriffe, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, sollten nur vorgenommen werden dürfen, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, daß jemand eine der im Straftatenkatalog in § 2 Abs. 1 G-10 aufgeführten Straftaten plant, begeht oder begangen hat. Sie sollten nur zulässig sein, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Im übrigen geht auch das G-10 in § 2 Abs. 2 davon aus, daß sich entsprechende Maßnahmen nur gegen den Verdächtigen oder gegen Personen richten dürfen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, daß sie für den Verdächtigen Mitteilungen entgegennehmen oder weitergeben.

— Um dem Betroffenen die Möglichkeit zu geben, sich gegen eine mögliche Verletzung seiner Rechte zur Wehr zu setzen, muß er - der in § 5 Abs. 5 G-10 getroffenen Regelung entsprechend - vom Einsatz der nachrichtendienstlichen Mittel unterrichtet werden, sobald eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Eine solche Benachrichtigungspflicht ist bereits in § 4 Abs. 2 des bremischen Verfassungsschutzgesetzes enthalten.

— 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 festgelegt werden.

— Entsprechend § 7 Abs. 4 G-10 sollte die unverzügliche Vernichtung der durch die Maßnahmen erlangten Unterlagen vorgesehen werden, wenn diese zu dem o.g. Zweck nicht mehr erforderlich sind. Die Vernichtung ist aktenkundig zu machen.

3.9.1.4 Einsicht in amtliche Register

Die Frage, ob die Nachrichtendienste in amtliche Register Einsicht nehmen dürfen, kann nur bereichsspezifisch, d.h. in dem jeweils einschlägigen Spezialgesetz geregelt werden. Schließt man sich dieser Auffassung nicht an, so sind jedenfalls an eine Regelung im BVerfSchG-E selbst folgende Anforderungen zu stellen:

— Die amtlichen Register, in die die Nachrichtendienste Einsicht nehmen dürfen, sollten zugunsten einer für den Bürger transparenten Regelung im Gesetz abschließend aufgeführt werden. Zumindest ansatzweise ist diese Forderung bisher in § 4a Abs. 1 des nordrhein-westfälischen Verfassungsschutzgesetzes berücksichtigt worden, wo einige in Betracht kommende Register beispielhaft genannt werden.

— Auch die Befugnis, amtliche Register einzusehen, muß nach den einzelnen Aufgabenbereichen des Verfassungsschutzes differenziert geregelt werden. Nach dem Grundsatz der Erforderlichkeit solcher Maßnahmen muß die Einsichtnahme meines Erachtens auf den Bereich der Spionageabwehr und der Terrorismusbeobachtung beschränkt werden.

— Selbst wenn man zur Erfüllung bestimmter Aufgaben des Verfassungsschutzes und der anderen Dienste die Einsicht in amtliche Register zuläßt, rechtfertigt dies nicht die Einrichtung von on-line-Anschlüssen.

3.9.1.5 Speicherung, Änderung und Nutzung personenbezogener Daten

Die bisher im BVerfSchG-E vorgesehenen Regelungen zu der zentralen Frage des Umfangs der Speicherbefugnis werden den Anforderungen des Bundesverfassungsgerichts an Rechtsnormen zur Einschränkung des Grundrechts auf informationelle Selbstbestimmung nicht gerecht:

— Im Entwurf wird lediglich die Speicherung personenbezogener Daten in Dateien geregelt. Notwendig ist aber auch eine bereichsspezifische Regelung der Speicherung in Akten.

— Desweiteren muß klargestellt werden, daß Speicherungen nur gerechtfertigt sind, wenn in der Person des Betroffenen selbst tatsächlich Anhaltspunkte für den Verdacht von verfassungsfeindlichen Bestrebungen, terroristischen Handlungen oder Spionagetätigkeiten liegen.

— Erhebliche Regelungsdefizite gibt es schließlich bei der Speicherbefugnis in bezug auf Daten, die im Rahmen von Sicherheitsüberprüfungen erhoben worden sind. Vorgesehen ist eine Speicherung, wenn das Bundesamt für Verfassungsschutz bei Sicherheitsprüfungen und technischen Sicherheitsmaßnahmen tätig wird. 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 z.B. auch Daten über Auskunftspersonen, Verwandte etc. erfaßt werden dürfen.

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 Aufgaben 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.

3.9.1.6 Errichtung bzw. Unterhaltung gemeinsamer Verbund- und Textdateien

Im vorgelegten Entwurf wird auch die Bereithaltung gemeinsamer Datenbestände der Verfassungsschutzbehörden geregelt. Diese Vorschrift soll die Rechtsgrundlage für das nachrichtendienstliche Informationssystem (NADIS) schaffen. Sie soll offenbar die gegenwärtige Praxis absichern, ohne sie an irgendwelche einengende Voraussetzungen zu knüpfen.

Besondere datenschutzrechtliche Risiken birgt die Aufnahme von Textzusätzen aus Akten der Verfassungsschutzbehörden in automatisierte Dateien. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen. Sollten dennoch Textzusätze in eingeschränktem Umfang zugelassen werden, ist es über die bereits im Entwurf getroffenen Beschränkungen und Schutzvorkehrungen hinaus unerläßlich, in der Datei die für die Bewertung und Überprüfung solcher Textzusätze maßgeblichen Unterlagen anzugeben. Ferner muß sichergestellt sein, daß durch die Automation keine Verkürzung und Verzerrung von Sachverhalten entsteht.

Aus diesen Gründen halte ich eine gesetzliche Festlegung der Kriterien, bei deren Vorliegen die Automatisierung eingeleitet werden darf, für zwingend erforderlich.

3.9.1.7 Aufbewahrungs- bzw. Löschungsfristen

Es ist notwendig, gesetzliche Regelfristen für die Überprüfung und Löschung der gespeicherten Daten festzulegen. Dabei muß wiederum zwischen den einzelnen Aufgabenbereichen (Extremismusbeobachtung/Spionageabwehr/Terrorismusbeobachtung /Sicherheitsüberprüfung) unterschieden werden.

Die bisher in Verwaltungsvorschriften festgelegten Löschungsvorschriften dürfen nicht pauschal übernommen, sondern müssen überprüft werden. Insbesondere ist die bislang vorgesehene Regelfrist von 15 Jahren im Extremismusbereich zu lang.

Sicherzustellen ist ferner, daß Löschungen nicht nur bei der speichernden Stelle erfolgen, sondern daß die Tatsache der Löschung an andere Stellen nachberichtet wird. Diese Nachberichtspflicht muß nicht nur gegenüber Dritten gelten, die Kenntnis von der gespeicherten Information erhalten haben, sondern auch und gerade gegenüber den Verbundteilnehmern.

3.9.1.8 Beachtung des Zweckbindungsgebotes bei der Nutzung und Übermittlung personenbezogener Daten

Nach dem Zweckbindungsgebot dürfen personenbezogene Daten grundsätzlich nur zu dem Zweck genutzt werden, zu dem sie erhoben worden sind. Jede Zweckänderung stellt einen weiteren Eingriff in das Recht auf informationelle Selbstbestimmung dar; sie ist daher nur auf gesetzlicher Grundlage im überwiegenden Allgemeininteresse zulässig. Hieraus folgt, daß auch innerhalb des Verfassungsschutzes nicht jede Information, die zur Erfüllung einer bestimmten Aufgabe erhoben worden ist, unabhängig von ihrer Herkunft für jede andere Aufgabe verwendet werden darf.

3.9.1.8.1 Übermittlungen an und durch den Verfassungsschutz

— Die bisher vorgesehenen Übermittlungsverbote reichen schon deshalb nicht aus, weil die übermittelnde Stelle nicht ausdrücklich verpflichtet wird zu prüfen, ob schutzwürdige Belange des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen.

— Die ebenfalls vorgesehene Regelung der sog. „Spontanübermittlungen", d.h. der Befugnis anderer Behörden, Informationen unaufgefordert an das BfV zu übermitteln, sieht im Grunde genommen keinerlei wirksame Einschränkungen vor. Da es nur darauf ankommen soll, daß die übermittelnde Behörde die ihr bekanntgewordene Information für die Erfüllung der Aufgaben des BfV für erforderlich hält, steht es dieser praktisch frei, ihren eigenen Maßstab bei der Frage der Erforderlichkeit

anzulegen. Die genannten Stellen können sich, wenn sie den Maßstab entsprechend niedrig ansetzen, bei der Weitergabe der bei ihnen vorhandenen Daten sozusagen wie ein „verlängerter Arm" des Verfassungsschutzes verhalten. Um die Übermittlungspraxis zum Schutze des Bürgers einzuschränken, sollte im Gesetz klargestellt werden, daß „Spontanübermittlungen" auf keinen Fall zulässig sind, wo es um Informationen über gewaltfreie extremistische Bestrebungen geht.

3.9.1.8.2 Übermittlungen zwischen Verfassungsschutz- und Sicherheitsbehörden unter Beachtung des Trennungsgebotes

Aus dem Trennungsgebot ergeben sich für die informationelle Zusammenarbeit zwischen Verfassungsschutz- und Strafverfolgungs- bzw. Sicherheitsbehörden insbesondere folgende Konsequenzen:

— Der Gesetzgeber muß von den unterschiedlichen Aufgaben der verschiedenen Polizei- und Verfassungsschutzbehörden ausgehen und auf dieser Grundlage festlegen, wann Zweckdurchbrechungen im überwiegenden Allgemeininteresse zugelassen werden können. Dabei bedarf es einer präzisen Bestimmung der Aufgaben der jeweiligen Behörden, zu deren Erfüllung eine Übermittlung zulässig sein soll. Was die Aufgaben des Verfassungsschutzes anbetrifft, so fehlt es hieran aber gerade. Deshalb reicht der im Entwurf enthaltene Verweis auf die Aufgaben des BfV nicht aus, um die „Spontanübermittlungen" von Polizei und Strafverfolgungsbehörden an den Verfassungsschutz normenklar zu begrenzen.

— Der BVerfSchG-E sieht für die Polizei- und Strafverfolgungsbehörden weitgehende Verpflichtungen zu „Spontanübermittlungen" von personenbezogenen Informationen an die Nachrichtendienste vor. Derartige Pflichten sind zwar grundsätzlich anzuerkennen, sollten aber - anknüpfend an die übermittelnde Behörde - in den einzelnen Polizeigesetzen (Länderpolizeigesetze, BKAG, BGSG) und in der StPO bereichsspezifisch geregelt und an präzise Voraussetzungen gebunden werden.

— Folgt man diesem Ansatz nicht, so muß jedenfalls - nach dem Vorbild des bremischen Verfassungsschutzgesetzes - bei den geregelten Übermittlungen 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 gleichsam 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.

— Für Daten, die die Polizei bei Hausdurchsuchungen oder mit verdeckten Ermittlungsmethoden, z.B. durch den Einsatz von V-Leuten, verdeckten Ermittlern oder technischen Geräten, polizeiliche Beobachtung oder längerfristige Observation gewonnen hat, müssen einschränkende Verwertungsregelungen geschaffen werden. Da die Erhebung personenbezogener Daten mit diesen Mitteln einen schwerwiegenden Eingriff in das Persönlichkeitsrecht des Betroffenen mit sich bringt, halte ich eine Übermittlung an den Verfassungsschutz aus Gründen der Verhältnismäßigkeit allenfalls im Bereich der Spionageabwehr und der Terrorismusbeobachtung für zulässig.

— Die Weitergabe von Daten durch den Verfassungsschutz an Polizei und Strafverfolgungsbehörden muß ebenfalls restriktiver als in den Entwürfen vorgesehen geregelt werden. Nach dem BVerfSchG-E sollen solche Übermittlungen „zur Verhinderung oder Verfolgung von Staatsschutzdelikten" zulässig sein. Hält man Mitteilungen des BfV an die Polizei zur Verhinderung von Straftaten überhaupt für geeignet, dann

muß zumindest klargestellt werden, daß es nur um die Verhinderung einer konkret drohenden Straftat, d.h. um die Abwehr einer konkreten Gefahr gehen kann.

Die im Entwurf enthaltene Definition der „Staatsschutzdelikte" ist darüber hinaus sehr unpräzise. Neben den in §§ 74a und 120 GVG genannten Straftaten sollen alle sonstigen Straftaten relevant sein, bei denen tatsächliche Anhaltspunkte dafür vorliegen, daß sie wegen „ihrer Zielsetzung, des Motivs des Täters oder des Beschuldigten oder deren Verbindung zu einer Organisation" gegen die in Art. 73 Nr. 10b oder c GG vage umschriebenen Schutzgüter gerichtet sind. Diese Definition ermöglicht es, fast jedes Delikt bei einer bestimmten Fallgestaltung zu einem Staatsschutzdelikt zu erklären. Die Delikte, die sich gegen Schutzgüter des Staatsschutzes richten, sollten in einem Katalog abschließend aufgezählt werden; als Muster käme z.B. § 2 G-10 in Betracht.

Zu berücksichtigen ist ferner, daß Informationen, die der Verfassungsschutz durch den Einsatz nachrichtendienstlicher Mittel gewonnen hat, einer besonders strengen Zweckbindung unterliegen müssen. 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 plant, begeht oder begangen hat. Nach diesem Vorbild sollte auch die Verwendung von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen werden, eingeschränkt werden.

— Für die im Entwurf vorgesehene Einrichtung von automatisierten Direktabrufverfahren zwischen Polizeibehörden und Nachrichtendiensten ist ein Bedürfnis nicht dargelegt. Wegen der mit on-line-Zugriffen generell verbundenen massiven Durchbrechung des Trennungsgebotes erscheint die ersatzlose Streichung der entsprechenden Erlaubnis angebracht.

3.9.1.9 Auskunftsersuchen und Schutzrechte der Bürger

— Mit Blick auf die neuere Rechtsprechung zum Auskunftsanspruch gegenüber den Nachrichtendiensten ist im Gesetz selbst klarzustellen, daß der Betroffene einen Anspruch auf ermessensfehlerfreie Entscheidung über sein Auskunftsbegehren hat. Die routinemäßige Ablehnung der Auskunftserteilung mit dem pauschalen Hinweis auf das Geheimhaltungsinteresse der Nachrichtendienste ist mit der Bedeutung des Auskunftsanspruchs auf keinen Fall vereinbar.

Bei der Ausgestaltung des Anspruchs ist es wiederum erforderlich, nach den jeweiligen Aufgaben der Verfassungsschutzbehörden zu differenzieren. Es dürfte klar sein, daß für personenbezogene Daten, die anläßlich einer Sicherheitsüberprüfung erhoben und gespeichert werden, andere Maßstäbe an die Geheimhaltungsbedürftigkeit anzulegen sind als bei Erkenntnissen aus dem Bereich der Terrorismusbeobachtung und der Spionageabwehr. Da bei Sicherheitsüberprüfungen dem Betroffenen die Tatsache der Erhebung und Speicherung seiner Daten regelmäßig bekannt ist, ist in diesen Fällen in aller Regel Auskunft zu erteilen.

— Schließlich müßte klargestellt werden, daß grundsätzlich auch über Vorgänge, die abgeschlossen sind, Auskunft zu erteilen ist. Selbst das G-10 sieht in seinem § 5 Abs. 5 eine Mitteilungspflicht über die Beschränkungsmaßnahmen gegenüber den Betroffenen vor, sobald eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann.

— In den übrigen Fällen bedarf es einer Abwägung im Einzelfall. Im Gesetz muß festgelegt werden, daß bei einer Auskunftsverweigerung die Gründe nachvollziehbar dargelegt werden müssen, um dem Betroffenen eine gerichtliche Überprüfung der Entscheidung zu ermöglichen. Daneben müssen intern die Gründe im einzelnen dokumentiert werden.

3.9.2 Erfassung von Aus- und Übersiedlern

Im Juli des Berichtsjahres ist in der Öffentlichkeit bekannt geworden, daß das Bundesamt und die Landesämter für Verfassungsschutz die Datei „ADOS" eingerichtet haben,

in der sämtliche Aus- und Übersiedler sowie die Asylbewerber aus den osteuropäischen Staaten einschließlich der DDR mit Ausnahme dreier südosteuropäischer Staaten über ihre Registriernummer zusammen mit ihren Adressen und Arbeitgebern aus den vergangenen Jahren in den Herkunftsländern erfaßt werden sollen. Die Datei soll der Spionageabwehr dienen. Nach einer umfassenden rechtlichen Prüfung dieses Vorhabens bin ich zu dem Ergebnis gekommen, daß die Erhebung, Weitergabe und Speicherung der früheren Arbeitsstellen und Wohnungen der Betroffenen unzulässig ist. Schon für die Erhebung dieser Daten fehlt es an einer nach der Rechtsprechung des Bundesverfassungsgerichts erforderlichen gesetzlichen Befugnisnorm. Sie ist darüber hinaus auch dann nicht zulässig, wenn man rechtssystematisch verfehlt von den Aufgaben der Aufnahmebehörden auf ihre Befugnisse schließen wollte und die Erforderlichkeit am Zweck des Aufnahmeverfahrens mißt.

Nach § 1 des Gesetzes über die Aufnahme von Deutschen in das Bundesgebiet vom 22.8.1950 (BGBl. S. 367), zuletzt geändert durch Gesetz vom 18.2.1986 (BGBl. I S. 265) - AufnG - bedürfen deutsche Staatsangehörige und deutsche Volkszugehörige, die ihren ständigen Aufenthalt im Bundesgebiet oder in West-Berlin begründen wollen, einer besonderen Erlaubnis, die nur verweigert werden darf, wenn sie

— dem in der sowjetischen Besatzungszone und im sowjetisch besetzten Sektor von Berlin herrschenden System erheblich Vorschub geleistet haben oder

— während der Herrschaft des Nationalsozialismus oder in der sowjetischen Besatzungszone oder im sowjetisch besetzten Sektor von Berlin durch ihr Verhalten gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen haben oder

— die freiheitliche demokratische Grundordnung der Bundesrepublik Deutschland einschließlich des Landes Berlin bekämpft haben.

Für die danach anzustellenden Prüfungen sind die im Fragebogen „Angaben zur Aufnahme" auf Seite 2 vorgesehenen Fragen nach den Wohnungen der letzten zehn Jahre und den Arbeitgebern der letzten 15 Jahre offensichtlich nicht erforderlich. Sie dürften einzig und allein zur Befriedigung des Informationsinteresses anderer Behörden, insbesondere der Verfassungsschutzbehörden, gestellt werden.

Dies wäre nach der vorgegebenen Rechtslage allenfalls auf freiwilliger Basis möglich. Dann müßten die Betroffenen jedoch gem. § 9 Abs. 2 BDSG bzw. § 9 Abs. 2 HmbDSG auf die Freiwilligkeit ausdrücklich hingewiesen werden, was unzweifelhaft nicht geschieht. Stattdessen werden die Betroffenen sogar getäuscht und unter Druck gesetzt.

Sie werden nämlich darauf hingewiesen, daß bewußt unrichtige Angaben zur Rücknahme eines erteilten Aufnahmescheins gem. § 1 AufnG und zur Erstattung erhaltener finanzieller Zuwendungen führen könne. Dadurch wird ihnen der Eindruck vermittelt, alle Angaben seien zur Prüfung des Aufnahmebegehrens erforderlich, was jedoch im Hinblick auf die gesetzlichen Bestimmungen nicht zutrifft. Zugleich werden sie damit zur vollständigen und richtigen Beantwortung der Fragen praktisch gezwungen.

Diese Art und Weise der Datenerhebung ist unzulässig.

Auch für die Weitergabe der erhobenen Daten an die Verfassungsschutzbehörden fehlt es an einer gesetzlichen Grundlage und auch hier werden die Betroffenen getäuscht: Auf Seite 4 des Aufnahmebogens wird von den Betroffenen ausdrücklich ihr Einverständnis dafür eingeholt, daß die gemachten Angaben auf Anforderung an Behörden weitergegeben werden, bei denen sie die Gewährung von Leistungen und Vergünstigungen beantragt haben oder beantragen werden. Die Verfassungsschutzbehörden, die ausnahmslos sämtliche Aufnahmefragebogen erhalten, werden mit keinem Wort erwähnt.

Wenn danach die Erhebung und Weitergabe der oben näher bezeichneten Daten unzulässig ist, ist nach allgemeiner Auffassung ihre Speicherung in der Datei ADOS

ebenfalls unzulässig - ohne daß es noch darauf ankommt, daß auch für die Speicherung eine gesetzliche Grundlage nicht zur Verfügung steht.

Darüber hinaus habe ich Zweifel, ob selbst der Gesetzgeber für die Zukunft eine verfassungsmäßige Grundlage für die Datei ADOS schaffen kann. Die Datei wird damit begründet, daß die in ihr erfaßten Personen in späteren Spionageverdachtsfällen möglicherweise als Zeugen und Auskunftspersonen herangezogen werden können. Ein möglicher Ertrag aus einer im Einzelfall vorgesehenen Befragung ist völlig ungewiß. Die vage Aussicht auf einen sinnvollen Einsatz der Datei kann meines Erachtens die Speicherung einiger Millionen Datensätze nicht rechtfertigen, wenn der Grundsatz der Verhältnismäßigkeit noch eine rechtspraktische Relevanz haben und nicht zu einer blassen Verfassungstheorie verkommen soll.

Außerdem dürfte es mit den Anforderungen des vom Grundgesetz gewollten freiheitlich demokratischen Rechtsstaats unvereinbar sein, Menschen, die auch wegen der übermäßigen Überwachung in totalitären Gesellschaftsordnungen in die Bundesrepublik Deutschland kommen, als eine der ersten staatlichen Maßnahmen die - durch Druck und Täuschung unterstützte - Erfassung durch die Verfassungsschutzbehörden erdulden zu lassen.

Aufgrund dieser Erwägungen verbietet es sich, für die Datei ADOS vermeintliche Befugnisse nach der „Übergangsrechtsprechung" des Bundesverfassungsgerichts in Anspruch zu nehmen.

Vor diesem rechtlichen Hintergrund habe ich das hamburgische Landesamt für Verfassungsschutz aufgefordert, sämtliche bisher von Hamburg in ADOS erfaßten Daten zu löschen und weitere Datenspeicherungen zu unterlassen. Dessen Leiter hat mir mitgeteilt, daß bis auf weiteres keine Daten mehr gespeichert und demnächst darüber entschieden werden soll, ob die Datei überhaupt fortgeführt werden soll.

3.9.3 Gemeinsame Tagung mit Vertretern der Verfassungsschutzbehörden

In den vergangenen Jahren habe ich immer wieder feststellen müssen, daß das bei der Verarbeitung personenbezogener Daten notwendige Zusammenwirken der Datenschutzbeauftragten und der Verfassungsschutzbehörden in vielen Bereichen aufgrund von Berührungsängsten und fehlerbehafteter Kommunikation erheblich gestört ist. Ich habe deshalb von Anfang an aktiv das Bemühen unterstützt, diese Störungen durch besseres Kennenlernen der unterschiedlichen Standpunkte und der Erörterung gemeinsam interessierender Themen abzubauen. Daraus ist die Durchführung einer gemeinsamen Tagung von Datenschutzbeauftragten und Leitern verschiedener Verfassungsschutzbehörden im Dezember 1989 entstanden, auf der nicht nur über die Verfassungsschutzgesetzgebung diskutiert, sondern auch sehr konkrete Fragen der Aufgaben dieser Ämter und den daraus folgenden Datenverarbeitungsmaßnahmen erörtert wurden. Nach meinem Eindruck wurde das Ziel der Tagung erreicht. Es scheint mir, daß bei den Teilnehmern ein besseres Verständnis für die jeweiligen Aufgaben gebildet werden konnte, und ich hoffe, daß weitere Veranstaltungen dieser Art folgen können. Dem Datenschutz, aber auch dem Verfassungsschutz kann nicht mit dem Festhalten an möglicherweise bestehenden Feindbildern gedient werden.

3.10 Justiz

Die Automation der Justiz macht nicht nur in Hamburg, sondern bundesweit rasche Fortschritte. Mit bedeutenden Zuwachszahlen werden Präsidialverwaltungen, Geschäftsstellen, aber auch die einzelnen Richter und Spruchkörper mit dezentralen Datenverarbeitungsanlagen ausgestattet. Dagegen sind die gesetzgeberischen Initiativen, die der Justiz die verfassungsrechtlich gebotenen Rechtsgrundlagen für die Datenverarbeitung schaffen sollten und die dringend benötigt werden, auch in dieser Legislaturperiode wieder im Ansatz stecken geblieben. So hat der Bundesjustizminister dem Rechtsausschuß des Deutschen Bundestages mitgeteilt, daß die folgenden

Gesetzgebungsvorhaben voraussichtlich erst in der nächsten Legislaturperiode behandelt werden können:

— Justizmitteilungsgesetz

— Bundeszentralregistergesetz

— Schuldnerverzeichnis (§ 915 ZPO)

— Strafprozeßordnung

— Strafvollzugsgesetz

Was hinter den gesetzgeberischen Aktivitäten häufig steckt, hat der Bundesjustizminister mit seltener Klarheit im Zusammenhang mit der Überarbeitung des Zwangsvollstreckungsrechts offengelegt: nämlich um die „datenschutzfeste" Festschreibung der bisher geübten Praxis. Zwar mußte sich der Eindruck, daß eben dies das wesentliche Anliegen der Reform war, schon bei vielen Gesetzentwürfen aufdrängen, so unverblümt hat sich bislang jedoch kein politisch Verantwortlicher geäußert.

3.10.1 Novellierung der Strafprozeßordnung

Im November 1988 hat der Bundesminister der Justiz nach langen Vorarbeiten einen Referentenentwurf zur Novellierung der StPO (im folgenden: StVÄG 1988) vorgelegt. Dieser ist nach Abstimmung mit den Justizverwaltungen der Länder im Juni 1989 nochmals erheblich verändert werden (im folgenden: StVÄG 1989).

3.10.1.1 Wichtige Kritikpunkte

Der Novellierungsentwurf verfolgt das Ziel, bereichsspezifische Rechtsgrundlagen für die Erhebung und Verarbeitung personenbezogener Daten im Strafverfahrensrecht zu schaffen sowie die Fahndung und das Recht der Akteneinsicht neu zu regeln. Dies ist von den Datenschutzbeauftragten im Hinblick auf die im Volkszählungsurteil enthaltenen Vorgaben begrüßt worden. Allerdings entspricht der Entwurf noch nicht den Anforderungen, die die Datenschutzbeauftragten im Jahre 1986 an eine Novellierung des Strafverfahrensrechts gestellt haben (vgl. 5. TB, 5.10.1, S. 80). Da ich an dieser Stelle nicht auf alle Einzelprobleme eingehen kann, die ich in einer umfangreichen Stellungnahme behandelt habe, beschränke ich meine Ausführungen auf die Problematik der besonderen Ermittlungsmethoden, die Übermittlung von Daten zu polizeilichen und geheimdienstlichen Zwecken und auf die Regelung der Datenverarbeitung:

3.10.1.1.1 Rasterfahndung und allgemeiner Fahndungsabgleich

Wie ich bereits zur Novellierung des Polizeirechts ausgeführt habe, halte ich die Rasterfahndung nur im Bereich der Strafverfolgung, und zwar zur Aufklärung bestimmter schwerwiegender Delikte, für zulässig. Es ist zu begrüßen, daß der StPO-Entwurf den Versuch unternimmt, den Einsatz der Rasterfahndung mit Hilfe eines Straftatenkatalogs zu beschränken. Allerdings halte ich diesen Katalog für zu weit. Für die Rasterfahndung ist charakteristisch, daß eine Vielzahl Unbeteiligter in die Ermittlungen einbezogen wird. Um dem Grundsatz der Verhältnismäßigkeit gerecht zu werden, muß der Straftatenkatalog deshalb stärker begrenzt werden.

In seiner neuesten Fassung sieht der Entwurf neben der Rasterfahndung einen allgemeinen Abgleich des polizeilichen Fahndungsbestandes mit „anderen personenbezogenen Daten" vor. Damit wird der routinemäßige Abgleich des Fahndungsbestandes mit allen Dateien bei anderen öffentlichen Stellen ermöglicht, soweit nicht besondere bundes- oder landesrechtliche Verwendungsregelungen entgegenstehen. Er unterliegt keinerlei weiteren Einschränkungen. Diese Vorschrift geht weit über den bislang praktizierten Datenabgleich mit Dateien der Einwohnermeldeämter, den ich ohnehin für unzulässig halte (vgl. oben 4.11.1.2.9), und mit Kfz-Halterdaten hinaus. Meines Erachtens bedarf der Abgleich von Fahndungsdaten mit den Dateien anderer Behörden einer bereichsspezifischen Ermächtigungsnorm in dem jeweiligen Fachgesetz, so wie sie bereits im Straßenverkehrsgesetz enthalten ist. Deshalb ist die vorgesehene Regelung zum allgemeinen Fahndungsabgleich in ihrer jetzigen Form nicht akzeptabel.

3.10.1.1.2 Besondere Erhebungsmethoden

Zu den besonderen Erhebungsmethoden zählt der StPO-Entwurf die polizeiliche Beobachtung, die Observation, den Einsatz technischer Mittel und den Einsatz verdeckter Ermittler. Es ist zu begrüßen, daß der Entwurf jede besondere Erhebungsmethode gesondert regelt. Allerdings sind bisher folgende datenschutzrechtliche Anforderungen dabei noch nicht berücksichtigt worden:

Das Verhältnis zwischen der Ermittlungsgeneralklausel und den Spezialvorschriften zu den besonderen Ermittlungsmethoden bedarf der Klarstellung. Es muß deutlich herausgestellt werden, daß die Ermittlungsgeneralklausel keine Eingriffe gestattet, die in ihrer Eingriffstiefe den besonders geregelten gleichkommen. Dies gilt vor allem im Hinblick auf den Einsatz von V-Leuten, auf den in Zukunft sicher nicht verzichtet werden soll, für den aber keine spezielle Regelung im Entwurf getroffen wird. Da die verdeckte Informationsbeschaffung durch V-Leute sehr tief in das Persönlichkeitsrecht der Betroffenen eingreift, müssen die Voraussetzungen ihres Einsatzes ebenfalls besonders geregelt werden.

