Der Hamburgische Datenschutzbeauftragte
20459 Hamburg
Telefon: 040-3504-2044
Telefax: 040-3504-2372
email: HmbDSB@t-online.de
Homepage: www.hamburg.de/Behoerden/HmbDSB/index.htm

15. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

- zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich

vorgelegt im Januar 1997 (Redaktionsschluß: 2. Dezember 1996)
Dr. Hans-Hermann Schrader

Brichtsjahr: 1996

INHALTSVERZEICHNIS
Zusammenfassung wichtiger Punkte

1. Zur Lage des Datenschutzes

1.1 Gesamtentwicklung

Für den Datenschutz ist das Jahr 1996 besonders wichtig gewesen. Auf der Datenschutzkonferenz im Frühjahr in Hamburg haben die Datenschutzbeauftragten ihre Forderungen zur Modernisierung und europäischen Harmonisierung des Datenschutzrechts im Anschluß an die EG-Datenschutzrichtlinie beschlossen, um den Anforderungen „in der sich rapide verändernden Welt der Datenverarbeitung“ zu entsprechen (1.4). Auf der Herbstkonferenz haben sie ihre Vorstellungen zum Datenschutz durch Technik zusammengefaßt mit dem Ziel, u. a. durch weitgehende Datenvermeidung die informationelle Selbstbestimmung des Bürgers besser zu wahren (1.3).

Nach jahrelangen Vorarbeiten sind die Beratungen über die Novellierung des Hamburgischen Datenschutzgesetzes im Unterausschuß Datenschutz der Bürgerschaft am 27. November 1996 abgeschlossen worden (1.5.1). Hauptpunkte zur Verbesserung des Datenschutzes sind die Pflicht zur Risikoanalyse vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens, die Regelung der Datenverarbeitung bei Verbunddateien und die Ergänzung der Vorschrift zur Mitarbeiterdatenverarbeitung. Die Rechte des Hamburgischen Datenschutzbeauftragten sollen gestärkt werden, z. B. durch das Recht, sich jederzeit an die Bürgerschaft wenden zu können. Wesentlich für den Datenschutz ist außerdem die vorgesehene Regelung, daß der Grundsatz der Datenvermeidung generell bei der Verarbeitung personenbezogener Daten und bei der Auswahl und Gestaltung technischer Einrichtungen zu berücksichtigen ist (1.3 und 3.1.1); damit soll dieser wichtige Grundsatz erstmals in einem Datenschutzgesetz ausdrücklich festgelegt werden.

Ein weiterer Ausbau des Datenschutzes ist bei der Anpassung des Gesetzes an die EG-Datenschutzrichtlinie in den nächsten zwei Jahren zu erwarten. Die Richtlinie (1.4) ist für die Weiterentwicklung des Bundes- und Landesdatenschutzrechts von großer Bedeutung. Sie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: „Die Datenverarbeitungssysteme stehen im Dienste des Menschen“.

Dadurch trägt die Richtlinie auch zur Klärung bei, daß der Mensch das Schutzgut des Grundrechts auf informationelle Selbst-Bestimmung ist. In der lang andauernden Diskussion sind demgegenüber bisher einzelne Aspekte wie der Wille des Bürgers als seine Bestimmung hervorgehoben worden; andererseits ist auf das Wissen des Bürgers über die Verwendung seiner Daten und damit mehr auf den informationellen Aspekt abgestellt worden (so Bundesverfassungsrichter Prof. Grimm).

Angesichts der immer umfassenderen Vernetzung wird es für die Bürger aber ständig schwieriger, mit eigenem Wissen und Willen ihr Persönlichkeitsrecht selbst zu schützen. In einer Parallelwelt der Daten sehen sich die Bürger kaum noch in der Lage, ihre digitalen Doppelgänger unter Kontrolle zu behalten. Eine Emnid-Umfrage, wie hoch die Bürger ihre persönliche Gefährdung einschätzen, hat ergeben, daß sie an erster Stelle – mit weitem Abstand z. B. vor Diebstählen oder Überfällen – einen Mißbrauch durch den Handel mit ihren Daten befürchten. Die Bürger haben auch große Angst vor einem Datenmißbrauch durch andere Stellen in Wirtschaft und Verwaltung.

Dahinter steht die grundlegende Sorge der Bürger um ihre persönliche Autonomie, die einen hohen Rang in der Wertehierarchie hat. Die Bürger erwarten, daß ihre Persönlichkeit und damit ihr Selbst stärker von Verwaltung und Wirtschaft respektiert werden. Sie verlangen mehr Achtung vor ihrer Selbstbestimmung und damit zugleich weniger Fremdbestimmung.

Auf dem weiteren Weg in die Informationsgesellschaft muß die Selbstbestimmung der Bürger demgemäß gewahrt werden. Durch immer neue Regelungen insbesondere im Bereich der inneren Sicherheit darf der Datenschutz nicht unverhältnismäßig eingeschränkt werden. Statt dessen braucht der Bürger einen Sicherheitsabstand gegenüber wachsenden Datenansprüchen der Verwaltung, z. B. der Sicherheitsbehörden im neuen Telekommunikationsrecht (16.1).

Außerdem darf sich aus den Sparzwängen durch leere öffentliche Kassen keine Tendenz beim Datenschutz durchsetzen nach dem Motto: „Verwaltungsschutz geht vor Grundrechtsschutz". Billige Lösungen mit Verzicht auf Datenschutzvorkehrungen können sich langfristig als sehr kostenträchtig herausstellen. Geboten ist vielmehr eine systematische Datenvermeidung, mit der in erheblichem Umfang Kosten eingespart werden können (1.3).

Zugleich läßt sich in vielen Fällen darstellen, daß die Akzeptanz der Datenverarbeitung beim Bürger deutlich steigt, wenn er sich auf einen effektiven Datenschutz verlassen kann. Insoweit muß stärker bewußt gemacht werden, daß Datenschutz nicht nur ein Kostenfaktor, sondern vor allem auch ein Nutzenfaktor sein kann.

Inhaltlich und finanziell ist daher der Datenschutz nicht etwa eine Belastung für die Zukunft, die wir uns wegen anderer Prioritäten nicht mehr leisten können. Mehr denn je sind die Bürger und die Gesellschaft insgesamt im „Leben online" auf einen wirksamen Datenschutz angewiesen, damit die unaufhaltsame technische Entwicklung überhaupt grundrechtskonform und sozialverträglich umgesetzt werden kann.

1.2 Grundrecht auf Datenschutz

In der Stellungnahme des Senats vom 28. Mai 1996 zum 14. Tätigkeitsbericht (Bürgerschaftsdrucksache 15/5554) werden derzeit keine Erfolgsaussichten für eine Gesetzesinitiative gesehen, das Grundrecht auf informationelle Selbstbestimmung ausdrücklich in das Grundgesetz aufzunehmen. Inzwischen hat sich aber ein neuer Ansatzpunkt daraus ergeben, daß bei den Europaministern der Länder eine Aufnahme des Grundrechts auf Datenschutz in den EG-Vertrag bei der Maastricht-Revision erörtert wird.

Gegenüber der Europaministerkonferenz habe ich als Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für das Jahr 1996 befürwortet, die Grundrechte auf europäischer Ebene um das Grundrecht auf Datenschutz zu ergänzen. Dazu habe ich auf die Entschließung der Datenschutzbeauftragten vom 9./10. November 1995 zur „Weiterentwicklung des Datenschutzes in der Europäischen Union" und auf die Resolution der Konferenz der Datenschutzbeauftragten der Europäischen Union vom 8. September 1995 hingewiesen. Dort wird übereinstimmend gefordert, bei der Regierungskonferenz anläßlich der Überarbeitung des EG-Vertrags das Grundrecht auf Datenschutz in einen europäischen Grundrechtskatalog aufzunehmen.

1.3 Schwerpunkt Datenvermeidung durch Technik

Im Anschluß an die Internationale Datenschutzkonferenz im Herbst 1995 hatten sich die Datenschutzbeauftragten für das Jahr 1996 vorgenommen, die Möglichkeiten für einen Datenschutz durch Technik intensiv zu klären. Grundgedanke war dabei, daß aus der Computertechnik auch neue Chancen für den Datenschutz entstehen. Damit soll insbesondere den Datenschutzrisiken bei der zunehmenden Vernetzung begegnet werden. Die Gestaltung und Auswahl datenschutzfreundlicher Technologien soll daran ausgerichtet werden, daß keine oder so wenige personenbezogene Daten wie möglich entstehen. Beispielhaft ist dafür die Verwendung von Guthabenkarten als Chipkarten z. B. im Nahverkehr oder beim interaktiven Fernsehen.

In einer Arbeitsgruppe haben die Datenschutzbeauftragten daraufhin Lösungsansätze zur Datenvermeidung durch Anonymisierung und Pseudonymisierung aufgezeigt. Wertvolle Anregungen lieferte hierzu die Veranstaltung des schleswig-holsteinischen Landesbeauftragten für den Datenschutz im August 1996 über „Datenschutz durch Technik – Technik im Dienste der Grundrechte“ und die Internationale Konferenz im September 1996. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat anschließend am 22./23. Oktober 1996 in Hamburg dem als Anlage zu diesem Tätigkeitsbericht (TB) abgedruckten Kurzbericht als Grundlage für die weitere Arbeit zugestimmt.

Wegweisend für diese Bemühungen ist die Ergänzung des Hamburgischen Datenschutzgesetzes, die der bürgerschaftliche Unterausschuß für Datenschutz beraten hat. Danach soll in die gesetzliche Regelung zur Zulässigkeit der Datenverarbeitung ein Zusatz aufgenommen werden, daß das Ziel der Datenvermeidung auch bei der Auswahl und Gestaltung technischer Einrichtungen zu berücksichtigen ist (3.1.1).

Die Zielsetzung eines wirksamen Datenschutzes durch Technik wurde für den Telekommunikations- und Medienbereich weiterverfolgt und von Bund und Ländern ausdrücklich unterstützt. In der Beschlußempfehlung des Bundestagsausschusses für Bildung, Wissenschaft, Forschung, Technologie und Technikfolgen-Abschätzung vom 27. Juni 1996 zu „Multimedia und Informationsgesellschaft“ heißt es dazu: „Soweit als möglich muß die Erhebung von Daten vermieden und die Anonymität der Betroffenen gewahrt werden ...“.

Diese Entwicklung wird nachstehend näher dargestellt (3.1) und an weiteren Beispielen aus dem öffentlichen und nicht-öffentlichen Bereich erläutert (siehe dazu auch im Stichwortverzeichnis unter „Datenvermeidung durch Technik“).

1.4 EG-Datenschutzrichtlinie und Bundesdatenschutzgesetz

Nach der Annahme der EG-Datenschutzrichtlinie am 24. Oktober 1996 (14. TB, 1.4) ist mittlerweile schon über ein Jahr der dreijährigen Anpassungsfrist für das deutsche Datenschutzrecht abgelaufen. Die Datenschutzbeauftragten hatten bereits auf ihrer Konferenz am 14./15. März 1996 in Hamburg ihre zentralen Forderungen an den Gesetzgeber in der Entschließung zusammengefaßt, die am Ende dieses TB abgedruckt ist.

Auch in diesem Zusammenhang haben die Datenschutzbeauftragten ihre Auffassung bekräftigt, daß für einen modernen Datenschutz bei den neuen Techniken eigene Regelungen für Multimedia und elektronische Dienste notwendig sind, insbesondere mit dem Recht der Teilnehmer, diese Dienste anonym nutzen zu können (siehe dazu bereits 1.3).

Bei Chipkarten ist der Schutz vor unfreiwilliger Preisgabe der Daten zu gewährleisten. Der Karteninhaber darf nicht zum Informationsträger ohne oder gegen seinen Willen gemacht werden. Er muß eine umfassende Kenntnis über den Karteninhalt haben, und an seine Einwilligung sind strenge Anforderungen zu stellen.

Die Videoüberwachung ist gesetzlich zu regeln, u. a. mit der Pflicht zu deutlichen Hinweisen bei verdeckten Aufnahmen und einem Auskunftsrecht der Bürger. Zum Schutz vor Persönlichkeitsbewertungen durch den Computer – z. B. bei Feststellung der Zuverlässigkeit – sind automatisierte Einzelentscheidungen zu verbieten, so daß der jeweils Verantwortliche selbst die Bewertung abschließend vorzunehmen hat und sich dabei nicht ausschließlich auf automatisiert gewonnene Erkenntnisse stützen darf.

Nach intensiven Vorarbeiten haben die Datenschutzbeauftragten ein Positionspapier zur Umsetzung der EG-Datenschutzrichtlinie und zur Novellierung des Bundsdatenschutzgesetzes abgefaßt, das der Bundesbeauftragte für den Datenschutz am 7. Juli 1996 dem Bundesministerium des Innern zugeleitet hat. In dem Positionspapier ist eine Vielzahl von konkreten Änderungsvorschlägen für das Bundesdatenschutzgesetz zusammengefaßt.

In unserer öffentlichen Veranstaltung zu den Auswirkungen der EG-Datenschutzrichtlinie (1.6.2) befürwortete Prof. Simitis, Verbesserungen des Datenschutzes bei der Novellierung des Bundesdatenschutzgesetzes umfassend umzusetzen und dabei auch die von der Richtlinie offen gelassenen Regelungsmöglichkeiten für eine höheres deutsches Datenschutzniveau zu nutzen.

1.5 Hamburgische Datenschutzvorschriften

1.5.1 Hamburgisches Datenschutzgesetz

Auf der Grundlage des Senatsentwurfs vom 21. November 1995 (Bürgerschaftsdrucksache 15/4411) und meiner ergänzenden Vorschläge (14. TB, 1.3.1) ist im zuständigen bürgerschaftlichen Ausschuß der Gesetzentwurf zur Änderung des Hamburgischen Datenschutzgesetzes beraten worden (1.1). Die zahlreichen, von mir unterstützten Verbesserungen des Datenschutzes gemäß dem Senatsentwurf wurden von den Abgeordneten in den Auschußberatungen weitgehend übernommen.

Einige meiner Anregungen, z. B. zum Widerspruchsrecht, wurden eingearbeitet. Zur Weiterentwicklung des Datenschutzes kann es wesentlich beitragen, daß der Grundsatz der Datenvermeidung ausdrücklich erstmals in ein Datenschutzgesetz aufgenommen werden soll (1.1, 1.3, 3.1.1). Die von mir kritisierte Beschränkung des Datenschutzes bei öffentlichen Unternehmen in privater Rechtsform (vgl. 14. TB, 1.3.1) blieb allerdings unverändert, so daß Hamburg nun in diesem Punkt im Bund-/Ländervergleich den schwächsten Datenschutz haben wird.

1.5.2 Bereichsspezifische Datenschutzvorschriften

Der Gesetzentwurf des Senats vom 28. Mai 1996 zum Hamburgischen Schulgesetz (Bürgerschaftsdrucksache 15/5553) ist einschließlich der Datenschutzvorschriften im Schulausschuß in mehreren Anhörungen eingehend erörtert worden (8.2).

Im bürgerschaftlichen Verfassungsausschuß wird der Entwurf eines Untersuchungsausschußgesetzes voraussichtlich erst 1997 behandelt werden. Der Entwurf eines hamburgischen Sicherheitsüberprüfungsgesetzes befindet sich noch in der Behördenabstimmung. Der vielfach angekündigte Entwurf eines hamburgischen Gesundheitsdienstgesetzes liegt dagegen noch immer nicht vor.

Für diese Gesetzesvorhaben verbleibt nur noch wenig Zeit, bis der sog. Übergangsbonus mit Ende der Legislaturperiode dieser Bürgerschaft endgültig abgelaufen sein wird.

1.6 Verhältnis zum Bürger

Es spricht für die Akzeptanz unserer Datenschutzberatung und -kontrolle, daß sich Bürger täglich mit schriftlichen oder telefonischen Anliegen an uns wenden oder persönlich in die Dienststelle kommen. Die Bürgersprechstunden wurden zweimonatlich fortgesetzt.

1.6.1 Eingaben

Aus dem öffentlichen und dem nicht-öffentlichen Bereich richteten die Bürger zahlreiche Eingaben an uns. Bis Ende November gingen 399 schriftliche Eingaben zu folgenden Themen ein:

Öffentlicher Bereich	201
davon Inneres und Justiz	99
Gesundheit und Soziales	41
Sonstiges	61
Nicht-öffentlicher Bereich	198
davon Versandhandel	8
Versicherungswirtschaft	25
Kreditwirtschaft	33
Werbung	38
Arbeitnehmer-Datenschutz	13
Schufa und Auskunfteien	23
Gesundheitswesen	10
Wohnungswirtschaft	7
Verkehrswesen	5
Markt-und Meinungsforschung	1
Sonstiges	35

1.6.2 Öffentlichkeitsarbeit

In der Reihe unserer öffentlichen Veranstaltungen in Zusammenarbeit mit dem Kommunikationsverein Hamburger Juristen sprach der langjährige Hessische Datenschutzbeauftragte und jetzige Berater der Europäischen Kommission, Prof. Simitis, über das Thema „Was bringt uns die europäische Datenschutzrichtlinie: Verbesserungen oder Verschlechterungen?“ (1.4).

Auf unseren vierteljährlichen Pressekonferenzen wurden diesmal im Frühjahr und im Herbst die wichtigsten Ergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Rathaus bekanntgegeben. Hauptpunkt der Pressekonferenz vom 6. Juni 1996 waren die bei unserer Netzprüfung festgestellten schweren Datenschutzmängel im Datennetz der hamburgischen Verwaltung (3.2).

Mit gesonderten Presseerklärungen veröffentlichten wir Mitte Mai 1996 die Entschließung der Datenschutzbeauftragten des Bundes und der Länder mit ihren Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten sowie die Entschließung mit Eckpunkten für die datenschutzrechtliche Regelung von Mediendiensten.

Zusammen mit dem Berliner Datenschutzbeauftragten und den Landesbeauftragten für Bremen und für Niedersachsen haben wir ein Faltblatt über „Handels- und Wirtschaftsauskunfteien“ veröffentlicht, das auch die Verbraucherzentrale zur Verteilung erhielt.