Der Entwurf betont zu Recht, daß bei jeder einzelnen Ermittlungs- und Datenverarbeitungsmaßnahme der Grundsatz der Verhältnismäßigkeit zu beachten ist. Die Voraussetzungen für den Einsatz der einzelnen besonderen Methoden werden indessen nicht restriktiv genug geregelt. So können die polizeiliche Beobachtung, die Observation und der Einsatz technischer Mittel bereits angeordnet werden, wenn eine „Straftat mit erheblicher Bedeutung" begangen worden ist. Dieser Begriff ist nicht geeignet, die Befugnisse der Strafverfolgungsbehörden zur Datenerhebung normenklar zu begrenzen. Denn nach der Begründung können darunter alle Straftaten fallen, die den Rechtsfrieden empfindlich stören oder geeignet sind, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Diese Voraussetzungen können sogar bei Bagatelldelikten zutreffen. Der Begriff der Straftat mit erheblicher Bedeutung sollte deshalb durch einen Straftatenkatalog ersetzt werden.

Der Einsatz verdeckter Ermittler wird demgegenüber auf Straftaten aus bestimmten Kriminalitätsbereichen wie Betäubungsmittel- oder Waffenhandel und auf in bestimmter Weise begangene Delikte beschränkt. Damit wird zumindest der Versuch unternommen, den Bereich der organisierten Kriminalität abzudecken. Die gewählte Umschreibung reicht aber nicht aus, um den problematischen Einsatz verdeckter Ermittler auf das unbedingt erforderliche Maß zu begrenzen. Wünschenswert wäre eine präzisere Definition des Begriffes „organisierte Kriminalität". Der Einsatz verdeckter Ermittler sollte auf diesen Bereich sowie einige abschließend aufgezählte schwere Straftaten - etwa in Anlehnung an den Katalog in § 138 StGB - beschränkt werden.

Die Anordnung von Ermittlungs- und Fahndungsmethoden, die besonders stark in das Recht auf informationelle Selbstbestimmung eingreifen, ist dem Richter vorzubehalten. Selbst in Eilfällen darf der Richtervorbehalt nicht durch Entscheidungen von Polizeibeamten ersetzt werden. Auch die Eilkompetenz der Staatsanwaltschaft muß auf wenige Ausnahmefälle beschränkt werden. Beim Einsatz verdeckter Ermittler, der lange vorher geplant und vorbereitet werden muß, halte ich beispielsweise Eilkompetenzen weder für die Polizei noch für die Staatsanwaltschaft für erforderlich. Soweit die Staatsanwaltschaft in Eilfällen eine Anordnung trifft, dürfen die erlangten Daten nicht weiter verwendet werden, wenn die richterliche Bestätigung ausbleibt. Demgegenüber ist in dem Entwurf ein Verwertungsverbot nur dann vorgesehen, wenn das erkennende Gericht in einem späteren Prozeß feststellt, daß die Eilmaßnahme von vornherein rechtswidrig war. Dies reicht aber nicht aus, da die Daten nicht nur zur Aufklärung einer bestimmten Straftat, sondern auch für andere Zwecke - z.B. im Rahmen präventiver Maßnahmen, als Ansatz für neue Ermittlungen, zur Ermittlung des Aufenthalts von Tätern in anderen Strafverfahren etc. - verwendet werden dürfen.

Werden Daten unter Verstoß gegen die Regelungen zu den besonderen Erhebungsmethoden erlangt, so dürfen sie im Strafverfahren nicht verwendet werden.

Es ist zu begrüßen, daß eine Verwertung von Zufallsfunden nur im Rahmen des Katalogs von Straftaten zulässig ist, bei denen die jeweiligen Ermittlungsmethoden selbst angewandt werden dürfen. Unter dem Gesichtspunkt der Verhältnismäßigkeit ist es

aber darüber hinaus erforderlich, daß außerhalb des Katalogs die Verwertung nicht nur „zu Beweiszwecken", sondern auch für alle anderen Zwecke ausgeschlossen ist. Zufallserkenntnisse, die sozusagen als Nebenprodukt einer nur unter speziellen Voraussetzungen zulässigen Maßnahme von besonderer Eingriffsintensität erlangt werden, dürfen z.B. nicht als Ansatz für weitere Ermittlungen bei einem Bagatelldelikt genutzt werden, das u.U. sogar von einem anderen als demjenigen, gegen den sich die Maßnahme richtete, begangen worden ist.

Da die Datenerhebung mit verdeckten Mitteln besonders tief in das Persönlichkeitsrecht der Betroffenen eingreift, ist es umso wichtiger, bei ihrem Einsatz zwischen Beschuldigten bzw. Verdächtigen und „anderen Personen" deutlich zu unterscheiden. Nach meiner Auffassung ist der im Entwurf vorgesehene gezielte Einsatz verdeckter Mittel gegen Dritte, von denen man lediglich aufgrund bestimmter Tatsachen annimmt, daß sie mit einem Verdächtigen „in Verbindung stehen" oder eine solche Verbindung zu ihm herstellen werden, unverhältnismäßig. Hält man die gezielte Einbeziehung Dritter in Überwachungsmaßnahmen überhaupt für erforderlich, so sind diese jedenfalls auf das unbedingt notwendige Maß zu beschränken. Solche Maßnahmen dürfen deshalb nur zur Aufklärung bestimmter - im Gesetz aufzuführender - schwerer Straftaten zugelassen werden. Zu denken wäre an den Straftatenkatalog des § 138 StGB. Außerdem müssen Begriffe wie „Kontaktperson" und „Begleitperson" im Gesetz selbst definiert werden, um Art und Intensität der erforderlichen „Verbindung" zu einem Verdächtigen eindeutig festzulegen.

3.10.1.1.3 Nutzung der Daten für polizeiliche und geheimdienstliche Zwecke

Der Entwurf sieht vor, daß die Polizei personenbezogene Informationen, die sie in einem Strafverfahren gewonnen hat, auch zum Zwecke der Gefahrenabwehr nutzen darf. Eine solche Zweckänderung ist hinnehmbar, wenn im Gesetz klargestellt wird, daß es sich bei der „Gefahr für die öffentliche Sicherheit und Ordnung" um eine konkrete Gefahr handeln muß, daß z.B. eine bevorstehende Straftat verhindert werden soll. Dies wird meines Erachtens durch die jetzige Formulierung im Entwurf nicht sichergestellt.

Sind die Daten mit besonderen Mitteln erhoben worden, so dürfen sie nur zur Verhütung solcher Straftaten genutzt werden, zu deren Aufklärung sie ebenfalls hätten erhoben werden dürfen. Außerdem muß gewährleistet sein, daß das Polizeirecht vergleichbare Eingriffe gestattet. Dies ist erforderlich, um zu verhindern, daß die Polizei zur Gefahrenabwehr Daten aus Strafverfahren verwendet, die sie aufgrund eigener Befugnisse für diesen Zweck nicht erheben dürfte.

Auch die neu in den Entwurf eingefügte Regelung zur Nutzung von Daten aus Strafverfahren für geheimdienstliche Zwecke wird den Anforderungen an eine normenklare Begrenzung der Zweckänderung nicht gerecht. Statt auf die im Entwurf zum Bundesverfassungsschutzgesetz (BVerfSchG-E) und zum BND-Gesetz (BND-GE) enthaltenen Übermittlungsvorschriften zu verweisen, müßte der Entwurf selbst eine abschließende Regelung zur Datenweitergabe an die Dienste treffen. Dies gilt umso mehr, als die in Bezug genommenen Bestimmungen im BVerfSchG-E bzw. im BND-GE dem Zweckbindungsgebot nicht entsprechen. Zum einen fehlt es an einer präzisen Bestimmung der Aufgaben der Dienste, für deren Erfüllung eine Übermittlung zulässig sein soll. Deshalb ist es besonders wichtig, die in den Entwürfen vorgesehene Verpflichtung der Strafverfolgungsbehörden zur Weitergabe von Informationen an strenge Voraussetzungen zu binden, die den unterschiedlichen Aufgaben des Verfassungsschutzes Rechnung tragen. Zum anderen bleibt offen, welche Behörde die Erforderlichkeit der Übermittlung prüft. Da im BVerfSchG-E bzw. im BND-GE weitreichende Ausnahmen von der Begründungspflicht bei Anfragen der Dienste vorgesehen sind, entscheiden diese letztlich selbst darüber, welche Informationen aus Strafverfahren ihnen zu übermitteln sind.

Die vorgesehenen Übermittlungs- und Verwertungsbeschränkungen für solche Informationen, die mittels einer Rasterfahndung, der polizeilichen Beobachtung, der längerfristigen Observation, des Einsatzes technischer Mittel oder verdeckter Ermittler gewonnen worden sind, sind ein Schritt in die richtige Richtung. Diese Beschränkun-

gen müssen auch auf andere Erkenntnisse erstreckt werden, welche die Strafverfolgungsbehörden aufgrund von Befugnissen erlangt haben, die den Diensten selbst nicht eingeräumt sind (z.B. Hausdurchsuchungen, Telefonabhörmaßnahmen usw.).

Schließlich ist zu fordern, daß bei der Übermittlung von Informationen an die Geheimdienste nach Beschuldigten bzw. Verdächtigen und „anderen Personen" differenziert wird. Eine Weitergabe von Daten „anderer Personen" halte ich aus Gründen der Verhältnismäßigkeit allenfalls für Zwecke der Terrorismusbekämpfung und der Spionageabwehr, nicht aber im Bereich der Extremismusbeobachtung für zulässig.

3.10.1.1.4 Nutzung der Daten für „Zwecke künftiger Strafverfolgung"

Der Entwurf enthält bisher keine klare Regelung des Verhältnisses zwischen polizeilicher Datenverarbeitung und der geplanten Datenverarbeitung der Strafverfolgungsbehörden „für Zwecke künftiger Strafverfolgung". Nach der jetzigen Fassung soll sich die Verarbeitung zu präventiven Zwecken in Dateien der Staatsanwaltschaft nach den geplanten Regelungen in der StPO richten, während die Datenverarbeitung der Polizei in den Polizeigesetzen der Länder geregelt werden soll. Diese Konzeption würde zu einem Nebeneinander polizeilicher und staatsanwaltschaftlicher Datenverarbeitung zum gleichen Zweck, aber unter verschiedenen Voraussetzungen führen. Für den Betroffenen folgt daraus die mehrfache Speicherung desselben Sachverhaltes in verschiedenen Systemen, was weder mit dem Grundsatz der Erforderlichkeit noch mit dem Grundsatz der Verhältnismäßigkeit in Einklang steht. Deshalb muß die Datenverarbeitung im Bereich der Strafverfolgung einheitlich und abschließend in der StPO geregelt werden. Dabei müssen die vorhandenen polizeilichen und die geplanten staatsanwaltschaftlichen Informationssysteme so strukturiert werden, daß es nicht zu unzulässigen Doppelspeicherungen kommt.

Zu der geplanten Regelung im Entwurf ist im einzelnen folgendes anzumerken:

Es leuchtet ein, daß Polizei und Staatsanwaltschaft über jeweils eigene Aktennachweissysteme verfügen müssen. Auf den Aufbau staatsanwaltschaftlicher Systeme, die über reine Nachweissysteme hinausgehen, muß meines Erachtens aber im Hinblick auf die bereits vorhandenen polizeilichen Informationssysteme verzichtet werden, um unzulässige Doppelspeicherungen zu vermeiden. Stattdessen sollten die polizeilichen Systeme dem Zugriff der Staatsanwaltschaft unterliegen und ihrer Kontrolle unterstellt werden. Auf diese Weise könnte die Staatsanwaltschaft ihre gesetzlich vorgesehene Stellung als „Herrin des Ermittlungsverfahrens" wieder einnehmen, die sie in bezug auf die polizeiliche Datenverarbeitung in der Praxis längst verloren hat.

Die Voraussetzungen für eine Speicherung personenbezogener Daten für „Zwecke künftiger Strafverfolgung" müssen restriktiver und klarer gefaßt werden. Die Übernahme der in Strafverfahren erlangten Informationen zu präventiven Zwecken ist nur zulässig, wenn aufgrund einer nachvollziehbaren Prognose davon auszugehen ist, daß der Täter weitere schwerwiegende Straftaten begehen wird. Die Möglichkeit, daß sich jemand künftig wegen eines Bagatelldelikts strafbar machen könnte, rechtfertigt jedenfalls nicht eine jahrelange Speicherung auf Vorrat. Außerdem sollte die Prognoseentscheidung aktenkundig gemacht werden, um sowohl dem Sachbearbeiter selbst als auch externen Kontrollinstanzen eine bessere Überprüfung zu ermöglichen. Weiterhin ist im Gesetz selbst festzulegen, welche Informationen zur Person der Betroffenen gespeichert werden dürfen. Auf Angaben, die die Betroffenen stigmatisieren oder diskriminieren, muß verzichtet werden.

Darüber hinaus muß klargestellt werden, daß eine Weiterspeicherung auf jeden Fall unzulässig ist, wenn der Angeklagte wegen erwiesener Unschuld freigesprochen worden ist. Aber auch die Übernahme von Daten aus Strafverfahren, die mangels Tatverdachts oder wegen geringer Schuld des Betroffenen eingestellt oder in denen die Anklageerhebung mangels öffentlichen Interesses an der Strafverfolgung abgelehnt worden ist, ist regelmäßig auszuschließen. Soll die Speicherung in diesen Fällen ausnahmsweise aufrechterhalten werden, so ist zumindest das Vorliegen eines erhebli-

chen Restverdachtes zu fordern, der in seiner Qualität dem Anfangsverdacht gemäß § 152 StPO gleichkommt. An die Prognoseentscheidung sind besonders strenge Maßstäbe anzulegen.

Auch die beabsichtigte Speicherung der Daten von Personen, die Zeugen oder Opfer künftiger Straftaten werden könnten, sowie von Kontakt- und Begleitpersonen, Hinweisgebern und sonstigen Auskunftspersonen ist viel zu weitreichend. Sie soll zulässig sein, „soweit dies für Zwecke künftiger Strafverfolgung wegen einer Straftat mit erheblicher Bedeutung unerläßlich ist". Meines Erachtens wird diese Beschränkung in der Praxis nicht geeignet sein, die Speicherung „anderer Personen" wirksam zu begrenzen. Deshalb sollte die Speicherung von Daten Dritter nur im Zusammenhang mit bestimmten schwerwiegenden Straftaten zugelassen werden, die in einem abschließenden Katalog aufzuführen sind. Zu denken wäre wiederum an den Katalog des § 138 StGB. Außerdem ist die vorgesehene Speicherungsdauer von 3 Jahren zu lang; sie sollte auf 1 Jahr begrenzt werden.

3.10.1.1.5 Aufbau neuer Dateien und eines zentralen Verfahrensregisters

Die Vorschriften zur Datenerhebung und -speicherung führen im wesentlichen zu einer Festschreibung dessen, was heute bereits von der Polizei im Bereich der sog. vorbeugenden Straftatenbekämpfung praktiziert wird. Statt diese Praxis im Interesse des Persönlichkeitsschutzes der Bürger spürbar einzuschränken und auf das unbedingt erforderliche Maß zu reduzieren, vollzieht der Gesetzgeber wie im Polizeirecht größtenteils die bisherige Entwicklung nach. Darüber hinaus schafft der Entwurf Rechtsgrundlagen für neue Datenverarbeitungssysteme, die über die bisherigen weit hinausgehen:

Polizei, Staatsanwaltschaft, Gerichte und Vollstreckungsbehörden erhalten generalklauselartig die Befugnis, personenbezogene Informationen automatisiert „für Zwecke des Strafverfahrens" zu verarbeiten. Nach der Begründung zum Entwurf bezieht sich diese Befugnis jeweils auf ein bestimmtes Strafverfahren. Bisher gibt es im Zuge einzelner Ermittlungsverfahren Spurendokumentationssysteme bei der Polizei, auf die nur bestimmte Ermittlungsbeamte Zugriff haben. Nunmehr sollen diese umfangreichen Datensammlungen, die eine Fülle noch unbewerteter Informationen auch über Nichtbeschuldigte und Nichtverdächtige enthalten, von Staatsanwaltschaft, Gerichten und Vollstreckungsbehörden gleichermaßen genutzt werden können. Die genannten Stellen können hierzu gemeinsame Dateien - etwa auf regionaler Ebene oder landesweit - einrichten. Dies ist um so bedenklicher, als nicht zwischen Beschuldigten bzw. Verdächtigen und „anderen Personen" differenziert wird. Die Daten sämtlicher Betroffener dürfen bis zum Ende des Strafverfahrens einschließlich des Revisionsverfahrens gespeichert werden. Hierbei besteht die Gefahr, daß die im Entwurf vorgesehenen Löschungsfristen, insbesondere die 3-jährige Speicherungsdauer bei „anderen Personen", weit überschritten werden. Außerdem stehen die Daten während dieser Zeit auch noch für andere Strafverfahren und Gnadensachen zur Verfügung. Eine so weitreichende gemeinsame Datenverarbeitung verschiedener Behörden und Gerichte ist aus meiner Sicht weder erforderlich noch verhältnismäßig.

Neben der Errichtung gemeinsamer Dateien sieht der Entwurf außerdem die Möglichkeit vor, on-line-Verbindungen zwischen den genannten Behörden und Gerichten einzurichten, wenn dies „wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist". Mir leuchtet bisher nicht ein, warum neben gemeinsam betriebenen Dateien zusätzlich noch automatisierte Abrufverfahren für erforderlich gehalten werden. Hierüber gibt auch die Begründung zum Entwurf keinerlei Aufschluß.

Weiterhin ist beabsichtigt, ein bundesweites staatsanwaltschaftliches Verfahrensregister einzurichten, das beim Bundeszentralregister in Berlin geführt werden soll. In Anknüpfung an meine früheren Ausführungen zu diesem staatsanwaltschaftlichen Informationssystem - SISY - (vgl. 5. TB, 5.10.3, S. 88; 6. TB, 4.13.3, S. 96) bleibt festzuhalten, daß der Bedarf für ein solches System neben dem bestehenden Bundeszentralregister und den bundesweiten polizeilichen Informationssystemen nach wie vor nicht

überzeugend dargelegt ist. Bereits jetzt werden alle strafgerichtlichen Verurteilungen und sonstige Entscheidungen von Verwaltungsbehörden und Gerichten in das Bundeszentralregister eingetragen. Zu präventiven Zwecken werden sie in die polizeilichen Informationssysteme übernommen. Daneben verfügen die einzelnen Staatsanwaltschaften über Zentrale Namenskarteien, die zum Teil bereits auf regionaler Ebene miteinander verbunden sind. Ein durchschlagender Grund, weshalb darüber hinaus die Daten, die sich auf eine Tat mit erheblicher oder überörtlicher Bedeutung beziehen, in einem zentralen Register zusammengetragen werden sollen, ist mir nicht ersichtlich. Hierbei ist vor allem zu berücksichtigen, daß es sich um ein sehr viel umfangreicheres Register als das Bundeszentralregister handeln wird, wenn man bedenkt, daß nur ein Bruchteil aller Ermittlungsverfahren zu einer rechtskräftigen Verurteilung führt. Man kann außerdem davon ausgehen, daß die Staatsanwaltschaft bereits zu Beginn eines Ermittlungsverfahrens ein derartiges Verfahrensregister abfragen würde. Dann stellt sich die Frage, ob die ermittelnden Stellen sich noch von Gesichtspunkten der Unvoreingenommenheit und Objektivität leiten lassen würden, wenn sie mit der Summe aller, auch der eingestellten Ermittlungsverfahren konfrontiert werden würden. Im übrigen gehe ich davon aus, daß der Betroffene von sich aus dazu beitragen wird, daß Doppelverfahren vermieden und Sammelverfahren gebildet werden können; insofern bedarf es entgegen der gegebenen Begründung keines zentralen Registers.

Besonders bedenklich ist außerdem, daß neben den Staatsanwaltschaften auch Strafgerichte, Vollstreckungsbehörden und Gnadenbehörden Auskünfte aus dem Register erhalten sollen. Zu diesem Zweck können obendrein on-line-Verbindungen eingerichtet werden. Damit wird den genannten Stellen ein umfangreicher Bestand sensibler Daten bundesweit zur Verfügung gestellt, der weit über das für ihre jeweilige Aufgabenerfüllung erforderliche Maß hinausgeht.

Schließlich ist die geplante Regelung zur Speicherungsdauer nicht akzeptabel. Endet ein Verfahren mit einer Verurteilung, so werden die Daten im zentralen Verfahrensregister gelöscht, weil sie dann in das Bundeszentralregister eingestellt werden. In allen übrigen Fällen, d.h. wenn der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens abgelehnt oder das Verfahren nicht nur vorläufig eingestellt worden ist, sollen die Daten noch zwei Jahre nach der Erledigung des Verfahrens im Zugriff der Behörden verbleiben. Völlig unannehmbar ist, daß in diesen Fällen nicht einmal danach differenziert werden soll, ob der Betroffene wegen erwiesener Unschuld freigesprochen worden oder ob noch ein erheblicher Restverdacht bestehen geblieben ist.

Außerdem steht diese pauschale Regelung der Speicherungsdauer meines Erachtens mit dem erklärten Zweck von SISY, verschiedene laufende Verfahren frühzeitig zusammenzufassen, das Verfahren auf wesentliche Tatteile zu beschränken und Vollstrekkungsmaßnahmen besser zu koordinieren, nicht im Einklang. Auch der Begründung zum Entwurf ist nicht zu entnehmen, warum die Speicherung von Informationen aus abgeschlossenen Ermittlungsverfahren für 2 weitere Jahre für erforderlich gehalten wird.

Insgesamt halte ich das Projekt SISY in seiner vorliegenden Ausprägung für einen gravierenden, unverhältnismäßigen Eingriff in die schutzwürdigen Belange der Betroffenen. Deshalb sollte auf den Aufbau eines zentralen Verfahrensregisters verzichtet werden.

3.10.1.2 Bewertung des Novellierungsentwurfs

Die Vorschriften zur Datenverarbeitung - aus datenschutzrechtlicher Sicht das Kernstück des Entwurfs - führen im Ergebnis nicht nur zu einer Festschreibung der bisherigen Praxis, sondern eröffnen einen weiten Spielraum für den Aufbau und die gemeinsame Nutzung künftiger Dateien. Für die Zukunft wird ein Ausmaß an Datenverarbeitung im Strafverfahren ermöglicht, das heute nicht einmal ansatzweise vorhanden ist. Begründet werden diese weitreichenden Befugnisse lediglich mit „Bedürfnissen der Praxis" und der technischen Entwicklung im Bereich der Informationsverarbeitung. Im

Hinblick auf zukünftige Bedürfnisse schneidert der Gesetzgeber der Praxis sozusagen vorsorglich weite Hosen, in die sie - dem technischen Fortschritt entsprechend - hineinwachsen kann.

Diesen überaus großzügigen Regelungen im Bereich der Datenverarbeitung stehen auf der anderen Seite erhebliche Regelungsdefizite gegenüber.

Neue technologische Entwicklungen, die heute bereits für das Strafverfahren nutzbar gemacht werden, werden nicht in die gesetzliche Neuregelung einbezogen. So erhalten z.B. erkennungsdienstliche Maßnahmen durch die Digitalisierung von Lichtbildern und die Entwicklung von Bilderkennungstechniken eine neue Eingriffsintensität. Diese in der Entwicklung und Erprobung befindlichen Techniken erlauben den Aufbau von Bilddatenbanken, die den Strafverfolgungsbehörden bisher ungeahnte Zugriffs- und Auswertungsmöglichkeiten eröffnen. Das gleiche gilt für die elektronische Auswertung von Fingerabdrücken, die bereits praktiziert wird. Hinzu kommt, daß die Daten von erkennungsdienstlich behandelten Personen bereits seit langem in das INPOL-System eingestellt werden und damit bundesweit dem Zugriff der Polizei unterliegen. Der Entwurf versäumt es, angesichts dieser Entwicklung engere Voraussetzungen für die erkennungsdienstlich Behandlung festzusetzen.

In diesem Zusammenhang ist außerdem eine präzise gesetzliche Regelung des Einsatzes der Genomanalyse im Strafverfahren zu fordern. Denn die vorhandenen Vorschriften der §§ 81a (Körperliche Untersuchung des Beschuldigten) und 81b (Erkennungsdienstliche Behandlung) StPO stellen keine geeigneten Rechtsgrundlagen für einen so weitreichenden Eingriff in das Persönlichkeitsrecht des Betroffenen dar (vgl. unten 3.11.1.1, S. 100). Regelungsbedürftig ist außerdem die Erhebung persönlicher Daten von Angeklagten und Zeugen in öffentlichen Verhandlungen, um deren Persönlichkeitsschutz besser zu wahren. Diese Bereiche müssen in die Novellierung einbezogen werden.

3.10.2 Kontrollkompetenz des Datenschutzbeauftragten bei den Gerichten

Im Jahre 1988 hatte ich die Datenverarbeitung beim Verwaltungsgericht überprüft und erhebliche Mängel festgestellt (7. TB, 4.13.2.2, S. 97). In seiner Stellungnahme zu dem Prüfbericht hatte das Verwaltungsgericht Zweifel an der Kontrollkompetenz des Datenschutzbeauftragten geäußert, weil es in § 20 Abs. 1 HmbDSG heißt, daß die Gerichte der Datenschutzkontrolle nur soweit unterliegen, wie sie in Verwaltungsangelegenheiten tätig werden. In dem Anschreiben, mit dem die Justizbehörde mir dieses Schreiben zugeleitet hat, hat sie mir ausdrücklich bestätigt, daß sie die Zweifel des Verwaltungsgerichts nicht teile und der Auffassung sei, daß die in den Geschäftsstellen der Gerichte eingesetzten IuK-Verfahren der Überwachung des Hamburgischen Datenschutzbeauftragten gem. § 20 Abs. 1 HmbDSG unterliegen. Dementsprechend findet sich auch in der Stellungnahme des Senats zu meinem 7. Tätigkeitsbericht (Bürgerschafts-Drs. 13/3838, S. 9) vom 6. Juni 1988 keine Andeutung, daß meine Kontrollkompetenz in Zweifel stehen könnte. Statt dessen geht der Senat auf meine inhaltlichen Kritikpunkte ein.

Gleichwohl hat mir die Justizbehörde mit Schreiben vom 18. April 1989 - also etwa 1 1/2 Monate vor Veröffentlichung der Stellungnahme des Senats - mitgeteilt, daß nunmehr in der Justizbehörde die Auffassung vorherrsche, „daß das vom Hamburgischen Datenschutzbeauftragten untersuchte DV-Verfahren beim Verwaltungsgericht der richterlichen Tätigkeit im Verwaltungsgericht diente und kein Raum für eine Datenschutzkontrolle bestand oder besteht". Später hat die Justizbehörde ihren nunmehrigen Standpunkt dahin konkretisiert, daß die Geschäftsstellentätigkeit lediglich „Hilfstätigkeit" zur richterlichen Arbeit darstelle und deshalb an der richterlichen Unabhängigkeit teilnehme.

Dieses Verfahren wirft zunächst die Frage auf, ob Äußerungen des Senats gegenüber der Bürgerschaft intern unter dem Vorbehalt einer anderweitigen Auffassung der zuständigen Fachbehörde stehen. Dies würde meine Arbeit erheblich erschweren.

In der Sache halte ich die Auffassung der Justizbehörde für falsch. Die Datenschutzgesetze wollen im öffentlichen Bereich eine umfassende Datenschutzkontrolle ermöglichen. Kontrollfreie Räume soll es nur dort geben, wo höherrangiges Recht dies erforderlich macht. Dies ergibt sich eindeutig aus § 2 Abs. 1 HmbDSG, auf den § 20 Abs. 1 S. 1 HmbDSG Bezug nimmt. Danach soll eine Datenschutzkontrolle bei sämtlichen öffentlichen Stellen, und zwar bei Behörden und sonstigen öffentlichen Stellen erfolgen. Es gibt in der Entstehungsgeschichte der Datenschutzgesetze keinen Anhaltspunkt dafür, daß für die Gerichte eine Sonderregelung, die über das verfassungsrechtlich Gebotene hinausgeht, getroffen werden sollte.

Da mit dem Vorbehalt für die Gerichte in § 20 Abs. 1 HmbDSG nur die verfassungsrechtlich gewährleistete Unabhängigkeit der Rechtsprechung gesichert werden soll - insoweit besteht mit der Justizbehörde Einigkeit -, ist lediglich zu prüfen, wie weit diese reicht. Dabei ist anerkannt, daß sich die durch Art. 92, 97 GG garantierte Unabhängigkeit der Gerichte ausschließlich auf die Gerichte in ihrer Eigenschaft als Spruchkörper bezieht und nicht die innere Organisation der Gerichte einbezieht. Daraus ergibt sich zwingend, daß verfassungsrechtliche Garantien, die die Kontrolle der Gerichte durch den Datenschutzbeauftragten außerhalb der richterlichen Tätigkeit (einschl. der autonomen Selbstverwaltung der Gerichte) ausschließen, nicht vorhanden sind. Dies wird im übrigen durch eine Stellungnahme des Bundesjustizministers gegenüber der Justizbehörde ausdrücklich bestätigt.

Es bedarf wohl keiner besonderen Ausführungen, daß die Geschäftsstellen nicht zu den Spruchkörpern der Gerichte gehören. Ich gehe deshalb weiter von meiner Kontrollkompetenz gegenüber den Tätigkeiten der Gerichte aus, die nicht von der durch das Grundgesetz gewährleisteten richterlichen Unabhängigkeit erfaßt werden, hoffe aber, daß ich bei einem für Anfang des nächsten Jahres verabredeten Versuch einer Verständigung die Justizbehörde von meinem Standpunkt, den sie ja früher auch geteilt hat, überzeugen kann.

3.10.3 Einsatz von Personalcomputern am Richterarbeitsplatz

Die Automation der Justiz wird auch vor dem Arbeitsplatz der Richter/-innen nicht Halt machen - sie hat von ihm schon teilweise Besitz ergriffen. Dies wirft eine Reihe schwieriger auch datenschutzrechtlicher Fragen auf. Wenn nämlich die Organisation der Datenverarbeitung am Richterarbeitsplatz der richterlichen Unabhängigkeit unterliegt, sie also frei von Weisungen und Kontrollen durchgeführt werden kann, trifft die Richter/-innen die gesamte Verantwortung des Betreibers, Anwenders und Benutzers des eingesetzten Systems, die sonst üblicherweise auf verschiedene Stellen oder Personen verteilt ist. Dies bedeutet, daß sie nicht nur für die Zulässigkeit, sondern auch für die Ordnungsmäßigkeit der Datenverarbeitung sowie für die Realisierung und Einhaltung der technischen und organisatorischen Maßnahmen (§ 8 HmbDSG nebst Anlage) zur Datensicherung verantwortlich sind. Schließlich haben sie die Rechte der Betroffenen (§ 6 Abs. 1 Nr. 2-8 HmbDSG) zu wahren. Dies gilt unabhängig davon, ob das eingesetzte ADV-System von der Justizverwaltung zur Verfügung gestellt oder privat angeschafft wurde, im Dienstzimmer oder im häuslichen Arbeitszimmer steht.

Die damit verbundenen Probleme sind den meisten Richter/-innen fremd. Ich habe deshalb im Rahmen meiner Beratungstätigkeit den Gerichtspräsidenten und den Richterräten ein Hinweispapier mit der Bitte um Verbreitung übersandt, in dem ich auf einige datenschutzrechtliche Grundprobleme aufmerksam gemacht, insbesondere aber umfangreiche Hinweise zur Gewährleistung der notwendigen Datensicherung gegeben habe. Das Papier soll den Anwendern helfen, sich der bestehenden Risiken und Verantwortlichkeiten bewußt zu werden, um entsprechende Vorkehrungen treffen zu können.

Die Beteiligten an gerichtlichen Verfahren treten den Richtern und Richterinnen im allgemeinen mit Vertrauen in deren Integrität und Verschwiegenheit gegenüber. Es liegt auch im Interesse der Justiz, dieses Vertrauen zu bewahren, denn die Furcht vor einem leichtfertigen Umgang der Gerichte mit den ihnen anvertrauten Informationen kann zu

einer erheblichen Einschränkung der Bereitschaft führen, wahrheitsgemäß am Prozeßgeschehen mitzuwirken. Deshalb dürfen bei der Einführung automatisierter Verfahren vordergründige Effizienzgesichtspunkte nicht die entscheidende Rolle spielen. Es obliegt den Richtern und Richterinnen, sich der eigenen Verantwortung bewußt zu sein, von den Gerichts- und Justizverwaltungen Beratungen und Haushaltsmittel einzufordern, so daß das Grundrecht auf informationelle Selbstbestimmung auch in der Justiz wirksam geschützt wird. Von ihr können es die Betroffenen zuerst erwarten.

3.10.4 Erstellung eines privaten zentralen Handelsregisters

Im letzten Tätigkeitsbericht (4.13.4, S. 104) hatte ich von der Absicht eines Wirtschaftsinformationsdienstes berichtet, sämtliche Handelsregister in der Bundesrepublik auf Mikrofilm abzulichten, durch Einspeisung der Eintragsveröffentlichungen im Bundesanzeiger ständig zu aktualisieren und im Wege der Erteilung von Auskünften und Informationen unter Einsatz moderner Techniken kommerziell zu verwerten.

Dieses Vorhaben habe ich nicht für zulässig gehalten, weil die Ablichtung des gesamten Registerinhalts zur Gewinnung eines vermarktbaren Produkts begrifflich nicht mehr als „Einsicht" im Sinne von § 9 Abs. 1 HGB angesehen werden könne. Außerdem habe der Gesetzgeber in § 8 HGB zum Ausdruck gebracht, daß das Handelsregister dezentral von den Gerichten geführt werden soll. Die Errichtung eines zentralen privaten Nebenhandelsregisters entspräche deshalb auch nicht dem Willen des Gesetzgebers.

Nunmehr hat der Bundesgerichtshof in einem Beschluß vom 12. Juli 1989 (IV a ARZ (VZ) 9/88) beide Argumentationslinien ausdrücklich bestätigt und damit den Antrag des Unternehmens endgültig abgelehnt. Ergänzend hat der Bundesgerichtshof darauf hingewiesen, daß die vollständige Mikroverfilmung des Handelsregisters auch nicht von Art. 3 Abs. 3 der Publizitäts-Richtlinie des Rates der Europäischen Gemeinschaft (Amtsblatt der Europäischen Gemeinschaft vom 14. März 1968 Nr. L 65-8) gedeckt sei, nach der vollständige oder auszugsweise Abschriften der in einem Handels- oder Gesellschaftsregister verzeichneten oder hinterlegten Urkunden oder Angaben auf schriftliches Verlangen zuzusenden sind.

3.10.5 Gerichtsvollzieher

In immer stärkerem Maße wird auch die Arbeit der Gerichtsvollzieher durch den Einsatz automatisierter Datenverarbeitung unterstützt. Dies wurde schon 1986 durch eine Allgemeine Verfügung der Justizbehörde (AV Nr. 3/1986) zugelassen. Aus Anlaß der Änderung dieser Verfügung hatte ich mich 1988 grundsätzlich mit dem Einsatz von ADV-Technik im Bürobetrieb der Gerichtsvollzieher auseinandergesetzt und dabei erhebliche Regelungsdefizite festgestellt. So fehlten vor allem hinreichende Bestimmungen über Datensicherungsmaßnahmen. Dazu hatte ich eine Reihe von Vorschlägen unterbreitet (7. TB, 4.13.5, S. 105). Ende Oktober des Berichtsjahres hat die Justizbehörde nunmehr einen Entwurf für eine neue Allgemeine Verfügung vorgelegt, in der ein Teil meiner Vorschläge berücksichtigt wurden. Über weitere - aus meiner Sicht offene - Punkte wird noch diskutiert.

Einer dieser Punkte ist die Regelung der Datenschutzkontrolle. Soweit nämlich die Büros der Gerichtsvollzieher in ihren privaten Wohnungen untergebracht sind, könnte es im Hinblick auf § 20 Abs. 4 Satz 1 Ziff. 2 HmbDSG zu bisher nicht bedachten Problemen kommen. Ich hatte deshalb vorgeschlagen, eine nach der Allgemeinen Verfügung erforderliche Genehmigung durch den Amtsgerichtspräsidenten mit der Bedingung zu versehen, daß sich die betroffenen Gerichtsvollzieher ausdrücklich und schriftlich einer datenschutzrechtlichen Kontrolle unterwerfen. Für mich völlig überraschend vertrat die Justizbehörde nunmehr die Auffassung, die Gerichtsvollzieher unterlägen überhaupt nicht der Datenschutzkontrolle, weil sie „zu den Gerichten" gehörten. Ich halte diese Auffassung für unvereinbar mit den Bestimmungen des Hamburgischen Datenschutzgesetzes. Nach meiner Auffassung, die ich auch schon früher geäußert habe, handelt es sich bei den Gerichtsvollziehern um „sonstige öffentliche Stellen" i.S.v. § 2 Abs. 1

HmbDSG, die der uneingeschränkten Kontrolle unterliegen. Dementsprechend habe ich 1985 und 1986 aus Anlaß von Eingaben die Datenverarbeitung von einzelnen Gerichtsvollziehern kontrolliert, ohne daß meine Kontrollkompetenz im geringsten bezweifelt worden wäre. Ich habe deshalb die Justizbehörde aufgefordert, ihren Standpunkt zu überprüfen. Bei Redaktionsschluß lag mir eine Antwort noch nicht vor.

3.10.6 Mitteilungspraxis nach der MiStra

Anläßlich einer Eingabe, bei der es um die vorzeitige Unterrichtung der Schulbehörde von einem Ermittlungsverfahren gegen einen Lehrer ging, habe ich die Justizbehörde darauf hingewiesen, daß die Mitteilungspraxis der Staatsanwaltschaft aus folgenden Gründen kritisch überprüft werden muß:

In meinen Tätigkeitsberichten habe ich wiederholt die Problematik staatsanwaltschaftlicher Mitteilungen an andere öffentliche und private Stellen auf der Grundlage der Anordnung über Mitteilungen in Strafsachen (MiStra) dargestellt (vgl. 1. TB, 6.8.1, S. 46; 2. TB, 3.13.1, S. 94; 4. TB, 4.11.2, S. 90; zuletzt 6. TB, 4.13.1, S. 95). Eine gesetzliche Grundlage für diese Mitteilungen fehlt, so daß sich die Staatsanwaltschaft bzw. die Strafgerichte z.Zt. nur auf die Übergangsrechtsprechung des Bundesverfassungsgerichts stützen können. Das Bundesverfassungsgericht hat in einer Entscheidung vom 14. Juli 1988 - 1 BvR 537/81 - seine frühere Rechtsprechung zum sog. Übergangsbonus mit der Feststellung fortgesetzt, daß während der Übergangsfrist die bisherige Rechtspraxis nicht ohne weiteres so weiterbestehen dürfe, als sei sie unbedenklich. Vielmehr „reduzieren sich die Befugnisse... zu Eingriffen in verfassungsrechtlich geschützte Positionen auf das, was für die geordnete Weiterführung eines funktionsfähigen Betriebs unverzichtbar ist". Unter Heranziehung dieses Maßstabes muß genau überprüft werden, welche Mitteilungen unter Beachtung der schutzwürdigen Belange des Betroffenen als „unverzichtbar" angesehen werden können.

Bereits vor Jahren haben sich die Justizverwaltungen des Bundes und der Länder darauf verständigt, die erforderlichen Rechtsgrundlagen in einem sog. Justizmitteilungsgesetz zu schaffen. Als Übergangslösung bis zur Verabschiedung des neuen Gesetzes haben sie eine leicht veränderte Fassung der MiStra mit Wirkung vom 1.4.1985 in Kraft gesetzt. Dabei sind wesentliche Grundsätze, die die Datenschutzbeauftragten des Bundes und der Länder bereits im Jahre 1983 im Hinblick auf eine Neuregelung der Mitteilungspflichten aufgestellt haben, unberücksichtigt geblieben. Ich habe diese Lösung damals auf der Grundlage akzeptiert, daß sie nur für eine relativ kurze Übergangsfrist bis zum Erlaß des Justizmitteilungsgesetzes gelten würde. In der Erwartung, daß dieses Gesetz noch in der 1987 abgelaufenen Wahlperiode des Bundestages verabschiedet werden würde, erschien es mir vertretbar, an das Kriterium der „Unerläßlichkeit" bzw. „Unverzichtbarkeit" keinen allzu strengen Maßstab anzulegen. Seitdem sind mehr als vier Jahre vergangen, ohne daß das Bundesjustizministerium über einen - inzwischen wieder verworfenen - Referentenentwurf hinausgelangt wäre. Damit ist die Grundlage, auf der die Datenschutzbeauftragten die bisherige Mitteilungspraxis hingenommen haben, längst entfallen.

Angesichts dieser Situation kann sich die Staatsanwaltschaft nicht wie bisher auf die verfassungsrechtlich bedenklichen Bestimmungen der MiStra stützen und ihre Mitteilungspraxis ohne Einschränkung fortführen. Diese muß vielmehr während der Übergangsfrist bis zum Inkrafttreten eines Justizmitteilungsgesetzes erheblich reduziert werden. Dabei sind folgende Grundsätze zu berücksichtigen:

Der Erforderlichkeitsgrundsatz gebietet es, daß Mitteilungen nur erfolgen dürfen, wenn sie für den Empfänger entscheidungserheblich sind. Dabei ist darauf abzustellen, zu welchem Zweck eine Mitteilung gemacht werden soll und ob der Empfänger nach dem von ihm anzuwendenden Recht voraussichtlich Konsequenzen aus der Mitteilung ziehen, etwa eine Disziplinarmaßnahme gegen einen Beamten treffen wird.

Der Inhalt der Mitteilungen muß sich auf das im Einzelfall erforderliche Maß beschränken. Im Regelfall genügt die Mitteilung der Tatsache einer im Strafverfahren ergange-

nen Entscheidung unter Angabe der Straftat. Die Übersendung des staatsanwaltschaftlichen Ermittlungsergebnisses oder der Urteilsgründe ist demgemäß unter besonderer Beachtung der schutzwürdigen Belange des Betroffenen nur in Ausnahmefällen zulässig.

Um unnötige Nachteile für den Betroffenen zu vermeiden, dürfen die Mitteilungen grundsätzlich erst nach dem rechtskräftigen Abschluß des Strafverfahrens erfolgen. Erst dann läßt sich ein strafrechtlich relevanter Sachverhalt abschließend beurteilen. Im Disziplinarrecht findet dies seinen Niederschlag beispielsweise darin, daß ein Disziplinarverfahren grundsätzlich bis zur Beendigung des wegen desselben Sachverhalts anhängigen Strafverfahrens ausgesetzt werden muß, und darin, daß die tatsächlichen Feststellungen, auf welchen das strafgerichtliche Urteil beruht, für die Entscheidung im Disziplinarverfahren bindend sind.

Eine Mitteilung zu einem früheren Zeitpunkt kann nur ausnahmsweise erfolgen, wenn - wegen der Bedeutung des möglicherweise verletzten Rechtsgutes - Grund zu der Annahme besteht, daß von der zu benachrichtigenden Behörde vorzeitige Maßnahmen zu veranlassen sind. Aber selbst dann dürfen Mitteilungen grundsätzlich erst zum Zeitpunkt der Erhebung der öffentlichen Klage gemacht werden, um sicherzustellen, daß wenigstens die Staatsanwaltschaft einen hinreichenden Tatverdacht bejaht. Hiervon kann meines Erachtens nur abgewichen werden, wenn aufgrund besonderer Umstände des Einzelfalles anzunehmen ist, daß die Behörde sofortige Maßnahmen gegen den Betroffenen einleiten muß.

Mitteilungen sollten, um eine sachgerechte Abwägung der Interessen im Einzelfall sicherzustellen, grundsätzlich vom Staatsanwalt oder vom Richter veranlaßt werden. Ausnahmen können allenfalls zugelassen werden, wenn Anlaß, Inhalt und Zeitpunkt der Mitteilungen abschließend und eindeutig festgelegt sind.

Damit der Bürger weiß, wer was wann und bei welcher Gelegenheit über ihn weiß, muß er grundsätzlich von Tatsache und Inhalt einer Mitteilung unterrichtet werden. Von einer Benachrichtigung darf nur ausnahmsweise abgesehen werden, wenn ansonsten der Zweck des Strafverfahrens gefährdet wäre oder in der Person des Betroffenen besondere Gründe vorliegen, die einer Unterrichtung entgegenstehen.

Mit Ablauf der jetzigen Legislaturperiode des Bundestags wird sich die Problematik der staatsanwaltschaftlichen Mitteilungspraxis noch verschärfen. So hat beispielsweise das OLG Frankfurt in einem Urteil zur Führung der zentralen Namenskartei bei der Staatsanwaltschaft ausgeführt, daß die Übergangsfrist mit dem Ende der laufenden Legislaturperiode, also Ende 1990, auslaufe. Nach den eigenen Erklärungen des BMJ kann bis dahin mit der Verabschiedung eines Justizmitteilungsgesetzes nicht mehr gerechnet werden. Es ist nicht ersichtlich, wie eine Fortsetzung der Mitteilungspraxis der Staatsanwaltschaft von 1991 an gerechtfertigt werden könnte.

3.10.7 Auskünfte aus der Zentralkartei der Staatsanwaltschaft

Die Eingabe eines Rechtsanwaltes gab mir Veranlassung, mit der Staatsanwaltschaft erneut die Frage der Auskünfte aus der Zentralkartei zu erörtern (vgl. dazu 3. TB, 3.11.1, S. 92). Der Eingabe lag folgender Sachverhalt zugrunde: In einer Hauptverhandlung wurde dem Mandanten des Anwaltes vom Sitzungsvertreter der Staatsanwaltschaft ein früheres Ermittlungsverfahren wegen Diebstahls vorgehalten. Der Sitzungsvertreter bezog sich dabei auf einen schriftlichen Auszug aus der Zentralkartei, der sich bei seiner Handakte befand. Diese kann weder vom Gericht noch von der Verteidigung eingesehen werden. Der Strafregisterauszug, der sich in der dem Gericht vorliegenden Verfahrensakte befand, wies demgegenüber keine entsprechende Eintragung auf. Die Eintragung in der Handakte war, wie sich später herausstellte, falsch; gegen den Angeklagten war nicht wegen Diebstahls, sondern wegen Sachbeschädigung ermittelt worden.

Meine Überprüfung ergab, daß die Eintragung des Delikts in der Zentralkartei bei der ersten Vorlage der Akte aufgrund der von der Polizei vorgenommenen rechtlichen Ein-

ordnung des Sachverhaltes erfolgt. Nach Auffassung der Staatsanwaltschaft erfüllt die Zentralkartei in erster Linie den Zweck eines internen Aktennachweissystems. Zu diesem Zweck reiche es aus, daß die Deliktsbezeichnung lediglich Stichwortcharakter habe, da für die näheren Einzelheiten ohnehin die Strafakte beigezogen werden müsse. Deshalb sei eine Berichtigung der Deliktsbezeichnung im Verlaufe des Verfahrens nicht vorgesehen.

Dieser Auffassung stehen aus datenschutzrechtlicher Sicht erhebliche Bedenken entgegen. Denn die Zentralkartei erfüllt nicht nur die Funktion eines internen Indexsystems, sondern wird auch herangezogen, um den Verfahrensbeteiligten sowie bestimmten anderen Personen - etwa Versicherungen, Anwälten von Geschädigten etc. - und Behörden Auskünfte zu erteilen. Soweit sich diese Auskünfte nicht nur auf das Aktenzeichen beschränken, sondern auch auf das Delikt beziehen, hat der Betroffene ein schutzwürdiges Interesse daran, daß nur solche Tatbestände mitgeteilt werden, wegen der auch tatsächlich ermittelt bzw. Anklage erhoben worden ist. Denn es handelt sich um für den Betroffenen sehr sensible Daten, die für seine soziale Stellung und Einordnung von Bedeutung sind.

Die Sorge, daß unzutreffende Deliktsbezeichnungen zu einem falschen oder verzerrten Bild des Betroffenen führen können, bezieht sich aber nicht nur auf die Erteilung von Auskünften an Dritte. Auch beim zuständigen Staatsanwalt kann ein falscher, für den Betroffenen u.U. negativer Eindruck entstehen, dem dieser mangels Kenntnis der Speicherungen nicht entgegenwirken kann.

Da sich die Staatsanwaltschaft aufgrund ihrer personellen und technischen Ausstattung zur Zeit nicht dazu in der Lage sieht, die in der Zentralkartei enthaltenen Deliktsbezeichnungen zu überprüfen und gegebenenfalls zu berichtigen, ist zunächst folgendes Verfahren vereinbart worden, um meinen Bedenken Rechnung zu tragen:

Jeder Ausdruck aus der Zentralkartei wird in Zukunft mit dem Hinweis versehen:

„Die in der Zentralkartei gespeicherten Tatvorwürfe beinhalten keine abschließende rechtliche Bewertung der Tat. Dieser Ausdruck kann daher die Beiziehung der Verfahrensakten nicht ersetzen. Vorhalte aus dem Ausdruck in der Hauptverhandlung sind unzulässig".

Die telefonische Erteilung von Auskünften aus der Zentralkartei wird weiter eingeschränkt. Vollständige Auskunft erhalten nunmehr nur noch Bedienstete der Hamburger Staatsanwaltschaften, Richter der hiesigen Strafgerichtsbarkeit und deren Geschäftsstellenmitarbeiter sowie Sachbearbeiter der Hamburger Kriminalpolizei. Den Mitarbeitern bestimmter anderer Behörden wie z.B. des Strafvollzugsamtes, der Gnadenabteilung, der Gerichtshilfe und der Ausländerbehörde dürfen lediglich die Aktenzeichen, also weder das Delikt noch die Erledigungsart, genannt werden. Werden weitergehende Auskünfte gewünscht, so müssen sich die Auskunftsuchenden an den zuständigen Dezernenten wenden. Im übrigen werden - wie schon bisher - keine telefonischen Auskünfte gegeben. Schriftliche Anfragen werden von den jeweils zuständigen Dezernenten unter Berücksichtigung der Grundsätze von § 10 (Datenübermittlung innerhalb des öffentlichen Bereiches) und § 12 (Datenübermittlung an Stellen außerhalb des öffentlichen Bereiches) HmbDSG beantwortet.

Ich habe die Staatsanwaltschaft darauf hingewiesen, daß es sich hierbei nur um eine vorübergehende Regelung handeln kann. Denn nach den im Novellierungsentwurf zur StPO vorgesehenen Bestimmungen müssen die in der Zentralkartei enthaltenen Informationen von Amts wegen berichtigt werden, wenn sie unrichtig sind. Auf diese Rechtsänderung sollte sich die Staatsanwaltschaft im Interesse der Betroffenen rechtzeitig einstellen.

3.10.8 Auskünfte aus Strafermittlungsakten

Eine weitere Eingabe betraf die Gewährung von Akteneinsicht in Ermittlungsakten. Der Petent lag mit seiner Hausratsversicherung darüber im Streit, ob ein als gestohlen

gemeldeter Gegenstand von dieser zu ersetzen sei. Die Versicherung brachte in Erfahrung, daß die Staatsanwaltschaft gegen den Petenten ermittelte, und erhielt über ihren Anwalt ohne nähere Begründung Akteneinsicht. In der Auseinandersetzung mit dem Petenten wurden ihm später von der Versicherung Erkenntnisse aus der Ermittlungsakte vorgehalten.

Für die Einsicht in Strafakten durch Dritte, die nicht am Verfahren beteiligt sind, fehlt bisher eine gesetzliche Regelung. Zur Zeit wird Akteneinsicht nach den in Nr. 182 - 189 RiStBV (Richtlinien für das Straf- und Bußgeldverfahren) enthaltenen Bestimmungen gewährt. Hierbei handelt es sich - wie bei der MiStra - um gemeinsame Verwaltungsvorschriften des Bundes und der Länder. Diese können eine gesetzliche Grundlage aber nicht ersetzen. Deshalb können sich Staatsanwaltschaften und Gerichte auch bei der Erteilung von Auskünften aus Strafakten bzw. der Gewährung von Akteneinsicht nur auf den sog. Übergangsbonus stützen. Auskünfte an und Akteneinsicht für Dritte sind also auf das „unverzichtbare" Maß zu begrenzen.

Da jede Gewährung von Akteneinsicht mit der Offenbarung sehr sensibler personenbezogener Daten des Betroffenen verbunden ist, bedarf es aus Gründen der Verhältnismäßigkeit in jedem Einzelfall einer gewissenhaften Abwägung zwischen dem Interesse des Antragstellers und den schutzwürdigen Belangen des Betroffenen. Um eine solche Abwägung zu ermöglichen, muß der Antragsteller sein Interesse an der Kenntnis des Akteninhalts im einzelnen darlegen. Diesen Anforderungen wird keinesfalls genügt, wenn Akteneinsicht aufgrund der bloßen Tatsache gewährt wird, daß ein Rechtsanwalt sie begehrt hat. Auch dessen pauschale Angabe, er sei als Vertreter eines Versicherers des Beschuldigten tätig, reicht zur Begründung eines Akteneinsichtsgesuchs nicht aus.

Die Staatsanwaltschaft hat sich meinen Argumenten nicht verschlossen. Künftig werden Akteneinsichtsgesuche nur noch bearbeitet, wenn sie nachvollziehbar begründet sind. Der Sachbearbeiter muß in jedem Einzelfall prüfen, ob ein berechtigtes Interesse des Anfragenden vorliegt. In atypischen Fällen und in laufenden Verfahren entscheidet über den Antrag nicht der Rechtspfleger, sondern der zuständige Dezernent. Medizinische und psychologische Gutachten sind in der Regel von der Akteneinsicht auszunehmen und vor Überlassung der Akte herauszunehmen. Einsicht in derartige Gutachten kann ausnahmsweise nur gewährt werden, wenn insoweit ein berechtigtes Interesse im Einzelfall ausdrücklich nachgewiesen wird.

Ich möchte nicht unerwähnt lassen, daß das Gespräch mit Vertretern der Staatsanwaltschaft in einer kooperativen Atmosphäre stattgefunden und zu aus meiner Sicht befriedigenden Ergebnissen geführt hat.

3.11 Wissenschaft und Forschung

3.11.1 Genomanalysen

In meinem 7. Tätigkeitsbericht (4.14.3, S. 109) hatte ich einen Überblick gegeben über die Anwendungsbereiche gentechnischer Untersuchungen am Menschen und über ihre datenschutzrechtlichen Probleme. Diese habe ich mit meinen Kollegen aus anderen Bundesländern in einem Arbeitskreis „Gentechnologie" intensiv erörtert. Mit einer gemeinsamen Entschließung „Genomanalyse und informationelle Selbstbestimmung" führte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder diese Diskussion am 26.10.1989 zu einem vorläufigen Abschluß.

Ich hatte mich im Berichtsjahr besonders mit den Fragen der Genomanalyse im Arbeitsverhältnis und der Genomanalyse für Versicherungen zu beschäftigen. Eine Kleine Anfrage aus der Bürgerschaft (Drs. 13/4309) warf darüber hinaus das Problem der Genomanalyse im Strafverfahren auf.

Genomanalysen sind Methoden, mit denen die Erbsubstanz des Menschen, der in jedem Zellkern auf 46 Chromosomen verteilte DNS-Faden, daraufhin untersucht wird, ob er bestimmte Merkmale oder „Fehler" aufweist, aus denen Schlüsse auf Krankheits-

anlagen oder sonstige erbliche Dispositionen gezogen werden können. Neben diesen sog. codierenden Merkmalen, den Genen, besteht die DNS aus „Leerstellen", den sog. nicht-codierenden Sequenzen, die keine inhaltlichen Informationen enthalten, aber bei jedem Menschen in einer einzigartigen typischen Weise aufgebaut sind.

Unter dem Begriff Genomanalyse werden meist drei Verfahren zusammengefaßt:

— die mikroskopische Chromosomenanalyse, die aus Formveränderungen, Brüchen und Doppelungen der Chromosomen als DNS-Träger auf bestimmte Erbkrankheiten schließt, z.B. auf das Down-Syndrom ("Mongolismus");

— die chemische Genprodukt-Analyse, die aus der Menge bzw. dem Fehlen bestimmter Proteine Normabweichungen bei jenen Genen ableitet, die für die „Produktion" dieser Proteine verantwortlich sind;

— die DNS-Analyse, die mit Hilfe von sog. Gen-Sonden, künstlich hergestellten DNS-Teilstücken, direkt auf der DNS das Fehlen oder Vorhandensein bestimmter (Krankheits-) Gene oder bestimmter nicht-codierender Sequenzen feststellt.

3.11.1.1 Genomanalyse bei Strafverfahren

In letzter Zeit sind auch in der Bundesrepublik Strafurteile ergangen, die sich bei der Schuld- bzw. Unschuldsfeststellung auf den sog. genetischen Fingerabdruck stützen. Dies ist eine DNS-Analyse, welche die individuelle Eigenart der nicht-codierenden DNS-Sequenzen einer Person aus Tatspuren und/oder Blutproben sichtbar macht. Ergebnisvergleiche ermöglichen eine zuverlässige Täteridentifikation.

Einige Gerichte, die diese gentechnischen Verfahren zuließen, kommen zu derselben rechtlichen Wertung wie eine Arbeitsgruppe der Justizminister zu Fragen der Genomanalyse: Danach reiche § 81a der Strafprozeßordnung als Ermächtigungsgrundlage für den genetischen Fingerabdruck aus. Ich halte dies nicht für richtig. § 81a StPO läßt seinem Wortlaut nach den körperlichen Eingriff einer Blutentnahme zu Ermittlungszwecken zu und wird zur Legitimation der Blutalkohol- und Blutgruppenbestimmung herangezogen. Das durch § 81a StPO betroffene Rechtsgut ist die köperliche Unversehrtheit, Art. 2 Abs. 2 GG. Die Analyse des entnommenen Blutes offenbart darüber hinaus bestimmte Informationen über die betroffene Person, also personenbezogene Daten, und berührt damit das allgemeine Persönlichkeitsrecht in der Form des informationellen Selbstbestimmungsrechts, Art. 1, Art. 2 Abs. 1 GG. Bei Einführung des § 81a in die Strafprozeßordnung wurde diese Unterscheidung noch nicht getroffen. Bei den damals bekannten - vergleichsweise harmlosen - Blutuntersuchungen trat die mögliche Grundrechtsrelevanz der Datenerhebung in der allgemeinen Wertung hinter den mit der Blutentnahme verbundenen Grundrechtseingriff zurück. Bei der Genomanalyse ist dies jedoch nicht mehr vertretbar. Zwar beschränkt sich der genetische Fingerabdruck auf die „nicht-codierenden", also persönlichkeitsneutralen DNS-Sequenzen. Die Gefahr eines schwerwiegenden Mißbrauchs ist jedoch nicht von der Hand zu weisen: Abgesehen von der Möglichkeit, den genetischen Fingerabdruck in anderen Verfahren zweckwidrig wiederzuverwenden, bedarf es nur einer anderen DNS-Sonde (einer anderen biochemischen Substanz in einem kleinen Fläschchen), um die Blutprobe auch nach codierenden Sequenzen, also Krankheitsanlagen oder anderen Dispositionen zu untersuchen. Dabei ist ein potentielles Interesse der Strafverfolgungsbehörden an der Kenntnis bestimmter Merkmale eines Gesuchten ebenso naheliegend wie das Forschungsinteresse von Kriminologen an möglichen Zusammenhängen zwischen Erbanlagen und Straffälligkeit. Angesichts des rasanten Fortschritts auf dem Gebiet der Gentechnologie stehen jedenfalls theoretisch mit einer kleinen Menge Blut über kurz oder lang die gesamten genetischen Informationen über einen Menschen zur Verfügung. Letztlich ist auch nicht auszuschließen, daß selbst die erst seit wenigen Jahren bekannten nicht-codierenden DNS-Sequenzen nicht doch - ggf. durch ihre Stellung oder Anordnung zu bestimmten Genen - eines Tages inhaltliche Aufschlüsse zulassen. Ein intensiverer Eingriff in Menschenwürde und Persönlichkeitsrecht läßt sich kaum vorstellen; der Eingriff in die körperliche Unversehrtheit durch die Blutentnahme tritt in seinem Gewicht weit zurück.