Seit dem Sommer 1996 gibt es ein „offizielles“ Angebot des Hamburgischen Datenschutzbeauftragten im Internet. Es ist unter folgender Adresse abrufbar: http://www.hamburg.de/Behoerden/HmbDSB/index.htm. Neben den Tätigkeitsberichten können auch Broschüren und aktuelle Presseerklärungen abgerufen werden (siehe auch die letzte Seite dieses TB).

Aus Anlaß der Novellierung des Hamburgischen Datenschutzgesetzes bereiten wir eine Broschüre über das neue Gesetz mit Text und Erläuterungen vor. Die bisherige Broschüre ist nach großer Nachfrage seit langem vergriffen.

1.6.3 Zusammenarbeit mit Verwaltung und Justiz

Mit den hamburgischen Behörden und Kammern sowie der Justiz wurde die Zusammenarbeit konstruktiv fortgesetzt. Beim Datenschutz-Jahrestreffen bestand zum fünften Mal Gelegenheit zum Meinungsaustausch mit Vertretern der Bürgerschaft, Justiz, Verwaltung, Kammern und Gewerkschaften.

Förmliche Beanstandungen konnten dadurch vermieden werden, daß bei schweren Datenschutzverstößen umgehend die Mängel behoben wurden, insbesondere aufgrund der Ergebnisse unserer Netzprüfung (3.2). In anderen Fällen waren Entwürfe für eine förmliche Beanstandung bereits vorbereitet worden; die Beanstandungen konnten auch hier wegen angemessener Abhilfe durch die zuständigen Stellen noch vermieden werden.

2. Entwicklung der Dienststelle

Im Jahr 1996 gab es wiederum nur wenige personelle Veränderungen. Zu den Sparmaßnahmen mußten auch wir durch die Bereitschaft beitragen, eine Stelle anteilig für 1997 streichen zu lassen. Seit Anfang 1996 werden andererseits zunehmend Aufgaben von der Justizbehörde auf die Dienststelle verlagert, ohne daß dafür bisher ein personeller oder sonstiger Ausgleich erfolgt ist.

Angesichts der Sparmaßnahmen wird die Bewilligung notwendiger zusätzlicher Stellen immer schwieriger. Immerhin gibt es voraussichtlich die Möglichkeit, daß ein Mitarbeiter aus

dem Bereich der Polizei zu uns abgeordnet wird. Weiter klärungsbedürftig ist die Möglichkeit, aus den Personalkostenreduzierungen bei großen IuK-Projekten der Behörden uns eine personelle Verstärkung zur Verfügung zu stellen (14. TB, 2.).

Im Sachhaushalt wurden im Jahr 1996 erhebliche Einsparungen vorgenommen, zum Teil ohne meine – nach § 22 Abs. 2 Hamburgisches Datenschutzgesetz gebotene – vorherige Beteiligung. Erst nach langwierigen Bemühungen konnte ich eine für uns untragbare Kürzung der Haushaltsmittel für Dienstreisen rückgängig machen, da die regelmäßige Teilnahme an den gemeinsamen Arbeitskreisen der Datenschutzbeauftragten des Bundes und der Länder für die arbeitsteilige, aktuelle Behandlung von Datenschutzfragen unerläßlich ist.

Dagegen war eine wesentliche Kürzung der Haushaltsmittel für Veröffentlichungen vertretbar mit der Folge, daß dieser TB – gegenüber der bereits im Vorjahr gekürzten Fassung von zuletzt 140 Seiten – nur noch einen Umfang von 85 Seiten hat.

Eine große Einsparung war außerdem für die Folgejahre dadurch möglich, daß die Führung des Dateiregisters und die kostspielige Veröffentlichung der Übersicht über das Dateiregister im Amtlichen Anzeiger mit zuletzt über 220 Seiten ganz entfällt, zumal die Bürger diese Informationsmöglichkeit fast gar nicht genutz haben.

3. Informations- und Kommunikationstechnik

3.1 Datenvermeidung durch Technik

3.1.1 Grundsatz der Datenvermeidung

Nicht zuletzt die weitaus stärkere Nutzung des Internet, aber auch der zunehmende Einsatz von Chipkarten haben dazu geführt, daß computergestützte Verfahren mittlerweile Einzug in fast sämtliche Lebensbereiche erhalten haben. Elektronische Geldbörsen, Patienten-Chipkarten, Online-Dienste und vieles andere mehr sorgen dafür, daß über jeden Einzelnen eine Fülle von personenbezogenen Daten gespeichert werden. Die datenschutzrechtlichen Risiken, die von solchen Anwendungen ausgehen, liegen hauptsächlich darin, daß die an vielen Orten gespeicherten Daten zusammengeführt und detaillierte Persönlichkeitsprofile gewonnen werden können. Es besteht die Gefahr, daß der datenfreie Raum, in dem sich der Bürger noch unbeobachtet bewegen kann, immer kleiner wird.

Allein mit den traditionellen datenschutzrechtlichen Grundsätzen der Erforderlichkeit und Zweckbindung können derartige Risiken nicht mehr eingegrenzt werden. So kann von Betreibern der EDV-Systeme zumeist plausibel begründet werden, zu welchem Zweck die einzelnen personenbezogenen Daten erhoben bzw. übermittelt werden sollen. Auch die technisch-organisatorischen Vorgaben des Datenschutzrechts beschränken sich auf die Absicherung der eingesetzten Technik und haben kaum Einfluß auf die Systementscheidung. Die viel entscheidendere Frage, ob nicht eventuell technische Alternativen existieren, die lediglich einen Bruchteil der gespeicherten personenbezogenen Daten benötigen, wurde in den zurückliegenden Jahren zu wenig diskutiert. Eine ausführliche Technikfolgenabschätzung, die auch den Vergleich mehrerer technischer Alternativen unter dem Gesichtspunkt der Datenvermeidung zum Gegenstand hatte, fand nur in den seltensten Fällen statt.

Dies ist erstaunlich, weil das Bundesverfassungsgericht schon im Volkszählungsurteil von 1983 – am Beispiel der Statistik – das Grundrecht auf Anonymität anerkannt hat. Dazu heißt es im Volkszählungsurteil, daß bereits bei der Erhebung von Einzelangaben zu prüfen ist, „ob das Ziel der Erhebung nicht auch durch eine anonymisierte Ermittlung erreicht werden kann . . . Eine personenbezogene Erhebung . . . wäre deshalb von vornherein ein Verstoß gegen das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte Persönlichkeitsrecht“ (BVerfGE 65,1 – 48 f. –).

Außerdem weist das Gericht darauf hin, daß es „zur Sicherung des Rechts auf informationelle Selbstbestimmung besonderer Vorkehrungen für Durchführung und Organisation der Datenerhebung“ bedarf: „Für den Schutz des Rechts auf informationelle Selbstbestimmung ist – und zwar auch schon für das Erhebungsverfahren – . . . die Einhaltung des Gebots einer möglichst frühzeitigen faktischen Anonymisierung unverzichtbar, verbunden mit Vorkehrungen gegen die Deanonymisierung“ (BVerfGE a.a.O., S. 49).

In der Rechtsprechung zum Medienrecht ist dieses Grundrecht ebenfalls seit längerem als besondere Ausprägung des Persönlichkeitsrechts anerkannt, beispielsweise vom Bundesgerichtshof: „Das Recht auf informationelle Selbstbestimmung schützt . . . davor, aus dem Bereich der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden“ (BGH AfP 1994, 306 – 307 –).

Angesichts der zunehmenden Technisierung haben die Datenschutzbeauftragten des Bundes und der Länder das Anonymisierungsgebot verstärkt aufgegriffen und bei der Gestaltung und Auswahl technischer Systeme mehr als bisher umzusetzen versucht. Auch bei Gesetzesvorhaben wurde darauf gedrängt, Anonymisierung und Pseudonymisierung entsprechend vorzusehen, und zwar gerade auch in Form der Anonymität von Anfang an (vgl. 1.3).

Erfreulicherweise hat auch der Rat für Forschung, Technologie und Innovation, der unter Federführung des Bundeskanzleramts und des Bundesministers für Bildung, Wissenschaft, Forschung und Technologie einen ausführlichen Bericht über Chancen, Innovationen und Herausforderungen der Informationsgesellschaft erstellt hat, das Thema Anonymisierung aufgegriffen. Der Rat führt in Kap. 2.5 über Datenschutz folgendes aus: „Den Vorrang verdienen Verfahren, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern“. Entsprechende Passagen finden sich auch in den Bundestags- und Bundesratsdrucksachen über „Deutschlands Weg in die Informationsgesellschaft“ wieder.

Es ist daher zu begrüßen, daß der Grundsatz der Datenvermeidung auch in den Entwürfen zum Teledienstedatenschutzgesetz und zum Mediendienstestaatsvertrag enthalten ist. Anbieter von Tele- bzw. Mediendiensten haben den Nutzern die Inanspruchnahme und Bezahlung entweder vollständig anonym oder unter Verwendung eines Pseudonyms zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Ebenso sind Nutzungsprofile nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erfaßte Nutzungsprofile dürfen nicht mit Daten zusammengeführt werden, die den Träger des Pseudonyms betreffen.

Der Grundsatz der Datenvermeidung soll nunmehr als generelle Regelung in das Hamburgische Datenschutzgesetz aufgenommen werden (vgl. 1.3). In § 5 HmbDSG, der die

allgemeinen Anforderungen an die Zulässigkeit der Datenverarbeitung regelt, soll folgender Absatz 4 angefügt werden:

„Die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung technischer Einrichtungen haben sich auch an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiter zu verarbeiten. Dabei ist jeweils zu prüfen, inwieweit es möglich ist, personenbezogene Daten anonym oder pseudomym zu verarbeiten. Erforderlich sind Maßnahmen zur anonymen oder pseudonymen Datenverarbeitung nur, wenn ihr Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht."

Damit wird die Zielsetzung der Datenvermeidung zum verbindlichen Grundsatz für die gesamte Datenverarbeitung. Die hamburgische Regelung kann wegweisend für die weitere Diskussion zur Modernisierung des Datenschutzes werden.

3.1.2 Anonymität

Ein Höchstmaß an Anonymität wird erreicht, wenn personenbezogene Daten gar nicht erst entstehen. In der Praxis bewährte Beispiele sind anonyme Telefonkarten und anonyme Karten im öffentlichen Personennahverkehr.

Sind personenbezogene Daten bereits erhoben worden, ist eine faktische Anonymisierung so bald wie möglich sicherzustellen. Anonymisieren ist gemäß § 3 Absatz 7 BDSG „das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können". Beispiele sind die Anforderungen im Statistikrecht und die Forschungsklauseln im BDSG.

Auch wenn anonyme Daten nicht (mehr) personenbezogen sind, entfällt nicht von vornherein vollständig die Geltung des Datenschutzrechts. Vielmehr sind die gesetzlichen Anforderungen an Art und Zeitpunkt der Anonymisierung einzuhalten und technisch-organisatorische Maßnahmen gegen unbefugten Zugriff zu treffen.

3.1.3 Pseudonyme

Pseudonyme werden anstelle personenbezogener Identifikationsdaten verwendet, wie beispielsweise Name, Anschrift und Geburtsdatum oder Aktenzeichen. Sie ermöglichen es, den Personenbezug herzustellen, ohne daß die Identität der Person jederzeit erkennbar ist.

Pseudonyme sollten nicht generell, sondern nur für jeweils ein Verfahren eingesetzt werden. Jede generelle Benutzung eines einzigen Pseudonyms würde die Gefahr erhöhen, daß aus sämtlichen, mit dem Pseudonym verbundenen Daten doch wieder ein detailliertes Personenprofil erstellt werden kann, das den Rückschluß auf eine bestimmte Person erleichert.

Insgesamt wird zwischen drei Arten von Pseudonymen unterschieden:

1. Selbstgenerierte Pseudonyme:

Selbstgenerierte Pseudonyme werden ausschließlich vom Betroffenen vergeben. Somit kann auch der Personenbezug nur vom Betroffenen selbst wiederhergestellt werden, nicht jedoch durch den Betreiber der EDV-Systeme.

Selbstgenerierte Pseudonyme sollten Verwendung finden bei wissenschaftlichen Studien, die einerseits aggregierte Auskünfte über bestimmte Personengruppen geben sollen, andererseits aber auch den Betroffenen die Möglichkeit einräumen möchten, sich über ihre persönlichen Einzelergebnissen unerkannt zu informieren. Da es für die auswertende Stelle nicht erforderlich ist, die erhobenen Daten personenbezogen auszuwerten, kann statt des Namens ein vom Betroffenen selbstgewähltes Pseudonym verwendet werden, mit dessen Hilfe der Betroffene – und nur er selbst – die Ergebnisse in Erfahrung bringen kann, die ausschließlich seinen Einzelfall betreffen.

2. Referenz-Pseudonyme:

Bei Referenz-Pseudonymen kann der Personenbezug über entsprechende Referenzlisten wiederhergestellt werden. Ohne Hinzuziehung entsprechender Referenzlisten ist die Identität des Betroffenen jedoch nicht zu ermitteln.

Referenz-Pseudonyme eignen sich für Anwendungen, bei denen der Betroffene nur in bestimmten Ausnahmefällen ermittelt werden muß, beispielsweise bei fehlerhaften Zahlungsvorgängen. Um zu erreichen, daß die Pseudonyme nicht aufgelöst werden, empfiehlt es sich, die Referenzliste räumlich unabhängig von den mit Pseudonymen versehenen Datensätzen bei einer vertrauenswürdigen Stelle, einem sogenannten Trust-Center, zu speichern. Um einen besseren Schutz gegen die unbefugte Auflösung eines Pseudonyms zu erreichen, können die Codes, die in den Referenzlisten zur Wiederherstellung des Personenbezugs gespeichert sind, auch auf zwei oder mehrere vertauenswürdige Instanzen verteilt werden. Nur wenn sämtliche vertrauenswürdigen Stellen bereit sind, ihre jeweiligen Referenzlisten zur Verfügung zu stellen, kann das verwendete Pseudonym einer Person zugeordnet werden.

Beispiel 1: Nutzung von Online-Diensten

Zahlreiche Anbieter von Online-Diensten sehen die Möglichkeit vor, daß die Anwender einen Teil der angebotenen Dienste – beispielsweise Diskussionsrunden – nicht unter ihrer Benutzerkennung, sondern unter einem Pseudonym benutzen. Die von den Anwendern benutzten Pseudonyme sind den Anbietern von OnlineDiensten allerdings bekannt, so daß es sich hierbei um Referenz-Pseudonyme handelt.

Beispiel 2: Qualitätssicherung im Gesundheitswesen (vgl. 13. TB, 21.2)

Beispiel 3: Basisdokumentation der Drogenberatungsstellen (vgl. 19.1)

Beispiel 4: Barcode-Verfahren des Zentralinstituts für Transfusionsmedizin bei Blutspenden

Die Spenderblutbeutel werden ausschließlich mit der Blutgruppe und einer Konservennummer gekennzeichnet. Weder der Name noch – wie bis Oktober 1995 – das Geburtsdatum des Blutspenders werden dem Krankenhaus übermittelt. Für Kontrollzwecke

werden jedoch im Zentralinstitut die Konservennummern den Spendernamen zugeordnet. Bei sogenannten Kreuzproben, die das Blut eines Patienten mit anderem Blut vergleichen, werden hierdurch dem behandelnden Krankenhaus die jeweiligen Ergebnisse namensbezogen mitgeteilt.

3. Einweg-Pseudonyme:

Einweg-Pseudonyme zeichnen sich dadurch aus, daß sie mittels Einweg-Funktion aus personenbezogenen Identitätsdaten – zumeist auf der Basis asymmetrischer Verschlüsselungsverfahren – gebildet werden. Dabei werden Einweg-Funktionen verwendet, die mit hoher Wahrscheinlichkeit ausschließen, daß die Identitätsdaten zweier Personen auf ein gemeinsames Pseudonym abgebildet werden.

Ohne Kontextwissen läßt sich bei Einweg-Pseudonymen – anders als bei selbstgenerierten oder Referenz-Pseudonymen – der Personenbezug nur mit unverhältnismäßig hohem Aufwand wiederherstellen. Dies gilt sowohl für den Betroffenen als auch für den Betreiber des Verfahrens. Mit detailliertem Kontextwissen und Kenntnissen über die Einweg-Funktion kann die jeweilige Person allerdings erheblich leichter ermittelt werden: Falls sämtliche Personen bekannt sind, aus deren Reihen der Betroffene ermittelt werden soll, beispielsweise die Schüler einer Klasse (vgl. Beispiel 5), muß lediglich mittels Einweg-Funktion aus den Identitätsdaten dieser Personen das jeweilige Pseudonym gebildet und mit dem bereits vorhandenen Pseudonym verglichen werden.

Einweg-Pseudonyme eignen sich zum einen für Längsschnittuntersuchungen, bei denen nachträglich erhobene personenbezogene Daten mit Bestandsdaten zusammengeführt werden, ohne daß der Personenbezug für die statistische Auswertung der Daten erforderlich ist. Zum anderen können Einweg-Pseudonyme bei Auskunftssystemen eingesetzt werden, die Auskunft über die Zugehörigkeit bzw. Nicht-Zugehörigkeit einer Person zu einer bestimmten Gruppe geben, ohne daß dabei personenbezogene Identitätsdaten gespeichert werden müssen.

Beispiel 5: Lernausgangslagen-Untersuchung (vgl. 8.1)

Beispiel 6: Auskunfteien

Theoretisch besteht auch bei Auskunfteien die Möglichkeit, auf die Speicherung von Personenstammdaten wie Name, Geburtsdatum und Adresse zu verzichten und statt dessen ein Einweg-Pseudonym zu benutzen. Sämtliche Auskünfte würden dann nicht mehr über den Namen, sondern durch Nennung des Pseudonyms eingeholt, das von der Auskunft einholenden Stelle vorab durch Einwegfunktion errechnet würde. Auf die gleiche Weise könnte Betroffenen gemäß § 34 BDSG Auskunft über die zu ihrer Person gespeicherten Daten gegeben werden. Auch Ergänzungen zu den gespeicherten Datensätzen könnten über das Pseudonym mit den bereits vorhandenen Daten problemlos verknüpft werden.