Vor diesem Hintergrund bedarf es einer spezifischen normenklaren gesetzlichen Regelung, die vor allem vor Mißbrauch schützt und eine Beschränkung der Genomanalyse auf die nicht-codierenden DNS-Sequenzen festlegt. DNS-Sonden, die darüberhinaus einen personenbezogenen Informationsüberschuß erzeugen, sind nicht zuzulassen, ihre Anwendung ist unter Strafe zu stellen. Die Untersuchung darf nur in einem konkreten Strafverfahren an Vergleichspersonen oder an Spuren einer Straftat erfolgen. Sie setzt eine richterliche Anordnung voraus, in der das Ziel, die anzuwendende Methode der Untersuchung und das ausführende Institut festzulegen sind. Letzteres bedarf einer besonderen Zulassung. Die Untersuchung ist anonym durchzuführen, d.h. an Zellmaterial mit einer Kennziffer, aber ohne Akten, Aktenzeichen und Namen des Betroffenen. Solange sonstige Beweismittel zur Überführung oder Entlastung eines Verdächtigen ausreichen, ist auf eine Genomanalyse zu verzichten. Schließlich ist eine Verwendung von genomanalytischen Ergebnissen zu präventiv-polizeilichen Zwecken auszuschließen; nach Abschluß eines Strafverfahrens dürfen diese Ergebnisse nicht weiter gespeichert werden.

3.11.1.2 Genomanalyse im Arbeitsverhältnis

In der Bundesrepublik werden genomanalytische Verfahren an Arbeitnehmern vor allem in der chemischen Großindustrie durchgeführt. Mit Hilfe von Chromosomenanalysen und Genprodukt-Analysen werden Bewerber oder Arbeitnehmer auf genetische Dispositionen zu bestimmten Krankheiten oder Empfindlichkeiten gegenüber bestimmten Arbeitsstoffen überprüft. Solche Tests sind sowohl bei Eignungsuntersuchungen im Interesse des Arbeitgebers als auch bei Vorsorgeuntersuchungen zum Schutz der Arbeitnehmer oder Dritter (z.B. von Fluggästen) denkbar. Vorsorgeuntersuchungen sind für Arbeiten mit gefährlichen Arbeitsstoffen oder hohem Risiko rechtlich vorgeschrieben. In Unfallverhütungsvorschriften der Berufsgenossenschaften werden genomanalytische Testverfahren für bestimmte Arbeitsverhältnisse empfohlen.

Ich halte die Anwendung von Genomanalysen im Arbeitsverhältnis für datenschutzrechtlich bedenklich und trete für ein generelles gesetzliches Verbot ein: Zur Beurteilung des gegenwärtigen Gesundheitszustandes im Rahmen einer Eignungsuntersuchung sind Genomanalysen in allen drei Formen nicht geeignet. Sie können lediglich die Diagnose für eine bereits ausgebrochene Krankheit, also einen schon bekannten Befund, absichern. Genomanalysen geben in erster Linie Aufschluß über die genetische Disposition, möglicherweise zukünftig einmal zu erkranken. Dieses Risiko hat der Arbeitgeber jedoch nach dem geltenden Arbeitsrecht mitzutragen. Auch für Vorsorgeuntersuchungen gilt, daß die Prognose, ob der Untersuchte aufgrund der genetischen Veranlagung tatsächlich erkrankt, in den meisten Fällen von Umwelteinflüssen und Lebensweise abhängig ist. Nur bei wenigen Krankheiten ist der Ausbruch unvermeidbar. Der Zeitpunkt einer evtl. Erkrankung kann aber in keinem Fall vorausgesagt werden. Die hohen Anforderungen an einen wirksamen Vorsorgeschutz können deshalb durch Genomanalysen mit ihrer eingeschränkten Aussagekraft nicht ausreichend erfüllt werden. Darüberhinaus drohen dem Arbeitnehmer durch Genomanalysen Nachteile und Mißbrauchsgefahren: Er wäre z.B. gezwungen, die Disposition für eine unheilbare zukünftige Krankheit zur Kenntnis zu nehmen. Untauglichkeitsfeststellungen und die in diesem Zusammenhang bekannt gewordenen genetischen Veranlagungen können zu personalrechtlichen Konsequenzen bis zur Kündigung führen. Arbeitsschutz könnte hier hinter Arbeitnehmerselektion zurücktreten. Genetische Daten in Personalinformationssystemen könnten unzulässige Personalentscheidungen erleichtern oder zumindest wegen des unsicheren Aussagewerts die langfristige berufliche Entwicklung des Arbeitnehmers nachteilig beeinflussen.

Dem Arbeitnehmer ist es unbenommen, außerhalb des Arbeitsverhältnisses bei einer zugelassenen Einrichtung oder Arztpraxis seiner Wahl, jedoch nicht beim Betriebsarzt, genomanalytische Untersuchungen durchführen zu lassen. Es muß jedoch verhindert werden, daß Stellensuchende positive Gen-Atteste zum Bestandteil von Bewerbungsunterlagen machen, um einen Vorteil vor anderen Mitbewerbern zu erreichen. Dies

könnte sonst zu einer allgemeinen Praxis werden und würde denjenigen faktisch diskriminieren, der das Ergebnis einer privaten Genomanalyse nicht vorlegt. Arbeitgebern ist deswegen gesetzlich unter Strafandrohung zu untersagen, von Bewerbern oder Arbeitnehmern Bescheinigungen über genomanalytische Befunde zu fordern oder entgegenzunehmen, die der Betroffene auf eigene Initiative erstellen ließ.

Soweit arbeitsmedizinische Forschung im Betrieb mit Hilfe von Genomanalysen an Arbeitnehmern stattfindet, ist sie gegenüber der sonstigen betriebsärztlichen Tätigkeit abzuschotten. Das Freiwilligkeitsprinzip muß hier uneingeschränkt gelten.

3.11.1.3 Genomanalysen für Versicherungen

Anders als die Träger der gesetzlichen Krankenversicherungen machen private Kranken- und Lebensversicherer den Vertragsschluß oder auch die Höhe der Prämie abhängig von Risiken, die sich für die Zukunft aus dem gegenwärtigen Gesundheitszustand des Versicherungsnehmers ergeben können. In bestimmten Fällen fordert der Versicherer vor Vertragsabschluß eine gründliche medizinische Untersuchung. Der Versicherungsnehmer hat nach § 16 Abs. 1 Versicherungsvertragsgesetz (VVG) „alle ihm bekannten Umstände, die für die Übernahme der Gefahr erheblich sind, dem Versicherer anzuzeigen. Erheblich sind Gefahrenumstände, die geeignet sind, auf den Entschluß des Versicherers, den Vertrag überhaupt oder zu dem vereinbarten Inhalt abzuschließen, einen Einfluß ausüben."

Im Februar 1989 fand ein Gespräch des Hamburgischen Datenschutzbeauftragten mit Verantwortlichen der bundesdeutschen Versicherungswirtschaft zu diesem Thema statt. Als Fazit kann festgestellt werden, daß derzeit Genomanalysen bei Versicherungsvertragsverhandlungen so gut wie keine Rolle spielen. Ein potentieller Versicherungsnehmer wird weder zu einer genomanalytischen Untersuchung aufgefordert noch nach dem Ergebnis einer früheren Genomanalyse befragt. Diese Zurückhaltung ist auch rechtlich geboten: Genomanalysen sind nicht geeignet, dem Versicherer zusätzliche Erkenntnisse über den Gesundheitszustand des Versicherungsnehmers bei Vertragsschluß zu verschaffen. Sie können allenfalls Hinweise auf mögliche Erkrankungen in der Zukunft geben, aber gerade ein zukünftiger Krankheitsausbruch oder Todeseintritt soll - weil er unsicher ist - versichert werden; darauf beruht die wirtschaftliche Kalkulation des Versicherers. Gäbe es absolut sichere Prognosen, würde dieses Prinzip zulasten des Versicherungsnehmers ausgehöhlt. Genomanalysen können jedoch nur selten das „Ob", nie das „Wann" eines Krankheitsausbruches vorhersagen. Der Versicherungsfall kann trotz genetischer Disposition durch Umwelteinflüsse, Lebensführung oder Medikamente hinausgezögert oder gar verhindert werden. Er kann aber auch völlig unabhängig von der genetischen Disposition eintreten - durch Unfälle oder nicht genetisch bedingte Krankheiten. Eine sichere individuelle Risikoprognose ist auch mit Hilfe von Genomanalysen nicht möglich. Durch vorgeschriebene Genomanalysen vor Vertragsschluß würde der Versicherungsnehmer z.B. gezwungen, auch von der Disposition zu einer unheilbaren Krankheit Kenntnis zu nehmen. Die weitgehend automatisierte Verarbeitung der Versichertendaten ohne Kontext birgt die Gefahr, daß in hohem Maße interpretationsbedürftige und prognostisch unsichere genetische Daten sich zu Schein-Fakten verfestigen. Aus ihnen würden dann möglicherweise Risiken errechnet und die Betroffenen in Wagnis-Dateien erfaßt. Da der Versicherungsnehmer überdies seine Ärzte in weitgehendem Maße von der Schweigepflicht entbinden muß, verlöre er die Möglichkeit, im einzelnen über Offenbarung und Verbleib der besonders sensiblen genetischen Daten zu entscheiden.

Damit ist die Genomanalyse keine geeignete und verhältnismäßige Methode für die vor einem Vertragsschluß geforderte ärztliche Untersuchung des gegenwärtigen Gesundheitszustandes. Sie darf wegen ihrer geringen prognostischen Aussagekraft und angesichts der Mißbrauchsgefahren auch keinen Einfluß auf den Entschluß des Versicherers ausüben, den Vertrag überhaupt oder mit einem bestimmten Inhalt abzuschließen. Da die Genomanalyse im Verhältnis zum allgemeinen Lebensrisiko im Regelfall keine zusätzlichen „erheblichen" Gefahrenumstände offenbart, trifft den Versicherungsneh-

mer grundsätzlich auch keine Anzeigepflicht nach § 16 Abs. 1 VVG. Eine entsprechende Klarstellung sollte ins VVG aufgenommen werden. Das Verlangen des Versicherers, daß der Versicherungsnehmer seine Ärzte von der Schweigepflicht entbindet, darf sich daher nicht auf die Ergebnisse von Genomanalysen beziehen.

Die Vertreter der Versicherungswirtschaft machten allerdings deutlich, daß sie eine sog. „Gegenauslese" ausschließen möchten, d.h. den Fall, daß eine Person durch eine private Genomanalyse von dem wahrscheinlichen baldigen Eintritt einer schweren Erbkrankheit Kenntnis erlangt und aufgrund dessen eine hohe private Kranken- oder Lebensversicherung abschließt, ohne der Versicherung das Analyseergebnis zu offenbaren. In diesen seltenen Ausnahmefällen halte auch ich eine Offenbarungspflicht des Betroffenen für möglich. Dies rechtfertigt jedoch nicht die Aufnahme von Genomanalysen in die ärztliche Untersuchung vor Vertragsschluß.

3.12 Gesundheitswesen

3.12.1 Stand der Gesetzgebung

3.12.1.1 Krankenhausgesetz

Ein „Dauerbrenner" meiner Tätigkeitsberichte zum Gesundheitswesen sind Stellungnahmen zu den Entwürfen eines Hamburgischen Krankenhausgesetzes. Auch im vergangenen Jahr hat wiederum eine Abstimmungsrunde zur nunmehr dritten Fassung des Referentenentwurfs stattgefunden, aber ein Senatsbeschluß oder gar ein Abschluß des Gesetzgebungsverfahrens ist immer noch nicht in Sicht.

Zwar sind in der Neufassung des Entwurfes einige Vorschriften über den Patientendatenschutz verbessert, es verbleiben aber noch gewichtige, grundsätzliche Differenzen, und zwar nicht nur in Detailfragen, wie die federführende Behörde für Arbeit, Gesundheit und Soziales meint.

Meinungsverschiedenheiten bestehen z.B. bei der Bestimmung der speichernden Stelle. In den bisherigen Diskussionen und Stellungnahmen zum Krankenhausgesetz habe ich immer die Auffassung vertreten, daß im Krankenhaus eine strikte Funktionstrennung zwischen Verwaltungsbereich und ärztlichem Bereich, aber auch zwischen den einzelnen Behandlungseinheiten (Fachabteilungen, Stationen) besteht. Speichernde Stelle für die Daten aus dem ärztlichen Bereich muß meiner Meinung nach die Behandlungseinheit sein. Dies gebietet die ärztliche Schweigepflicht, die an die Person des einzelnen behandelnden Arztes anknüpft. Nicht „das Krankenhaus" erhebt, nutzt und übermittelt Patientendaten, sondern der jeweilige Funktionsbereich im Rahmen der ihm obliegenden Aufgaben. Die Neufassung des Entwurfs geht dagegen, wie sich insbesondere aus der Begründung ergibt, davon aus, daß das Krankenhaus speichernde Stelle ist, so daß selbst innerhalb einer Großklinik keine Datenübermittlungsvorgänge stattfinden. Das Krankenhaus wird als organisatorische Einheit definiert, das Arztgeheimnis wird zum Krankenhausgeheimnis. Auch wenn durch Zwecksbindungsgebote versucht wird, die Datennutzung im Hinblick auf die den einzeln Funktionsbereichen zufallenden Aufgaben zu begrenzen, wird doch das Patientengeheimnis weniger geschützt als bei Anwendung gesetzlich festgelegte Übermittlungsvoraussetzungen. Eine solche Konzeption kann aus datenschutzrechtlicher Sicht nicht akzeptiert werden.

Besonders deutlich zeigen sich die damit zusammenhängenden Probleme im Forschungsbereich. Nach der Begründung des Referentenentwurfs bilden die Patientendaten aller im gesamten Krankenhaus behandelten Patienten einen Datenfonds für Forschungsvorhaben, auf die ohne Information und Beteiligung des Betroffenen zugegriffen werden kann. Zwar sieht der Entwurf eine „Widerspruchslösung" vor, diese läuft aber weitgehend leer, da sie eine Verletzung schutzwürdiger Belange des Patienten voraussetzt, über deren Vorliegen zuvor das Krankenhaus entscheidet, ohne den Betroffenen anzuhören. Unter Berufung auf eine angebliche Schicksalsgemeinschaft

aller Patienten wird das informationelle Selbstbestimmungsrecht des einzelnen außer Kraft gesetzt und der Patient entmündigt.

Dagegen ist aus datenschutzrechtlicher Sicht zu fordern, daß der betroffene Patient in aller Regel über eine Zweckentfremdung von Behandlungsdaten zu Forschungszwecken informiert und an der Entscheidung gemäß den gesetzlichen Vorschriften, je nach Intensität des Eingriffs in sein Grundrecht, beteiligt wird. Bei Forschungsvorhaben, die innerhalb des Rahmens der Fachabteilung bzw. Fachklinik bleiben, halte ich ein Widerspruchsrecht für angemessen. Der Patient ist zuvor über die Forschung aufzuklären, so daß er Gelegeheit hat, seine schutzwürdigen Belange zur Geltung zu bringen. Eine Übermittlung von personenbezogenen Daten zu Forschungszwecken an Dritte sollte grundsätzlich nur mit Einwilligung des Betroffenen zugelassen werden. Nur in eng begrenzten, gesetzlich geregelten Ausnahmefällen darf auf eine Information und Beteiligung des beforschten Patienten verzichtet werden.

Nachbesserungsbedarf besteht auch bei den Vorschriften für die Auftragsdatenverarbeitung, die für den Schutz der besonders sensiblen Daten aus dem ärztlichen Bereich nicht einmal den Standard erreichen, der im Sozialgesetzbuch für die Auftragsdatenverarbeitung von Sozialdaten vorgeschrieben ist.

3.12.1.2 Änderung des Krebsregistergesetzes

Die geplante Änderung des Krebsregistergesetzes, über die ich im Vorjahr berichtet hatte (7. TB, 4.16.1.4, S. 116), ist inzwischen vom Senat beschlossen und liegt der Bürgerschaft zur Beratung vor. Mit dem Novellierungs-Vorschlag ist ein Erfahrungsbericht zum Meldeverfahren verbunden, der auch zur Form der Einwilligungserklärung Stellung bezieht. Aus datenschutzrechtlicher Sicht hatte ich seinerzeit im Gesetzgebungsverfahren zum Krebsregistergesetz und in der Stellungnahme zum ersten Erfahrungsbericht eine schriftliche Einwilligungserklärung als Regelfall empfohlen. Demgegenüber bevorzugen die Ärzte nach Untersuchungen der Behörde für Arbeit, Gesundheit und Soziales nach wie vor die mündliche Form der Einwilligungserklärung, weil sie ein individuelleres und persönlicheres Eingehen des Arztes auf die Situation des Patienten ermögliche, die Aufklärung über die Art der Erkrankung häufig schrittweise in einem längeren Prozeß erfolge und bei der formalen, unpersönlichen Schriftform mit einer höheren Ablehnungsquote zu rechnen sei. Gleichzeitig wird betont, daß die Schriftform das mündliche Gespräch nicht ersetzen könne, so daß insgesamt bei schriftlicher Einwilligungserklärung der zeitliche Aufwand erhöht werde.

Das Zeitargument ist kaum nachvollziehbar, da der Arzt eine mündliche Einwilligungserklärung in seine Aufzeichnungen aufzunehmen hat. Zuzustimmen ist der Auffassung, daß die Schriftform das mündliche Gespräch nicht ersetzen, sondern nur den wesentlichen Inhalt der Aufklärung und die Tatsache der Einwilligung dokumentieren kann. Die aus datenschutzrechtlicher Sicht optimale Lösung ist eine schriftliche Einwilligungserklärung, kombiniert mit einem persönlichen Aufklärungsgespräch mit dem behandelden Arzt. Da aber keine Meldepflicht des Arztes besteht, kann die Behörde dieses Verfahren offensichtlich nicht durchsetzen. Für den zweitbesten Weg, die Kombination von individueller Aufklärung mit dokumentierter mündlicher Einwilligungserklärung sind dann aber gewisse Mindestanforderungen zur Sicherung des Aufklärungsstandards unabdingbar. Es darf nicht dem Zufall und Selbstlauf überlassen werden, welche Informationen der einzelne betroffene Patient über die Meldung zum Krebsregister erhält, vielmehr ist durch organisatorische Maßnahmen sicherzustellen, daß ihm durch schriftliches Aufklärungsmaterial die Informationen vermittelt werden, die er benötigt, um von seinem Grundrecht auf informationelle Selbstbestimmung Gebrauch machen zu können. Es reicht nicht aus, Informationsmaterial in Wartezonen auszulegen, es muß den für eine Meldung in Betracht kommenden Patienten ausgehändigt werden, um dann Anknüpfungspunkt für weitere Aufklärungsgespräche zu sein. Auch Patienten, deren Krebserkrankung nicht mehr behandelt werden kann, haben grundsätzlich Anspruch auf Aufklärung über ihre Erkrankung, auch wenn ein solches Aufklärungsgespräch besonders schwierig ist und großes Einfühlungsvermö-

gen erfordert. Eine schwierige Aufklärungssituation rechtfertigt es nicht, von der gesetzlichen Ausnahmeregelung Gebrauch zu machen.

Den Ärzten sind durch Dienstanweisung ihre Pflichten im Zusammenhang mit der Aufklärung von Patienten zu verdeutlichen. Nur wenn klare Regelungen zum Meldeverfahren erlassen werden, kann nachvollzogen und überprüft werden, ob die ärztliche Schweigepflicht und das informationelle Selbstbestimmungsrecht der Patienten gewahrt worden sind und ob die Ausnahmeregelung korrekt angewendet worden ist.

3.12.2 Kindergartenstudie

In Hamburg mußten 1986 einige Kindertagesheime geschlossen werden, da die Raumluft infolge der Verwendung dioxinhaltiger Holzschutzmittel zu hoch mit Schadstoffen belastet war. Zur Untersuchung der Kinder auf etwaige gesundheitliche Folgeschäden gab die Gesundheitsbehörde 1987 eine Studie in Auftrag, die von der Kinderklinik und vom Institut für Medizinsoziologie des Universitätskrankenhauses Eppendorf durchgeführt wurde.

Die datenschutzrechtlichen Rahmenbedingungen der Studie wurden mit meiner Dienststelle abgestimmt. Da für die Datenerhebung keine gesetzliche Grundlage vorhanden war und die untersuchten Kinder auch nicht als Patienten im UKE untersucht wurden, war eine Datenerhebung, -auswertung und -speicherung ausschließlich im Rahmen der von den Eltern gegebenen Einwilligungserklärung zulässig. Diese wurde unter der Voraussetzung erteilt, daß keine Weitergabe der Daten an Dritte erfolgt, die Daten nach Abschluß der Erhebung anonymisiert und nach Beendigung der Auswertung so verändert werden, daß eine Reidentifizierung der Studienteilnehmer unmöglich war. Befunde und Labordaten sollten im Original an die Eltern herausgegeben und keine Duplikate angelegt werden. Bereits im Oktober 1987 gab es Hinweise, daß diese Regelungen vom Labor nicht eingehalten und die Namen betroffener Kinder auf dem Laborrechner gespeichert wurden. Die Eltern erhielten daraufhin die Zusage, daß nur noch Kennziffern verwendet und möglicherweise gespeicherte Namen umgehend gelöscht werden. Bei Rückgabe der Untersuchungsunterlagen stellten dann einige Eltern fest, daß diese Zusage nicht eingehalten worden war, da sie die Unterlagen mit Namensbezug und nicht mit Kennziffer zurückerhielten.

Auf meine Bitte um Aufklärung, an welchen Stellen im UKE Daten aus der Kindergartenstudie aufbewahrt oder gespeichert werden, erhielt ich die Auskunft, daß in der Abteilung für klinische Chemie Kopien von anonymisierten Untersuchungsergebnissen in Stahlschränken aufbewahrt und daß wahrscheinlich im Rechenzentrum des UKE Mikroverfilmungen der Labordaten archiviert werden. In den Laborjournalen der Abteilung für klinische Immunologie und Allergologie seien keine personenbezogenen, sondern nur nicht entschlüsselbare Daten vorhanden.

Bei einer Prüfung vor Ort mußte ich feststellen, daß diese Informationen nicht mit der Wirklichkeit übereinstimmten. Die Kinder, die zwischen dem 25. August und dem 8. Oktober 1987 im UKE untersucht worden waren, waren mit ihrem Namen an verschiedenen Stellen gespeichert. Diese rechtswidrige Speicherung personenbezogener Daten habe ich dem UKE gegenüber förmlich beanstandet. Daraufhin wurde der Personenbezug der Daten in der Datei des Labordatensystems und in den Laborjournalen gelöscht und auf den Mikrofilmen durch eine Chiffrierung ersetzt. Die Untersuchungsunterlagen aus der klinischen Chemie wurden vernichtet. Im Institut für Medizinsoziologie gibt es noch eine Namensliste der beteiligten Eltern ohne die Kennziffern der untersuchten Kinder auf einer Diskette und auf Briefbogen, um die Kurzfassung des Untersuchungsberichts versenden und zu einem letzten Treffen einladen zu können. Diese Speicherung erfolgt im Einverständnis mit den betroffenen Eltern und ist datenschutzrechtlich unbedenklich.

Bei Einhaltung der datenschutzrechtlichen Vorgaben wären mühselige Löschungsprozeduren und die verständliche Verärgerung der Eltern der betroffenen Kinder vermeidbar gewesen.

3.12.3 Überwachung des Verkehrs mit Betäubungsmitteln

Die Überwachung des Verkehrs mit Betäubungsmitteln gehört zu den Aufgaben der Gesundheits- und Umweltämter der Bezirke mit Ausnahme der Apothekenüberwachung, die von der Behörde für Arbeit, Gesundheit und Soziales wahrgenommen wird. Die Gesundheits- und Umweltämter erfüllen ihre Aufgabe durch stichprobenartige Kontrollen der Ärzte, die zur Verordnung von Betäubungsmitteln berechtigt sind. Betäubungsmittel dürfen nur auf besonderen, vom Bundesgesundheitsamt ausgegebenen und durchnummerierten Rezepten verschrieben werden. Das Bundesgesundheitsamt informiert die Gesundheits- und Umweltämter darüber, welche Ärzte in ihrem Zuständigkeitsbereich Betäubungsmittelrezepte in welcher Anzahl und mit welcher Nummerierung erhalten haben.

Im Rahmen ihrer Überwachungstätigkeit wollten die Gesundheits- und Umweltämter nicht nur Informationen über die überprüften Ärzte, sondern auch über die Empfänger von Betäubungsmittelrezepten speichern und bezirksübergreifend abgleichen. Zur Begründung führten sie an, im Einzelfall könne der Umstand, daß ein Patient regelmäßig oder in erheblichen Mengen Betäubungsmittel erhalte, ein Indiz dafür sein, daß der Arzt seine Sorgfaltspflichten bei der Verschreibung von Betäubungsmitteln verletzt habe, besonders wenn die Verordnung bei Würdigung der Diagnose und Therapie nicht erforderlich sei.

Aus dieser Argumentation läßt sich aber keine Berechtigung der Überwachungsbehörde herleiten, vorsorglich Patientendaten aller Rezeptempfänger zu speichern und auch noch bezirksübergreifend abzugleichen. Die Speicherung und Übermittlung von Daten der Empfänger von Betäubungsmittelrezepten stellt einen Eingriff in deren informationelles Selbstbestimmungsrecht dar, der einer normenklaren gesetzlichen Grundlage bedarf. Nach dem Betäubungsmittelgesetz darf die Überwachungsbehörde zwar bei Ärzten Unterlagen einsehen, davon Ablichtungen oder Abschriften anfertigen und Auskünfte verlangen, wobei der Arzt duldungs- und mitwirkungspflichtig ist. Nicht gedeckt ist die Überwachung und Registrierung von Personen, die Betäubungsmittel verschrieben bekommen.

Aufgrund meiner Einwände werden die Gesundheits- und Umweltämter künftig darauf verzichten, Informationen über die Empfänger von Betäubungsmittelrezepten zu sammeln und abzugleichen.

3.13 Prüfung der Patientendatenverarbeitung im Universitätskrankenhaus Eppendorf

Schwerpunkt meiner Prüftätigkeit im Gesundheitswesen war im Berichtsjahr die Überprüfung der Patientendatenverarbeitung im Universitätskrankenhaus Eppendorf. Dabei habe ich festgestellt, daß

- auf dezentralen Datenverarbeitungsanlagen Daten gespeichert wurden, die nicht für Behandlungszwecke erforderlich waren (Verstoß gegen § 5 HmbDSG), und daß diese Patientendaten unbefugt Dritten zu Forschungszwecken offenbart wurden (Verstoß gegen § 203 StGB und § 2 der Berufsordnung der Hamburger Ärzte),
- die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten z.T. unterblieben oder unzureichend waren (Verstoß gegen § 8 Abs. 1 HmbDSG),
- die Ausführung des HmbDSG und die Wahrung des Patientengeheimnisses nicht sichergestellt wurde, insbesondere
  * keine aktuelle und vollständige Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger geführt wurde (Verstoß gegen § 16 HmbDSG),
  * die Meldungen zum Datenschutzregister nur unvollständig und verspätet erfolgten (Verstoß gegen § 13 HmbDSG),

* eine dem geltenden Recht genügende Dienstanweisung über die Führung von Krankenakten und den Patientendatenschutz fehlt.

Diese Mängel habe ich gegenüber der Leitung des UKE beanstandet.

3.13.1 Unzulässige Datenverarbeitung

Die Prüfung der Patientendatenverarbeitung auf materielle Rechtmäßigkeit wurde durch das Fehlen verbindlicher konkreter Rechtsmaßstäbe erschwert, denn der Umgang mit Patientendaten im Krankenhaus ist in Hamburg noch nicht bereichsspezifisch geregelt. Unter diesen Voraussetzungen muß sich die Datenverarbeitung - soweit sie nicht auf die Einwilligung der Betroffenen gestützt werden kann - auf das unbedingt Erforderliche beschränken. Zur Wahrung des informationellen Selbstbestimmungsrechts des Patienten, das durch den Aufenthalt in einem Krankenhaus nicht außer Kraft gesetzt wird, empfehle ich die Anwendung der Grundsätze, die ich auch für das zu erwartende Hamburgische Krankenhausgesetz vorgeschlagen habe (vgl. 3.12.1.1). Keinesfalls darf die Verarbeitung von Patientendaten die Grenzen überschreiten, die der Entwurf für ein Krankenhausgesetz vorsieht.

Das zwischen Forschungsfreiheit und informationellem Selbstbestimmungsrecht bestehende Spannungsverhältnis bei der Forschung mit Patientendaten muß aufgrund einer beiden Grundrechten gerecht werdenden Abwägung durch den Gesetzgeber aufgelöst werden. Die erforderliche Wertentscheidung des Parlaments kann nicht durch eine Entscheidung des einzelnen Arztes ersetzt werden, die einseitig zugunsten der Forschungsfreiheit ausfällt und pauschal aus dem Interesse des Patienten an seiner eigenen optimalen Behandlung auf eine Einwilligung in die Forschung mit seinen personenbezogenen Daten rückschließt.

Die Einwilligung des Patienten kann i.d.R. unterstellt werden, soweit der Behandlungsvertrag reicht. Sie erstreckt sich aber nicht auf die Forschung mit Patientendaten. Aus der Tatsache, daß sich ein Patient in die Universitätsklinik zur Behandlung begibt, läßt sich keine konkludente Einwilligung in die personenbezogene Nutzung seiner Daten zu Forschungszwecken herleiten. Diese würde voraussetzen, daß der Patient eine konkrete Vorstellung über die Verwendung seiner Daten hat. Davon ist aber nicht auszugehen. Eine Information des Patienten über beabsichtigte Forschungsvorhaben findet weder bei seiner Aufnahme noch während seiner Behandlung statt, wie die im Rahmen meiner Prüfung dazu befragten, für die Datenverarbeitung verantwortlichen Ärzte bestätigten.

Für die Forschung innerhalb einer Fachklinik bzw. -abteilung halte ich eine Widerspruchslösung für angebracht. Sie setzt die Information des Patienten über geplante Forschungsvorhaben und den Hinweis auf sein Widerspruchsrecht gegen die Nutzung seiner Daten zu Forschungszwecken voraus. In Ausnahmefällen, wenn dem Betroffenen keine Gelegenheit zum Widerspruch gegeben werden kann, ist zwischen dem Forschungsinteresse und den Belangen des Betroffenen abzuwägen. Bei einer Übermittlung personenbezogener Daten an Dritte zu Forschungszwecken sollte als Regelfall die schriftliche Einwilligung des Patienten vorausgesetzt werden.

In jedem Fall ist vorab zu klären, ob für das Forschungsvorhaben überhaupt personenbezogene Daten benötigt werden. Wenn die Patientendaten von der behandelnden Fachabteilung vor der Weitergabe zu Forschungszwecken anonymisiert werden, sind Belange des Patienten nicht betroffen.