Angesichts des Tätigkeitsfeldes von Auskunfteien wäre die Benutzung von Pseudonymen aber mit Schwierigkeiten verbunden. Auskunfteien wären nicht mehr in der Lage, bonitätsgeprüfte Adressen weiterzugeben, was teilweise erfolgt. Auch müßten neue Verfahren entwickelt werden, die die in § 33 BDSG geforderte Benachrichtigung der Betroffenen regeln.

3.1.4 Rechtliche Bewertung

Mit Referenz- und Einweg-Pseudonymen versehene Daten sind weiterhin personenbezogene Daten. Da bei Referenz-Pseudonymen die Herstellung des Personenbezugs nicht auf den Betroffenen beschränkt bleibt, kann nicht von Anonymität im Sinne des § 3 Absatz 7 BDSG gesprochen werden. Dies gilt auch für den Fall, daß der Personenbezug nur durch eine besonders vertrauenswürdige Stelle herstellbar ist. Einweg-Pseudonyme sind ebenfalls nicht anonym im Sinne des BDSG, da zumindest überprüft werden kann, ob nicht einzelne Personen unter einem bestimmten Pseudonym gespeichert werden.

Datensätze, die mit einem Referenz- oder Einweg-Pseudonym versehen sind, entziehen sich demnach nicht dem Geltungsbereich des BDSG. Grundsätze der Erforderlichkeit und der Zweckbindung sind ebenso zu beachten wie allgemeine Löschungsfristen. Auch ist den Betroffenen auf Wunsch Auskunft über die zu einem Pseudonym gespeicherten Daten zu erteilen, wenn der Betroffene zweifelsfrei nachweisen kann, daß sich das Pseudonym auf seine Person bezieht. Schließlich ist der Zugriff auf Pseudonyme durch geeignete technisch-organisatorische Maßnahmen entsprechend zu sichern.

Selbstgenerierte Pseudonyme sind dagegen vollständig anonym. Der Betroffene erstellt das Pseudonym selbst und ist gleichzeitig auch der einzige Geheimnisträger, der den Personenbezug herstellen kann.

3.2 Prüfung des Datennetzes der hamburgischen Verwaltung

Nachdem wir wiederholt auf die Probleme der flächendeckenden Vernetzung der hamburgischen Verwaltung hingewiesen haben (zuletzt im 14. TB, 3.1), haben wir die zugrundeliegende Infrastruktur im Berichtszeitraum einer intensiven Prüfung unterzogen.

Die Prüfung erfolgte unter Verwendung des Netzzuganges in der Dienststelle des Hamburgischen Datenschutzbeauftragten mit verschiedenen Standardprogrammen und Prüfwerkzeugen.

Dabei wurde eine Reihe schwerwiegender technischer und administrativer Mängel festgestellt. Sie sind folgenden beiden Bereichen zuzuordnen:

Lokale Computer in den Behörden und Ämtern

- Verwendung von Kennungen ohne Paßwortschutz oder mit leicht erratbaren Paßwörtern
- Aktivierung von Netzwerkdiensten ohne Erforderlichkeit
- mangelhafter Zugriffschutz auf Dateiebene

Vom LIT betriebenes, behördenübergreifendes Netzwerk

- mangelnde Zugriffskontrolle im Netz
- fehlende Sicherung von Routern

Das Datennetz war im Prüfzeitraum im wesentlichen für sämtlichen Datenverkehr zwischen den angeschlossenen Computern der Verwaltung geöffnet. Die Verbindungen dieser Rechner untereinander waren nicht auf das für die Aufgabenerfüllung erforderliche Maß beschränkt. Dies konnte in Verbindung mit der mangelhaften Administration einer Reihe der vernetzten Computer für einen unzulässigen Zugriff auf gespeicherte Daten ausgenutzt werden. Unsere

Kritik betraf daher sowohl das LIT als Netzbetreiber als auch die einzelnen betroffenen Behörden als Verantwortliche für die lokale Technik.

Als Reaktion auf die Prüfung des Datennetzes wurde vom LIT umgehend eine flächendeckende Filterung des Netzverkehrs technisch umgesetzt. Sie orientiert sich an der Erforderlichkeit von Kommunikationsverbindungen der angeschlossenen Dienststellen. Die Wirksamkeit dieser Maßnahme wurde von uns in einer Nachprüfung bestätigt.

Nachbesserungen fanden auch bei der lokalen Technik statt, insbesondere hinsichtlich der Paßwortverwaltung und der Aktivierung von Netzwerkdiensten. Auch hier wurde das für die Aufgabenerfüllung Erforderliche als Maßstab angesetzt.

Insgesamt hat die Prüfung zu einer deutlichen Verbesserung der Datensicherheit im hamburgischen Verwaltungsnetz geführt und die Sensibilität für die datenschutzrechtlichen Probleme der flächendeckenden Vernetzung erheblich erhöht.

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4. Parlamentsspezifischer Datenschutz

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Konferenz am 22./23. Oktober 1996 in Hamburg Fragen des parlamentsspezifischen Datenschutzes erörtert. Grundlage dieser Diskussion waren unsere „Empfehlungen“, die in der Anlage abgedruckt sind.

Die Verarbeitung personenbezogener Daten für Zwecke parlamentarischer Aufgabenerfüllung berührt vielfach Persönlichkeitsrechte der Betroffenen. Insbesondere für parlamentarische Anfragen und Untersuchungsausschüsse werden auch sensible, durch Berufsgeheimnisse besonders geschützte Daten, z. B. über den Gesundheitszustand, genutzt. Der – legitime – Öffentlichkeitsbezug verstärkt dabei das Gewicht des Grundrechtseingriffs. Im Rahmen unseres gesetzlichen Beratungsauftrags treten wir für eine umfassende bereichsspezifische Regelung mit Rechtsnormqualität, insbesondere durch formelles Gesetz, ein. Ferner haben wir konkrete Vorschläge für eine datenschutzgerechte Verfahrensgestaltung, z. B. im Falle von Schweigepflichtsentbindungen, vorgelegt.

5. Neue Medien / Telekommunikation

5.1 Digitales Fernsehen

Das digitale Fernsehen (vgl. 14. TB, 4.2.1) stellt nicht bloß eine Vervielfachung von Übertragungskapazitäten bereit, sondern es ermöglicht auch neue Sende- und Abrechnungsformen. Eine dieser neuen Formen ist das sogenannte „pay per view“, d. h. die Einzelabrechnung der jeweils gesehenen Sendungen. Dabei werden die verschlüsselt übertragenen Signale durch ein Zusatzgerät, die sogenannte „set top box“ entschlüsselt und auf dem Fernseher sichtbar gemacht, wenn der in die set top box eingebaute Decoder freigeschaltet ist, d. h. ein entsprechendes Signal empfangen hat.

Durch die individuelle Freischaltung entsteht die Gefahr, daß das Fernsehverhalten registriert wird und so im nachhinein festgestellt werden kann, welcher Nutzer wann welche Sendungen gesehen hat. Diese Nutzungsdaten könnten zu Mediennutzungsprofilen zusammengeführt und für verschiedene Zwecke ausgewertet werden. So könnten Programmveranstalter und andere Unternehmen die Daten für gezielte Werbung nutzen. Auch staatliche Stellen könnten Interesse an einem Zugriff auf die Mediennutzungsdaten haben, z. B. Polizei und Staatsanwaltschaft.

Wenn durch die neuen Formen der Verbreitung und Abrechnung von Fernsehsendungen das Mediennutzungsverhalten der Bürgerinnen und Bürger kontrollierbar würde, berührt dies nicht nur das Recht auf informationelle Selbstbestimmung, sondern auch die durch Artikel 5 Grundgesetz garantierte Informations- und Meinungsfreiheit.

Die 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu diesem Thema die in der Anlage enthaltene Entschließung verabschiedet. Die datenschutzrechtliche Kernforderung besteht darin, daß auch beim digitalen Fernsehen eine unbeobachtete Mediennutzung möglich bleiben muß. Die technischen Voraussetzungen für derartige datenschutzfreundliche Zugriffs- und Abrechnungsverfahren sind gegeben. Entsprechende anonyme Abrechnungsverfahren könnten realisiert werden, indem vorausbezahlte Chipkarten zum Einsatz kommen. Dadurch soll auch der Datenschutz durch Datenvermeidung umgesetzt werden (vgl. 3.1).

Die datenschutzrechtlichen Vorgaben für pay per view sollten bei dem derzeit vorbereiteten Vierten Rundfunkänderungsstaatsvertrag berücksichtigt werden, bei dem ohnehin die Entwicklungen im Bereich des digitalen Fernsehens im Mittelpunkt stehen werden. Die entsprechenden Datenschutzvorschriften könnten sich dabei an dem Standard orientieren, den der Entwurf eines Mediendienste-Staatsvertrages (vgl. 5.2) vorsieht.

5.2 Datenschutzregelungen für Medien- und Teledienste

Für den Einsatz neuer Informations- und Kommunikationstechniken ist es dringend erforderlich, einen einheitlichen rechtlichen Rahmen für die neuen Tele- und Mediendienste zu schaffen (vgl. 13. TB, 4.2). Ein derartiger Rahmen zeichnet sich jetzt ab: Nach Absicht der Länder soll ein Staatsvertrag über Mediendienste (Mediendienste-StV) noch in der ersten Hälfte des Jahres 1997 in Kraft treten. Parallel hierzu hat die Bundesregierung den Referentenenwurf eines Informations- und Kommunikationsdienste-Gesetzes vorgelegt (IuKDG), der unter anderem Datenschutzbestimmungen für Teledienste enthält.

Nach den weitgehend miteinander abgestimmten Datenschutzregelungen beider Entwürfe wird in Zukunft für Medien- und Teledienste ein hohes Schutzniveau vorgeschrieben. Hinzuweisen ist insbesondere auf die Verpflichtung für die Anbieter, die Gestaltung und Auswahl technischer Einrichtungen an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben und zu verarbeiten. Die Anbieter haben dem Nutzer die Inanspruchnahme von Mediendiensten und ihre Bezahlung anonym (vgl. 3.1.2) oder unter Pseudonym (vgl. 3.1.3) zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Personenbezogene Daten, die bei der Mediennutzung erhoben werden, sollen einer strikten Zweckbindung unterliegen.

Problematisch ist hingegen eine im IuKDG vorgesehene Regelung, die die Diensteanbieter dazu verpflichten soll, Bestandsdaten für die Verfolgung von Straftaten und

Ordnungswidrigkeiten und für die Gefahrenabwehr an die Sicherheitsbehörden zu übermitteln. Auch an die Verfassungsschutzbehörden, den BND und den MAD sollen diese Daten übermittelt werden, soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.

6. Soziales

6.1 Auflösung einer Krankenkasse

Die Betriebskrankenkasse (BKK) Hamburg-Süd hat nach unseren Informationen kurz vor ihrer zum 30. Juni 1996 erfolgten Auflösung Versichertendaten an eine andere BKK übermittelt, damit von dort Krankenversichertenkarten ausgestellt werden konnten. Diese Übermittlungen erfolgten unabhängig davon, ob die Versicherten sich für eine künftige Versicherung bei dieser anderen BKK entschieden hatten, und waren daher unzulässig.

Durch die Auflösung der BKK Hamburg-Süd trat erstmalig die bislang ungeklärte Frage auf, wie eine aufzulösende Krankenkasse mit den von ihr gespeicherten Versichertendaten umzugehen hat. Während Krankenkassen Versichertendaten üblicherweise mehrjährig speichern müssen und dürfen, hat eine aufzulösende Krankenkasse ein Interesse daran, sich möglichst bald der Versichertendaten zu entledigen.

§ 304 Abs. 2 Sozialgesetzbuch/Fünftes Buch erlaubt aber nicht die Übermittlung aller Versichertendaten an die von dem Versicherten gewählte neue Krankenkasse; insbesondere Daten über abgerechnete Leistungen dürfen der gewählten neuen Krankenkasse nur bei Erforderlichkeit im Einzelfall und auf ein entsprechendes Ersuchen hin übermittelt werden. Das würde allerdings eigentlich voraussetzen, daß die aufzulösende Krankenkasse als speichernde und übermittelnde Stelle so lange erhalten bleibt, wie die Versichertendaten nach den Vorschriften des Sozialgesetzbuchs zu speichern sind; die Auflösungsphase würde sich damit erheblich verlängern.

Mangels einer gesetzlich abgesicherten Lösung werden wir mit dem Auflösungsvorstand der BKK Hamburg-Süd nach einer eher pragmatischen Lösung suchen. In Betracht kommt dabei auch eine Art treuhänderischer Speicherung bzw. Aufbewahrung durch den BKK-Landesverband NORD, der auch bislang schon die elektronische Datenverarbeitung im Auftrag der BKK Hamburg-Süd durchführte.

6.2 Umgang mit Schwerbehindertendaten im Landesamt für Rehabilitation

Im Landesamt für Rehabilitation der Behörde für Arbeit, Gesundheit und Soziales haben wir ein EDV-gestütztes Verfahren für die Eingliederungshilfe bei stationärer und teilstationärer Unterbringung geprüft. Zu unseren Verbesserungsvorschlägen lag uns auch nach fünf Monaten noch keine Stellungnahme vor.

Als zentrales Problem im Verfahren erwies sich die Anforderung sog. Entwicklungsberichte über die Behinderten bei Rehabilitationseinrichtungen. Wir haben dem Landesamt empfohlen, die Rehabilitationseinrichtungen gemäß

§ 67 a Abs. 4 SGB X darauf hinzuweisen, inwieweit sie zu diesen Berichten verpflichtet sind. Damit der Inhalt der Berichte sich auf erforderliche Angaben beschränkt, sollte das Landesamt die Rehabilitationseinrichtungen zudem darauf hinweisen, welche inhaltlichen Bereiche die Berichte abdecken sollen. Der Umstand, daß die Mitarbeiter in den Rehabilitationseinrichtungen im Regelfall einer durch § 203 StGB strafbewehrten Schweigepflicht unterliegen, erfordert nach unserer Auffassung zudem, daß Entwicklungsberichte nur angefordert werden sollten, wenn der betroffene Behinderte bzw. sein gesetzlicher Vertreter insoweit von der Schweigepflicht entbunden haben. Die betroffenen Behinderten selbst sollten aus Gründen der Transparenz über den Bericht informiert werden.

Verbesserungsbedürftig sind zudem die Anforderung und Aufbewahrung ärztlicher und psychologischer Unterlagen sowie die Fassung der verwendeten Schweigepflichtentbindungserklärung. Mängel mußten wir auch hinsichtlich der in der EDV realisierten Zugriffsrestriktionen und Protokollierungen feststellen.

6.3 Sonstiges

Einzelne weitere Problemfelder des Sozialleistungsbereichs waren im Berichtszeitraum

– der Umfang der Datenerhebung und -speicherung im automatisierten Sozialhilfe-Verfahren (PROSA) sowie die Hinweise in der Hilfeempfängererklärung,
– die Kennzeichnung von Sozialleistungen auf Überweisungsträgern,
– die Rehabilitationsverfahren der Landesversicherungsanstalt (vgl. 14. TB, 5.5),

– die Vergabe der Abrechnung von Arznei-, Heilund Hilfsmitteln durch die Betriebskrankenkasse der Freien und Hansestadt Hamburg an einen privaten Dienstleister,

– das Verfahren „Dokumentation in der Pflege“ (DiP) des Landesbetriebes Pflegen & Wohnen,

– ein vernetztes IuK-Projekt des Landesamtes für Rehabilitation für die Stammdatenverwaltung und Schriftguterstellung in der Landesbetreuungsstelle und ihren Regionalgruppen.

Verbesserungsbedürftig sind nach unseren Feststellungen die Informationsgrundlagen der Sachbearbeiter/innen in den Sozialdienststellen. Die geltenden Datenschutzbestimmungen des Sozialgesetzbuch/Zehntes Buch stehen vielen von ihnen nicht zur Verfügung; die Fachliche Weisung der Behörde für Arbeit, Gesundheit und Soziales zum Schutz der Sozialdaten ist dringend ergänzungs- und korrekturbedürftig. Mit dem Senatsamt für Bezirksangelegenheiten sind wir wegen einer Verbesserung der Schulungen im Gespräch.

Sofern datenschutzrechtliche Fragen mit dem Landessozialamt oder dem Landesamt für Rehabilitation zu klären sind, müssen wir leider immer wieder feststellen, daß wir Antworten auf unsere Fragen nicht bzw. erst sehr spät und nach mehrfacher Erinnerung erhalten. Beides dient der Sache nicht und erschwert unsere Arbeit – unnötig – ganz erheblich.

7. Personalwesen

7.1 Kostenstellenrechnungen und Zeitanschreibungen

Durch eine Eingabe haben wir erfahren, daß die Mitarbeiter der Hamburger Stadtentwässerung auf der Grundlage des Tarifvertrages über die dortige Einführung leistungsbezogener Entgeltbestandteile (LEB) von der Geschäftsführung aufgrund einer Verfügung verpflichtet wurden, Arbeitsaufzeichnungsbögen zu führen, um das Verfahren für die spätere Abrechnung zu erproben.

Auf dem rechten Teil des Bogens sind unter Angabe des Namens täglich detaillierte Nachweise u. a. über die einzelnen Arten der Tätigkeiten, deren stundenmäßige Verteilung auf die gesamte Arbeitszeit sowie Abwesenheitszeiten (z. B. Krankheit, Kur, Sonderurlaub) festzuhalten. Auf dem linken Teil wird die Monatssumme der Stunden pro Tätigkeit unter Angabe einer Organisationseinheit festgehalten. Der gesamte Arbeitsaufzeichnungsbogen ist dem Vorgesetzten vorzulegen und von diesem zu unterschreiben. Der linke Teil – ohne Namensangabe – wird anschließend an die Prüfstelle für leistungsbezogene Entgeltbestandteile (LEB-Prüfstelle) weitergeleitet, wo sie zunächst weder ausgewertet noch elektronisch gespeichert wurden.

Da der Tarifvertrag in § 3 Abs. 5 Satz 3 einen allgemeinen Verweis auf das Hamburgische Datenschutzgesetz enthält, war die Zulässigkeit der Maßnahme auf der Grundlage von § 28 Hamburgisches Datenschutzgesetz sowie der allgemeinen datenschutzrechtlichen Anforderungen zu bewerten. Wir haben der Geschäftsführung der Hamburger Stadtentwässerung in einem ersten Gespräch mitgeteilt, daß die Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn der Zweck der Erhebung vorher von der erhebenden Stelle definiert ist und sie darlegen kann, warum die personenbezogenen Angaben zur Erreichung dieses Zwecks geeignet und erforderlich sind (siehe dazu bereits 14. TB, 6.3).

Der Zweck der Erhebung besteht gemäß § 3 Abs. 1 des Tarifvertrages darin, Qualität und Menge der erbrachten Arbeitsleistungen modellbezogen nachzuweisen, um auf dieser Grundlage Prämien für evtl. erbrachte Mehrleistungen ebenfalls modellbezogen berechnen zu können. Wir haben darauf hingewiesen, daß hierfür ein Personenbezug nicht erforderlich ist. Weiterhin haben wir bemängelt, daß die Hamburger Stadtentwässerung zunächst nicht nachweisen konnte, daß die Arbeitsaufzeichnungsbögen ein geeignetes Mittel zur Erreichung dieses Zwecks darstellen, da die Bögen zum Zeitpunkt unserer ersten Gespräche nicht ausgewertet und entsprechende Auswertungsfragen noch nicht formuliert worden waren. Es handelte sich daher zu dem Zeitpunkt um eine unzulässige Datenverarbeitung auf Vorrat.

Wir hatten die Hamburger Stadtentwässerung daher aufgefordert, die Datenerhebung einzustellen. Dem ist die Hamburger Stadtentwässerung nicht

nachgekommen. In anschließenden intensiven Erörterungen unter Beteiligung des Personalrates hat die Stadtentwässerung dann dargelegt, warum die einzelnen Angaben zur Prämienberechnung erforderlich sind, und entsprechende Auswertungsfragen formuliert. Die nicht prämienrelevanten Angaben, wie z. B. Krankheit, Kur und Sonderurlaub werden nicht mehr differenziert, sondern nur noch zusammengefaßt unter einer Nummer erfaßt. Des

weiteren wurde ein Vorschlag für eine Verfügung erarbeitet, den wir für datenschutzgerecht halten. Die wesentliche Elemente dieser neuen Verfügung sind:

– Der rechte Teil der Anschreibungsbögen mit personenbezogenen Angaben dient ausschließlich der Plausibilitätskontrolle durch den Vorgesetzten und ist dem Mitarbeiter sofort persönlich zurückzugeben. Die Anfertigung von

Kopien durch Vorgesetzte ist unzulässig. Die personenbezogenen Angaben dürfen nicht zu anderen Zwecken, insbesondere nicht zu Zwecken der Verhaltens- und Leistungskontrolle des einzelnen Mitarbeiters genutzt werden.

– Umfaßt die auf dem linken Teil der Anschreibungsbögen anzugebende

Organisationseinheit weniger als 4 Mitarbeiter (einschließlich Vorgesetztem), ist die nächst höhere Organisationseinheit mit einer größeren Mitarbeiterzahl einzutragen. Eine personenbezogene Wiederherstellung des Monatsabschnittes und damit ein personenbezogenes Leistungsbild ist dann nicht mehr möglich. Nach der EDV-Erfassung werden die Monatsabschnitte sofort vernichtet.

– Die Datenerfassung und Auswertung erfolgt ausschließlich durch die LEB-Prüfstelle. Alle weiteren Daten sind zu vernichten.

– Die Erfassung, Auswertung und Löschung der in den Monaten Juli bis November 1996 erhobenen Daten erfolgt rückwirkend nach diesen Vorgaben.

7.2 Prüfung beim Personalrat der Justizbehörde

Im letzten Tätigkeitsbericht (14. TB, 6.6) haben wir über unsere Erkenntnisse bei der Prüfung des Personalrats der Justizbehörde berichtet und entsprechende Änderungsvorschläge für die dortige Datenverarbeitung unterbreitet. Der Personalrat hat die von uns angeregten Maßnahmen bisher weitgehend durchgeführt, so daß ein datenschutzgerechter Zustand nahezu erreicht worden ist.

Die von uns für den Personalrat der Justizbehörde dargelegten Maßstäbe für die Datenverarbeitung sind für alle Personalräte anwendbar.

7.3 Sonstiges

Im Berichtszeitraum ergab sich außerdem folgende weitere Entwicklung:

– Das Projekt Personalwesen (PROPERS) hat nach Abschluß der Pilotierung der zweiten Stufe (vgl. 14. TB, 6.1) inzwischen die Stammdatenverarbeitung in verschiedenen Personalverwaltungen realisiert. Dabei werden jedoch bisher keine personenbezogenen Daten zwischen den einzelnen Personalabteilungen automatisiert ausgetauscht. Spätestens wenn eine solche behördenübergreifende Übertragung personenbezogener Daten über das Netz der Freien und Hansestadt Hamburg stattfindet, ist dieses datenschutzrechtlich nur vertretbar, wenn vorher eine entsprechende Verschlüsselung erfolgt.

– Nach intensiven Verhandlungen mit dem Personalamt und der Finanzbehörde über unseren Entwurf einer Arbeitshilfe „Empfehlungen zum Datenschutz bei Mitarbeiterbefragungen“ sowie über unsere Vorschläge zur Ergänzung des Musterberatervertrages (vgl. 14. TB, 6.2) hatten wir nahezu einen Konsens erreicht. Da die Finanzbehörde kurzfristig nochmals einige Punkte zur Diskussion gestellt hat, konnte aber die Abstimmung noch nicht abgeschlossen werden.

8. Schule und Berufsbildung

8.1 Lernausgangslagenuntersuchung bei Schülern

Im 14. TB (7.2) haben wir über die Vorstudie zur sog. Lernausgangslagenuntersuchung berichtet, mit der 1995 die Fähigkeiten der Fünftklässler im Lesen, Schreiben und Rechnen/Mathematik sowie hinsichtlich des Sachwissens, der Kreativität und der Lernmotivation festgestellt werden sollten.

Unser zentraler Kritikpunkt an der Vorstudie war und ist der Personenbezug der verwendeten Testverfahren. Einerseits enthalten die verwendeten Testunterlagen Codenummern; andererseits verfügen die Forscher über Referenzlisten, in denen dieser Code zusammen mit dem Vor- und Nachnamen, dem Geburtsdatum sowie dem Namen der Schule und der Klasse gespeichert wird. Zweck dieses Verfahrens ist es, auch noch nach zwei Jahren im Rahmen einer sogenannten Verlaufskontrollstudie Lernfortschritte bei den Schülern feststellen und mit den zurückliegenden Ergebnissen vergleichen zu können.

Für die Hauptstudie hat die Behörde für Schule, Jugend und Berufsbildung unserer Kritik Rechnung getragen. Statt des alten personenbezogenen Codes werden dreistellige Pseudonyme verwendet, die aus den ersten drei Buchstaben des Nachnamens und des Vornamens sowie aus dem Geburtsdatum gebildet werden. Derartige Einweg-Pseudonyme (vgl. 3.1) haben gegenüber personenbezogenen Merkmalen den Vorteil, daß Bestandsdaten mit neueren Untersuchungsergebnissen verknüpft werden können, ohne daß dem Forschungsinstitut dabei der Rückschluß auf einen bestimmten Schüler möglich ist.

Die Schule selbst erhält von dem Institut ohne Einwilligung der Betroffenen ohnehin keine einzelfallbezogenen Daten.

8.2 Sonstiges

Des weiteren beschäftigten uns im Schulbereich

– die Novellierung des Schulgesetzes, und zwar insbesondere die Frage, inwieweit Schüler an der Beratung personenbezogener Angelegenheiten beteiligt werden sollen,

– das Projekt „Berufsstart und Eignung“ der Jahnschule, bei dem Daten von Achtklässlern ohne schriftliches Einverständnis der Betroffenen über ein Münchner Institut an eine Krankenkasse und eine Bank übermittelt wurden.

9. Wissenschaft und Forschung

9.1 Datenschutzgerechte Forschung

Die Deutsche Forschungsgemeinschaft (DFG) hat 1996 eine Denkschrift zur Forschungsfreiheit herausgebracht, in der sie dem Datenschutz (u. a. neben dem Tier- und Umweltschutz) eine Behinderung der Forschung vorwirft. Dieser Vorwurf ist so alt wie der Datenschutz selbst und im allgemeinen unverändert unzutreffend.

Die DFG verkennt, daß der Datenschutz wie die Forschungsfreiheit ein Grundrecht darstellt, so daß beide Grundrechte im Konfliktfall berücksichtigt werden müssen. Dies ist mittlerweile in einer ganzen Fülle datenschutzrechtlicher Bestimmungen im einzelnen geregelt, ohne daß dabei der Verzicht auf ein Forschungsvorhaben die notwendige Folge ist.

Nach den Erfahrungen aus unserer reichhaltigen Beratungspraxis gelingt es praktisch immer, Forschungsprojekte datenschutzgerecht zu gestalten. Relevante praktische Probleme für Forscher gibt es typischerweise nur dann, wenn sie den Datenschutz bei ihren Studienkonzepten nicht oder erst viel zu spät berücksichtigen. Dieser Vorwurf trifft allerdings die Forscher selbst und nicht den Datenschutz.

Eine Ad-hoc-Gruppe der Vereinigung Deutscher Wissenschaftler (VDW) hat sich in erfreulich deutlicher Weise von den Vorwürfen der DFG distanziert.

9.2 Sonstiges

Gegenstand unserer Beschäftigung waren des weiteren

– die Novellierung des Hamburgischen Hochschulgesetzes mit der Einfügung von Regelungen für Evaluationsvorhaben,

– die Aufnahme privater Daten, insbesondere von Privatanschriften in Hochschulführer.

10. Statistik

10.1 Prüfung der Mikrozensuserhebung 1996

des Statistischen Landesamts

Der jährlich durchgeführte Mikrozensus – die „kleine Volkszählung“ – betrifft in Hamburg etwa 17.000 Bürgerinnen und Bürger. Ein umfangreicher, durch das Mikrozensusgesetz vorgegebener Fragenkatalog ist dabei zu beantworten. Es besteht Auskunftspflicht.

Die Durchführung der Mikrozensuserhebung 1996 durch das Statistische Landesamt war Gegenstand einer datenschutzrechtlichen Prüfung. Dabei wurde der gesamte Ablauf der Erhebung einer kritischen Würdigung unterzogen.

Die Prüfung hat ergeben, daß die Erhebung teilweise nicht mit den Vorgaben des Bundesstatistikgesetzes (BStatG) und des Mikrozensusgesetzes (MZG) übereinstimmte. Die Mängel betrafen vor allem folgende Punkte:

– Die Auswahl der Interviewerinnen und Interviewer erfolgte nicht in allen Fällen mit der gebotenen Sorgfalt; insbesondere hat das Statistische Landesamt Interviewer beschäftigt, die ihre Bewerbungsbögen nur unvollständig ausge- – füllt hatten. So wurde eine Sachbearbeiterin eines bezirklichen Sozialamtes in ihrem beruflichen Zuständigkeitsbereich eingesetzt. Dies widersprach der Vorgabe aus § 14 Abs.1 BStatG, wonach Erhebungsbeauftragte nicht eingesetzt werden dürfen, wenn ein Konflikt mit ihrer beruflichen Tätigkeit zu befürchten ist.

– Die Einwohnerdaten, die die Meldebehörde für die Erhebung an das Statistische Landesamt übermittelt hatte, wurden dort nicht angemessen gesichert aufbewahrt. Zudem war die Verarbeitung dieser Daten nicht ordnungsgemäß dokumentiert.

– Bei der Prüfung stellte sich heraus, daß die Melderegisterdaten aus der Erhebung 1995 immer noch in Dateien auf nicht besonders gesicherten Disketten vollständig im Statistischen Landesamt vorhanden waren, obwohl dies nicht erforderlich war. Dies widersprach dem Gebot zur möglichst frühzeitigen Löschung der Hilfsmerkmale gemäß § 12 Abs. 1 BStatG.

– Bei der Erhebung der Daten für den Mikrozensus in verschiedenen Heimen wurden die Auskünfte ausschließlich von der Heimleitung erteilt, ohne daß ersichtlich war, ob die Betroffenen selbst hätten Auskunft geben können. Demgegenüber sieht § 7 MZG die Auskunftserteilung durch die Heimleitung nur ersatzweise vor, wenn die Betroffenen diese Auskünfte nicht selbst erteilen können. Zudem befand sich in den Erhebungsunterlagen auch ein kompletter Belegungsplan eines Heims, einschließlich derjenigen Bewohnerinnen und Bewohner, die gar nicht auskunftspflichtig waren. Dies war durch die statistikrechtlichen Regelungen nicht gedeckt.

– Bei der automatisierten Aufbereitung der Daten aus früheren Mikrozensuserhebungen waren verschiedene Arbeitsgänge, die im Ablaufplan des Statistischen Bundesamts vorgesehen sind, vom Statistischen Landesamt nicht ausgeführt worden. Durch diese Arbeitsgänge soll gewährleistet werden, daß eine nachträgliche Zuordnung von Erhebungsdaten zu einzelnen Auskunftspflichtigen (Deanonymisierung) unterbleibt. Diese Unterlassung widersprach dem Gebot zur möglichst frühzeitigen Anonymisierung nach § 9 Abs. 3 MZG.

– Die Vernichtung der Unterlagen früherer Erhebungen war nicht lückenlos nachzuvollziehen. Insbesondere fehlten einzelne Aufträge zur Vernichtung der Unterlagen. Dies widerspricht § 5

Abs. 2 Hamburgisches Statistikgesetz, wonach einzelne Arbeiten nur auf schriftlichen Auftrag an Dritte vergeben werden dürfen.

Das Statistische Landesamt ist – allerdings ohne unsere rechtliche Bewertung im einzelnen zu teilen – auf die von uns gestellten Forderungen eingegangen und hat die Abstellung der festgestellten Mängel zugesagt. Von einer förmlichen Beanstandung ist deshalb abgesehen worden.

Lediglich hinsichtlich der Erteilung von Einzelaufträgen für die Vernichtung der Erhebungsunterlagen will das Statistische Landesamt unseren Forderungen nicht nachkommen, da es hierin einen „unangemessenen Bürokratismus“ sieht. Dem ist entgegenzuhalten, daß es sich um eine gesetzlich vorgeschriebene Maßnahme handelt, die der Sicherung der „Entsorgungskette“ für statistisches Material dient. Zudem dürfte sich der zusätzliche Aufwand für die Auftragserteilung in äußerst engen Grenzen halten. Wir haben das Statistische Landesamt deshalb aufgefordert, seine Praxis zu ändern.

10.2 Übermittlung von Daten aus der Befragung älterer ausländischer Mitbürger an die Meldebehörde

Für die Durchführung einer Befragung über die Lebenssituation ausländischer Mitbürger hatte die Meldebehörde an die Behörde für Arbeit Gesundheit und Soziales (BAGS) Adreßdaten des Personenkreises übermittelt, der in die Befragung einbezogen werden sollte. Die Befragung wurde aufgrund der Ausländer-Seniorenbefragungsverordnung (Hmb. GVBl. 1996, S.15), einer Verordnung gemäß § 2 Abs. 3 Hamburgisches Statistikgesetz (HmbStatG), von der BAGS als Landesstatistik durchgeführt.

Das Amt für Zentrale Meldeangelegenheiten beim Bezirksamt Harburg hatte die BAGS bei der Übermittlung darum gebeten, die Daten derjenigen Personen an die örtlich zuständigen Einwohnerdienststellen weiterzuleiten, bei denen die BAGS anhand der Rückläufe festgestellt habe, daß sie verzogen oder verstorben seien. Die so übermittelten Daten sollten zur Aktualisierung des Melderegisters genutzt werden.

Aus dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 (BVerfGE 65, 1) ergibt sich, daß die bei der Volkszählung 1983 vorgesehene Meldung von Einwohnerdaten an die Meldebehörden zur Aktualisierung der Melderegister unvereinbar mit dem statistischen Zweck der Zählung war, weil Statistik- und Verwaltungsdaten getrennt zu halten sind.

Die vom Amt für Zentrale Meldeangelegenheiten geforderte und von der BAGS teilweise durchgeführte Übermittlung der Daten war daher unzulässig.

Wir haben der BAGS und der Behörde für Inneres unsere datenschutzrechtlichen Bedenken mitgeteilt und gefordert, die Übermittlungen in Zukunft zu unterlassen und die den Einwohnerämtern bereits übermittelten Daten unverzüglich zu löschen. Die Behörde für Inneres ist inzwischen unserer Forderung gefolgt.

11. Bauwesen und Stadtentwicklung

Im Berichtszeitraum hat sich folgende Weiterentwicklung ergeben:

– Das Vermessungsamt hat das Projekt HALB (Hamburgisches Automatisiertes Liegenschaftsbuch) als beschreibenden Teil des Flächenbezogenen In– formationssystems (FIS) abgenommen (vgl. 14. TB, 10.2). Seit Anfang November 1996 wird ein mehrmonatiges Pilotverfahren (Parallelbetrieb) beim Bezirksamt Hamburg-Nord durchgeführt. Aufgrund der vom Senat beschlossenen Reorganisation des Vermessungswesens, mit der auch eine räumliche Zusammenführung der Dienststellen vorbereitet wird, soll HALB aber erst danach in die Produktion übernommen werden.

– Als weitere Maßnahme wurde zwischenzeitlich die Fachliche Weisung über die Übermittlung und Nutzung von Daten des FIS und der Landesvermessung erlassen. Die Verordnung über den automatisierten Abruf und die Speicherung, Veränderung und Löschung von Daten aus dem FIS (FISOnlineVO) auf Grund von § 14 Abs. 5 und 6 Hamburgisches Gesetz über

das Vermessungswesen wurde in das behördliche Abstimmungsverfahren gegeben.

– Die Pilotierungsphase des computerunterstützten Baugenehmigungsverfahrens (BACom) im Bereich des Bezirksamtes Wandsbek ist beendet. Mit Ablauf 1996 sollen alle Bauprüf-Kern-Abteilungen und bis Ende 1997 auch die Ortsämter – soweit noch nicht geschehen – mit BACom ausgerüstet sein. Eine Prüfung des BACom-Verfahrens werden wir voraussichtlich im 2. Quartal 1997 vornehmen (vgl. 14. TB, 10.3).