Einen weiteren Problembereich bilden DV-Systeme, auf denen Patientendaten sowohl für die aktuelle Behandlung als auch für Dokumentationszwecke verarbeitet werden. Mit dem Abschluß der Behandlung erfahren die gespeicherten Daten eine Zweckänderung, die nur auf der Grundlage einer bereichsspezifischen Regelung zulässig ist. Solange eine Regelung für den Patientendatenschutz im Krankenhaus noch fehlt, ist eine Trennung von aktuellen Behandlungsfällen und archivierten Falldaten zu fordern. Nach Abschluß des Behandlungsfalls halte ich eine Datei mit den Namen der Patienten zur Unterstützung der Archivierung und Erleichterung der Wiederauffindbarkeit vor-

handener Akten für denkbar. Im übrigen sollten Identifizierungsmerkmale und medizinische Daten nach Abschluß des Behandlungsfalls getrennt gespeichert werden.

Bei der Prüfung von zwei Patientendokumentationsdateien der Neurochirurgie und der Neuroradiologie, die mit Sicherheit keine Einzelfälle sind, habe ich festgestellt, daß die Datenverarbeitung den dargestellten Grundsätzen nicht genügt. In gemeinsamen Dateien werden aktuelle Behandlungsdaten zusammen mit Patientendaten aus zum Teil jahrelang zurückliegenden abgeschlossenen Behandlungsfällen gespeichert. Mit der aktuellen Dokumentation wird die medizinische Versorgung unterstützt. Daneben dient die Datensammlung dem Archivierungszweck und wird auch als Datenbasis für die Forschung angesehen. Genutzt werden die Daten ohne Einwilligung des Patienten nicht nur von den an der Behandlung beteiligten Ärzten, sondern auch von Dritten, denen Disketten mit nicht anonymisierten Patientendaten zur Verfügung gestellt werden.

Ich halte diesen Umgang mit Patientendaten nicht für rechtmäßig. Die direkt abrufbare Speicherung ist nach Abschluß des Behandlungsfalls, d.h. nach Erstellung des Abschlußberichts (Arztbrief) nicht mehr vom Behandlungsvertrag gedeckt. Ärztliche Aufzeichnungen müssen zwar aus Beweissicherungsgründen und als Informationsquelle für etwaige spätere Behandlungen aufbewahrt werden, dies geschieht aber bereits durch die Archivierung der Patientenakten; eine parallele Speicherung der Daten in online verfügbaren Datenbanken ist hingegen für die Dokumentation nicht erforderlich. Der Forschungszweck ist ebenfalls keine ausreichende Legitimation für die praktisch nur durch die Speicherkapazität des Computers begrenzte Vorhaltung von Patientendaten zum direkten Abruf und schon gar nicht für ihre Offenbarung an Dritte.

Bei unserer Prüfung haben wir festgestellt, daß den meisten für die Datenverarbeitung verantwortlichen Ärzten die rechtlichen Grenzen der Patientendatenverarbeitung nicht bewußt waren. Das fehlende Unrechtsbewußtsein mag dadurch erklärlich sein, daß die bei einer Behandlung anfallenden Daten nicht mehr als Patientendaten, sondern als zur freien ärztlichen Verfügung stehender Datenfundus angesehen werden, was gleichermaßen unter Datenschutzgesichtspunkten und bei korrekter Auslegung der ärztlichen Schweigepflicht unzulässig ist.

3.13.2 Unzureichende Datensicherungsmaßnahmen

Sowohl beim Rechenzentrum (RZ) als auch bei dezentralen Anwendungen war zu prüfen, ob die vom UKE getroffenen technischen und organisatorischen Maßnahmen den Anforderungen nach § 8 Abs. 1 HmbDSG bzw. § 6 Abs. 1 BDSG genügen.

Nach § 16 HmbDSG hat das UKE die Ausführung dieses Gesetzes sowie anderer Bestimmungen über den Datenschutz sicherzustellen. Gerade in einem Bereich, in dem in großem Umfang sensibelste personenbezogene Daten verarbeitet werden, kommt der koordinierenden Funktion der UKE-Leitung besondere Bedeutung zu. Die Prüfung hat hier ergeben, daß diese Aufgabe weitgehend nicht wahrgenommen wurde.

3.13.2.1 Dezentrale Verfahren

In den Krankenhäusern nimmt der Einsatz von Personalcomputern und anderen dezentralen Datenverarbeitungssystemen ständig zu. Obwohl auch auf diesen Systemen hochsensible Gesundheitsdaten verarbeitet werden, hat keine Stelle im UKE einen Überblick, wo welche Geräte für welche Aufgabe eingesetzt werden und welche personenbezogenen Daten dabei verarbeitet werden. Darin liegt ein Verstoß gegen § 16 S. 2 Nr. 1 HmbDSG, wonach die Behörden dafür zu sorgen haben, daß eine Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist sowie deren regelmäßige Empfänger (Dateiverzeichnis) geführt wird.

Die Zuständigkeit für die Führung des Dateiverzeichnisses liegt bei der Verwaltung des UKE. Von der Organisationsabteilung waren zwar auf Anstoß des Hamburgischen

Datenschutzbeauftragten hin Umfragen nach Dateien mit personenbezogenen Daten veranlaßt worden. Seit der letzten Umfrage im Jahre 1986 waren aber keine Dateimeldungen mehr eingegangen, obwohl seitdem in großem Umfang neue DV-Systeme eingesetzt wurden.

Offenbar ist in den Instituten und Kliniken des UKE die Organisationsabteilung als übersichtführende Stelle zu wenig bekannt. Das UKE hat nunmehr zugesagt, jährlich einen Informationsumlauf mit Hinweisen auf die Verpflichtung zur Meldung der Dateien aller Stellen, die personenbezogene Daten verarbeiten, zu veranlassen. Nach den bisherigen Erfahrungen ist es wenig wahrscheinlich, daß allein auf diesem Wege eine brauchbare und vollständige Dateienübersicht zustandekommen wird. Es ist also zu befürchten, daß die Praxis des UKE auch weiterhin nicht den gesetzlichen Vorgaben entsprechen wird.

Eine Überprüfung, ob alle meldepflichtigen Dateien vollständig in der Übersicht erfaßt wurden, fand bisher nicht statt, auch nicht stichprobenartig. Informationen über Datenverarbeitungsgeräte sind bei der Organisationsabteilung nur insoweit vorhanden, als diese Geräte aus Mitteln des UKE angeschafft wurden. Nicht erfaßt sind hierbei die vielen aus Drittmitteln oder aus privaten Mitteln angeschafften DV-Systeme. Es besteht auch keine Regelung darüber, unter welchen Voraussetzungen private Datenverarbeitungsgeräte zur Verarbeitung personenbezogener Daten genutzt werden dürfen.

Dieser Organisationsmangel ist deshalb besonders gravierend, weil ohne einen Überblick über die eingesetzten Geräte nicht sichergestellt werden kann, daß sich die Datenverarbeitung im Rahmen des Zulässigen bewegt und daß die erforderlichen Datensicherungsmaßnahmen getroffen werden.

Die Prüfung autonomer, d.h. nicht mit anderen Anlagen vernetzter, dezentraler DV-Anlangen hat sich zwar stichprobenartig auf die neurologische Universitätsklinik beschränkt, es spricht jedoch einiges dafür, daß auch in anderen Einsatzbereichen dezentraler Verfahren im UKE die im folgenden dargestellten Mängel auftreten:

— In weitaus größerem Maße werden personenbezogene Daten in Dateien verarbeitet, als sich aus der Dateienübersicht ergibt. Ein Teil dieser Dateien wurde auch nicht gem. § 13 HmbDSG zum Datenschutzregister gemeldet.

— Schriftliche Regelungen über Zuständigkeiten, Zugriffsbefugnisse und zu treffende Sicherungsmaßnahmen gibt es nicht.

— Datensicherungsmaßnahmen werden, z.T. nicht getroffen z.T. sind sie unzureichend.

— Es bedarf kaum noch einer Erwähnung, daß die Verfahren in der Regel nicht oder nicht ausreichend dokumentiert werden.

Ein besonderes Problem stellt die Nutzung privateigener PC's für dienstliche Zwecke oder für Forschungsvorhaben dar. Da der Datenträgerumlauf (Disketten!) nicht geregelt und nicht kontrolliert wird, ist nicht auszuschließen, daß Datenträger mit personenbezogenen Daten nach Hause mitgenommen und dort auf privaten PC's weiterverarbeitet und ausgewertet werden.

Angesichts dieser Ergebnisse habe ich die Leitung des UKE dazu aufgefordert, endlich verbindliche Regelungen für den Einsatz dezentraler Anlagen zu erlassen und deren Einhaltung regelmäßig zu überwachen.

Regelungsbedarf besteht nicht nur für den Einsatz der automatisierten Datenverarbeitung, sondern auch für den Umgang mit herkömmlichen Krankenunterlagen. Seit Jahren steht im UKE die Neufassung der Dienstanweisung über die Führung und Herausgabe von Krankengeschichten an. Vor über fünf Jahren hatte die Erkenntnis, daß die alte Dienstanweisung nicht mehr geltendem Recht entsprach, zur Erarbeitung des Entwurfs einer Dienstanweisung über die Führung von Krankenakten und den Schutz personenbezogener Daten im UKE geführt, der aber nicht in Kraft gesetzt worden ist. Zentrale Fragen des Patientendatenschutzes wie die klare Festlegung von Zugriffsbefugnissen und von Verantwortlichkeiten der datenverarbeitenden Stellen, die Zulässigkeit

der Weitergabe von medizinischen Daten an Dritte, ihre Nutzung außerhalb des konkreten Behandlungszusammenhangs, Einsichtsrechte der Betroffenen sind entweder überhaupt nicht oder unzureichend geregelt, was ich wiederholt, (vgl. 7. TB, 1.4, S. 7) kritisiert habe.

3.13.2.2 Rechenzentrum

Beim zentralen Rechenzentrum (RZ), das dem Institut für Mathematik und Datenverarbeitung in der Medizin zugeordnet ist, fließt eine Vielzahl der medizinischen Versorgung anfallender Daten zusammen:

— Mit dem Patientenaufnahmeverfahren werden Daten sämtlicher in das UKE aufgenommener Patienten automatisiert verarbeitet,

— Daten aus dem Patientenaufnahmeverfahren fließen in das Laborsystem und in das Verfahren Transfusionsdienst. Im Verfahren Transfusionsdienst werden neben Patientendaten auch Spenderdaten verarbeitet.

— Aus Daten des Patientenaufnahmeverfahrens wird auch das Verfahren Diagnosedokumentation nach der Bundespflegesatzverordnung gespeist. Daten aus der Diagnosedokumentation und der Patientenverwaltung werden in Form von Entlassungsanzeigen an die Krankenkassen übermittelt.

— Daten aus dem Patientenaufnahmeverfahren sind auch Grundlage für das in der DVZ der hamburgischen Verwaltung abgewickelte Leistungsabrechnungsverfahren.

Diese Daten sind in den Kliniken des UKE z.T. online verfügbar.

Die Prüfung hat Hinweise auf erhebliche Mängel hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen gegeben. Schwachstellen waren insb. die unzulängliche Gebäudesicherung, die unsichere Auslagerung von Datenträgern (Sicherungskopien), der Verzicht auf eine konsequente Funktionstrennung und fehlende Regelungen über Aufgaben, Zuständigkeiten und Verantwortlichkeiten.

Ein sicherer Rechenzentrumsbetrieb setzt eine strikte Trennung verschiedener Aufgaben voraus, um die Mißbrauchsmöglichkeiten für den einzelnen Mitarbeiter möglichst gering zu halten. Die Trennung der verschiedenen Funktionsbereiche war jedoch rechenzentrumsintern allenfalls ansatzweise gewährleistet: Zwar waren im Grundsatz bestimmte Zuständigkeiten für die Aufgaben der Programmierung, des Systemmanagements und des Operatings (Anlagenbedienung) vorgesehen, welche Befugnisse die jeweiligen Mitarbeiter haben, war jedoch nicht schriftlich fixiert. Die Prüfung hat ergeben, daß auch in der Praxis eine konsequente Trennung der Befugnisse unterbleibt.

Besonders gravierend ist das Fehlen entsprechender Regelungen für die Systemprogrammierer, die über die weitesten Zugriffsrechte verfügen. Auf unsere Anregung, eine Regelung entsprechend der für die Systemprogrammierung der DVZ zuständigen Mitarbeiter des Organisationsamtes geltenden Dienstanweisung (vgl. 2.1.3.3) auch für das RZ zu entwickeln, hat das UKE bislang nicht reagiert.

Obwohl in der Errichtungsanordnung des Instituts für Mathematik und Datenverarbeitung in der Medizin vorsieht, daß DV-Verfahren unter Beachtung der Richtlinien für die Organisation der automatisierten Informationsverarbeitung in der hamburgischen Verwaltung zu entwickeln sind, wurden die Freigaberichtlinie und die Dokumentationsrichtlinie nicht angewendet.

Auch war nicht geklärt, welche Stellen an der Entwicklung und Freigabe beteiligt werden müssen und welche Stellen für den Betrieb von Verfahren zuständig sind. Der Festlegung der Verfahrensverantwortung kommt deshalb besondere Bedeutung zu, weil allein die fachlich zuständige Stelle berechtigt ist, über die Verarbeitung und weitere Nutzung von personenbezogenen Daten zu entscheiden. Entgegen den Dokumentationsrichtlinien wird nicht dokumentiert, in welcher Weise, wann und durch wen Programme entwickelt, getestet und freigegeben wurden.

3.14 AIDS

3.14.1 Multizentrische Krankendokumentation von AIDS-Patienten

Unabhängig voneinander haben das Bundesarbeitsministerium und das Bundesgesundheitsministerium Dokumentationsprogramme zur Verarbeitung von AIDS-Patientendaten entwickeln lassen und ausgewählten Kliniken samt Computer zur Verfügung gestellt. In Hamburg sind das AK St. Georg und das Bernhard-Nocht-Institut damit ausgestattet worden.

Während das Programm KLIMACS, das von der Paul-Ehrlich-Gesellschaft in Frankfurt für das BMA entwickelt wurde, auf die Dokumentation ambulant behandelter Patienten zugeschnitten ist, sieht das Programm KLINAIDS des Bundesgesundheitsamtes die Verarbeitung von Patientendaten stationär behandelter HIV-Infizierter und -Kranker vor.

Mit Hilfe beider Dokumentationsprogramme wird die Erfassung, Speicherung und Auswertung äußerst sensibler medizinischer Daten - nicht nur über Krankheitsverläufe, sondern auch über Infektionswege und damit über die Zugehörigkeit zu Risikogruppen - ermöglicht. KLINAIDS sieht darüberhinaus Erhebungen über die sozialen Verhältnisse (Berufstätigkeit, Wohnsituation, Betreuung) und über die Risikogruppenzugehörigkeit des Sexualpartners vor.

Die Dokumentationsprogramme sollen einerseits den behandelnden Arzt bei der Betreuung des Patienten unterstützen, indem sie alle Befunddaten über den Krankheitsverlauf leicht und übersichtlich verfügbar machen, andererseits ist es erklärtes Ziel, die Daten für klinikinterne und für multizentrische Studien und für die Information der Auftraggeber BMA und BMJFFG nutzbar zu machen. An die Auftraggeber und andere Dritte sollen allerdings nur anonymisierte Daten herausgegeben werden.

Datenschutzrechtliche Probleme werfen die Dokumentationsprogramme im Hinblick auf die Rechtsgrundlage und auf Datensicherungsmaßnahmen auf. Rechtsgrundlage für die Datenverarbeitung im Arzt-Patienten-Verhältnis ist der Behandlungsvertrag. Auf ihn läßt sich eine Erhebung, Speicherung und Nutzung von Patientendaten aber nur insoweit stützen, als sie für Behandlungszwecke erforderlich ist. Da die Daten von den behandelnden Ärzten darüberhinaus zu Forschungszwecken genutzt werden sollen, die Forschung mit Patientendaten für Hamburg aber noch nicht gesetzlich geregelt ist, ist für diesen außerhalb des konkreten Behandlungsbezugs stehenden Verarbeitungszweck Einvernehmen mit dem Betroffenen herzustellen. Unter der Voraussetzung, daß die Patientendaten personenbezogen ausschließlich in der behandelnden Einheit zu Forschungszwecken genutzt werden und bei der Herausgabe an andere Stellen anonymisiert werden, ist im Vorgriff auf die zu erwartende Regelung im Hamburgischen Krankenhausgesetz die Anwendung der sog. „Widerspruchslösung" vertretbar. Danach ist der Patient über die geplante Datenverarbeitung, insbesondere über deren Zweck und über das Verfahren bei einer Datenübermittlung an Dritte zu informieren, und ihm ist Gelegenheit zum Widerspruch zu geben. Die Aufklärung ist vom Arzt zu dokumentieren. Einer schriftlichen Einwilligung des Patienten bedarf es in diesem Fall nicht.

Wenn der Patient der Verarbeitung seiner Daten widerspricht, darf er nicht in die automatisierte Krankendokumentation aufgenommen werden.

Diese Grundsätze gelten nur, soweit die Daten im Rahmen der üblichen Behandlung zu diagnostischen bzw. therapeutischen Zwecken erhoben werden. Werden darüberhinaus von dem Patienten Daten zu reinen Forschungszwecken erhoben, ist eine ausdrückliche, schriftliche Einwilligungserklärung nach Information des Patienten erforderlich. Dem Arzt obliegt in jedem Einzelfall die Prüfung, welche Daten aus dem umfangreichen Datenkatalog der Programme für Behandlungszwecke erhoben werden müssen. Beispielsweise ist nicht nachvollziehbar, warum zu Behandlungszwecken das Infektionsrisiko des Partners zu erheben ist.

Da die Krankendokumentation nicht nur dem einzelnen behandelnden Arzt, sondern der gesamten Abteilung zur Verfügung steht, ist insbesondere wegen der Zugriffsmög-

lichkeit auf die Daten außerhalb des konkreten Behandlungsbezugs eine getrennte Speicherung von Identifikationsmerkmalen und medizinischen Daten zu fordern. Dies kann durch die Chiffrierung der Daten in der Dokumentation, ggf. in Verbindung mit einer listenmäßigen Erfassung von Name und Chiffre oder durch die Speicherung von Identifikationsmerkmalen auf getrennten Datenträgern erfolgen.

Ich habe die betroffenen Klinikabteilungen gebeten, von der Paul-Ehrlich-Gesellschaft und dem Bundesgesundheitsamt, die den Kliniken die Dokumentationsprogrmme zum Einsatz anbieten, eine ordnungsgemäße Verfahrensdokumentation anzufordern, die es den für die Datenverarbeitung Verantwortlichen ermöglicht, den ordnungsgemäßen Einsatz des Programms zu überwachen. Hierzu gehören auch Aussagen zur Aufgabenstellung, zu den rechtlichen Grundlagen, zu Löschungsfristen und zu Datensicherungsmaßnahmen. Erforderlich ist auch die Klärung, zu welchem Zweck welche Daten an welche Stellen übermittelt werden sollen und ob die Benutzer der Programme zur Datenübermittlung verpflichtet sind.

Über konkrete Datensicherungsmaßnahmen der betroffenen Kliniken müssen weitere Gespräche nach Vorliegen der Dokumentation und unter Berücksichtigung der örtlichen Verhältnisse stattfinden.

3.14.2 HIV-Test im Krankenhaus

In meinem 7. Tätigkeitsbericht hatte ich kritisiert, daß das Verfahren zur Aufklärung und Einwilligung von Patienten vor Durchführung von HIV-Tests im Universitätskrankenhaus Eppendorf unzureichend geregelt ist. Der Senat hat in seiner Stellungnahme dazu erklärt, er erwäge, einheitliche Formulierungen für alle staatlichen Krankenhäuser zu entwickeln. Für den Landesbetrieb Krankenhäuser gilt seit 1. Juli 1988 eine Ergänzung zur Dienstanweisung über Aufklärung und Einwilligung, in der der Grundsatz festgeschrieben ist, daß vor jedem HIV-Test der Betroffene aufzuklären und seine ausdrückliche Einwilligung einzuholen ist. Um diesem Grundsatz auch im Universitätskrankenhaus Eppendorf Geltung zu verschaffen, habe ich mit der Behörde für Wissenschaft und Forschung und der Behörde für Arbeit, Gesundheit und Soziales Einvernehmen darüber erzielt, daß im Rahmen der für das UKE geltenden „Dienstanweisung über das Verfahren bei ärztlichen Eingriffen" vom 1.5.1977 folgendes klargestellt wird:

Der HIV-Test ist ein Eingriff im Sinne der Dienstanweisung, der nur nach Aufklärung und Einwilligung des Patienten vorgenommen werden darf. Aufzuklären ist nicht nur über den technischen Eingriff (Venenpunktion), sondern zugleich über Wesen, Bedeutung und Tragweite des HIV-Tests. Der Test darf nicht im Rahmen der routinemäßigen Diagnostik durchgeführt werden, sondern nur, wenn er im Einzelfall erforderlich ist. Der Patient ist über das Testergebnis zu unterrichten.

3.14.3 HIV-Test im Strafvollzug

Bei Antritt des Strafvollzugs wird dem Gefangenen mit der Zugangsuntersuchung auch ein HIV-Test angeboten, der zwar auf freiwilliger Grundlage durchgeführt, von der Anstalt aber dringend empfohlen wird. Im Rahmen meiner Stellungnahme zum Landesprogramm AIDS hatte ich zu überprüfen, ob bei dem Testverfahren dem informationellen Selbstbestimmungsrecht des Gefangenen Rechnung getragen wird.

Für die Zulässigkeit des HIV-Tests im Strafvollzug gilt der gleiche Grundsatz wie für Krankenhäuser, Beratungsstellen und niedergelassene Ärzte: Vor dem Test muß der Betroffene umfassend über den Zweck des Tests und über Bedeutung und Tragweite des Testergebnisses aufgeklärt werden und mit der Durchführung des Tests einverstanden sein. Wenn der Test, wie im Strafvollzug, überwiegend im Interesse und zum Schutz Dritter durchgeführt werden soll, ist eine ausdrückliche, schriftlich erteilte Einwilligung erforderlich. Die Mitteilung des Testergebnisses an Dritte ist nur mit Einwilligung des Betroffenen oder bei Vorliegen besonderer Rechtfertigungsgründe, z.B. unter den Voraussetzungen des rechtfertigenden Notstands, zulässig.

Meine Prüfung führte zu dem Ergebnis, daß das Selbstbestimmungsrecht des Gefangenen bei Einholung der Einwilligung und bei der Entscheidung über die Information Dritter nicht genügend beachtet wurde. Zwar informierte die Vollzugsanstalt vor der Untersuchung mit einem Merkblatt über Gefahren und Übertragungswege einer HIV-Infektion und über das Testangebot, eine ausdrückliche Entscheidung über die Durchführung des Tests war aber nicht vorgesehen. Dem Gefangenen wurde lediglich auf einem Laufzettel zur Kenntnis gegeben, daß neben anderen Untersuchungen auch ein HIV-Test „auf freiwilliger Grundlage" durchgeführt werde. Über die Offenbarung eines positiven Testergebnisses an den Anstaltsleiter und sonstiges Anstaltspersonal wurde der Gefangene erst bei Mitteilung des Ergebnisses aufgeklärt.

Zur Wahrung der Rechte der Gefangenen habe ich mit der Justizbehörde vereinbart, daß vor der Untersuchung ein Merkblatt zur allgemeinen Information ausgeteilt wird und der Gefangene anschließend auf dem neugestalteten Laufzettel ankreuzen kann, ob er den Test wünscht, nicht wünscht oder vor einer Entscheidung näher persönlich beraten werden möchte. Die Blutprobe wird erst dann zur Untersuchung eingeschickt, wenn der Gefangene, ggf. nach Beratung, ausdrücklich der Durchführung des Tests zugestimmt hat.

Daß der Anstaltsleiter über ein positives Testergebnis informiert wird, erfährt der Gefangene nun bereits aus dem Merkblatt, so daß er diesen Umstand in die Entscheidung über den Test einbeziehen kann. Die regelmäßige Information des Anstaltsleiters ist nach Ansicht der Justizbehörde erforderlich, da die Anstaltsärzte außerstande sind, eine mögliche Gefährdung Dritter durch den Gefangenen abzuschätzen. Über den Anstaltsleiter hinaus werden im Regelfall Mitarbeiter der Vollzugsanstalt oder andere Personen nur mit Einverständnis des Gefangenen informiert. Nur unter den engen Voraussetzungen eines besonderen Rechtfertigungsgrundes, etwa § 34 StGB, ist eine Information gegen den Willen des Betroffenen zulässig, um einer Gefährdung des Gefangenen selbst oder Dritter entgegenzuwirken. Dagegen ist aus § 154 Abs. 1 Strafvollzugsgesetz, wonach alle im Vollzug Tätigen eng zusammenarbeiten und daran mitwirken, die Aufgaben des Vollzugs zu erfüllen, keine Offenbarungsbefugnis über ein positives Testergebnis herzuleiten. Auch bei Einhaltung der Schweigepflicht ist es allerdings in der Praxis kaum vermeidbar, daß Dritte aus bestimmten Umständen (Unterbringung des Gefangenen in einer Einzelzelle mit Fernsehapparat, Ausführung zu Untersuchungen im Bernhard-Nocht-Institut) Rückschlüsse auf eine HIV-Infektion ziehen.

3.15 Bau- und Bebauungslückendatei

Seit Mai 1988 habe ich mit der Baubehörde die Frage diskutiert, ob und unter welchen Voraussetzungen die Speicherung personenbezogener Daten in einer Bau- und Bebauungslückendatei rechtlich zulässig ist:

Eine spezielle Rechtsvorschrift für die Einrichtung einer Bau- und Bebauungslückendatei ist nicht vorhanden. Meine Anregung, vor der Einrichtung der Datei die Betroffenen über den Zweck und die beabsichtigte Nutzung der Datei aufzuklären und ihre Einwilligung zur geplanten Datenverarbeitung einzuholen, hat die Baubehörde nicht aufgegriffen.

Die Bau- und Bebauungslückendatei wäre demnach nur zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Baubehörde liegenden Aufgaben erforderlich wäre (§ 9 Abs. 1 HmbDSG).

Ich habe von der Baubehörde bisher trotz mehrfacher Nachfragen nur sehr allgemein gehaltene Aussagen darüber erhalten, welche Aufgabe mit der Einrichtung dieser Datei erfüllt werden soll. Im wesentlichen wird auf die Ziele der wohnungspolitischen Beschlüsse der Koalitionsvereinbarung verwiesen und darauf, daß nur die Zusammenfassung nicht oder nicht vollständig entsprechend den bauplanerischen Vorgaben genutzter Flächen in einer Datei es ermögliche, „die versteckten Flächenpotentiale festzustellen und rational zu nutzen".

Meiner Bitte, mir mitzuteilen, welche konkrete Aufgabe mit dieser Datei erfüllt werden soll, wie diese Datei genutzt werden soll und inwieweit diese Nutzung geeignet und erforderlich ist, die zu erfüllende Aufgabe zu unterstützen, ist die Baubehörde bisher nicht nachgekommen. Sollte die Baubehörde auch weiterhin dazu nicht in der Lage sein, wäre sie verpflichtet, die in der Datei gespeicherten personenbezogenen Daten zu löschen (§ 15 Abs. 3 HmbDSG). Dies habe ich der Baubehörde mit Schreiben vom 15. November 1989 mitgeteilt.

Nachtrag:

Kurz vor Redaktionsschluß habe ich eine Nachricht von der Baubehörde erhalten, in der sie mir mitteilt, für welche - rechtlich zulässige - Aufgabe die Datei künftig genutzt werden soll:

Wegen der aktuellen Situation auf dem Hamburger Wohnungsmarkt sei es dringend erforderlich, alle Möglichkeiten zur Ausschöpfung des Flächenpotentials zu nutzen, um die erforderlichen Wohnungsbauprogramme des Senats umzusetzen. Die Baubehörde werde auf der Grundlage von § 175 Baugesetzbuch die Eigentümer der in der Datei erfaßten Grundstücke über die Zielsetzungen der Stadt informieren, sie beraten und auf die bestehenden Finanzierungsmöglichkeiten aus öffentlichen Kassen hinweisen, um auf eine Bebauung mit Wohnhäusern hinzuwirken. Äußerstenfalls würden Eigentümer verpflichtet, ihr Grundstück entsprechend den Festsetzungen des Bebauungsplanes zu bebauen oder ein vorhandenes Gebäude oder eine vorhandene sonstige bauliche Anlage den Festsetzungen des Bebauungsplanes anzupassen (§ 176 BauGB).

Da die in Rede stehenden Wohnungsbauprogramme des Senats bei Einrichtung der Datei noch nicht beschlossen waren, bleibt offen, ob die Verarbeitung der Daten in der Vergangenheit zulässig war. Immerhin hat die Baubehörde aber jetzt dargelegt, daß die Datei in Zukunft zur Erfüllung einer gesetzlichen Aufgabe - letztlich dem Erlaß von Baugeboten gem. § 176 BauGB - erforderlich ist.

4. EINZELNE PROBLEME DES DATENSCHUTZES IM NICHT-ÖFFENTLICHEN BEREICH

4.1 Kreditwirtschaft/SCHUFA

Die Wettbewerbssituation im Kreditgewerbe wird gegenwärtig von zwei neueren Phänomenen überlagert. Zum einen nimmt die Tendenz zu, daß nicht nur die Unternehmen, sondern auch die privaten Verbraucher im Ausland Kredite aufnehmen. Zum anderen bieten ausländische Kreditinstitute über Kreditvermittler oder andere „Repräsentanzen" auf dem nationalen Markt DM-Kredite an. Deshalb besteht seitens ausländischer Kreditinstitute ein starkes Interesse, von der SCHUFA eine Auskunft über die Bonität des deutschen Kreditnehmers zu erhalten. Häufig wird zur Kompensation der fehlenden SCHUFA-Anfragemöglichkeit die Kreditvergabe an die Beibringung einer SCHUFA-Selbstauskunft geknüpft. Dies wiederum liegt nicht im Interesse der SCHUFA. Aus diesen Gründen verstärkt die SCHUFA ihre Bemühungen um internationale Zusammenarbeit. Dies führt zu einer Reihe datenschutzrechtlicher Probleme.