– Die datenschutzrechtliche Prüfung des Fehlbelegungsabgabe-Verfahrens der Mietenausgleichszentrale (MAZ) als Abteilung der Hamburgischen Wohnungsbaukreditanstalt (WK) ist endlich mit einem überwiegend positiv zu bewertenden Ergebnis abgeschlossen worden. Nach umfangreichen Gesprächen mit der WK sind die erforderlichen Maßnahmen zur Beseitigung der von uns beanstandeten und im 14. TB (10.4) aufgeführten Mängel von der WK und MAZ getroffen worden.

12. Meldewesen

12.1 Regelmäßige Übermittlung von Melderegisterdaten an die Gebühreneinzugszentrale (GEZ)

Eine Reihe von Bundesländern (Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, Saarland, Schleswig-Holstein) haben durch formelles Gesetz oder Rechtsverordnung die Meldebehörden ermächtigt, den Landesrundfunkanstalten oder der GEZ aus bestimmten Anlässen (Anmeldung, Abmeldung, Tod) regelmäßig bestimmte personenbezogene Daten volljähriger Einwohner zum Zwecke des Rundfunkgebühreneinzugs zu übermitteln.

Die Landesrundfunkanstalten haben nach der Verfassung Anspruch auf eine funktionsgerechte Finanzierung. Deshalb bestehen von unserer Seite keine

grundsätzlichen Bedenken gegen eine entsprechende Übermittlungsregelung zugunsten des Norddeutschen Rundfunks (NDR).

Von einer regelmäßigen Meldedatenübermittlung bei allen An- und Abmeldungen sind aber auch die Personen betroffen, die nicht der Rundfunkgebührenpflicht unterliegen oder die ihre Anzeigepflicht gegenüber der GEZ erfüllt haben. Daher bedarf es einer sorgfältigen Güterabwägung durch das Parlament, ob und in welchem Umfang die Datenübermittlung zugelassen werden soll. Die Verantwortung des Gesetzgebers beinhaltet auch, die Auswirkungen der regelmäßigen Meldedatenübermittlung für die Grundrechte, insbesondere die Erforderlichkeit der einzelnen übermittelten Daten für den Gebühreneinzug, in angemessenen Zeitabständen zu beobachten und die Rechtsgrundlage der Übermittlung ggf. im Sinne eines ausgeprägteren Datenschutzes nachzubessern.

Hierfür bedarf es regelmäßiger und aussagefähiger Erfahrungsberichte. Der Intendant des NDR hat in einem Schreiben an die Senats- und Staatskanzleien der NDR-Staatsvertragsländer seine Bereitschaft erklärt, mindestens alle

zwei Jahre einen detaillierten Bericht über die Anwendung und Auswirkungen des Übermittlungsverfahrens und auch über die Maßnahmen zur Datensicherung vorzulegen. Wir begrüßen diesen Schritt des NDR ausdrücklich. Er entspricht unseren Erwartungen an eine datenschutzgerechte Verfahrensgestaltung und sollte bei einer künftigen gesetzlichen Regelung berücksichtigt werden.

13. Ausländerangelegenheiten

13.1 Allgemeine Verwaltungsvorschrift zum Ausländerzentralregister

Der Bundesrat hat am 24. Mai 1996 der Allgemeinen Verwaltungsvorschrift zum Gesetz über das Ausländerzentralregister (AZRG) und zur AZRG-Durchführungsverordnung (AZR-VV) mit Änderungen zugestimmt. Die Anregungen, die wir zu dem Entwurf unterbreitet haben, sind zu einem erheblichen Teil

aufgegriffen worden.

Werden Daten gegen den Willen des Betroffenen übermittelt, zu dessen Gunsten eine Übermittlungssperre gespeichert ist, hat die Registerbehörde zu dokumentieren, warum die Einwendungen nicht berücksichtigt wurden. Die ersuchende Stelle hat aktenkundig zu machen, warum sie die Übermittlung von Begründungstexten für unerläßlich hält. Die schutzwürdigen Interessen des Betroffenen, die einer Übermittlung an ausländische Stellen entgegenstehen, wurden – unter Einbeziehung auch der nahen Angehörigen – präzisiert. Schließlich konnte über den Bundesrat erreicht werden, daß ein Widerruf oder eine nachträgliche Beschränkung der Ermächtigung zum automatisierten Abruf der Registerstelle unverzüglich mitzuteilen ist.

13.2 Anfragen an Staatsanwaltschaft und Landeskriminalamt (LKA) im Rahmen von Einbürgerungsverfahren

Aus Anlaß einer Eingabe haben wir uns eingehend mit der Frage beschäftigt, in welchem Umfang das Einwohner-Zentralamt (EZA) als Einbürgerungsbehörde formularmäßige Auskünfte bei der Staatsanwaltschaft und beim LKA auch über eingestellte Ermittlungs- bzw. Strafverfahren gegen den Bewerber einholen darf.

In der Diskussion mit der Behörde für Inneres haben wir insbesondere darauf hingewiesen, daß nach der Neufassung des § 8 Abs. 1 Nr. 2 des Reichs- und Staatsangehörigkeitsgesetzes (RuStAG) im Jahre 1993 Bagatellverstöße gegen Rechtsvorschriften als Ablehnungsgrund in Einbürgerungsverfahren ausgeschlossen sein sollen. Dies wird auch durch die Verweisung auf § 46

Nr. 2 des Ausländergesetzes (AuslG) deutlich.

Die Behörde für Inneres hat unsere Anregungen aufgeschlossen geprüft und konstruktiv aufgegriffen. Einvernehmen konnte zunächst darin erzielt werden, daß die Auskunftsersuchen des EZA in Einbürgerungsverfahren künftig Einstellungen mangels hinreichenden Tatverdachts nach § 170 Abs. 2 der Strafprozeßordnung (StPO) generell nicht mehr einbeziehen.

Auch Einstellungen wegen geringer Schuld nach § 153 StPO sollen künftig von den Auskunftsersuchen grundsätzlich ausgenommen bleiben. Lediglich in Ausnahmefällen, die vor der Übermittlung zu klären sind, können Einstellungen nach § 153 StPO auch weiterhin mitgeteilt werden, z. B. bei längerfristigen Serienstraftaten im Bagatellbereich oder Delikten, die als solche Rückschlüsse auf sonstige Einbürgerungshindernisse zulassen. Eine generelle Übermittlung von Erkenntnissen über Bagatellverstöße findet dagegen nicht mehr statt.

Wir sehen hierin eine sachgerechte Lösung, die auch den Ermessensspielraum der Einbürgerungsbehörde angemessen berücksichtigt.

14. Verkehrswesen

14.1 Zugriffsbefugnisse auf Daten von Führerscheininhabern im Landesbetrieb Verkehr

Nach wie vor haben alle Sachbearbeiter der drei Führerscheinstellen uneingeschränkten Zugriff auf die Daten aller in Hamburg automatisiert erfaßten Führerscheininhaber (vgl. 14. TB, 14.1.1). Diese unbegrenzten Zugriffe sind auch als Begründung herangezogen worden, um die bisherige organisatorische Gliederung des Fahrerlaubniswesens in Landesverkehrsverwaltung und die Bezirksämter Bergedorf und Harburg aufzugeben und einen einheitlichen Landesbetrieb Verkehr zu gründen. Aber selbst wenn das Fahrerlaubniswesen ab 1997 unter einheitlicher Organisation in einem gemeinsamen Landesbetrieb

durchgeführt wird, ändert dies nichts daran, daß die Mitarbeiter der einzelnen Dienststellen dieses Landesbetriebes nur insoweit zuständig sein werden, als in ihrem Bereich ein Anlaß für die Bearbeitung entstanden ist.

Wenn in Harburg ein Führerschein beantragt wird, haben die in Bergedorf beschäftigten Mitarbeiter des Landesbetriebs keinen Grund, die Daten abzurufen. § 8 Abs. 2 Nr. 5 HmbDSG verlangt vielmehr geeignete Maßnahmen zur Begrenzung der Zugriffsmöglichkeiten auf den erforderlichen Umfang. Um Bürgern zu ermöglichen, verschiedene Dienststellen in Hamburg bei ihren Führerscheinangelegenheiten in Anspruch zu nehmen, können allerdings besondere Funktionen vorgesehen werden, die eine Übertragung des bisher in anderer Zuständigkeit geführten Fahrerlaubnisvorgangs an die neu zuständige Dienststelle ermöglichen.

Wir haben diese Gesichtspunkte den beteiligten Fachbehörden vor der Entscheidung über die Bildung des Landesbetriebs Verkehr mitgeteilt. Eine Reaktion hierauf gab es zunächst nicht. Die Behörde für Inneres kündigte lediglich an, daß eine Protokollierung von überörtlichen Zugriffen erfolgen solle, die jedoch noch nicht realisiert ist. Eine Protokollierung stellt aber kein hinreichendes Korrektiv für unzulässig weite Zugriffsbefugnisse dar. Sie würde nur zusätzlichen Kontrollaufwand hervorrufen, jedoch nicht gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, wie es das HmbDSG fordert.

Als Kompromiß haben wir angeboten, die zuständigkeitsübergreifenden Zugriffe auf die Einzelangaben zu Fahrerlaubnisinhabern zu begrenzen, die auch im bundesweiten zentralen Fahrerlaubnisregister vorgesehen sind. Wenn der Bundesgesetzgeber – entgegen der von der Mehrzahl der Datenschutzbeauftragten geäußerten Ablehnung (siehe 14.TB, 14.2.2) – durch eine Novelle zum Straßenverkehrsgesetz dieses zentrale Register einführt, werden bundesweit überregionale Zugriffe rechtlich möglich sein. Dies gilt allerdings nur für Angaben zur Person und zur erteilten Fahrerlaubnis. Weitergehende Zugriffsmöglichkeiten, wie sie das derzeitige Verfahren in Hamburg zuläßt, sind dagegen auszuschließen, zumal nach dem Entwurf für ein Straßenverkehrsgesetz die örtlichen Register ohnehin nach einer gewissen Übergangsfrist abzuschaffen sind und dann nur noch der begrenzte Bestand des zentralen Registers zur Verfügung steht.

Daraufhin hat die Behörde mitgeteilt, daß im Zuge der Einrichtung des neuen Landesbetriebs Verkehr auch über die Zuständigkeitsaufteilung zwischen allgemeinen Führerscheinangelegenheiten und besonderen Maßnahmen wie

z. B. die Entziehung der Fahrerlaubnis neu zu befinden sei. In diesem Zusammenhang soll geprüft werden, ob zwischen Zugriffen auf die Grunddaten, die auch aus den bundesweiten Registern abrufbar sind, und solchen, die nur Mitarbeitern mit besonderer Zuständigkeit zugänglich sind, unterschieden werden kann.

15. Polizei

15.1 Europol

Die Bundesregierung hat den Entwurf eines Zustimmungsgesetzes zum Übereinkommen über die Errichtung eines Europäischen Polizeiamtes (Europol-Übereinkommen) vorgelegt. Er entspricht im wesentlichen unseren Forderungen zur Wahrung der datenschutzrechtlichen

Verantwortlichkeit der Länderpolizeien bei Europol-Speicherungen und zur Beteiligung der Landesbeauftragten an der Datenschutzkontrolle bei Europol (vgl. 14. TB, 15.6).

Inzwischen werden auf europäischer Ebene bereits Durchführungsbestimmungen für die Zeit nach Inkrafttreten des Übereinkommens beraten. Dies betrifft insbesondere die sogenannten Arbeitsdateien zu Analysezwecken. Gegen die bisher hierzu bekanntgewordenen Vorstellungen haben wir massive Bedenken geäußert. Zunächst ist unklar, was überhaupt Gegenstand und Ziel der Europol-Analysen sein soll. Geht es um die Unterstützung strafrechtlicher Ermittlungen im Einzelfall oder um eine fallunabhängige Zielsetzung?

Unzweideutig ist jedenfalls, daß geplant ist, diese Analysen mit umfassendsten personenbezogenen Daten durchzuführen. Nicht nur die üblichen Daten zur Person und zum Delikt sind geplant, sondern vielmehr auch Angaben zu den Eltern, zur Ausbildung, zu wirtschaftlichen Verhältnissen, zu Verhaltensmerkmalen bis hin zu Charaktermerkmalen und Verweise auf Speicherungen in nicht-polizeilichen Datenbanken. Eine vergleichbare Häufung höchstsensibler Daten gibt es in keiner inländischen polizeilichen Datei. Somit bleibt insgesamt auch unklar, woher die genannten für Analysedateien vorgesehenen Informationen eigentlich stammen sollen. Wenn schließlich nicht einmal Angaben zu religiösen Überzeugungen oder zum (straflosen) Sexualleben von der Verarbeitung in Analysedateien ausgeschlossen werden sollen, stellt sich die Frage, welche Relevanz diese besonderen Daten überhaupt für die Verhütung und Verfolgung von europaweiten Straftaten haben sollen.

Ungeklärt ist bei der Analysetätigkeit von Europol schließlich das Verhältnis zur Sachleitungsbefugnis der Staatsanwaltschaft. Während nach unserem Recht die Polizei zwingend ihre Unterlagen über strafrechtliche Ermittlungen an die Staatsanwaltschaft abliefert, ist dies bei den Europol-Analysen gerade nicht vorgesehen, denn über sie sollen allein die Analyse-Beamten in Den Haag verfügen. Entsprechende Weisungen der Staatsanwaltschaft sind ausgeschlossen, denn das Personal von Europol darf Weisungen anderer Behörden nicht entgegennehmen.

Die Behauptung, Europol unterstütze die Strafverfolgung der zuständigen Behörden der Mitgliedstaaten, ist vor diesem Hintergrund fragwürdig. Es wird vielmehr darauf ankommen, auch die Datenverarbeitung zu Analysezwecken bei Europol auf ein vertretbares Maß zu reduzieren. Insbesondere sollte über Möglichkeiten zur Datenvermeidung nachgedacht werden. In Betracht kommen z. B. Lagebilder ohne Personenbezug, wie sie die Polizei traditionell erstellt, und die verstärkte Nutzung von Sachdaten.

Erfreulicherweise hat das Europäische Parlament am 17. September 1996 in seiner „Entschließung zur Achtung der Menschenrechte“ hinsichtlich der Datenbanken von Europol gefordert, „alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in diesen Datenbanken auszuschließen“.

15.2 Probleme bei Rasterfahndungen

Nachdem im Jahr 1991 in der Strafprozeßordnung (StPO) die Befugnis zur Rasterfahndung eingeführt worden ist, hat das Landeskriminalamt Hamburg drei solche Maßnahmen durchgeführt. Es ist damit nach unserer Kenntnis die einzige Polizeibehörde, die von dieser

Möglichkeit zum Abgleich automatisierter Datenbestände zur Strafverfolgung Gebrauch gemacht hat.

Wir haben die jeweiligen Maßnahmen überprüft und dabei in zwei Fällen erhebliche Probleme festgestellt. (Eine Darstellung der zugrunde liegenden Sachverhalte, der jeweils abgeglichenen Dateien und Abgleichsmerkmale soll hier unterbleiben.)

Die Durchführung einer Rasterfahndung wird bestimmt durch die richterliche Anordnung. Der zuständige Richter muß prüfen, ob es sich um eine Straftat handelt, zu deren Aufklärung nach § 98 a StPO eine Rasterfahndung zulässig ist, und ob es kein anderes weniger eingreifendes Mittel zur Erforschung des Sachverhalts gibt. Diese Fragen waren in beiden Fällen positiv beantwortet; es gab daher hiermit keine Probleme. Schwierigkeiten gab es dagegen bei der Frage, welche Dateien mit welchen Einzelmerkmalen zum gegenseitigen automatisierten Abgleich herangezogen werden durften.

Eine der Anordnungen war in dieser Hinsicht äußerst unklar, weil sie die zum Abgleich vorgesehenen Dateien nicht exakt benannte, obwohl dies möglich gewesen wäre. Vielmehr wurden die Dateien nach ihrer Zweckbestimmung und ihrem Inhalt beschrieben, was zu erheblichen Auslegungsproblemen führte.

Die Polizei stellte fest, daß ein automatisierter Abgleich nach dieser Beschreibung gar nicht möglich war, weil die entsprechende Datei nicht automatisiert geführt wird, sondern als manuelle Kartei. Sie führte statt dessen einen Abgleich mit einer anderen automatisierten Datei durch, die viel umfangreicher war und unserer Auffassung nach nicht von der richterlichen Anordnung erfaßt war.

Wir haben des Vorgehen kritisiert, weil wesentlich mehr Personendaten als richterlich zugelassen in den Abgleich einbezogen worden sind und somit auch die Schnittmenge als Abgleichsergebnis weit über die gesuchten Träger bestimmter Merkmale hinausging. Die Polizei und die zuständige Staatsanwaltschaft (außerhalb Hamburgs) hielten jedoch die Verfahrensweise für gerechtfertigt, weil der Abgleich mit der umfangreichen Datei nur ein Zwischenschritt gewesen sei und man aus diesem Abgleichsergebnis die Datensätze, die die in der richterlichen Anordnung genannten Merkmale aufwiesen, anschließend einzeln herausgesucht habe. Wir haben nur deshalb von einer Beanstandung der Verfahrensweise gemäß § 25 HmbDSG abgesehen, weil die Probleme letztlich auf die von der Polizei nicht zu verantwortenden Unklarheiten in der richterlichen Anordnung zurückzuführen waren und im Ergebnis die Löschungspflichten hinsichtlich der nicht benötigten Daten eingehalten wurden.

Bei der nächsten Fahndungsmaßnahme war die richterliche Anordnung zwar eigentlich klar und unmißverständlich. Dann stellte man jedoch fest, daß die abzugleichenden Dateien gar nicht alle Merkmale enthielten, die in der Anordnung zur Eingrenzung der abzugleichenden Datenbestände festgelegt waren. Gleichwohl benutzte die Polizei die Dateien auch ohne die eingrenzenden Merkmale. Dies führte wiederum zu dem Ergebnis, daß wesentlich mehr Personen in die Rasterfahndung einbezogen wurden, als richterlich zugelassen war, und die Schnittmenge erheblich größer war als beabsichtigt. Die Staatsanwaltschaft Hamburg hat unsere diesbezügliche Kritik für berechtigt gehalten.