Beispielsweise beschwerte sich bei mir ein Petent darüber, daß die SCHUFA in Hamburg über ihn Informationen gespeichert hatte, die seine Kreditaufnahme bei einem österreichischen Bankhaus betrafen. Dieses hatte die Kreditdaten des Betroffenen (Art des Kredites, Höhe der Kreditsumme, Ratenanzahl und Fälligkeit) an den Kreditschutzverband Wien übermittelt, der die Daten seinerseits an die Hamburger SCHUFA weitergegeben hatte. Der Petent hatte in seinem Darlehensvertrag eine Klausel unterzeichnet, in der er sich pauschal damit einverstanden erklärte, daß alle ihn betreffenden und im Rahmen des Kreditverhältnisses bekannt werdenden Daten in banküblicher Form, insbesondere im Interesse des Gläubigerschutzes oder zur Abwicklung von Bankgeschäften, weitergegeben werden können.

Ich habe der SCHUFA mitgeteilt, daß ich das Löschungsbegehren des Petenten für gerechtfertigt halte. Dabei waren für mich die folgenden Erwägungen ausschlaggebend:

Nach § 35 Abs.3 Satz 2 BDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig war. § 32 Abs.1 BDSG deckt die Speicherung bei der SCHUFA nicht. Eine Beeinträchtigung schutzwürdiger Belange im Sinne dieser Vorschrift ist immer dann anzunehmen, wenn die der Speicherung vorangegangenen Datenübermittlungen unzulässig waren. Dieses wiederum ergibt sich aus dem 1978 in Kraft getretenen österreichischen Datenschutzgesetz, das Beurteilungsmaßstab für die Übermittlung des österreichischen Bankhauses an den österreichischen Kreditschutzverband und für die sich anschließende Übermittlung des Verbandes an die SCHUFA ist.

§ 18 des österreichischen Datenschutzgesetzes stellt an eine gültige Einwilligung eher noch strengere Anforderungen als § 3 BDSG. Danach kann eine Datenübermittlung nur dann auf eine Einwilligung gestützt werden, wenn der Betroffene der Übermittlung ausdrücklich schriftlich zugestimmt hat, wobei ein schriftlicher Widerruf dieser Zustimmung möglich ist. Die spezifizierte Beschreibung der Datenübermittlung nach Art der Daten, Anlaß und Empfänger der Übermittlung ist nach österreichischem (wie auch nach deutschem) Recht Voraussetzung einer gültigen Einwilligung. Im konkreten Fall hatte der Betroffene sicherlich nicht „ausdrücklich" eingewilligt, weil die entsprechende Vertragsklausel dazu viel zu unbestimmt war. Die dort verwendetete Formulierung entspricht aber der alten SCHUFA-Klausel, die der Bundesgerichtshof im Urteil vom 19.9.1985 für nichtig erklärt hat und die daraufhin für die bundesrepublikanische Praxis durch eine neue ersetzt worden ist.

Die Übermittlung des österreichischen Kreditschutzverbandes an die SCHUFA gehörte auch nicht „zum berechtigten Zweck des Rechtsträgers" im Sinne von Nr.2 der Vorschrift. Nach der Satzung des österreichischen Verbandes hat er die Aufgabe, die Vermögenswerte von Mitgliedern, nicht aber von sonstigen juristischen Personen zu schützen. Werden Daten an Nicht-Mitglieder, wie z.B. an die SCHUFA, übermittelt, so

liegt darin eine nach österreichischem Recht unzulässige Zweckänderung der für die Übermittlung an Mitglieder erhobenen Daten.

Schließlich konnte auch nicht die dritte Alternative des § 18 des österreichischen Datenschutzgesetzes die Übermittlung sicher stützen. Danach müßten die berechtigten Interessen eines Dritten die Belange des Betroffenen überwiegen. In Anbetracht des Protestes der Betroffenen halte ich es für außerordentlich problematisch, davon auszugehen, daß deren Belange geringer zu bewerten seien, als das Interesse deutscher Kreditinstitute, ein möglichst vollständiges Bild über die Verschuldung des Kunden zu erhalten.

Meine Ansicht wird von der österreichischen Datenschutzkommission geteilt, die ich um eine Stellungnahme zu den aufgeworfenen Fragen gebeten habe. Die Daten des Petenten wurden auf Veranlassung des österreichischen Kreditinstitutes bei der SCHUFA gelöscht, wobei diesem jedoch „als Ersatz" die Auflage gemacht wurde, in regelmäßigen Abständen eine Selbstauskunft vorzulegen. Ferner ist die BUNDES-SCHUFA bestrebt, sicherzustellen, daß für alle künfigen österreichischen Kreditverträge, in deren Verlauf auch Daten an die SCHUFA übermittelt werden sollen, die deutsche SCHUFA-Klausel zu verwenden ist. Ob damit allerdings sämtliche Probleme des grenzüberschreitenden Datentransfers gelöst sind, wage ich zu bezweifeln. Dies wäre nur dann anzunehmen, wenn die SCHUFA-Klausel als eine umfassende Einwilligung gewertet werden dürfte, aufgrund derer die gesamte Datenverarbeitung der SCHUFA nach § 3 BDSG erlaubt wäre. So aber ist es nicht.

Die SCHUFA-Klausel für Kreditanträge hat aufgrund des BGH-Urteils vom 19.9.1985 eine Fassung erhalten, nach der sie zwar bezüglich der Positivmerkmale eine Einwilligung darstellt, aber bezüglich der Negativmerkmale (wie z.B. Zwangsvollstreckung) lediglich als eine Unterrichtung über die gesetzlichen Voraussetzungen für die Übermittlung ausgestaltet ist (vgl. dazu 5. TB, 6.4.1, S. 108 ff). In jener Entscheidung erklärte das Gericht die seinerzeit verwandte SCHUFA-Klausel wegen Verstoßes gegen § 9 des Gesetzes zur Regelung des Rechts der allgemeinen Geschäftsbedingungen für nichtig. Ausschlagebend dafür war die Erwägung, daß eine pauschale Ermächtigung, auch negative Merkmale ohne Interessenabwägung im Einzelfall und sogar in den Fällen zu übermitteln, in denen eine Interessenabwägung negativ ausfallen würde, eine unangemessene Benachteiligung des Kunden bedeutet. Aufgrund dieser Rechtsprechung verbietet sich sowohl eine Interpretation der heutigen SCHUFA-Klausel als eine alle Datenübermittlungen umfassende Einwilligung als auch eine Neuformulierung der SCHUFA-Klausel mit dem Ziel, eine solche Einwilligung herbeizuführen.

Somit ist für den Datenexport aus der Bundesrepublik § 24 Abs.1 Satz 1 BDSG maßgeblich. Soweit sich die Zulässigkeit der Übermittlungen nicht daraus ergibt, daß sie im Rahmen eines Vertragsverhältnisses liegen, sind die schutzwürdigen Belange des Betroffenen mit den berechtigten Interessen der übrigen Beteiligten abzuwägen. Nach allgemeiner Auffassung besteht stets dann Grund zur Annahme, daß schutzwürdige Belange des Betroffenen beeinträchtigt sein können, wenn in dem ausländischen Staat, in den die Daten übermittelt werden sollen, kein dem Bundesdatenschutzgesetz gleichwertiger Schutz vorhanden ist.

Für den Datenimport ist u.a. das nationale Recht des Staates maßgeblich, das die Daten in die Bundesrepublik übermitteln will. Wie das Beispiel Österreich zeigt, können die ausländischen Gesetze durchaus schärfere Bestimmungen enthalten, als sie das deutsche Recht vorsieht (s. 4.5.5).

4.2 Versicherungswirtschaft

4.2.1 Zentrale Dateien der Versicherungswirtschaft

4.2.1.1 Strukturcodeverfahren

Die meisten zentralen Warn- und Hinweissysteme in der Versicherungswirtschaft beruhen inzwischen auf Verfahren, bei denen personenbezogene Daten mit Hilfe eines

sogenannten Matchcodes verschlüsselt und in diesem verschlüsselten Zustand vom Verband an andere Versicherungsunternehmen übermittelt werden. So ist z.B. für die Sparte der Unfallversicherer das folgende Verfahren geplant (vgl. dazu unten 4.2.1.4):

Die Unfallversicherer melden dem HUK-Verband Personendaten, die in das zentrale Warn- und Hinweissystem eingestellt werden sollen. Diese Meldungen werden beim HUK-Verband gesammelt. Vor Weitergabe an die Versicherungsunternehmen bildet der Verband einen Matchcode, der aus

— dem Nachnamen (die ersten fünf Stellen)

— der Postleitzahl (die ersten zwei Stellen)

— dem Geburtsdatum (sechs Stellen)

— der Geschlechtskennziffer (eine Stelle)

besteht. Der Matchcode wird ergänzt um die Angabe des meldenden Versicherers (VU-Nummer), des Aktenzeichens sowie der Telefonnummer der meldenden Abteilung. Die zusammengestellten Datensätze werden auf Magnetband gespeichert und an die dem Verfahren angeschlossenen Versicherungsunternehmen versandt. Diese erhalten so die Möglichkeit festzustellen, ob einzelne Matchcodes der Verbandsdatei auf die Daten der Personen zutreffen, die bei ihnen einen Versicherungsantrag gestellt haben oder bereits versichert sind. Fällt eine solche Prüfung positiv aus, kann sich der Sachbearbeiter zur weiteren Sachaufklärung mit dem Versicherungsunternehmen in Verbindung setzen, das die Daten eingemeldet hat. Auf diese Weise kann geklärt werden, ob die Personen tatsächlich identisch sind, und es können gegebenenfalls weitere Informationen vom meldenden Unternehmen erfragt werden.

Derartige Informationssysteme wurden lange Zeit betrieben, ohne die Datensätze zu verschlüsseln. Damit waren Übermittlungen gang und gäbe, die weit über das nach § 24 BDSG zulässige Maß hinausgingen. Erst aufgrund der Intervention der Aufsichtsbehörden wurden Matchcodes in die Verfahren integriert, um die Kenntnis über personenbezogene Angaben nicht weiter als unbedingt erforderlich zu streuen (vgl. z.B. 4.TB, 5.4.1, S. 128). Gleichwohl habe ich manche der Chiffrierungen kritisiert, da sie zum Teil so durchsichtig gestaltet sind, daß ein Blick ins Telefonbuch genügt, um einen „codierten" Datensatz zu deanonymisieren, vgl. z.B. 7.TB, 5.4.1.2, S. 135. Solche Matchcodes verfehlen ihren Sinn.

Die Versicherungswirtschaft plant, für alle zentralen Warnsysteme ein sogenanntes „phonetisches Strukturcodeverfahren" einzuführen. Dabei werden phonetisch ähnlich klingende Laute in die gleiche numerische Ziffernfolge umgesetzt. Bei diesem Verfahren erhalten z.B. die Nachnamen Bayer und Pfeiffer den gleichen Code. Bei einem Deanonymisierungsversuch ohne Zusatzwissen könnte dementsprechend nicht geklärt werden, ob Bayer oder Pfeiffer sich hinter dem Codeschlüssel verbergen. Gegenwärtig ist zwar noch nicht in allen Versicherungszweigen geklärt, welche personenbezogenen Angaben chiffriert werden sollen. Nach meinen jetzigen Informationen erscheint mir jedoch - ungeachtet der im einzelnen einbezogenen Adreßkomponenten - eine Reidentifizierung ohne Zusatzwissen annähernd ausgeschlossen zu sein. Damit weist dieser Code die datenschutzrechtlichen Mängel der bislang gebräuchlichen Codes nicht mehr auf und stellt einen befriedigenden Abschluß der langen und kontroversen Diskussion über Matchcodes in der Versicherungswirtschaft dar.

Klarstellen möchte ich, daß die Verwendung des Strukturcodeverfahrens dennoch nicht zu einer Suspendierung vom Bundesdatenschutzgesetz führt.

Die Daten verlieren nämlich aufgrund der Codierung nicht ihren Personenbezug. Zwar verfügt ein Verband, der von seinen Mitgliedsunternehmen Datensätze empfängt, diese codiert, zusammenstellt und die codierten Datensätze an die angeschlossenen Mitgliedsunternehmen verschickt, in der Regel nicht über das nötige Zusatzwissen, um die Datensätze wieder zu deanonymisieren. Für den Verband sind die Daten daher nicht personenbezogen. Das nötige Zusatzwissen ist jedoch bei den meldenden und den empfangenden Versicherungsunternehmen vorhanden. Die empfangenden Unter-

nehmen haben die Möglichkeit, durch Nachfrage beim meldenden Versicherungsunternehmen die Identität einer im Hinweisystem vorhandenen Person festzustellen.

Die dem Verband angeschlossenen Versicherungsunternehmen treffen dementsprechend die datenschutzrechtlichen Pflichten des 3. Abschnittes des BDSG. Daraus folgt, daß sie sich nur eines solchen Verfahrens bedienen dürfen, in dem z.B. sichergestellt ist, daß die Übermittlung personenbezogener Daten von einem (dem speichernden) Versicherungsunternehmen zu einem anderen (dem anfragenden) Versicherungsunternehmen zulässig ist. Sofern eine Einwilligung nicht vorliegt, kommt als Erlaubnistatbestand nur die 3. Alternative des § 24 Abs.1 Satz 1 BDSG in Betracht. Denn die Warnung anderer Unternehmen ist nicht von einem Versicherungsvertrag gedeckt. § 24 Abs.1 Satz 1 3.Alt. BDSG fordert, in jedem Einzelfall eine Interessenabwägung zwischen den schutzwürdigen Belangen des Betroffenen und den berechtigten Interessen der Versicherungswirtschaft vorzunehmen. Diese Vorschrift kann nur dann in der Praxis verwirklicht werden, wenn ein Betroffener die Gelegenheit erhält, seine Belange dem Versicherungsunternehmen zu unterbreiten, das ihn in ein Warnsystem einmelden will. Es muß also sichergestellt sein, daß die Betroffenen von der Speicherung in einem zentralen Warnsystem in zumutbarer Weise haben Kenntnis nehmen können. Außerdem muß kontrolliert werden, ob die vereinbarten Voraussetzungen für die Aufnahme in das Warnsystem von allen beteiligten Einzelversicherern eingehalten werden. Dies kann etwa dadurch erreicht werden, daß der Verband Stichprobenkontrollen durchführt.

4.2.1.2 Sachversicherer-Informationssystem

Im Berichtszeitraum konnten die Verhandlungen zwischen den Datenschutz-Aufsichtsbehörden und dem Verband der Sachversicherer (VdS) über die zentrale Sachschadendatei, das Sachversicherer-Informationssystem (SAVIS), zu einem erfolgreichen Abschluß geführt werden.

Das Verfahren läßt sich in groben Zügen folgendermaßen umreißen (vgl. auch 7.TB, 5.4.1.5, S. 146; 6.TB, 5.4.1.5, S. 136):

Zweck des Informationssystems ist es, Hinweise zur Risikobeurteilung und zur Abwehr unberechtigter Forderungen zu geben. Die einzelnen Sachversicherer melden dem Verband Schadensfälle, bei denen ein Schaden von mindestens DM 10.000,– eingetreten und der Versicherungsvertrag gekündigt worden ist, weil strafrechtliche (z.B. Einleitung eines Ermittlungsverfahrens) oder vertragsbezogene (z.B. Verschweigen von Vorverträgen oder -schäden, Obliegenheitsverletzungen im Versicherungsfall u.a.) Anhaltspunkte für unlauteres Verhalten vorliegen. Ferner werden alle Fälle von Brandstiftung erfaßt, sofern der Schaden größer als DM 10.000,– ist. Der Verband der Sachversicherer sammelt die - codierten - Datensätze. Das weitere Verfahren läuft ebenso wie das der Zentralen Registrierstelle Unfallversicherung (vgl. oben 4.2.1.1).

Zu den noch offenen Fragen gehörte die Speicherungsdauer. Sie soll nun, vom Zeitpunkt der Aufnahme in das Warnsystem an gerechnet, maximal 10 Jahre betragen, wobei generell nach Ablauf von 5 Jahren geprüft wird, ob die Voraussetzungen für eine weitere Speicherung noch vorliegen oder ob gelöscht werden muß.

Zunächst hatte man sich lediglich über das Verfahren bei Versicherungsnehmern und solchen Personen verständigen können, die mit diesen in engen wirtschaftlichen (z.B. Geschäftsführer eines versicherten Unternehmens) oder familiären Beziehungen stehen, vgl. hierzu 7.TB, 5.4.1.5, S. 146. Bislang ungelöst war die Behandlung sonstiger Dritter, also jener Personen, die diese Voraussetzungen nicht erfüllen (z.B. Zeugen oder Sachverständige in einem Versicherungsfall). Ihre Lage ist dadurch gekennzeichnet, daß sie in der Regel von ihrer Aufnahme in das Warnsystem keine Kenntnis besitzen. Für diese Gruppe konnte nunmehr die folgende Lösung gefunden werden:

— Personen, die zunächst dem Kreis der Verdächtigen bei einem meldepflichtigen Schaden zuzurechnen waren, bei denen aber ein strafrechtliches Ermittlungsverfahren zur Einstellung geführt hat, oder die vor Gericht freigesprochen worden sind,

werden nicht (länger) gespeichert. Einzige Ausnahme ist, daß gegen sie gleichwohl ein erheblicher Tatverdacht fortbesteht. Dann aber werden die Betroffenen davon unterrichtet.

— Auch solche Personen, die in einen nach den oben genannten Voraussetzungen meldepflichtigen Schaden verwickelt sind, gegen die aber das Versicherungsunternehmen trotz eines Betrugsverdachtes keine Strafanzeige erstattet hat (z.B. wegen einer aussichtslosen Beweissituation), dürfen nur gespeichert werden, wenn sie über die Speicherung in der zentralen Datei unterrichtet worden sind.

Einigkeit konnte darüber erzielt werden, daß eine qualifizierte Unterrichtung erforderlich ist, die den Betroffenen über die Aufnahme seiner Daten in das Hinweissystem des VdS informiert. Sie erfolgt, wenn das Ermittlungs- bzw. das Strafverfahren oder die Schadensregulierung abgeschlossen ist. Der VdS wird ein Formblatt dafür entwerfen und mit den Aufsichtsbehörden abstimmen.

Wenn es darum geht, daß die von einer Speicherung in einer Warndatei betroffenen Personen darüber in Kenntnis gesetzt werden sollen, bin ich immer wieder auf eine generell ablehnende Haltung der Versicherungswirtschaft gestoßen. Den Aufsichtsbehörden wird entgegengehalten, daß eine Benachrichtigung zu schweren Nachteilen für die Versicherungswirtschaft führen würde. Zum einen sei ein extrem hoher Verwaltungsaufwand zu befürchten, um die dann eingehenden Löschungs-, Sperrungs- oder Auskunftsverlangen zu bearbeiten, zum anderen würden die Benachrichtigten gewarnt und könnten ihr künftiges unlauteres Verhalten darauf einstellen. Damit würde letztlich der Zweck eines solchen Hinweissystems, dem Versicherungsbetrug vorzubeugen, in Frage gestellt.

Dies ist nach meiner Auffassung eine grundsätzlich falsche Sicht. Ein Hinweissystem, bei dem die Speicherung personenbezogener Daten nicht auf vagen und zudem subjektiven Wertungen beruht, sondern das nachprüfbare Tatsachen zur Voraussetzung hat, ist gegenüber Berichtigungs- und Sperrungs- oder Löschungsverlangen nach § 27 BDSG weitgehend immun. Dabei verkenne ich nicht, daß die Feststellung der Wahrheit in Einzelfällen auch einmal aufwendig sein kann. Der notwendige Verwaltungsaufwand dürfte im allgemeinen jedoch weit überschätzt werden und ist darüberhinaus kein akzeptables Argument, um von Datenschutzbestimmungen zu suspendieren. Im übrigen meine ich, daß die Kenntnis über die Aufnahme in ein Warnsystem eine heilsame, da abschreckende Wirkung auf potentielle Betrüger entfaltet und gerade dadurch zur Eindämmung der Flut von Straftaten zu Lasten der Versichertengemeinschaft geeignet ist. Um das Ziel der Verhütung von Straftaten zu Lasten der Versichertengemeinschaft zu erreichen, ist daher eine umfassende Aufklärung sowohl des individuell Betroffenen als auch der Öffentlichkeit dringend zu empfehlen.

4.2.1.3 Zentrale Registrierstelle Rechtsschutz

Im Berichtszeitraum erreichten mich mehrere Eingaben von Personen, die sich darüber beschwerten, in die beim HUK-Verband geführte Zentrale Registrierstelle Rechtsschutz gemeldet worden zu sein. In dieses Hinweissystem sollen Personen aufgenommen werden, deren Rechtsschutzversicherungsvertrag vom Versicherungsunternehmen gekündigt wurde, weil in einem Kalenderjahr mindestens zwei Versicherungsfälle aufgetreten sind. § 19 Abs.2 der Allgemeinen Bedingungen für die Rechtsschutzversicherung (ARB) eröffnet dem Versicherungsunternehmen in diesen Fällen die Möglichkeit, sich vom Vertrag zu lösen. Mit der Aufsichtsbehörde ist abgestimmt, daß in solchen Fällen das kündigende Versicherungsunternehmen zugleich auch bestimmte Daten der betroffenen Person an den HUK-Verband melden darf. Zweck ist es, für andere Rechtsschutzversicherer bei der Bearbeitung eines Versicherungsantrages einen Hinweis darauf zu geben, daß die antragstellende Person möglicherweise ein besonderes Risiko für einen Rechtsschutzversicherer darstellt.

In einigen Eingaben war der Vertrag nicht nach § 19 Abs.2 ARB außerordentlich gekündigt, sondern nach Ablauf der vorgesehenen Laufzeit nicht verlängert worden, soge-

nannte Ablaufkündigung nach § 8 ARB. Dadurch entstanden zunächst einige Irritationen. Nunmehr aber ist klargestellt, daß eine Meldung an den Verband stets dann erfolgen darf, wenn die materiellen Voraussetzungen des § 19 Abs.2 ARB vorliegen. Es kommt also nicht darauf an, ob der Vertrag durch außerordentliche oder durch ordentliche Kündigung beendet worden ist, sondern nur darauf, ob mindestens zwei Versicherungsfälle in einem Kalenderjahr aufgetreten sind.

4.2.1.4 Zentrale Registrierstelle Unfallversicherung

Der HUK-Verband hat im Frühjahr dieses Jahres mit mir Kontakt aufgenommen, um ein von ihm geplantes neues Warn- und Hinweissystem für die Unfallversicherungen - die Zentrale Registrierstelle Unfallversicherung - abzustimmen. Durch die frühzeitige Beteiligung der Aufsichtsbehörde konnte ein offener und daher konstruktiver Dialog geführt werden. Dieses Verfahren hat nunmehr folgende Gestalt angenommen:

Meldungen dürfen nur aus den folgenden drei Gründen vorgenommen werden:

a) Bei erheblicher Verletzung der vorvertraglichen Anzeigepflicht, wenn also ein Antragsteller unwahre oder unvollständige Angaben macht. Die Verletzung der Anzeigepflicht ist dabei nur dann erheblich, wenn der Versicherer aus diesem Grund den Antrag abgelehnt, den Vertrag angefochten hat oder vom Vertrag zurückgetreten ist.

b) Bei Leistungsablehnung wegen vorsätzlicher Obliegenheitsverletzung im Schadensfall, wegen Vortäuschung eines Unfalles oder von Unfallfolgen. Eine solche Obliegenheitsverletzung berechtigt nur dann zur Leistungsablehnung und damit auch zur Meldung an die Zentrale Registrierstelle Unfallversicherung, wenn sie generell geeignet war, die berechtigten Interessen des Versicherers ernsthaft zu gefährden.

c) Bei einer außerordentlichen Kündigung durch den Versicherer gemäß § 7 II (2) AUB 61 bzw. § 4 II (2) AUB 88, also aus Anlaß eines Schadensfalles. In dieser Gruppe sind auch Personen enthalten, die ohne ihr Verschulden ein besonderers Risiko für eine Unfallversicherung darstellen (sog. „Unfaller").

Aus welchem der oben genannten Anlässe die Meldung erfolgt, wird jeweils gekennzeichnet. Das sich anschließende weitere Verfahren habe ich bereits oben zur Illustration der Funktionsweise eines Matchcodes beschrieben (siehe 4.2.1.1).

Ein besonderer Schwerpunkt in den Verhandlungen lag darin, die Tatbestände zu präzisieren, die zu einer Meldung berechtigen sollen. So war zunächst seitens des HUK-Verbandes nicht geklärt, ob auch Personen eingemeldet werden sollen, bei denen kein Verdacht auf betrügerisches Verhalten vorliegt. Nunmehr hat der Verband beschlossen, auch solche Personen, die unverschuldet ein besonderes Risiko für einen Unfallversicherer darstellen, unter Punkt c. in das Warnsystem aufzunehmen.

Damit ergibt sich folgende Zweiteilung der zur Meldung berechtigenden Tatbestände:

Den Meldungen nach Punkt a. oder b. liegt unlauteres Verhalten der Versicherungsnehmer zugrunde. Bei ihnen ist zu besorgen, daß sie sich möglicherweise auch in Zukunft unkorrekt verhalten werden. Andere Versicherer sollen vor ihnen gewarnt werden, um bei einem neuen Schadensfall die Hintergründe eingehend überprüfen zu können. Insoweit ist die Zentrale Registrierstelle Unfallversicherung eine Verdächtigendatei.

Demgegenüber kann den Personen, die wegen Grund c. eingemeldet werden, in der Regel kein Vorwurf wegen ihres Verhaltens gemacht werden. Sie stellen z.B. aus gesundheitlichen Gründen ein besonderes Risiko dar. Insoweit verfolgt die Registrierstelle den Zweck, bei Vertragsanbahnung das einzugehende Risiko besser abschätzen und gegebenenfalls durch besondere Prämienvereinbarungen abfangen zu können.

In Abstimmung mit den anderen Aufsichtsbehörden bin ich der Ansicht, daß Speicherung und Übermittlung von Datensätzen beider Personengruppen datenschutzrecht-

lich zulässig sind. In beiden Fallgruppen erkenne ich das berechtigte Interesse der Unfallversicherer an und bewerte die schutzwürdigen Belange der Betroffenen nicht als überwiegend. Ausschlaggebend dafür ist, daß nicht vage, subjektive Erwägungen Anlaß für eine Meldung sein sollen, sondern nur solche Fälle erfaßt werden, in denen der Vertrag entweder gelöst (Punkt a. und c.) oder die Erbringung einer Leistung abgelehnt worden ist (Punkt b). Dadurch ist eine Meldung in die Zentrale Registrierstelle mit einer wirtschaftlichen Entscheidung verknüpft, die im Regelfall von einem Versicherer nur ungern getroffen wird, da damit ein Kunde verlorengehen dürfte. Auf der anderen Seite werden mit Hilfe der Warndatei nur Angaben überprüft, die nach dem Versicherungsvertragsgesetz ohnehin - sei es bei Vertragsanbahnung oder im Schadensfall - wahrheitsgemäß gemacht werden müssen.

Ferner war sicherzustellen, daß die Betroffenen von dem neuen Hinweissystem auch Kenntnis erhalten. Im Gegensatz zu dem Warnsystem der Sachversicherer ist hier jedoch die Ausgangssituation wesentlich einfacher. Es sollen lediglich solche Personen gespeichert werden, die entweder Versicherungsnehmer sind oder zumindest einen Antrag auf Abschluß eines Versicherungsvertrages gestellt haben. Dieser Personenkreis kann schon bei Antragstellung umfassend aufgeklärt werden. Um dies zu erreichen, sind in das Merkblatt zur Datenverarbeitung (siehe unten 4.2.2) Erläuterungen eingearbeitet worden, die eine exakte Beschreibung der Voraussetzungen für eine Aufnahme in die Warndatei darstellen.

Die Speicherungsdauer soll 10 Jahre betragen, wobei (in Anlehnung an das Verfahren der Sachversicherer) nach 5 Jahren geprüft wird, ob die Notwendigkeit weiterer Speicherung fortbesteht.

Die in meinen Tätigkeitsberichten bereits des öfteren behandelten Ermittlungsrundschreiben, vgl. 7.TB, 5.4.1.4, S. 145; 6.TB, 5.4.1.1, S. 131, sollen parallel zur Zentralen Registrierstelle Unfallversicherung fortgeführt werden. Ich habe dies aufgrund der unterschiedlichen Zweckbestimmungen beider Verfahren akzeptiert. Die Ermittlungsrundschreiben sollen es einem Versicherungsunternehmen ermöglichen, einem aktuellen Verdacht auf verschwiegene Mehrfachversicherungen oder auf manipulierte Schadensfälle nachzugehen. Mit der Zentralen Registrierstelle Unfallversicherung sollen (auch ohne Anfangsverdacht) Hinweise darauf gegeben werden, ob es Grund zur besonderen Vorsicht gibt.

4.2.1.5 Kfz-Dateien

Im Berichtszeitraum wurden die Gespräche über die Kfz-Dateien des HUK-Verbandes fortgeführt, vgl. dazu 7.TB, 5.4.1.3, S. 136 ff.

Der HUK-Verband sagte zu, die Kfz-Dateien einer grundsätzlichen Revision zu unterziehen. Ich gehe davon aus, daß der Verband mir in naher Zukunft ein neues Konzept vorstellen wird.

4.2.2 Schweigepflicht-Entbindungsklauseln und Einwilligungsklausel nach dem BDSG

Über die Schweigepflicht-Entbindungsklauseln in der Lebens-, Kranken- und Unfallversicherung sowie über die Einwilligungsklausel nach dem BDSG und das dazugehörige Merkblatt zur Datenverarbeitung, in dem unter anderem die Datenflüsse zu Rückversicherern und die Funktionsweise der zentralen Warnsysteme näher erläutert werden, habe ich ausführlich in meinem letzten Tätigkeitsbericht referiert (7.TB, 5.4.2, S. 150 und 5.4.3, S. 151).