Zu kritisieren war auch, daß in beiden genannten Fällen nach Beendigung der Maßnahmen der zuständige Datenschutzbeauftragte nicht von der jeweils zuständigen Staatsanwaltschaft informiert wurde, wie dies in § 98 b Abs. 4 Satz 2 StPO vorgeschrieben ist. Wir haben

vielmehr jeweils aus anderen Quellen davon erfahren, daß die Rasterfahndungen stattgefunden hatten.

Zur Vermeidung derartiger Probleme haben wir der Polizei konkrete Verbesserungsvorschläge zur Verfahrensweise unterbreitet. Kernpunkt ist, daß zu-nächst sorgfältig geprüft werden muß, welche Abgleichskriterien benötigt

werden, welche Datenbestände zur Verfügung stehen und ob sie die benötigten Kriterien enthalten. Erst wenn diese Klärung soweit wie möglich abgeschlossen ist, sollte die richterliche Anordnung beantragt werden. Im Antrag sollten die erforderlichen Angaben zu den Dateien und den Abgleichmerkmalen so exakt wie möglich beschrieben werden, um mißverständliche Formulierungen zu vermeiden. Wenn sich gleichwohl nachträglich herausstellt, daß man auf der Grundlage der richterlichen Anordnung nicht weiterkommt, kann sie nicht einfach umgedeutet werden und ein größerer Datenbestand benutzt werden. Vielmehr wäre dann eine entsprechend geänderte richterliche Anordnung zu beantragten.

Polizei und Staatsanwaltschaft haben daraufhin eine Verfahrensrichtlinie zum Ablauf von Rasterfahndungen erarbeitet.

Die bisherigen Erfahrungen mit Rasterfahndungen legen auch erhebliche Skepsis an der Geeignetheit dieses Mittels nahe. In allen Fällen, in denen die Polizei Hamburg bisher eine Rasterfahndung durchgeführt hat, hat dies nicht zur Ergreifung des Täters beigetragen. Rasterfahndungen sind immer abhängig von einer Ermittlungshypothese, wonach der oder die Täter bestimmte dateimäßig erfaßte Merkmale erfüllen. Wenn sich diese Hypothese auch nur in einem der Abgleichsmerkmale als unrichtig herausstellt, war – wie in den bisherigen Fällen – der erhebliche Aufwand zur Durchführung der Maßnahme vergebens. Im schlimmsten Falle kann die Rasterfahndung sogar irreführend für die Ermittlungen sein und Betroffene, die nur aufgrund des Abgleichs in einen scheinbaren Verdacht geraten, erheblichen weiteren Eingriffen wie z. B. Abhörmaßnahmen aussetzen.

15.3 Sonstiges

Bei der Polizei wurden unter anderem Prüfungen in folgenden Bereichen durchgeführt:

– Einsatz von Personalcomputern

– Speicherungen im Schengener Informationssystem

– Anordnungen zum Einsatz von verdeckten technischen Mitteln zur Datenerhebung

– Übermittlungen polizeilicher Informationen an Vermieter und Arbeitgeber.

Beratungen und Empfehlungen bezogen sich unter anderem auf

– das Einsatzlenkungssystem der Polizei (HELP)

– die Dateiführung bei der zentralen Beschwerdestelle.

16. Staatsanwaltschaft

16.1 Auskünfte über den Fernmeldeverkehr

Die Entwicklung neuer Technologien im Bereich der Informations- und Kommunikationstechniken, insbesondere die Digitalisierung des Fernmeldeverkehrs, wirft neue Probleme auf, wenn die Strafverfolgungsbehörden von ihren herkömmlichen Zugriffsbefugnissen Gebrauch machen. Hiermit hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter meinem Vorsitz im Jahr 1996 eingehend befaßt. Auf die im Anhang wiedergegebene Entschließung wird verwiesen.

Im Berichtszeitraum haben wir uns aufgrund von Eingaben mit folgender Fallkonstellation auseinandergesetzt: Jemand gerät in den Verdacht, eine Straftat begangen zu haben. Im Zuge der Ermittlungen ist es von Interesse, ob er mit anderen Personen Kontakt gehabt hat. Wenn dieser Kontakt telefonisch über einen ISDN-Anschluß, ein Autotelefon oder ein Handy stattgefunden hat, ist er registriert. Der Telefondienstanbieter speichert für Abrechnungszwecke Verbindungsdaten, insbesondere, welche Rufnummern angewählt wurden. Die Rufnummern werden nach Rechnungsversand noch achtzig Tage aufbewahrt. Dies erfolgt regelmäßig um die letzten drei Ziffern gekürzt, wenn der Kunde sich nicht für eine vollständige Speicherung oder gänzliche Löschung ausgesprochen hat. Die Frage, ob eine bestimmte bekannte Telefonnummer angerufen worden ist, läßt sich bei Kenntnis weiterer Umstände oft auch anhand gekürzter Telefonnummern beantworten.

Nach § 12 des Fernmeldeanlagengesetzes kann aufgrund richterlicher Anordnungen in Strafermittlungsverfahren Auskunft über den Fernmeldeverkehr verlangt werden, „wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und daß die Auskunft für die Untersuchung Bedeutung hat“. Die Gesetzesformulierungen lassen ahnen, daß diese Vorschrift ursprünglich gar nicht für den Telefonverkehr gemeint war. Als sie vor Jahrzehnten geschaffen wurde, gab es im analogen Telefonverkehr noch keine Aufzeichnungen von Verbindungsdaten, es ging vielmehr allein um Telegramme. Die neuen technischen Rahmenbedingungen des digitalen Fernmeldeverkehrs stellen den Strafverfolgungsbehörden daher bei unveränderten Befugnissen einen viel größeren „Datenpool“ zur Verfügung.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher mehrfach Kritik an der Regelung in § 12 FAG geübt. Dem neuen wesentlich erweiterten Umfang von Auskünften trägt der Wortlaut der Vorschrift nicht Rechnung, da er außer dem Richtervorbehalt keine weiteren Einschränkungen enthält. Er sieht insbesondere auch keine Vorkehrungen zur Begrenzung des Eingriffs auf das unverzichtbare Maß vor. Mit der Rechtsprechung (z. B. BGH NJW 1993, 1212 ff.) ist daher zu fordern, daß die Anwendung von § 12 FAG nach dem Verhältnismäßigkeitkeitsprinzip auf gewichtige Strafvorwürfe eingeschränkt wird.

Soweit nach diesem Maßstab Auskünfte über Verbindungsdaten in Betracht kommen, dürfen sie nur in dem zur Strafverfolgung im Einzelfall erforderlichen Umfang verwendet werden. In den Eingabefällen war das Telefonunternehmen jeweils zur Herausgabe aller Verbindungsdaten verpflichtet worden, die von einem Telefonanschluß im Zeitraum von

mehreren Wochen geführt worden waren. Erst anhand dieser Listen sollte festgestellt worden, ob ein bestimmter, als verdächtig angesehener Kontakt zu einer anderen Person stattgefunden hatte. Diese Vorgehensweise ist problematisch, weil mit ihr das gesamte telefonische Kommunikationsverhalten des Betroffenen offengelegt wird, auch soweit es strafrechtlich völlig belanglos ist. Wenn die betroffene Person z. B. Arzt, Anwalt oder Journalist ist, kann mit umfänglichen Auskünften über den Fernmeldeverkehr auch das jeweilige gesetzlich geschützte Vertrauensverhältnis zu Patienten, Mandanten oder Informanten empfindlich beeinträchtigt werden.

Diese Auswirkungen können vermieden oder abgemildert werden, wenn sich Auskunftsverlangen darauf beschränken, ob ein bestimmter als verdächtig angesehener telefonischer Kontakt stattgefunden hat. Sofern es nach dem Stand der Ermittlungen unverzichtbar ist, die Auskunftsverlangen auf bestimmte längere Zeiträume zu beziehen, müssen nicht erforderliche Verbindungsdaten unverzüglich nach Auswertung durch die zuständige Strafverfolgungsbehörde gelöscht werden.

Diese Gesichtspunkt werden bei einer Neufassung der Regelung zu Auskünften über Verbindungsdaten zu berücksichtigen sein, da der bisherige § 12 FAG mit Ablauf des Jahres 1997 außer Kraft tritt. Der Bundesrat hatte bereits 1991 festgestellt, daß ein umfassender Grundrechtsschutz verlangt, den durch § 12 FAG ermöglichten Eingriff auf das unerläßliche Maß zu beschränken. Der Gesetzgeber sei deshalb gehalten, auch unter Beachtung des Bestimmtheitsgebotes eine Neuregelung des § 1 FAG vorzunehmen, mit der die Eingriffsmöglichkeiten – abgestimmt mit den Vorschriften der Strafprozeßordnung – unter engen Voraussetzungen und abschließend festgelegt werden (Beschlußdrucksache des Bundesrates 416/91 vom 27. September 1991).

16.2 Automation bei der Staatsanwaltschaft

Die im 14. TB (16.4) angekündigte Entscheidung der Justizbehörde über die künftige automatisierte Vorgangsverwaltung und -bearbeitung bei der Staatsanwaltschaft ist Anfang 1996 getroffen worden: Hamburg hat gemeinsam mit den Ländern Brandenburg, Hessen und Schleswig-Holstein den Auftrag zur Entwicklung eines neuen Verfahrens erteilt. Diese sogenannte Mehrländer-Staatsanwaltschafts-Automation (MESTA) soll auf dem in Schleswig-Holstein bereits bestehenden Verfahren zur Geschäftsstellen-Automation der Staatsanwaltschaft (GAST) aufbauen und ab 1997 in den beteiligten Staatsanwaltschaften eingeführt werden.

Die Justizbehörde, die den Vorsitz in der länderübergreifenden Lenkungsgruppe hat, hat uns an den Entscheidungen zum Projektfortschritt eingehend beteiligt. Aus unserer Sicht kommt es bei dem neuen Verfahren darauf an, ob und wie zwischen den Personendaten von Beschuldigten einerseits und Tatopfern, Anzeigeerstattern und Zeugen andererseits unterschieden wird. Wir haben deutlich gemacht, daß ein Zugriff auf Daten von Tatopfern, Anzeigenerstattern und Zeugen nur den Mitarbeitern eingeräumt werden kann, die für das einzelne Verfahren zuständig sind. Zuständigkeitsübergreifende Zugriffe darf es dagegen nur auf Daten von Beschuldigten geben. Das automatisierte Verfahren muß daher nach den Personenrollen und der Zuständigkeit der Zugriffsberechtigten differenzieren.

Die im Herbst vorgelegten ersten Fassungen des Funktionenmodells für MESTA enthielten diese Differenzierung noch nicht. Mit dem Projekt besteht jedoch Übereinstimmung, daß die

Unterscheidung der Personenrollen und der Zugriffsberechtigungen im Zuge der weiteren Fortschreibung des Funktionenmodells geleistet wird.

Ein anderer Problemkreis ist die Übermittlung von Daten von den örtlichen Verfahren der Staatsanwaltschaften zum zentralen staatsanwaltschaftlichen Verfahrensregister (ZStV). Dieses Register wird zwar frühestens ab 1999 seine Tätigkeit aufnehmen, die Planungen auf Bundesebene haben allerdings bereits begonnen. Abgesehen von den grundsätzlichen Bedenken gegen dieses Register und die Rechtsvorschriften zu seiner Einführung (13. TB, 19.1.1; 14. TB, 16.2) ist eine zentrale datenschutzrechtliche Forderung, daß die Daten zwischen ZStV und örtlicher Staatsanwaltschaft nur verschlüsselt übertragen werden.

Die Notwendigkeit, Daten von der Sensibiliät staatsanwaltschaftlicher Informationen nur verschlüsselt in Telekommunikationsnetzen zu übertragen, die auch Dritten zugänglich sind, ist allgemein anerkannt. Auch der ADV-Koordinierungsausschuß von Bund, Ländern und Gemeinden (KoopA-ADV) empfiehlt dies. Bei den Planungen für das künftige bundesweite INPOL-System der Polizei ist die Verschlüsselung unstreitig. Allein die Justizressorts des Bundes und der Länder sehen dies für das ZStV anders. Sie halten bisher die Einrichtung einer geschlossenen Benutzergruppe für ausreichend. Nur widerstrebend waren sie dazu zu bewegen, die Frage der Zugriffssicherung bei der Datenübertragung erneut durch eine Risikoanalyse der Registerbehörde beurteilen zu lassen. Sie soll erst nach Erstellung des Feinkonzepts erfolgen,

das noch nicht vorliegt; daher gibt es in dieser Frage noch keinen Fortschritt.

17. Justiz

17.1 Entwurf eines Justizmitteilungsgesetzes

Die Bundesregierung hat am 22. Mai 1996 den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz – JuMiG) im Bundestag eingebracht. Eine bereichsspezifische gesetzliche Regelung des Justizmitteilungswesens wird von den Datenschutzbeauftragten seit Jahren gefordert (vgl. 10. TB, 19.1.3; 12. TB, 19.2).

Der nun vorgelegte Gesetzentwurf beschränkt sich in weiten Bereichen auf bloße Mitteilungsermächtigungen, während die Begründung von Mitteilungspflichten den Justizverwaltungsvorschriften überlassen bleibt. Eine Benachrichtigung der Betroffenen von Amts wegen gleichzeitig mit der Übermittlung ihrer Daten ist nur noch in wenigen Ausnahmefällen vorgesehen. Anders als im früheren Gesetzentwurf fehlt auch eine Aussage zur Anordnungsbefugnis für

Mitteilungen. Diese Befugnis sollte nach unserer Auffassung besonders qualifizierten Bediensteten (Richtern, Staatsanwälten, Beamten des gehobenen Justizdienstes) vorbehalten bleiben.

Bedenken bestehen ferner gegen eine Reihe von Einzelregelungen. Sie richten sich insbesondere gegen die weitgehende Durchbrechung des Steuergeheimnisses bei Mitteilungen

aus Strafverfahren gegen Beamte sowie gegen die Verwendung der aus anderem Anlaß übermittelten Daten für Zwecke der Sicherheitsüberprüfung. Der Bundesrat hat jedenfalls durchgesetzt, daß die im Gesetzentwurf zunächst vorgesehenen Verwendungsbeschränkungen für gerichtliche Entscheidungen, die nicht in ein Führungszeugnis für Behörden aufzunehmen sind, gestrichen wurden.

Damit sind aus Sicht des Datenschutzes erhebliche Defizite bei der sich bislang abzeichnenden gesetzlichen Regelung festzustellen.

17.2 Öffentliche Fahndung im Strafverfahren

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Konferenz am 14./15. März 1996 in Hamburg die in der Anlage abgedruckten Grundsätze für die öffentliche Fahndung im Strafverfahren zustimmend zur Kenntnis genommen.

18. Strafvollzug

18.1 Sicherheitsüberprüfung externer Arbeitskräfte durch das Strafvollzugsamt

Aus Anlaß einer Eingabe führen wir gegenwärtig Gespräche mit dem Strafvollzugsamt darüber, unter welchen Voraussetzungen und in welchem Umfang Handwerker und Vermessungskräfte, die während ihres Arbeitseinsatzes

– häufig nur kurzfristig – das Gelände einer Justizvollzugsanstalt (JVA) betreten, einer Sicherheitsüberprüfung durch das Strafvollzugsamt, insbesondere durch formularmäßige Abfrage von Erkenntnissen beim Landeskriminalamt (LKA), unterzogen werden dürfen.

Mit dem Strafvollzugsamt besteht weitgehend Einvernehmen darüber, daß hier nach dem Grundsatz der Verhältnismäßigkeit datenschutzrechtlich ein strengerer Maßstab anzulegen ist als bei ehrenamtlichen Vollzugshelfern, die gezielt einen längeren und intensiveren Kontakt zu einzelnen Gefangenen suchen. Insbesondere haben wir vorgeschlagen, die Anfrage des Strafvollzugsamtes beim LKA auf Erkenntnisse über schwere Straftaten zu beschränken, die wegen des Tatbestandes (z. B. Gefangenenbefreiung, Geiselnahme, Verstöße gegen das Waffen- oder Betäubungsmittelgesetz) oder wegen der Höhe der verhängten Strafe konkret auf ein Sicherheitsrisiko für die JVA hindeuten. Anfragen an das LKA, die auch Freisprüche oder Einstellungen mangels hinreichenden Tatverdachts oder wegen geringer Schuld einbeziehen, halten wir in den genannten Fällen der Sicherheitsüberprüfung für unzulässig.

Das Strafvollzugsamt möchte stärker nach den Sicherheitsbelangen der jeweiligen JVA differenzieren. Schließlich könnte auch danach unterschieden werden, ob der Einsatz auf dem Anstaltsgelände erkennbar Sicherheitsinteressen berührt, z. B. weil der Betroffene Zugang zu Räumen erhält, in denen sensible Akten verwahrt werden.

Über die Notwendigkeit verkürzter Speicherungsfristen für LKA-Erkenntnisse besteht Einigkeit. Die Diskussion mit dem Strafvollzugsamt ist noch nicht abgeschlossen.

19. Gesundheitswesen

19.1 AOK-Prüfung

Eine Prüfung der Abrechnung der AOK Hamburg mit den verschiedenen Leistungserbringern ergab mehrere Kritikpunkte.

19.1.1 Zugriff auf Versichertendaten

In dem von der AOK eingesetzten hierarchischen EDV-System „IDVS II“ haben die Mitarbeiterinnen und Mitarbeiter, die Leistungsaufträge bearbeiten bzw. Rechnungen überprüfen, jeweils Zugriff auf die Datenbanken

– Versicherten-Datenbank (Stammdaten),

– Leistungs-Datenbank (Krankenhausdaten und Arbeitsunfähigkeitsdaten),

– Sachleistungs-Datenbank (Hilfsmittel, Zahnersatz und Kieferorthopädie).

Dieses Zugriffsrecht haben die entsprechenden Sachbearbeiterinnen und Sachbearbeiter in allen Geschäftsstellen der AOK Hamburg hinsichtlich aller Versicherten der AOK Hamburg.

Wir halten diese Regelung, die so oder ähnlich auch bei anderen gesetzlichen Krankenkassen anzutreffen ist, für einen Verstoß gegen § 35 Sozialgesetzbuch I (SGBI) (vgl. 13. TB, 6.4 und 14. TB, 5.3). Nach dieser Vorschrift ist auch innerhalb der AOK sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.

Die AOK hat uns zugesagt, sich bei der anstehenden Reform des IDVS

II-Systems im AOK-Bundesverband dafür einzusetzen, daß die einzelnen AOK-Unternehmen die Zugriffsmöglichkeiten ihrer Sachbearbeiterinnen und Sachbearbeiter entsprechend ihrer jeweiligen Organisationsstruktur differenzierter regeln können; die AOK will dann eine solche Möglichkeit auch nutzen und die Zugriffsrechte der Mitarbeiterinnen und Mitarbeiter auf einzelne Datenbanken bzw. Teile von ihnen beschränken.

Hinsichtlich der geschäftsstellenübergreifenden Zugriffsrechte der AOK-Mitarbeiterinnen und Mitarbeiter auf die Sozialdaten aller Versicherten konnte ein Konsens hingegen nicht erreicht werden. Selbst dann, wenn eine überarbeitete Version des IDVS-II-Systems die Möglichkeit böte, solche geschäftsstellenübergreifenden Zugriffe zu unterbinden, will die AOK allen Versicherten die unbeschränkte Möglichkeit offenhalten, spontan bei jeder Hamburger Geschäftsstelle vollen Service in Anspruch zu nehmen.

Wir halten demgegenüber unverändert eine stärkere Berücksichtigung des informationellen Selbstbestimmungsrechts der Versicherten in der Weise für geboten, wie wir es im 13. und 14. TB (a.a.O.) im einzelnen dargestellt haben: Den Versicherten sollte die Entscheidung

darüber überlassen bleiben, bei welcher Geschäftsstelle oder bei welchen Geschäftsstellen (ggf. allen) die Mitarbeiterinnen und Mitarbeiter auf ihre gesamten Sozialdaten zugreifen können. Sie sollten die Möglichkeit haben, anderen AOK-Mitarbeiterinnen und -Mitarbeitern den Zugriff auf ihre Daten zu verwehren.

Vor einer möglichen formellen Beanstandung haben wir wegen der bundesweiten Bedeutung dieser Frage – auch für andere Krankenkassen, bei denen ähnliche Regelungen bestehen, – den Bundesbeauftragten für den Datenschutz einbezogen.

19.1.2 Weitere Prüfungsergebnisse

Die von der AOK gespeicherten Abrechnungsdaten der Krankenhäuser enthalten Informationen über die Krankenhauspatienten, die nicht erforderlich sind, z. B. über die Ursache der Behandlungsbedürftigkeit. Wir forderten die AOK auf, eine auf Bundesebene vereinbarte weniger detaillierte Datenliste zu verwenden.

Außerdem hat die Abrechnung von Heil- und Hilfsmitteln (z. B. Krankengymnastik oder ein Rollstuhl) ohne die Angabe von Diagnosen durch den Leistungserbringer zu erfolgen. Durch Richtlinien auf Bundesebene hat die AOK jedoch das Rezept abzufordern, auf dem der Arzt oft die Diagnose vermerkt. Wir baten die AOK, gegenüber dem Bundesverband auf ein datenschutzfreundliches Verfahren hinzuwirken.

Für die Abrechnung von Arzt- und Zahnarztleistungen sieht § 295 SGB V vor, daß die Kassen(zahn)ärztliche Vereinigung die Daten nur „fallbezogen, nicht versichertenbezogen“ an die Kassen übermittelt. Dem widerspricht die Praxis aller Krankenkassen. Wir konzentrieren uns mit den anderen Datenschutzbeauftragten weiter auf eine datenschutzgerechte Rahmenregelung des zukünftigen Datenträgeraustauschs, die die Spitzenverbände der gesetzlichen Krankenkassen mit der Kassen(zahn)ärztlichen Bundesvereinigung vereinbaren.

19.2 Basisdokumentation Suchthilfe

Der Drogenbeauftragte der Behörde für Arbeit, Gesundheit und Soziales (BAGS) und die privatrechtlichen Drogen- und Suchtberatungsstellen führten lange eine Auseinandersetzung über ein neues Dokumentations- und Monitoringsystem für die Suchthilfe.

Gegenstand des Streits war einerseits ein standardisierter Erhebungsbogen mit einer Vielzahl von Daten über die Klienten der Beratungsstellen und andererseits die Übermittlung dieser Daten in anonymisierter Form zu wissenschaftlichen Auswertungen. In mehreren Gesprächen, Trägertreffen und Briefwechseln vertraten wir folgende datenschutzrechtliche Vorgaben:

– Die Dokumentation der Beratungen und Maßnahmen in den Beratungsstellen ist – auch im Interesse der Klienten – fachliche Aufgabe dieser Stellen. Nach § 28 BDSG ist ihre Speicherung „im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses“ auch ohne die Einwilligung des betroffenen Klienten zulässig. Von der Speicherung der Daten in einem EDV-System ist der Betroffene jedoch zu benachrichtigen.

– Ein von der BAGS eingeführter einheitlicher Erhebungsbogen mit vorgegebenen Angabefeldern kann die Beratungsstellen nicht dazu zwingen, alle Felder auszufüllen. In dem Bogen müssen vielmehr nur solche Angaben gemacht werden, die nach der Art, Ausrichtung und Methode der jeweiligen Beratungsstelle aus ihrer fachlichen Sicht für die Tätigkeit benötigt werden.

– Eine Übermittlung von Klientendaten an eine dritte Stelle darf nur in nicht-identifizierender Form erfolgen. Weder die Mitarbeiterinnen und Mitarbeiter der Beratungsstellen noch die Klienten dürfen für Außenstehende erkennbar sein.

Diese Anforderungen führten zum einen zur Streichung einzelner Angaben im Erhebungsbogen wie dem tag-genauen Beginn und Abschluß der Beratung und der Frage nach „illegalen Einkünften“. Zum anderen wurde zusammen mit der BAGS folgendes Verfahren zur Teil-Anonymisierung entwickelt:

In den Beratungsstellen wird der Klientenname durch einen leicht – auch manuell – zu bildenden Einweg-Schlüssel aus Buchstaben des Namens, der Postleitzahl des Wohnortes und dem Geburtsjahr ersetzt. Darüber hinaus wird dem Klienten bzw. seinem Code eine (einmalige) nicht-personenbezogene Registriernummer zugeordnet, die nur die Art der Beratungsstelle offenbart. Von den Beratungsstellen werden in bestimmten Zeitintervallen die Klientendaten ausschließlich mit der Registriernummer an einen neuen Verein (BADO e.V.) übermittelt, der über die weitere wissenschaftliche Auswertung der Falldaten entscheidet und diese mit der Nummer weiterleitet.

Eine bei der Universität Hamburg angesiedelte Referenzstelle erhält von den Beratungsstellen ausschließlich den Code und die Registriernummer (ohne die Erhebungsdaten). Diese Stelle kann nun Doppel- und Mehrfachmeldungen zu derselben Person feststellen, indem sie aus den verschiedenen Beratungsstellen Registriernummern mit demselben Code zusammenstellt. Das Ergebnis, z. B. daß die Registriernummern 1,2,3 zu derselben Person gehören – und damit für Verlaufsuntersuchungen genutzt werden können –, übermittelt die Referenzstelle über den Verein an das auswertende Institut.

Auch wenn ein Restrisiko einer Re-Anonymisierung über die Beratungsdaten und entsprechendes Zusatzwissen nicht ganz auszuschließen ist, erscheint dieses Verfahren angesichts der Zusammensetzung und Zielsetzung des BADO e.V. (mit starker Vertretung der Beratungsstellen selbst) und der Forschungsklausel in § 27 HmbDSG datenschutzrechtlich vertretbar. Es schließt mangels konkretem Personenbezug vor allem eine – rechtlich grundsätzlich zulässige – Beschlagnahme von Klientenunterlagen beim Verein faktisch aus.

Es ist nun Aufgabe des BADO e.V., für die Beratungsstellen und die Auftragsvergabe an Forschungsstellen einheitliche datenschutzrechtliche Rahmenbedingungen zu schaffen. So sind die Klienten über das gesamte Verfahren und ihr Auskunftsrecht zu informieren. Die Datensicherheit der EDV in den Beratungsstellen und die sichere Aufbewahrung und spätere Vernichtung der Codes, Registriernummern und Erhebungsbögen bei Referenzstelle, Verein und Forschungsstelle ist zu regeln. Der Hamburgische Datenschutzbeauftragte soll bei der Erstellung der Richtlinien beteiligt werden.

19.3 Sonstiges

Weitere Schwerpunkte unserer Tätigkeit im Bereich des Gesundheitswesens bildeten folgende Themen:

– Bundesweit werden flächendeckende Dokumentationen über kindliche Fehlbildungen angestrebt. Unsere Beratung des federführenden Hamburger Amtes für Gesundheit soll vor allem die Anonymisierung der sensiblen Falldaten und die Einhaltung der Zweckbindung gewährleisten, der die schon bestehenden Perinatal- und Neonatalerhebungen unterliegen.

– Der automatisierte Datenaustausch zwischen den kassen(zahn)ärztlichen Vereinigungen und den Leistungserbringern einerseits und den gesetzlichen Krankenkassen andererseits wirft eine Fülle datenschutzrechtlicher Fragen auf. Jedes einzelne übermittelte Datum muß für die Erfüllung der gesetzlichen Aufgaben der Kassen erforderlich sein und darf nur dort einen Personenbezug aufweisen, wo das Sozialgesetzbuch dies vorsieht.

– In diesem Zusammenhang haben wir auch zur gesetzlich vorgesehenen Verschlüsselung der Diagnosen nach dem sog. ICD-10 (International Code of Deseases, 10. Auflage) kritisch Stellung genommen. Die dort vorgeschriebe– nen Schlüssel gehen zum Teil weit über medizinische Diagnosen hinaus und unterschieden zunächst nicht zwischen Verdachts- und bestätigten Diagnosen. Inzwischen wurde die Pflicht zur Anwendung des ICD-10 bundesweit ausgesetzt, um eine geeignetere Version zu erstellen.

– Für die Krankenhäuser wird wegen Raummangels eine externe Archivierung von Patientenakten immer dringender. In unseren Beratungen wiesen wir darauf hin, daß bereits die offene Aufbewahrung und ggf. Herausgabe durch private Archive einen Verstoß des Krankenhauses gegen die ärztliche Schweigepflicht darstellt. Datenschutzrechtlich kommen nur Transporte und Verwahrungen in geschlossenen Behältnissen oder in einzelnen verschlossenen Umschlägen mit einem Namenscode in Betracht.

– Wie schon im letzten Jahr (14. TB, 19.2) begleiteten wir die Einführung der umfassenden Krankenhaus-Software SAP IS-H in den verschiedenen Kliniken des Landesbetriebs Krankenhäuser. Neben Fragen der Erforderlichkeit von Patientenaufnahmedaten und des Zugriffsberechtigungs-Konzepts waren auch Probleme der Datenübertragung zwischen kooperierenden Krankenhäusern, insbesondere eine Verschlüsselung, Gegenstand der Beratungsgespräche.

– Für die von uns zuletzt kritisierte Abrechnung der staatlichen Krankenhäuser mit Sozialämtern (14. TB, 19.4) konnte inzwischen ein Verfahren gefunden werden, das auch den datenschutzrechtlichen Belangen entspricht. Die Weitergabe von Patientendaten an das zuständige Sozialamt erfolgt nun erst nach Mahnungen des Kostenschuldners und einer Ankündigung der Übermittlung im Falle der Nichtzahlung.

– Hinsichtlich der Fernwartung der Patientenüberwachungsanlage im UKE hat das Krankenhaus seinen im 14.TB (19.7) mitgeteilten Vorschlag inzwischen wieder verworfen und eine externe Software-Firma mit der Umsetzung des ursprünglich mit uns vereinbarten Monitoring-Verfahrens beauftragt.

20. Personenstandswesen

20.1 Novellierung des Personenstandsgesetzes (PStG)

Die Behörde für Inneres hat uns im April 1996 den von der Bund-LänderArbeitsgruppe „Novellierung des Personenstandsgesetzes“ erarbeiteten Vorentwurf (Stand: 25. März 1996) für ein Fünftes Gesetz zur Änderung des Personenstandsgesetzes (5. PStÄndG) zugesandt.

Wir begrüßen, daß mit diesem Vorentwurf die Arbeiten für eine Überarbeitung des Personenstandsgesetzes wieder aufgenommen wurden, die seinerzeit nach der Vereinigung und der unterschiedlichen Strukturen des Personenstandswesens in der Bundesrepublik und in der ehemaligen DDR ausgesetzt worden waren (vgl. 11. TB, 14.).

Der Vorentwurf enthält gegenüber dem geltenden Personenstandsgesetz eine Reihe von Änderungen hinsichtlich des Einsatzes von elektronischer Datenverarbeitung in den Standesämtern. Er berücksichtigt weitgehend die seit Jahren vorgetragenen Forderungen der Datenschutzbeauftragten des Bundes und der Länder (vgl. 7. TB, 4.10.2), insbesondere

– die Mitteilungspflichten des Standesbeamten gesetzlich zu verankern,
– die Einsicht in die Personenstandsbücher und die Erteilung von Auskünften und Urkunden präziser zu regeln,

– eigenständige Vorschriften über die Auskunft und Einsicht für Zwecke der wissenschaftlichen Forschung zu schaffen.

Gleichwohl halten wir Änderungen für erforderlich, die beim weiteren Fortgang des Gesetzesvorhabens berücksichtigt werden sollten. Dies betrifft insbesondere folgende Bereiche:

Der Standesbeamte kann künftig personenbezogene Daten, die zum Zweck der Eintragung in ein Personenstandsbuch erhoben werden, auch über den Zeitpunkt der Beurkundung hinaus für anstehende Änderungen des Personenstandes oder für die Fortführungen der Personenstandsbücher nutzen (§ 5 Abs. 1 PStÄndGE). Er kann die Zweitbücher künftig auch auf elektronischen Datenträgern führen (§ 44 Abs. 1 PStÄndGE). Dafür fehlen aber Vorgaben für entsprechende technische und organisatorische Maßnahmen zur Datensicherung. Diese sollten entweder in das Personenstandsgesetz aufgenommen werden; anderenfalls wäre auf die entsprechenden Bestimmungen in den Landesdatenschutzgesetzen (in Hamburg: § 8 HmbDSG) zu verweisen.

Gemäß dem rechtstaatlichen Gebot der Normenklarheit sollten auch die Bestimmungen über Mitteilungen und Mitteilungspflichten des Standesbeamten (§§ 5 Abs. 3; 6 Abs. 7; 13 Abs. 5; 14 Abs. 2; 15 Abs. 3; 30 Abs. 2 PStÄndGE), erheblich präziser gefaßt werden. Insbesondere die vorgesehene Regelung des § 66 PStÄndGE als Generalklausel für die Mitteilungspflichten des Standesbeamten begegnet datenschutzrechtlichen Bedenken. Sie dürfte den Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil als Voraussetzung für eine normenklare bereichsspezifische Datenverarbeitungsregelung angegeben hat (BVerf 65/1, 42, 44), in keiner Weise gerecht werden.

Zur Gewährleistung datenschutzrechtlicher Anforderungen sollten bei der Datenweitergabe die als Mitteilungsempfänger vorgesehenen Behörden abschließend genannt und der Umfang der mitzuteilenden Daten beschrieben werden. Es sollte außerdem klargestellt werden, daß die Mitteilung nur zu einem bestimmten Verwendungszweck erfolgen darf, der in der Zuständigkeit des Empfängers liegt und gesetzlich bestimmt ist.

Hinsichtlich der Einsicht in Personenstandsbücher und der Erteilung von Auskünften über Eintragungen zu Personen sind die Voraussetzungen für die Benutzung durch Personen, durch Behörden und zur Durchführung wissenschaftlicher Forschungsarbeiten in jeweils eigenen Vorschriften geregelt.

So ist nach der geplanten Neufassung des § 61 Abs. 1 PStÄndGE für die Benutzung der Personenstandsbücher durch Personen ein berechtigtes Interesse glaubhaft zu machen, wenn seit dem Tod des Betroffenen mindestens

30 Jahre oder, falls der Todestag nicht bekannt ist, seit der Geburt mindestens 120 Jahre vergangen sind. Es ist davon auszugehen, daß durch diese datenschutzrechtliche Regelung insbesondere die private Ahnen- bzw. Familienforschung in angemessener Weise erleichtert wird. Damit dürften künftig auch die häufig vorgebrachten Beschwerden von Bürgern, der Datenschutz verhindere die private Ahnenforschung, beendet sein (vgl. 12. TB, 14.1).

Im Gegensatz zum geltenden Recht ist das in § 61a PStÄndGE vorgesehene behördliche Einsichts- und Auskunftsrecht auf die Erfüllung von hoheitlichen Aufgaben beschränkt worden. Damit werden die Behörden im Vergleich zu dem Benutzungsrecht durch Personen (§ 61 PStÄndGE) und der Benutzung der Personenstandsbücher zur Durchführung wissenschaftlicher Forschung

(§ 61 b PStÄndGE) erheblich schlechter gestellt.

Da bei den Behörden aber auch nichthoheitliche öffentliche Aufgaben vorkommen können, sollte eine Möglichkeit geschaffen werden, wie die Behörden diese Daten erhalten können. Ein derartiger Fall liegt beispielsweise bei der Ermittlung der Daten von Toten zwecks öffentlicher Ehrung durch eine Behörde vor. In diesem Zusammenhang wird insbesondere an die Problematik beim Projekt der KZ-Gedenkstätte Neuengamme erinnert (vgl. 14. TB, 9.3). Während nach geltendem Recht eine Übermittlung der Daten als zulässig erachtet wurde, wäre sie nach den Regelungen des § 61a PStÄndGE nicht mehr möglich. Einerseits kommt § 61 PStÄndGE nicht in Betracht, weil dort auf die Benutzung der Personenstandsbücher durch Personen abgestellt wird, andererseits handelt es sich in diesem Fall wohl kaum um eine hoheitliche Aufgabe oder ein Forschungsvorhaben einer Behörde, so daß auch die §§ 61 a und 61 b PStÄndGE nicht zur Anwendung gelangen können.