Danach wurden noch verschiedene Änderungen erforderlich, um beispielsweise die Zentralen Registrierstellen zur Rechtsschutz- und Unfallversicherung richtig und vollständig im Merkblatt zu beschreiben. Deshalb hat sich die Einführung der neuen Klauseln in die Vertragspraxis der Versicherungsunternehmen verzögert. Das Bundesaufsichtsamt für das Versicherungswesen (BAV) hat aber inzwischen die Klauseln zur Entbindung von der ärztlichen Schweigepflicht genehmigt und im November 1989 in seinen amtlichen „Veröffentlichungen des Bundesaufsichtsamtes für den Versicherungsdienst" - VerBAV - bekanntgemacht. Die Klausel zur Einwilligung in die Datenverarbei-

tung nach § 3 BDSG und das dazugehörige Merkblatt sollen im Januarheft 1990 abgedruckt werden. Das BAV wird den Versicherungsunternehmen eine Frist bis Mitte des Jahres 1990 setzen, um alte Druckstücke aufzubrauchen.

4.2.3 Datenverarbeitung selbständiger Versicherungsagenturen

Im Berichtszeitraum bin ich aufgefordert worden, mich zu einer Meinungsverschiedenheit zu äußern, die zwischen Versicherungsunternehmen einerseits und den von ihnen beauftragten selbständigen Versicherungsvertretern andererseits besteht.

Dem liegt der folgende Sachverhalt zugrunde:

Versicherungsunternehmen bedienen sich zur Betreuung ihrer Versicherungsnehmer und zur Anwerbung neuer Kunden häufig eines Versicherungsaußendienstes, in dem nicht nur Arbeitnehmer beschäftigt sind, sondern auch selbständige Gewerbetreibende, die rechtlich als Handelsvertreter im Sinne des § 84 HGB einzuordnen sind. Sie können lediglich für ein Unternehmen (Einfirmenvertreter) oder auch für mehrere (Mehrfirmenvertreter) tätig sein. Einige Versicherungsunternehmen lassen von diesen Vertretern sogenannte Kundeninformationsblätter anlegen. Dazu werden von den Unternehmen unterschiedliche Vordrucke ausgegeben, die in aller Regel der Vertreter aufgrund seiner Kenntnisse über die persönlichen Verhältnisse der Versicherungsnehmer ausfüllt. Die Informationen dienen dem Zweck, gezielte Werbemaßnahmen ergreifen und außerdem regelmäßig auf eine Anpassung bestehender Verträge hinwirken zu können. Die Angaben betreffen z.B. das geschätzte Jahreseinkommen, den Familienstand, die Anzahl der Kinder, Anzahl und Art der zum Haushalt gehörenden Pkw, Mitgliedschaft in Vereinen sowie dortige Aktivitäten und manches andere mehr; sie werden hier als Akquisitionsdaten bezeichnet. Die Betroffenen werden in aller Regel an diesen Datenerhebungen nicht beteiligt. Sie wissen meistens nicht einmal, daß solche Daten über sie gesammelt werden.

Versicherungsunternehmen und Vertreter streiten darüber, welche Daten als Vertrags- und welche als Akquisitionsdaten zu qualifizieren sind und wem die hier als Akquisitionsdaten bezeichneten Informationen zustehen. Dabei werden schon deshalb unterschiedliche Ergebnisse erzielt, weil die Versicherungswirtschaft alle Daten, die zur Feststellung eines Versicherungsbedarfs notwendig sind, zu den Vertragsdaten rechnet. Daraus wiederum wird geschlossen, daß deren Übermittlung an das vertragschließende Versicherungsunternehmen im Rahmen der Zweckbestimmung des Versicherungsvertrages liegt und folglich nach § 24 Abs.1 Satz 1 1.Alt. BDSG zulässig ist.

Nach der Gegenposition des Bundesverbandes der Versicherungs-Kaufleute e.V. (BVK) ist dies nicht der Fall. Es wird sogar befürchtet, daß Versicherungsvertreter sich wegen unbefugter Datenübermittlung strafbar machen könnten.

Ich habe dazu wie folgt Stellung bezogen:

Die Speicherung und Übermittlung von Kundendaten ist zulässig, wenn der Kunde wirksam eingewilligt hat oder die Voraussetzungen der §§ 23, 24 BDSG vorliegen.

Unproblematisch ist danach Speicherung und Übermittlung von Vertragsdaten. Dies sind nach meiner Auffassung Informationen, die zum Abschluß und zur Durchführung eines konkreten Versicherungsvertrages vom Versicherungsunternehmen benötigt werden. Hierin hat der Kunde in der Regel eingewilligt. Darüberhinaus liegen Speicherung bzw. Übermittlung gemäß § 23 Satz 1 bzw. § 24 Abs. 1 Satz 1, jeweils 1. Alt. BDSG im Rahmen der Zweckbestimmung des Versicherungsvertrages.

Problematisch hingegen ist die Speicherung (und die Übermittlung) von den hier als Akquisitionsdaten bezeichneten Angaben. Dazu gehören beispielsweise Angaben zum Wert des Hausrats, wenn und soweit der Betroffene lediglich eine Kfz-Haftpflicht-Versicherung abgeschlossen hat.

Es liegt keine Einwilligung vor. Deshalb ist die Speicherung nur erlaubt, wenn gemäß § 23 Satz 1 3. Alt. BDSG kein Grund zur Annahme besteht, daß dadurch schutzwürdige

Belange des Betroffenen beeinträchtigt werden. Dieser Erlaubnistatbestand ist erfüllt, wenn die berechtigten Interessen der speichernden Stelle gegenüber entgegenstehenden schutzwürdigen Belangen des Betroffenen überwiegen. Abzuwägen ist danach das Interesse der Versicherungsvertreter, auch solche Daten vorzuhalten, die künftige Akquisitionen erleichtern, mit dem Interesse des Betroffenen, persönliche Verhältnisse möglichst nicht zur geschäftlichen Verwertung freizugeben. Die Belange der betroffenen Kunden gewinnen mit zunehmender Sensibilität der Daten an Gewicht. Soweit es sich bei den Akquisitionsdaten z.B. um Angaben über Gesundheit, persönliche Gewohnheiten oder Einkommensverhältnisse handelt, ist die Annahme einer Beeinträchtigung schutzwürdiger Belange grundsätzlich gerechtfertigt. Lediglich soweit es sich um offenkundige Daten handelt, z.B. ob der Kunde ein Einfamilienhaus bewohnt, sind keine entgegenstehenden schutzwürdigen Belange erkennbar.

Daraus ziehe ich die Schlußfolgerung, daß die (geheime) Sammlung und Speicherung von Angaben über persönliche Verhältnisse der Kunden weitgehend unzulässig ist, ohne daß es darauf ankommt, ob diese Angaben beim Versicherungvertreter oder beim Versicherungsunternehmen gespeichert werden. Beide Stellen sind nach § 27 Abs. 3 Satz 2 BDSG zur Löschung verpflichtet.

Ich habe den Beteiligten empfohlen, eine Einwilligung von den Betroffenen einzuholen, und hinzugefügt, daß eine wirksame Einwilligung nur dann vorliegt, wenn der Einwilligende seine Angaben in voller Kenntnis der beabsichtigten Verwendung macht. Ihm muß bei der Erhebung klar sein, daß bestimmte Angaben nicht verlangt werden, um seinen derzeitigen Versicherungsbestand abzuwickeln, sondern lediglich der Akquisition des Vertreters dienen sollen. Ferner sollte deutlich gemacht werden, ob der Versicherungsvertreter die Daten letztlich für seinen eigenen Geschäftsbetrieb sammelt (so insbesondere häufig der Mehrfirmenvertreter) oder ob das Versicherungsunternehmen - unabhängig von dem gegenwärtig tätigen Versicherungsvertreter - die Angaben erhält.

Die streitige Frage nach der Herausgabepflicht habe ich darauf aufbauend wie folgt beantwortet:

Der Vertrag zwischen Vertreter und Versicherungsunternehmen, der den Rahmen für die Vermittlung einzelner Versicherungsverträge darstellt, ist als Geschäftsbesorgungsvertrag im Sinne des § 675 BGB einzuordnen. Der Umfang des Herausgabeanspruches bestimmt sich nach der darin getroffenen vertraglichen Regelung. Die Vertragsparteien sind frei, die Akquisitionsdaten in den Herausgabeanspruch einzubeziehen oder sie davon auszunehmen.

Aus der vorangegangenen datenschutzrechtlichen Bewertung zur Zulässigkeit der Speicherung ergibt sich allerdings die folgende Konsequenz:

Personenbezogene Daten, deren Speicherung nach § 23 BDSG unzulässig ist, dürfen auch nicht übermittelt werden. Insoweit stehen stets schutzwürdige Belange im Sinne von § 24 Abs.1 Satz 1, 3.Alt. BDSG entgegen. Dann ist die Übermittlung verboten. Eine Vertragsklausel, die einen Versicherungsvertreter gleichwohl zur Übermittlung verpflichtet, ist nach § 134 BGB nichtig. Deshalb sind Versicherungsunternehmen und Versicherungsvertreter gleichermaßen gut beraten, durch Einwilligung des Betroffenen und zwar sowohl in die Speicherung als auch in die Übermittlung seiner Daten die jetzige datenschutzrechtlich bedenkliche Situation zu beenden.

4.2.4 Datenübermittlung von Gebäudeversicherern an Hypothekengläubiger

Nach § 101 Versicherungsvertragsgesetz (VVG) hat ein Gebäudeversicherer einem Hypothekengläubiger, der seine Hypothek bei ihm angemeldet hat, unverzüglich schriftlich Mitteilung zu machen, wenn dem Versicherungsnehmer für die Zahlung einer Versicherungsprämie eine Zahlungsfrist bestimmt wird. Dies geschieht, um dem Hypothekengläubiger eine Gefahrerhöhung anzuzeigen. Wenn ein versichertes Gebäude etwa durch Brand zerstört wird, während der Versicherer von seiner Leistungspflicht wegen Prämienrückstandes des Versicherungsnehmers befreit ist, dann

verliert auch der grundpfandrechtlich abgesicherte Gläubiger seine Sicherheit. Er hat deshalb ein großes eigenes Interesse am Bestand des Versicherungsschutzes, das möglicherweise so weit geht, anstelle des Versicherungsnehmers selbst die Versicherungsprämie leisten zu wollen.

In einem Beschwerdefall hatte der Versicherungsnehmer einen Betrag von weniger als DM 20,- irrtümlich nicht gezahlt. Dies entsprach gerade der in die Prämie eingeschlossenen Versicherungssteuer. Das Versicherungsunternehmen hatte ohne weitere Rückfrage den Hypothekengläubiger mit einem Standardbrief über die offene Forderung gem. § 101 VVG unterrichtet, so daß dieser vermuten mußte, der Versicherungsschutz für die Immobilie werde verlorengehen. Daraufhin forderte er seinerseits den privaten Hausbesitzer zur Zahlung der Versicherungsprämie auf.

Dieser Beschwerdefall zeigt, wie problematisch es ist, wenn die Mitteilung an den Hypothekengläubiger schematisch und ohne vorherige Unterrichtung des Versicherungsnehmers erfolgt. Der Versicherungsnehmer hat dann keine Gelegenheit, zur Berechtigung der Forderung zu einem Zeitpunkt Stellung zu nehmen, zu dem Dritte noch nicht informiert worden sind. Er ist vielmehr bereits dann als potentielles Risiko für seine Gläubiger abgestempelt, wenn sich die Forderung im Nachhinein als z.B. unbegründet erweist oder dem Vorgang ein Versehen zugrundeliegt.

Ich habe mit dem betreffenden Versicherungsunternehmen die Problematik erörtert und konnte folgende Verfahrensverbesserung erreichen:

Künftig wird vor einer Fristsetzung nach § 101 VVG dem Versicherungsnehmer eine erste Zahlungserinnerung (ohne Fristbestimmung) aufgegeben. Der Sicherungsgläubiger wird erst nach fruchtlosem Ausgang dieses „Vorverfahrens" informiert, wenn also dem Versicherungsnehmer dann die nach § 101 VVG zur Mitteilung verpflichtende Frist gesetzt wird. Auch soll in dem Mitteilungsschreiben künftig von „Zahlungsrückstand" und nicht mehr von „Prämienrückstand" gesprochen werden. Es wird damit der nicht in jedem Fall zutreffende Eindruck vermieden, der Kunde befinde sich mit der gesamten Prämie im Zahlungsrückstand.

Damit hat das betroffene Versicherungsunternehmen dazu beigetragen, die zu Recht monierte Gefahr der Diskreditierung des Versicherungsnehmers bei seinem Hypothekengläubiger zu vermeiden. Im übrigen halte ich die Regelungen im VVG zumindest bei Bagatellrückständen für problematisch. Es müßten hier die Interessen der Hypothekengläubiger und der betroffenen Schuldner in einen Einklang gebracht werden, der den Persönlichkeitsschutz des Schuldners mitberücksichtigt.

4.3 Mieterdatenschutz

Aufgrund einer Eingabe habe ich von folgendem Sachverhalt Kenntnis erlangt:

Es ist branchenübliche Praxis der Haus- und Immobilienmakler, an (zum Teil nur vermeintliche) Kaufinteressenten für Mietshäuser eine Offerte zu schicken, in der nicht nur Angaben über das zum Verkauf stehende Gebäude, sondern auch detaillierte Informationen über die Mieter des Hauses enthalten sind. So werden personenbezogene Daten gestreut, die sich auf die Nettokaltmiete, die Betriebskosten, die letzte Mieterhöhung, das Einzugsdatum, die Mietvertragsart, die voraussichtliche Dauer des Mietverhältnisses und über eventuelle Auszugswünsche der Mieter beziehen.

Ich habe mit dem Ring Deutscher Makler den Problembereich erörtert und bin mit ihm übereingekommen, daß für die Zulässigkeit der Preisgabe von Mieterdaten genau zu unterscheiden ist, in welchem Stadium der Kaufverhandlungen man sich befindet. Solange kein Interesse an einem konkreten Objekt besteht, sondern erst durch Zusendung der Verkaufsofferte geweckt werden soll, ist die Übermittlung von Listen, aus denen persönliche Angaben über Mieter einer bestimmten Wohnung hervorgehen, nicht erforderlich und deshalb unzulässig. Insbesondere ist es unakzeptabel, sie sogar solchen Personen bekanntzumachen, bei denen es keine Anhaltspunkte für ein Interesse am Kauf eines Mietshauses gibt. Ein ernsthaft interessierter Käufer benötigt hin-

gegen auch Informationen über die von ihm zu übernehmenden Mietverhältnisse, da seine Kaufentscheidung wesentlich davon abhängen dürfte. Derartige Angaben sind allerdings erst dann offenzulegen, wenn der Kaufinteressent ausdrücklich nachfragt und dadurch ein auf das spezielle Objekt bezogenes Kaufinteresse dokumentiert.

Der Ring Deutscher Makler hat seine Mitglieder per Rundschreiben dementsprechend instruiert.

4.4 Mailboxen

In jüngerer Vergangenheit sind vermehrt Unternehmen auf dem Markt erschienen, die bislang nicht bekannte Dienstleistungen anbieten. Dazu gehören die sogenannte elektronische Kommunikation (Mailboxdienst im engeren Sinne), ein sogenanntes elektronisches Dienstleistungssystem und die Datenbankrecherche. Ich habe mich im Berichtszeitraum mit der Frage auseinandergesetzt, ob und gegebenenfalls in welchen Teilbereichen derartige Unternehmen personenbezogene Daten verarbeiten. Zu diesem Zweck habe ich ein Hamburger Mailbox-Unternehmen aufgesucht und mir deren Dienstleistungsangebot einschließlich der technischen Verfahrensweisen näher erläutern lassen. Dabei ergab sich im einzelnen folgendes:

Die technischen Mindestvoraussetzungen für einen Mailboxanschluß sind eine intelligente Schreibmaschine und eine Kommunikationsschnittstelle zum Datex-P-Netzwerk der Deutschen Bundespost (z.B. ein Modem und ein Telefonanschluß). Die Regelausstattung ist ein Personalcomputer und ein Datex-P-Hauptanschluß. Gegen eine Grundgebühr und weitere, vom Umfang der Nutzung abhängige Entgelte erhält der Kunde Anschluß an das Mailboxangebot.

Er kann dann mit jedem anderen Mailbox-Teilnehmer „elektronisch kommunizieren". Dazu schickt der Kunde von seinem Terminal aus an einen bestimmten anderen Teilnehmer Nachrichten, die im „elektronischen Briefkasten" des Empfängers eingehen und von ihm dort abgerufen werden können. Technisch wird dies dadurch realisiert, daß die Nachricht des Absenders über das Datex-P-Netz in den Rechner der Mailbox übermittelt, dort auf externe Speichermedien (Band- oder Plattenspeicher) aufgenommen, für den zugriffsberechtigten Empfänger zum Abruf bereitgehalten und bei Abruf (abermals über das Datex-P-Netz) an ihn abgesendet wird. Der „elektronische Briefkasten" eines jeden Teilnehmers ist also technisch nichts anderes als die Berechtigung, auf bestimmte Daten im Rechenzentrum der Mailbox zuzugreifen. Durch Erweiterung der Zugriffsberechtigung können Informationen auch an einen größeren Empfängerkreis weitergegeben werden. Dadurch kann der Mailboxanschluß z.B. zur täglichen Instruktion der Außendienstmitarbeiter eines Unternehmens durch die Zentrale genutzt werden.

Hinter dem „elektronischen Dienstleistungssystem" verbirgt sich die (zur Zeit für den Mailboxkunden ohne zusätzliche Nutzungsgebühr) angebotene Möglichkeit, an einen erweiterten Empfängerkreis - meistens an alle anderen Teilnehmer - Nachrichten zu senden. Dadurch kann der Effekt der „gelben Seiten" erreicht werden, indem Gewerbetreibende (z.B. Schreibdienste oder Übersetzer) auf diese Weise auf ihr Gewerbe aufmerksam machen.

Die Datenbankrecherche eröffnet dem Kunden den Zugang zu den an die Mailbox angeschlossenen Datenbanken. Die Recherche bleibt aber Sache des Kunden und wird nicht durch die Mailbox übernommen. Angeschlossen sind derzeit ca. 50 Hosts, in denen größtenteils medizinisches, technisches oder juristisches Fachwissen gespeichert ist. Es können auch die Datenbanken von Handels- und Wirtschaftsauskunfteien über den Mailboxanschluß erreicht werden, sofern der Kunde mit den Betreibern einen Zusatzvertrag schließt. Die Zusatzvereinbarung soll sicherstellen, daß die datenschutzrechtlichen Bestimmungen, denen Handels- und Wirtschaftsauskunfteien nach § 31 Abs.1 Nr.1 BDSG unterliegen, eingehalten werden.

Aus datenschutzrechtlicher Sicht waren bislang folgende Probleme zu erörtern:

1. Sind elektronische Nachrichten personenbezogene Daten?

Gemäß § 2 Abs.1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Alle Informationen, die über den Betroffenen etwas aussagen, sind als personenbezogen zu qualifizieren.

Nachrichten können den Absendern und Empfängern zugeordnet werden. Schon dadurch und nicht erst durch ihren Inhalt und die Umstände ihrer Übertragung erhalten sie ihren Personenbezug und sind somit als personenbezogene Daten i.S.v. § 2 Abs.1 BDSG einzuordnen.

Dies gilt auch für die Dienstleistung „schwarze Bretter", sofern in den elektronischen Anzeigen Angaben über den Absender gemacht werden.

2. Werden die Nachrichten im Sinne des BDSG „gespeichert" ?

Kein Speichern im Sinne des § 2 Abs.2 Nr.1 BDSG liegt vor, wenn die Daten lediglich in den Kernspeicher der EDV-Anlage aufgenommen, dort verarbeitet aber sodann wieder gelöscht werden. Dann sind Daten nur übergangsweise im System. Solche Vorgänge haben in der Regel keine Außenwirkung und erfüllen nicht die Voraussetzungen für „Speichern" im Sinne des BDSG. Mindestvoraussetzung ist somit die wenigstens vorübergehende Aufnahme der Daten in einen Speicher außerhalb des Kernspeichers.

Bei der elektronischen Kommunikation und beim Mitteilungsdienst werden die Texte auf Magnetplatten abgelegt. Sie werden damit außerhalb des Arbeitsspeichers unbestimmte Zeit (bis zum Abruf durch den Empfänger) aufbewahrt und mithin im Sinne des BDSG gespeichert.

Anders hingegen ist es bei der Datenbankrecherche. Bei dieser Dienstleistung übernimmt die Mailbox lediglich die Aufgabe, die Verbindung zwischen dem Mailboxkunden und der Datenbank herzustellen. Die Informationen aus den Datenbanken werden direkt an den Kunden übermittelt. Sie werden bei der Mailbox nicht außerhalb des Kernspeichers aufbewahrt. Somit ist diesbezüglich der Tatbestand der Speicherung nicht erfüllt.

3. Handelt es sich um Verarbeitung in Dateien?

Nach § 1 Abs.2 Satz 1 BDSG schützt das Bundesdatenschutzgesetz nur solche personenbezogenen Daten, die in Dateien verarbeitet werden. Eine Datei ist eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann.

Eine elektronische Nachricht erfüllt für sich betrachtet zwar nicht den Dateibegriff, da es etwa an der Umsortiermöglichkeit fehlt. Gleichwohl erfordert die Nachrichtenverwaltung eine dateimäßige Datenverarbeitung. Die elektronischen Nachrichten bilden jeweils eine automatisiert gespeicherte Texteinheit, die nach Absender und Empfänger, nach Datum und Uhrzeit der Einspeicherung und des Abrufs sortiert werden kann.

4. Handelt es sich um Auftragsdatenverarbeitung?

Gemäß § 31 Abs.1 Nr.3 BDSG liegt Auftragsdatenverarbeitung vor, soweit geschäftsmäßig geschützte personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeitet werden. Für die Datenverarbeitung im Auftrag ist entscheidend, ob und in welchem Umfang die Kunden sich zur Erreichung ihrer eigenen Ziele und Zwecke der Datenverarbeitung durch das Mailboxunternehmen bedienen. Die Datenverarbeitung im Auftrag ist von der Datenverarbeitung für eigene Zwecke, die eine Mailbox außerdem betreibt (z.B. Gebührenabrechnung), zu unterscheiden.

Es wird zwar gelegentlich die Meinung vertreten, daß bei Online-Anschluß der Kunden an ein Rechenzentrum nicht das Rechenzentrum, sondern der Kunde Datenverarbeitung betriebe, da allein der Kunde entscheiden könne, welche personenbezogenen

Daten wann und in welcher Weise verarbeitet würden. Diese Auffassung verkennt jedoch, daß der Gesetzgeber auch solche Stellen in den Geltungsbereich des Gesetzes mit eigenen Pflichten (z.B. § 6 BDSG) einbeziehen will, die keine inhaltliche Verfügungsberechtigung haben, sondern lediglich technische Hilfsfunktionen übernehmen. Schon das Aufbewahren von Kundendaten durch das Dienstleistungsunternehmen ist folglich ausreichend, um die Dienstleistung als Auftragsdatenverarbeitung zu qualifizieren.

Problematisch ist, wo die Grenzlinie zwischen der Datenverarbeitung im Auftrag und der für eigene Zwecke zu ziehen ist. Die bereits erwähnte Nachrichtenverwaltung (siehe Punkt 1.) ist notwendige technische Voraussetzung für die elektronische Kommunikation. Sie ist aber möglicherweise nicht selbst Bestandteil des Auftrages. Damit unterfiele die Tätigkeit einer Mailbox weitgehend nicht dem 4., sondern dem 3. Abschnitt des BDSG.

Jedoch ist nach meiner Auffassung die richtige Zuordnung einer Nachricht zum Empfänger und Absender, wie auch die gesamte Nachrichtenverwaltung untrennbarer Bestandteil der Dienstleistung der elektronischen Kommuniktion, also der Datenverarbeitung für die Zwecke der Kunden. Die Nachrichtenverwaltung ist somit Bestandteil der Auftragsdatenverarbeitung.

4.5 Sonstige Probleme aus dem nicht-öffentlichen Bereich

4.5.1 Datenverarbeitung bei einer privatrechtlichen Religionsgemeinschaft

Im Berichtszeitraum erreichten mich eine Reihe von Beschwerden, die die Verarbeitung personenbezogener Daten bei einer im Vereinsregister eingetragenen, also privatrechtlich organisierten Religionsgemeinschaft betrafen. Sie propagiert die geistig-seelische Befreiung und ethische Verbesserung des Menschen, um eine Gesellschaft ohne Krieg, ohne Geisteskrankheit und Kriminalität zu schaffen. Zu diesem Zweck können all jene, die sich davon angesprochen fühlen, bestimmte Kurse besuchen, das vom Religionsstifter verfaßte Buch erwerben und darüber hinaus an sonstigen gemeinsamen Aktivitäten zur Reinigung des Körpers und des Geistes (z.B. Saunabesuch) teilnehmen.

Die an mich gerichteten Eingaben kritisierten den Umgang der Vereinigung mit den von interessierten Bürgern erhobenen Daten. Viele, die mit der Religionsgemeinschaft Kontakt aufnehmen, füllen zum Auftakt einen Fragebogen aus, der 200 - zum Teil sehr tief in den Persönlichkeitsbereich eindringende - Fragen beinhaltet. Dieser Fragebogen wird EDV-mäßig zu einer „Standard Oxford Persönlichkeitsauswertung" verarbeitet. Dadurch wird der Betroffene unter den Gesichtspunkten Stabilität, Lebensfreude, Ausgeglichenheit, Verläßlichkeit, Aktivität, Durchsetzungsfähigkeit, Verantwortungbereitschaft, Urteilsvermögen, Sensibilität und Kommunikationsfähigkeit in die Kategorien gut, normal oder bedenklich eingestuft. Auf dieser Grundlage erfolgt ein Beratungsgespräch, das in der überwiegenden Anzahl der Fälle zu der Empfehlung führt, zunächst einmal das Standardwerk über die gemeinsame Weltanschauung zu erwerben, einen Einführungskurs zu belegen oder ein sogenanntes Auditing zu absolvieren, das die Funktion einer Beichte erfüllt. Diese Leistungen sind entgeltlich.

Die Beschwerden konzentrierten sich darauf, daß die Betroffenen weder die von ihnen ausgefüllten Fragebögen zurückerhalten, noch das daraus erstellte Persönlichkeitsprofil ausgehändigt bekommen, und zwar auch dann nicht, wenn sie diese Unterlagen ausdrücklich verlangen. Darüberhinaus wurde ich gebeten zu überprüfen, ob die Angaben aus den Fragebögen weiterhin gespeichert bleiben, auch wenn etwa die Betroffenen nach dem Einführungsgepräch keinen weiteren Kontakt zur Gemeinschaft wollen und sich sogar die Zusendung von Werbematerial verbitten. Schließlich wurde gerügt, daß die Adressen von Interessenten für Werbezwecke des Vereins genutzt werden.

Ich habe daraufhin die Religionsgemeinschaft vor Ort überprüft. Es ergab sich der folgende Sachverhalt:

Die Religionsgemeinschaft gab die Testauswertung an die Betroffenen generell nicht heraus. Die Antworten auf die 200 Testfragen einschließlich Name des Betroffenen und Datum der Bearbeitung blieben auch dann auf unbestimmte Zeit gespeichert, wenn der Betroffene kein Mitglied wurde. Die Testbögen wurden in Akten verwahrt. Weder auf die Speicherung noch auf die aktenmäßige Verwahrung wurde der Betroffene hingewiesen. Er erkannte häufig gar nicht, daß die Religionsgemeinschaft eine Fülle von Erkenntnissen über seine Persönlichkeitsstruktur besaß, und war folglich nicht in der Lage, die Löschung seiner Angaben zu verlangen. Von einer Einwilligung in die Speicherung konnte unter diesen Bedingungen keine Rede sein.

Außerdem habe ich festgestellt, daß neben dem Testauswertungsverfahren für Werbezwecke eine automatische Adreßdatei geführt wird, in der Namen und Adressen von Personen gespeichert sind, die bereits Schriften der weltanschaulichen Gemeinschaft abgenommen oder Seminare besucht haben. Dort wird auch vermerkt, zu welcher Kategorie der Abnehmer gehört, z.B. „Infopack", „Buchkäufer" oder „Kursteilnehmer". Ferner wird das Datum des letzten derartigen Kontaktes aufgenommen. Eine Löschung erfolgt auch dann nicht, wenn der Betroffene ausdrücklich keine Werbesendungen mehr wünscht. In einem solchen Fall wird die Adresse aber mit dem Hinweis „keine Werbung schicken" versehen. Dadurch soll sichergestellt werden, daß die Person auch dann kein Werbematerial mehr erhält, wenn dazu nicht der eigene Adressenbestand benutzt wird, sondern die Adressen von kommerziellen Marketing-Unternehmen angemietet werden.

Kurze Zeit nach meiner Prüfung hat mich die Religionsgemeinschaft darüber informiert, daß sie ihr Verfahren geändert habe: So sollen nunmehr weder die Testantworten noch die Testauswertung gespeichert, sondern die Daten nach dem Ausdruck der Testkurve sofort gelöscht werden. Die alten Datenbestände wurden - so die Gemeinschaft - mittlerweile ebenfalls gelöscht. Wenn ein Betroffener die Vernichtung des ausgefüllten Fragebogens oder der Auswertung verlangt, so sollen diese Unterlagen vor seinen Augen in einem Schredder zerschnipselt werden. Ferner soll einem Betroffenen in Zukunft seine Testauswertung nicht mehr vorenthalten, sondern ihm auf sein Verlangen hin ausgehändigt werden.

Damit ist die datenschutzrechtlich unzulässige geheime Speicherung höchst sensibler personenbezogener Angaben abgestellt worden. Gegen die Praxis, bei Widerspruch gegen Zusendung von Werbematerial nicht die Adresse zu löschen, sondern ihre Verwendung für Werbezwecke durch Zusatzvermerk zu verhindern, habe ich keine durchgreifenden Bedenken, sofern sichergestellt ist, daß die Adressen nicht für anderweitige Zwecke benutzt werden. Für begrüßenswert halte ich es, daß die Auswertungen in Zukunft dem Betroffenen ausgehändigt werden sollen. Damit wurde ein Schritt in Richtung Offenlegung nicht nur der Ziele, sondern auch der Methoden der Gemeinschaft getan. Die weitere Auseinandersetzung damit ist - soweit überhaupt von rechtlicher Natur - gewerberechtlicher oder verbraucherschutzrechtlicher Art und somit außerhalb meines Zuständigkeitsbereiches.

4.5.2 Testbögen zur Partnervermittlung

Wegen mehrerer Anfragen und Beschwerden mußte ich mich mit Fragebögen beschäftigen, die von einem Partner-Vermittlungs-Institut in verschiedenen Zeitungen und Zeitschriften als Anzeigen veröffentlicht werden.

Das Institut bietet an, einen Partnerschaftstest durchzuführen. Dazu fordert es den Leser auf, Namen, Anschrift, Telefonnummer, Alter, Beruf, Interessen, Ansichten, körperliche Merkmale u.a.m. anzugeben, um ihm eine Partnerschafts-Empfehlung zu erarbeiten und vorzulegen. Früher war der Fragebogen zu unterschreiben; seit kurzem wird das nicht mehr verlangt.

Wenn die ausgefüllten Fragebögen (wöchentlich zwischen 5.000 und 7.000) beim Institut eingehen, werden die versprochenen Partnerschafts-Empfehlungen erarbeitet. Sie bestehen aus Beschreibungen von Personen, die einen Vermittlungsvertrag mit dem Institut abgeschlossen haben, die aber nur mit Vornamen, Wohnort und Kunden-Nr. vorgestellt werden. Weitere Daten werden nicht bekanntgegeben, weil sich sonst das Institut die Chance einer Vermittlung selbst verbauen würde.

Das Institut versucht dann, beim Interessenten telefonisch zu erfragen, ob er einen persönlichen Besuch wünsche, und ggfs. einen Termin dafür zu vereinbaren. Wenn Interesse an dem persönlichen Besuch besteht, werden Name und Anschrift an den regionalen Vertreter übermittelt, der den Partnerschafts-Vorschlag dem Interessenten vorstellt und ihn zum Abschluß eines Partnerschafts-Vermittlungsvertrages bewegen will. Wenn ein solcher Vertrag zustandegekommen ist, wird ein sehr viel umfangreicherer Persönlichkeitstest vorgenommen, der Grundlage für die Auswahl der genau für ihn passenden Partnervorschläge ist.

Die Daten derjenigen, die an einem Vermittlungsvertrag nicht interessiert sind, werden nicht etwa gelöscht, sondern das Institut wertet sie aus, um sie als Adreßmaterial an andere Unternehmen vermieten zu können. Zu diesem Zweck werden eine Reihe von Angaben aus dem Fragebogen in die EDV übernommen, die als Auswahlmerkmale genutzt werden. Allerdings werden die Angaben zu Interessen oder Meinungen nicht festgehalten. Zur Zeit sind in diesem Bestand etwa 300.000 Datensätze vorhanden, die erst vier Jahre nach Einspeicherung wieder gelöscht werden. Die Vermietung zu Werbezwecken besorgt ein großes Unternehmen der Direktmarketing-Branche.

Beschwert haben sich mehrere Bürger, die gar nicht selbst die Fragebogen ausgefüllt haben, sondern Opfer von „Scherzen" geworden waren - andere hatte ihre Namen und Adressen angegeben. Sie fühlten sich belästigt und verlangten die Löschung ihrer Daten.

Das Partner-Vermittlungs-Institut ist dazu übergegangen, in derartigen Fällen die Angaben über Vor- und Zunamen und die Straßenbezeichnung jeweils mit „xxx" zu überschreiben. Die übrigen Daten bleiben im Bestand. Nach Angaben des Instituts würden diese noch für statistische Auswertungen benötigt werden, eine Verwendung für Werbezwecke sei damit jedoch unmöglich geworden.

Auf die vorhandenen Datensätze kann im Normalfall über den Namen zugegriffen werden. Darüberhinaus gestattet eine Ordnungsnummer des Datensatzes den Zugriff. Eine weitere theoretische Möglichkeit der Reidentifizierung besteht deshalb in den Fällen, in denen man markante Einzelmerkmale vom Betroffenen kennt, die als Suchkriterien verwendet werden können.

Rechtliche Würdigung:

Die Speicherung von Daten, die ein Interessent einem werbenden Unternehmen in einer Zuschrift angibt, um eine in der Werbung zugesagte Leistung zu erhalten, ist nicht zu beanstanden, wenn sie auf der Einwilligung des Betroffenen beruht.

Voraussetzung ist jedoch, daß der Kunde sich über die Verwendung seiner Daten vollständig im klaren ist und deshalb die Verarbeitung seiner persönlichen Daten vollen Umfangs seinem Willen entspricht. Eine Einwilligung liegt nicht vor, wenn eine Person unter Vorspiegelung falscher Tatsachen zu Angaben über sich veranlaßt wird, die sie in Kenntnis der realen Situation nicht gemacht hätte.

Bei der Datenerhebung mit Hilfe der Fragebögen zur Partnerschaftsvermittlung vermisse ich die notwendige Transparenz. Der Betroffene weiß z.B. nicht, daß seine Adresse auch dann, wenn ein Partner-Vermittlungsvertrag nicht zustandekommt, weiter gespeichert bzw. für eine von ihm überhaupt nicht gewollte Werbung an Dritte übermittelt werden soll. Er erhält aus dem Werbeversprechen den Eindruck, das Institut benötige seine Daten lediglich, um für ihn geeignete Partnervorschläge zu finden und ihm mitzuteilen. Nur deshalb ist er bereit, so weitgehende Angaben zu machen. Darüberhinaus wird er sich darauf verlassen, daß gerade Ehe-Anbahnungs-Institute besonders

auf Diskretion achten. Er wird in der Regel davon ausgehen, daß spätestens, nachdem ihm die Partner-Empfehlung zur Verfügung gestellt worden ist, der Zweck der Speicherung erfüllt ist. Die weitere Speicherung kann daher nicht mehr auf seine Einwilligung gestützt werden. Erst recht kann die weitere Verarbeitung dann nicht mehr mit einer Einwilligung gerechtfertigt werden, wenn der Betroffene es abgelehnt hat, den Besuch eines Vertreters zu empfangen.

Für mich stellt sich die Frage, ob nicht das Institut den Betroffenen nach § 26 Abs.1 BDSG über die weitere Speicherung zu Werbezwecken hätte unterrichten müssen, die nach Erledigung des Werbeversprechens fortgesetzt wird. Eine „Kenntnis auf andere Weise", die die Benachrichtigung ersetzen könnte, kann bei den mir bekannten Werbetexten nicht angenommen werden.

Jedenfalls ist eine Übermittlung der gespeicherten Daten nur gestattet, wenn im Einzelfall die schutzwürdigen Belange des Betroffenen gegenüber den berechtigten Interessen der übrigen Beteiligten geringer zu bewerten sind. Diese Abwägung kann das Institut jedoch gar nicht vornehmen. Mithin kann nicht ausgeschlossen werden, daß die Daten im Einzelfall in rechtswidriger Weise verarbeitet werden, denn der Betroffene kann mangels Kenntnis von der Speicherung seine Belange gar nicht geltendmachen.

Ich habe daher empfohlen, bei der Datenerhebung, also im Text der Werbung, über die beabsichtigte Verwendung der Daten in vollem Umfang aufzuklären.

Ein besonderes Problem stellt die Häufung der Fälle dar, in denen die Fragebögen von Personen ausgefüllt werden, die damit einer anderen einen üblen Scherz spielen wollen.

Meines Erachtens muß das Partnerschafts-Vermittlungs-Institut Vorkehrungen treffen, die diese Art der Schädigung Unbeteiligter verhindern oder wenigstens erschweren. Ich meine, daß das Institut mit der breiten Streuung der Fragebögen eine Gefahrenquelle schafft und deshalb auch die Pflicht hat, alles Zumutbare zu unternehmen, um zu verhindern, daß Schäden eintreten, sei es materieller oder auch nur immaterieller Natur. Andernfalls droht dem Institut, nach § 823 Abs.1, § 847 BGB auf Schadensersatz und Schmerzensgeld in Anspruch genommen zu werden.

Als zumutbare Vorkehrung habe ich vorgeschlagen, zur früheren Praxis zurückzukehren und eine Unterschrift im Fragebogen zu verlangen. Die Verwendung einer fremden Unterschrift in einem solchen Fragebogen stellt strafrechtlich eine Urkundenfälschung nach § 267 StGB dar. Eine abschreckende Wirkung würde zumindest dann erreicht werden, wenn im Fragebogen selbst darauf hingewiesen würde, daß sich derjenige, der eine Unterschrift fälscht, in die Gefahr einer Bestrafung begibt.

Darüberhinaus genügt das Vorgehen des Instituts, nachdem dieser „Scherz" als solcher erkannt wurde, den Anforderungen an eine Datenlöschung nicht in jeder Hinsicht, weil diese Angaben weiterhin über die Ordnungsnummer oder herausragende Einzelmerkmale einer ganz bestimmten Person wieder zugeordnet werden können. Damit bleiben sie personenbezogene Daten. Durch das Überschreiben des Namens mit anderen Zeichen wird lediglich eine Sperrung - und die damit verbundene Nutzungsbeschränkung - erreicht.

Ich meine, daß ein Datensatz, wenn er als „Scherz" erkannt ist, unverzüglich zu löschen ist.

4.5.3 Adressenvertrieb durch pornographische Zeitschrift

In einer Beschwerde wurde besonders deutlich, welch nachteilige Folgen es haben kann, wenn offenkundige personenbezogene Daten aus ihrem ursprünglichen Zusammenhang gerissen und in einem neuen Zusammenhang für einen völlig anderen Zweck wieder verwendet werden.

Mir wurde folgender Sachverhalt unterbreitet:

In verschiedenen Frauenzeitschriften können Inserate veröffentlicht werden, in denen Name und Anschrift des/der Inserenten/in ungekürzt und unchiffriert erscheinen. Dabei kann es sich um die Anknüpfung von Brieffreundschaften, den Tausch von Briefmarken und Kochrezepten, gelegentlich auch um eine Kontaktsuche handeln. In den meisten Fällen haben die Anzeigen jedoch nicht das Ziel einer Partnersuche, sondern sind auf völlig andere Zwecke gerichtet. Um so überraschender war es für eine der Inserentinnen, feststellen zu müssen, daß mit den Adressen aus den Inseraten - soweit Frauen die Anzeige aufgegeben hatten - ein schwunghafter Sexhandel betrieben wurde. Ihre Namen und Adressen wurden listenmäßig zusammengestellt und zum Kauf mit dem Werbeversprechen angeboten, es handele sich um Frauen, die an einem sexuellen Kontakt interessiert seien. Für den Bezug dieser Liste wurde in einer Sex-Zeitschrift geworben, die nicht am Kiosk, sondern nur in einschlägigen Geschäften zu erwerben war. Gegen ein erhebliches Entgelt können die Adressen vom Anbieter bezogen werden. Die ahnungslosen Frauen erhalten daraufhin anzügliche Briefe oder sogar unangemeldeten Hausbesuch. Sie sind damit einer unzumutbaren Situation ausgesetzt.

Für die Aufsichtsbehörde ist hier festzustellen, daß sowohl die Speicherung als auch die Übermittlung der personenbezogenen Daten unzulässig ist. Dies aber dürfte für die Betroffenen nur ein schwacher Trost sein. Sie sind vielmehr an einer Vergeltung der ihnen zugemuteten Unannehmlichkeiten interessiert. Insoweit steht ihnen zwar möglicherweise ein zivilrechtlicher Anspruch auf Schmerzensgeld zu. Der strafrechtliche Schutz erweist sich jedoch als lückenhaft. In Betracht käme lediglich eine Beleidigung, die jedoch nicht von den (ebenfalls hintergangenen) Kontakt suchenden Männern begangen sein kann, sondern allenfalls von dem Anbieter in der Pornozeitschrift. Die Strafvorschrift des § 41 BDSG, die den unbefugten Umgang mit Daten unter Strafe stellt, beschränkt sich auf solche Daten, die nicht offenkundig sind. Der Fall zeigt aber, daß es strafwürdigen Umgang auch mit offenkundigen personenbezogenen Daten geben kann.

4.5.4 Datenübermittlungen vom nicht-öffentlichen in den öffentlichen Bereich

Immer wieder werde ich darauf angesprochen, ob und gegebenenfalls unter welchen Voraussetzungen private Stellen an Behörden Auskünfte über Dritte erteilen müssen und/oder erteilen dürfen. Zum wiederholten Male möchte ich auf folgendes hinweisen:

Zunächst ist zu klären, ob es eine Verpflichtung zur Auskunftserteilung gibt, oder ob es letztlich dem Privatmann überlassen bleibt, den Informationswünschen nachzukommen oder sie zu verweigern. Eine Verpflichtung besteht nur dann, wenn die Verwaltung auf eine entsprechende Rechtsgrundlage verweisen kann. Leider sind die behördlichen Aufforderungen häufig so abgefaßt, daß daraus nicht zu erkennnen ist, ob die Übermittlung der gewünschten Angaben freiwillig ist oder nicht. In einem solchen Fall ist dann - bedauerlicherweise - der Privatmann genötigt, die Verwaltung zur Klarstellung aufzufordern. Kann eine zutreffende Rechtsgrundlage benannt werden, ist die Auskunft zu erteilen. Mangelt es daran, so darf sie verweigert werden.

Dann kann es nur noch darum gehen, ob die private Stelle über den Betroffenen eine Auskunft erteilen darf oder nicht. Dies bestimmt sich nach § 24 Abs.1 Satz 1 3.Alt. BDSG, wenn die Übermittlung aus einer Datei in Rede steht. Um die notwendige Interessenabwägung vornehmen zu können, ist der Zweck, zu dem die Information seitens der Behörde benötigt wird, dem Bürger offenzulegen. Dieser hat sorgfältig abzuwägen, ob schutzwürdige Belange des Betroffenen überwiegen. Die Entscheidung kann unter Umständen erst dann gefällt werden, wenn der Betroffene Gelegenheit zur Stellungnahme erhalten hat. Somit ist ein unbeteiligter Bürger durch derartige Ansinnen häufig überfordert, was auch die Vielzahl der an mich gerichteten Fragen zu diesem Thema belegt. Es ist deshalb auch seitens der Aufsichtsbehörde dringend an den Grundsatz zu erinnern, daß die Daten beim Betroffenen erhoben werden müssen und nur unter besonderen Voraussetzungen anderweitig beschafft werden dürfen.

4.5.5 Grenzüberschreitender Datenverkehr

Das Zusammenwachsen der europäischen Staaten macht sich auch in der Praxis der Aufsichtsbehörden für den Datenschutz bemerkbar, die zunehmend mit Fragen zum grenzüberschreitenden Datenverkehr befaßt sind. So wenden sich des öfteren betriebliche Datenschutzbeauftragte mit der Frage an mich, ob eine Datenübermittlung an das Ausland „wirklich" nur dann zulässig ist, wenn im Ausland ein dem Bundesdatenschutzgesetz gleichwertiges Gesetz in Kraft ist.

Die Fragestellung zeigt mir, daß zum grenzüberschreitenden Datenverkehr vieles unklar ist und daß die „Gleichwertigkeitsthese" häufig mißverstanden wird. Deshalb möchte ich hier folgendes klarstellen:

Auf die Gleichwertigkeit der Datenschutzbestimmungen kommt es dann an, wenn die Zulässigkeit der Datenübermittlung gemäß § 24 Abs. 1 Satz 1 3. Alt. BDSG nach Abwägung der schutzwürdigen Belange des Betroffenen mit den berechtigten Interessen anderer zu beurteilen ist. Nach allgemeiner Auffassung besteht stets dann Grund zur Annahme, daß schutzwürdige Belange des Betroffenen beeinträchtigt sein können, wenn in dem ausländischen Staat, in den die Daten übermittelt werden sollen, kein dem Bundesdatenschutzgesetz gleichwertiger Schutz vorhanden ist.

Zur Feststellung der Gleichwertigkeit genügt es nicht, nur die nationalen Datenschutzgesetze heranzuziehen. Vielmehr sind auch internationale Abkommen zu berücksichtigen. Hier ist z.B. die Europaratskonvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 zu nennen. Sie begründet eine völkerrechtliche Verpflichtung der Vertragsstaaten, die in der Konvention aufgestellten Grundsätze zum Datenschutz im innerstaatlichen Recht zu verwirklichen. Nun gibt es Länder, die zwar die Konvention ratifiziert, aber bis heute noch kein Datenschutzgesetz verabschiedet haben (z.B. Spanien). Außerdem gibt es Länder, die zwar über ein Datenschutzgesetz verfügen, jedoch der Konvention nicht beigetreten sind (z.B. Niederlande, Finnland) und schließlich solche, die sich im Datenschutz bislang gänzlich abstinent verhalten haben (Belgien, Luxemburg).

Daraus ergibt sich die Notwendigkeit zu folgender Differenzierung:

1. Der Datenverkehr mit Ländern, die sowohl die Europaratskonvention unterzeichnet haben als auch eigene Datenschutzgesetze besitzen, ist nach Art.12 der Datenschutzkonvention zu beurteilen. Danach darf eine Vertragspartei allein zum Zweck des Schutzes des Persönlichkeitsbereichs von Betroffenen den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei nicht verbieten oder von einer besonderen Genehmigung abhängig machen. Allerdings können für bestimmte, im nationalen Recht besonders geschützte personenbezogene Daten Ausnahmen des ungehinderten Datentransfers vorgesehen werden. Ferner darf nicht übersehen werden, daß der Datentransfer aus anderen Gründen als zum Schutz des Persönlichkeitsbereichs der Betroffenen mit Restriktionen versehen werden kann.
2. Haben einzelne Länder weder die Europaratskonvention ratifiziert noch eigene Datenschutzgesetze verabschiedet, so ist der Datentransfer in diese Länder allenfalls dann mit der Rechtslage in der Bundesrepublik zu vereinbaren, wenn auf vertraglicher Ebene mindestens der Datenschutzstandard der Europaratskonvention verbindlich gemacht wird. Zu diesem Standard gehören neben den Voraussetzungen für die Zulässigkeit der Datenverarbeitung Auskunfts-, Berichtigungs- und Löschungsansprüche für den Betroffenen sowie die Möglichkeit, diese Rechte in der Praxis durchsetzen zu können. Der durch solche Verträge begünstigte Dritte, also der von der Datenverarbeitung Betroffene, ist auf seine Datenschutzrechte hinzuweisen. Ferner muß die Nichteinhaltung datenschutzrechtlicher Bestimmungen sanktionierbar sein. Dazu kämen Vertragsstrafen in Betracht.
3. Länder, die, ohne ein eigenes Datenschutzgesetz verabschiedet zu haben, die Konvention ratifiziert haben, sind so zu behandeln, als wenn sie die Konvention nicht unterzeichnet hätten, siehe 2. Abgesehen davon, daß private Rechtsträger ohnehin

aus Art.12 Abs.2 der Europaratskonvention keine Ansprüche herleiten können, bindet diese Vorschrift in diesen Fällen auch staatliche Stellen der Bundesrepublik nicht, weil jene Länder ihrerseits ihren vertraglichen Pflichten nicht nachgekommen sind.

4. Bei Ländern, die die Europaratskonvention nicht unterzeichnet haben, aber eigene Datenschutzgesetze besitzen, ist zu prüfen, ob diese Gesetze dem Stand des deutschen Datenschutzgesetzes entsprechen oder zumindest der Europaratskonvention genügen. Ist dies zu verneinen, so sind diese Länder ebenso wie jene zu behandeln, die die Konvention nicht unterzeichnet haben und die auch kein eigenes Datenschutzgesetz besitzen, siehe 2.

Zwar verkenne ich nicht, daß eine solche „Vertragslösung" lückenhaft bleibt. So kann sie nicht die Gefahr beseitigen, daß in dem ausländischen Staat die Obrigkeit auf die personenbezogenen Daten zugreift. Sie kann darüber hinaus nicht ändern, daß im Ausland keine Datenschutz-Aufsichtsinstanz besteht. Gleichwohl meine ich, daß durch den Abschluß derartiger Verträge eine datenschutzrechtlich unbefriedigende Situation eher beseitigt werden kann als durch die Feststellung, der Datentransfer sei unzulässig. Allerdings wären derartige Vertragswerke, die von interessierten Wirtschaftskreisen zunächst einmal ausgearbeitet werden müßten, anhand der hier nur grob beschriebenen Meßlatte sorgfältig zu prüfen, wobei auch die Art der transferierten Daten zu berücksichtigen wäre.

Im übrigen ist der Datenexport ins Ausland auch zulässig, wenn der Betroffene nach umfassender Aufklärung über die beabsichtigten Übermittlungen eingewilligt hat. Bei einer Reihe von Datenübermittlungen dürfte die Einwilligung des Betroffenen entweder vorliegen oder ohne Schwierigkeiten einzuholen sein, weil die Datenübermittlung in seinem Interesse liegt, so z.B. bei einem Wechsel des Arbeitsplatzes ins Ausland, bei einer Auslandsreise u.v.a.m.. Diese Fälle dürften weitgehend mit denen deckungsgleich sein, bei denen sich die Zulässigkeit der Datenübermittlung wohl auch aus einem Vertrags- oder vertragsähnlichem Vertrauensverhältnis mit dem Betroffenen ergibt.

Unabhängig davon, in welches Land die Daten fließen sollen und welche Verträge mit dem Betroffenen abgeschlossen sind, plädiere ich dafür, durch Rahmenvereinbarungen mit der datenverarbeitenden Stelle im Ausland einen datenschutzrechtlichen Mindeststandard für den Betroffenen zu gewährleisten.

4.6 Arbeitnehmerdatenschutz

4.6.1 Beratung

Auch in diesem Berichtsjahr habe ich wieder eine Reihe von Betriebsräten hinsichtlich der Einführung personaldatenverarbeitender EDV-Systeme beraten, Schulungen durchgeführt, Vorträge zum Arbeitnehmerdatenschutz gehalten und Aufsätze zum Thema publiziert. Die Teilnahme meines zuständigen Mitarbeiters an einer Betriebsversammlung rief bei der Betriebsleitung Unmut hervor. Wie ich bereits im 1. TB, 3.4.2, S. 15) ausführte, ist die in § 30 BDSG genannte Unterstützungspflicht der Aufsichtsbehörde gegenüber dem betrieblichen Datenschutzbeauftragten keine abschließende Regelung für die Beratungsfunktion der Aufsichtsbehörde. Vielmehr läßt das Gesetz durchaus auch den Kontakt mit einzelnen Arbeitnehmern, mit der Geschäftsleitung und mit dem Betriebsrat, mit Arbeitgeberverbänden und Gewerkschaften zu. Jedem, der sich mit einer datenschutzrechtlichen Frage an mich wendet, stehe ich als neutraler Sachverständiger, nicht als „Partei", zur Verfügung.

Bei der Beratung im privatwirtschaftlichen Bereich gibt es für die Aufsichtsbehörde auch keine hierarchische Ordnung. Sie muß keinen „Dienstweg" einhalten - etwa über den betrieblichen Datenschutzbeauftragten oder die Geschäftsleitung an den Betriebsrat. Die Aufgabe, im Betrieb den Datenschutz zu gewährleisten, ist den genannten Institutionen gleichrangig übertragen. So haben der betriebliche Datenschutzbeauftragte und der Betriebsrat im Arbeitnehmerdatenschutz sich überschneidende Zuständigkeitskreise: Das Bundesdatenschutzgesetz gehört zu den „zugunsten

der Arbeitnehmer geltenden Gesetze", über deren Durchführung der Betriebsrat zu wachen hat, § 80 Betriebsverfassungsgesetz. Der betriebliche Datenschutzbeauftragte hat demgegenüber nach § 29 BDSG die Ausführung des BDSG „sowie anderer Vorschriften über den Datenschutz sicherzustellen", wozu wiederum einzelne Vorschriften des Betriebsverfassungsgesetzes gehören.

4.6.2 Einzelfälle

4.6.2.1 Fragen des Arbeitgebers nach Wehr- oder Ersatzdienst

Eine Spiegel-Meldung über die Nichteinstellung von Wehrdienstverweigerern beim Luft- und Raumfahrtkonzern MBB veranlaßte mich, die Landesvereinigung der Arbeitgeberverbände in Hamburg nach deren Auffassung zu befragen. Dabei machte ich datenschutzrechtliche Bedenken dagegen geltend, daß Arbeitgeber Bewerber überhaupt danach fragen, ob sie Wehrdienst oder ob sie Ersatzdienst geleistet haben. Allenfalls um herauszufinden, ob der Bewerber überhaupt noch einen Dienst absolvieren muß und für diese Zeit dem Arbeitgeber nicht zur Verfügung steht, kann die undifferenzierte Frage nach Ableistung des Wehr-/Ersatzdienstes zusammen gerechtfertigt sein.

Die Arbeitgebervereinigung teilte im wesentlichen meine Auffassung, hält eine Frage nach Ableistung des Ersatzdienstes aber bei Rüstungsunternehmen für zulässig. Ein überzeugter Kriegsdienstverweigerer werde in solchen Betrieben zwangsläufig in Gewissenskonflikte geraten, die arbeitsrechtliche Probleme nach sich ziehen. Ich halte diese Ausnahme - anders als andere Aufsichtsbehörden - nicht für überzeugend. Die Wahrnehmung des Grundrechts auf Kriegsdienstverweigerung würde hier zu einer Einschränkung der Arbeitsplatzfreiheit führen. Ob die Gründe für eine Kriegsdienstverweigerung auch die Annahme eines bestimmten Arbeitsplatzangebotes ausschließen, muß allein der Betroffene selbst entscheiden. Seine Entscheidung wird auch nicht für alle Arbeitsplätze in einem - auch Rüstungsgüter herstellenden Unternehmen gleich sein. Das vage Arbeitgeberrisiko künftiger Schwierigkeiten mit eingestellten Kriegsdienstverweigerern wiegt nach meiner Auffassung wesentlich weniger schwer als das Interesse des Bewerbers, seine religiöse oder weltanschauliche Gesinnung seinem Arbeitgeber nicht offenbaren zu müssen.

5.6.2.2 Weitergabe von Mitarbeiteradressen an eine Gewerkschaft

Eine Petentin beschwerte sich darüber, daß eine Gewerkschaft ein Werbeschreiben mit Blanko-Beitrittserklärung an ihre Privatadresse gerichtet hatte. Ich teilte der Gewerkschaft mit, daß Organisationswerbung grundsätzlich im Betrieb selbst ausgelegt bzw. verteilt werden sollte und eine Versendung an die Privatadressen nur dann in Betracht kommt, wenn die Mitarbeiter an wechselnden Orten beschäftigt und deshalb schwer zu erreichen sind. Betriebsräte dürfen Adressen von Mitarbeitern nur zur Erfüllung der betriebsverfassungsrechtlichen Aufgaben vom Arbeitgeber verlangen. Eine Weitergabe der Adressen an die gewerkschaftlichen Vertrauensleute bzw. die Betriebsgruppe oder an die Gewerkschaftszentrale zur Versendung von Werbebriefen ist ohne die Einwilligung des Betroffenen nicht zulässig.

4.6.2.3 Überlassung von Kündigungsschreiben an Krankenkassen

Zur Bearbeitung eines Krankengeldantrages eines Arbeitnehmers hatte der Arbeitgeber der zuständigen Ersatzkasse nicht nur das Ende des Arbeitsverhältnisses einer Petentin mitgeteilt, sondern eine Kopie des Kündigungsschreibens zur Verfügung gestellt. Aus diesem geht hervor, daß es sich um eine hilfsweise fristgerechte Kündigung handelt, nachdem zuvor schon eine fristlose Kündigung ausgesprochen worden war, und daß der Betriebsrat nicht widersprochen hatte. Auf meine Nachfrage räumte der Arbeitgeber ein, daß die Übersendung des Kündigungsschreibens nicht zulässig war. Er wertete den Vorgang als völlig unüblichen, anweisungswidrigen Einzelfall und erklärte, üblicherweise erhalte die Krankenkasse auf einem Formblatt lediglich den Termin des Ausscheidens.

4.6.2.4 Aufzeichnung von Telefongesprächen mit Kunden

Von einer Gewerkschaft erhielt ich den Entwurf einer Betriebsvereinbarung, die ein Versandhaus mit dem zuständigen Betriebsrat abschließen wollte. Danach sollten in einem Geschäftsbereich alle Arbeitsplätze mit Aufzeichnungseinrichtungen ausgestattet und die Mitarbeiter verpflichtet werden, mindestens einmal im Monat komplette Kundengespräche von ca. 1/2 Stunde aufzuzeichnen und diese Gespräche mit dem Vorgesetzten zu Schulungszwecken durchzusprechen. „Grundsätzlich" werde aus Gesprächsaufzeichnungen keine Disziplinarmaßnahme abgeleitet.

Ich bekräftigte die Bedenken der Gewerkschaft gegenüber diesem Betriebsvereinbarungsentwurf: Eine Aufzeichnung des Inhalts von Telefongesprächen ist nur mit ausdrücklicher Einwilligung des Mitarbeiters und vor allem auch des Kunden zulässig, Artikel 10 Grundgesetz (Fernmeldegeheimnis) und § 201 Strafgesetzbuch. Eine Einholung der Einwilligung während des Gesprächs erscheint praxisfremd und würde dem Schulungszweck, an „echten" Gesprächen zu lernen, zuwiderlaufen. Eine Anonymisierung durch - spätere - Löschung des Kundennamens und anderer Identifizierungsangaben im Gespräch wäre andererseits nicht ausreichend. Schließlich halte ich auch die - wenn auch nur ausnahmsweise - Verhängung von Disziplinarmaßnahmen aufgrund von aufgezeichneten Kundengesprächen für bedenklich. Nach Auskunft der Gewerkschaft wurde die Betriebsvereinbarung aufgrund meiner Bedenken von der Geschäftsführung nicht mehr weiterverfolgt.

Eingaben

Im Berichtszeitraum erreichten mich 252 Eingaben. Davon entfielen 136 auf den öffentlichen und 116 auf den nicht-öffentlichen Bereich. Die bis zum Redaktionsschluß abgeschlossenen Eingaben betrafen im einzelnen folgende Bereiche:

A) Öffentlicher Bereich	101
davon Sicherheitsbereich	23
Gesundheits- und Sozialbereich	26
übrige Bereiche	52
B) Nicht-öffentlicher Bereich	101
davon Versandhandel	2
Versicherungswirtschaft	9
Kreditwirtschaft	2
Werbung	17
Arbeitnehmer-Fragen	13
Sonstige des 3. Abschnitts	29
Auskunfteien	27
Sonstige des 4. Abschnitts	2