Wir haben daher vorgeschlagen, eine adäquate Regelung für die Erfüllung von nichthoheitlichen behördlichen Aufgaben in § 61a PStÄndG aufzunehmen oder auf eine Differenzierung in hoheitliche und nichthoheitliche Aufgaben zu verzichten.

Mit den vorgesehenen Bestimmungen in § 61 b PStÄndGE soll auch der wissenschaftlichen Forschung die Benutzung der Personenstandsbücher eröffnet werden. Dies wird ausdrücklich begrüßt, weil es in der Vergangenheit auch hierüber zu erheblichen Diskussionen mit Forschungsinstituten gekommen ist (vgl. 12. TB, 14.1). Allerdings sind dazu Änderungen des Entwurfs angebracht.

In Absatz 1 fehlt – im Gegensatz zu Regelungen in Landesdatenschutzgesetzen – eine Aussage, daß die Zustimmung der zuständigen Verwaltungsbehörde zu einem Forschungsvorhaben den Empfänger, die Art der zu übermittelnden Daten, den Kreis der Betroffenen, den konkreten Forschungszweck und die Dauer der Datenspeicherung zu bezeichnen hat und daß sie dem Landesdatenschutzbeauftragten mitzuteilen ist. Darüber hinaus sollte auch geregelt werden, daß die Daten zu löschen sind, sobald der Forschungszweck dies gestattet (vgl. § 27 Abs. 2 und 3 HmbDSG).

Weitere Abweichungen von Landesdatenschutzgesetzen sind in Absatz 2 enthalten, wonach z. B. der Empfänger die übermittelten Daten mit Zustimmung der zuständigen Verwaltungsbehörde auch für einen anderen als den ursprünglichen Forschungszweck verwenden oder weiterübermitteln darf; dies ist nach den Landesdatenschutzgesetzen nur mit Einwilligung des Betroffenen möglich (vgl. § 27 Abs. 4 HmbDSG). Wir haben daher vorgeschlagen, die Regelungen in § 61 b PStÄndGE den strengeren Anforderungen der Landesdatenschutzgesetze anzupassen.

Wir gehen davon aus, daß die Behörde für Inneres unsere Vorschläge bei der Abfassung einer Stellungnahme gegenüber dem Bundesministerium des Innern berücksichtigen wird.

21. Wirtschaftsverwaltung

21.1 Korruptionsbekämpfung bei der Vergabe öffentlicher Aufträge

Gegenwärtig werden auf Bundes- und Landesebene verschiedene Ansätze für eine effizientere Korruptionsbekämpfung diskutiert.

Die Finanzbehörde und die Baubehörde beabsichtigen in diesem Zusammenhang, eine Richtlinie für die Vergabe von Lieferungen und Leistungen einschließlich Bau- und sonstige Leistungen nach Nr. 2.4, 2.5 und 2.6 der Verwaltungsvorschriften zu § 55 Landeshaushaltsordnung zu erlassen. Danach sollen Bewerber und Bieter bei Vorliegen schwerer Verfehlungen, die ihre Zuverlässigkeit in Frage stellen, von der Vergabe öffentlicher Aufträge ausgeschlossen werden können.

Wir haben zunächst darauf hingewiesen, daß wir eine effiziente, präventive und repressive Korruptionsbekämpfung unterstützen. In einem Punkt haben wir jedoch erhebliche rechtliche Bedenken, die der Bundesbeauftragte für den Datenschutz teilt:

Nr. 2 des Richtlinienentwurfs sieht vor, daß der Nachweis einer schweren Verfehlung u. a. durch die von den Bewerbern oder Bietern geforderten Auszüge aus dem Gewerbezentralregister erbracht werden kann. Die Forderung einer solchen Selbstauskunft stellt nach unserer Auffassung eine offenkundige Umgehung des § 150 a Gewerbeordnung dar.

Mit dieser bereichsspezifischen Vorschrift hat der Bundesgesetzgeber abschließend geregelt, in welchen Fällen öffentliche Stellen Auskünfte aus dem Gewerbezentralregister erhalten dürfen. Auch die Frage, wann die Erteilung von Auskünften aus dem Gewerbezentralregister

auf Antrag des Betroffenen zur Vorlage bei Behörden erfolgen kann, ist nach derzeitiger Rechtslage abschließend in § 150 Abs. 5 Gewerbeordnung geregelt.

Eine Erweiterung der Zweckbestimmungen von Auskünften aus dem Gewerbezentralregister ist allein dem Bundesgesetzgeber vorbehalten. So hat der Bundesrat in seiner Stellungnahme zum Entwurf eines Gesetzes zur Bekämpfung der Korruption (Bundesratsdrucksache 553/96) z. B. eine Ergänzung des § 150 a Gewerbeordnung zum Zweck der Durchführung von Ordnungswidrigkeitenverfahren nach § 38 Abs. 1 Nr. 3 und Nr. 8 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) vorgeschlagen. Eine Erweiterung des § 150 a Gewerbeordnung für die Fälle einer Auskunftserteilung an die Vergabestellen bei der öffentlichen Auftragsvergabe ist nicht erfolgt.

Aufgrund dieser erheblichen rechtlichen Bedenken haben wir die Finanzbehörde unter Vorbehalt einer förmlichen Beanstandung aufgefordert, den Hinweis auf Selbstauskünfte aus dem Gewerbezentralregister in Nr. 2 des Richtlinienentwurfs zu streichen und dementsprechend auf die Einholung von Selbstauskünften bei der Vergabepraxis zu verzichten. Bisher liegt uns keine Antwort der Finanzbehörde vor.

21.2 Betriebsleitererklärung der Handwerkskammer

Mit der Handwerkskammer konnten wir im Berichtszeitraum eine längerwährende Diskussion darüber beenden, welche Daten über den Gewerbetreibenden und seinen Betriebsinhaber erhoben werden dürfen, um die Voraussetzungen für die Eintragung in die Handwerksrolle zu klären.

§ 17 Handwerksordnung (HandwO) i. V. m. § 6 Abs. 7 HandwO und § 3 der Verordnung über die Handwerksrolle regeln bereichsspezifisch und sehr normenklar, welche Angaben dazu im einzelnen erhoben werden dürfen. Nach § 17 HandwO ist der Gewerbetreibende insoweit auskunftspflichtig, nicht jedoch der Betriebsleiter.

Bislang erhob die Handwerkskammer formularmäßig mit einer sog. „Betriebsleitererklärung“ wesentlich mehr Daten, als vom Gesetz zugelassen, insbesondere zu anderweitigen Arbeitsverhältnissen des Betriebsleiters. Zudem verlangte sie eine unzulässige Einwilligungserklärung, auf deren Grundlage die Handwerkskammer Ermittlungen zum Betriebsleiterverhältnis u. a. beim Arbeitsamt und bei Krankenkassen anstellen wollte. Darüber hinaus wurde der Zweck der Datenerhebung nicht erläutert und auch nicht der Umstand, daß die Auskunftspflicht nur seitens des Gewerbetreibenden besteht; die Mehrzahl der Daten wurde beim Betriebsleiter erhoben.

Die Handwerkskammer hat das Formular inzwischen unter Berücksichtigung unserer Kritik so geändert, daß es keinen datenschutzrechtlichen Bedenken mehr begegnet.

21.3 Sonstiges

Einzelne weitere Problemfelder in der Wirtschaftsverwaltung waren im Berichtszeitraum

– ein Forschungsprojekt des zur Handwerkskammer gehörenden Zentrums für Arbeit und Gesundheit (ZAG) über arbeitsbedingte Erkrankungen im Friseurhandwerk,

– ein Musterentwurf für eine Allgemeine Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55c der Gewerbeordnung.

Einzelne Probleme des Datenschutzes

im nicht-öffentlichen Bereich

22. Versicherungswirtschaft

Die Arbeitsgruppe Versicherungswirtschaft unter Federführung der Obersten Aufsichtsbehörde für den Datenschutz in Hamburg behandelt in regelmäßigen Sitzungen mit Vertretern der Versicherungswirtschaft aktuelle Datenschutzfragen. Die Ergebnisse werden dem Düsseldorfer Kreis, der Konferenz der Obersten Datenschutzbehörden der Länder, vorgestellt.

In der Vergangenheit gelang es überwiegend, in angemessener Zeit mit der Versicherungswirtschaft Lösungen für die aufgetretenen Fragen zu erzielen. Seit etwa zwei Jahren ist jedoch zu beobachten, daß zugesicherte Stellungnahmen, Unterlagen und rechtliche Bewertungen seitens der Verbandsvertreter und Versicherungen trotz wiederholter Erinnerungen nur sehr zögerlich abgegeben werden.

Zwar ist die Versicherungswirtschaft rechtlich nicht verpflichtet, Datenschutzfragen mit der Arbeitsgruppe abzustimmen. Es hat sich jedoch gezeigt, daß auf diese Weise etliche Probleme im Vorfeld geklärt werden konnten und einschneidendere aufsichtsbehördliche Maßnahmen gegenüber Unternehmen und Verbänden entbehrlich wurden. Insofern sind die derzeitigen erheblichen Verzögerungen, auf die nachstehend näher eingegangen wird, außerordentlich zu bedauern.

Nach der europäischen Datenschutzrichtlinie können derartige Vereinbarungen künftig als „Verhaltensregeln“ verbindlich abgestimmt werden. Die Richtlinie ist bis 1998 in deutsches Recht umzusetzen (siehe 1.4).

22.1 Registrierung von Versicherungsvermittlern

Obwohl die Initiativen zur Benennung der registerführenden Stelle durch die Bundesregierung fortbestehen (vgl. 13. TB, 23.7; 14. TB, 22.3), ist weiterhin offen, ob es zu einer Umsetzung der EG-Empfehlung vom 18. Dezember 1991 kommen wird.

Das auf privater Basis gegründete Zentralregister für Versicherungsvermittler in Deutschland (vgl. 14. TB, 22.3) führt seine Vorbereitungen für eine Tätigkeitsaufnahme fort. Die bereits im 14. Tätigkeitsbericht aufgeführten Richtlinien sind mittlerweile überarbeitet worden, ohne jedoch die wesentlichen Kritikpunkte auszuräumen. Zwar wird das Register nicht mehr als „öffentliches Register“ bezeichnet, im übrigen wurde jedoch wenig geändert.

Eine nähere Befassung mit diesem Thema wurde zurückgestellt, bis die Entscheidung über die Umsetzung der EG-Empfehlung getroffen ist.

22.2 Auskunftsstelle über den Versicherungsaußendienst (AVAD)

Im Berichtszeitraum übersandte der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) den Entwurf einer Einwilligungserklärung in das Verfahren der Auskunftsstelle über den Versicherungsaußendienst (AVAD) (vgl. zuletzt 12. TB, 24.8) mit der Bitte um eine Stellungnahme.

Die – neue – Einwilligungserklärung, die Bezug auf ein neu zu fassendes Informationsblatt über den AVAD-Auskunftsverkehr nimmt, wurde den übrigen Obersten Aufsichtsbehörden verabredungsgemäß zugeleitet. Dem GDV wurde mitgeteilt, daß eine endgültige Stellungnahme erst in Verbindung mit dem noch nicht vorgelegten neugefaßten Informationsblatt abgegeben werden könne. Das Informationsblatt wurde in seiner Entwurfsfassung jedoch nicht, wie verabredet, nachgereicht. Ohne daß die Aufsichtbehörde Gelegenheit zu einer Stellungnahme hatte, wurde einige Wochen später die beschlossene und schon verwendete Einwilligungserklärung zusammen mit dem neuen Informationsblatt übersandt.

Die Verfahrensweise der Versicherungswirtschaft ist auch deshalb besonders zu kritisieren, weil in dem Informationsblatt über den AVAD-Auskunftsverkehr behauptet wird, die Datenschutzfragen seien von der zuständigen Datenschutzbehörde überprüft und mit ihr verfahrensmäßig im einzelnen abgestimmt worden.

Mittlerweile stellt die AVAD diese Behauptung in der Neufassung des Informationsblattes nicht mehr auf.

22.3 Schufa-Selbstauskünfte von Versicherungsvermittlern

Nach dem Bundesdatenschutzgesetz (BDSG) hat jeder Betroffene das Recht, Auskunft über seine gespeicherten Daten zu verlangen. Das gilt auch für die Daten, die die Schufa speichert, um ihre Vertragspartner vor Verlusten im Kreditgeschäft mit Konsumenten zu schützen.

Die dadurch eröffnete Möglichkeit, die Schufa-Daten zu erfahren, machen sich zunehmend Branchen zunutze, die keine Kredite gewähren und daher nicht Vertragspartner der Schufa werden können. Der Aufsichtsbehörde wurde dies zunächst im Bereich der Vermieter und Makler bekannt, die von Wohnungsinteressenten Schufa-Selbstauskünfte verlangen (vgl. 13. TB, 22.1). Jetzt ist sogar mindestens ein Versicherungsunternehmen dazu übergegangen, von seinen Vermittlern vor Abschluß einer Courtage-Vereinbarung diese Selbstauskunft einzuholen. Die Informationen werden nicht automatisiert verarbeitet.

Begründet wird dieses Verhalten im Versicherungsbereich damit, daß die Vertreter nach den vom Bundesaufsichtsamt für das Versicherungswesen (BAV) erlassenen Richtlinien zuverlässig und vertrauenswürdig sein müssen. Darüber hinaus werden Nachteile im Falle strafbarer Handlungen durch die Vermittler wegen etwaiger Rückgriffe auf die Unternehmen

befürchtet. Dem ist jedoch entgegenzuhalten, daß die von dem Unternehmen angeführten Richtlinien des BAV genaue Angaben über einzuholende Unterlagen machen, wie

z. B. die AVAD-Auskunft, die Aufschluß über das vergangene Verhalten von Betroffenen im Rahmen von Vermittlerverträgen geben. Nur dies kann auch entscheidend für Courtage-Vereinbarungen sein, nicht dagegen die Aufnahme etwaiger Privatkredite.

Die gegen eine Schufa-Selbstauskunft von Mietinteressenten sprechenden Gründe wurden bereits ausführlich dargestellt (vgl. 13. TB, 22.1) und gelten entsprechend auch für Versicherungsvermittler. Insbesondere kann keinesfalls von einer „freiwilligen“ Weitergabe an das Unternehmen die Rede sein, weil sonst der Abschluß der Courtage-Vereinbarung abgelehnt wird.

Erfreulicherweise hat eine Umfrage des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. (GDV) unter betrieblichen Datenschutzbeauftragten von Versicherungsunternehmen ergeben, daß die Einholung einer Schufa-Selbstauskunft bei Abschluß einer Courtage-Vereinbarung ganz unüblich ist. Es wird daher davon ausgegangen, daß es sich in dem bekannt gewordenen Fall um einen Einzelfall handelt.

22.4 Zentrale Warn- und Hinweissysteme

22.4.1 Haftpflicht- und Transportversicherer-Hinweissysteme

Wie bereits berichtet (vgl. 14. TB, 22.1), führt die Versicherungswirtschaft ein Haftpflicht-Hinweissystem ein und hat auch das System der Transportversicherer auf ein automatisiertes Verfahren umgestellt.

Für beide Dateien wurde ein Kriterienkatalog entwickelt, der Punktskalen enthält, nach denen die Unternehmen Betroffene einmelden. Die zugrunde liegenden Kriterien wurden den Aufsichtsbehörden zwar bekanntgegeben; eine Diskussion über Einzelheiten wurde jedoch unter Hinweis auf ausgewertete Statistiken abgelehnt.

Auch im Falle des Transportversicherer-Hinweissystems wird darauf zu achten sein, ob die in dem Versicherungsmerkblatt zur Datenverarbeitung aufgeführten Einmeldevoraussetzungen (Verdacht des Versicherungsmißbrauchs) vorliegen.

Die Versicherungswirtschaft beabsichtigt, die Wiedergabe des neuen Haftpflichtsystems in dem Merkblatt entsprechend dem Text für die Kfz-Hinweisdatei zu formulieren.

22.4.2 Aufbewahrung von Volltexten beim Verband

Im Rahmen der Umstellung aller zentralen Warn- und Hinweissysteme auf das phonetische Strukturcode-Verfahren sollten die von den Versicherungsunternehmen gemeldeten Klardaten nach der Codierung vernichtet werden (vgl.

10. TB, 25.1). Dies wurde von den Datenschutzaufsichtsbehörden aus Sicherheitsgründen ausdrücklich begrüßt und in einem Schreiben des Gesamtverbandes der deutschen Versicherungswirtschaft (GDV) noch einmal bestätigt.

Nachdem nunmehr sämtliche Dateien auf das neue Verfahren umgestellt wurden, fand bei dem Verband eine aufsichtsbehördliche Prüfung statt. Dabei stellte sich heraus, daß die an den Verband gelieferten Daten zunächst im Volltext auf Magnetbändern erfaßt und anschließend codiert werden. Eine Kopie der Magnetbänder mit den Volltexten wird beim Verband für fünf Jahre archiviert und unterliegt damit dem jederzeitigen Zugriff.

Die Aufsichtsbehörde hat aus Sicherheitsgründen gefordert , daß die Daten auf den Magnetbändern zu löschen sind und die weitere Vorhaltung derartiger Kopien unterbleiben muß. Die geforderte Vernichtung der Daten beim Verband

ist bisher nicht erfolgt.

Der Verband führte zunächst an, daß ein jederzeitiger Zugriff auf die Daten für den Fall etwaiger Änderungen (z. B. bei den Postleitzahlen oder der Vercodungslogik) erhalten bleiben müsse. Diese Argumentation kann schon deshalb nicht überzeugen, weil mit dem Parallelverfahren in der Zentralen Registrierstelle Rechtsschutz (vgl. 11. TB, 25.1) eine annehmbare Lösung gefunden wurde.

Nunmehr hat der GDV vorgeschlagen, die Magnetbänder einem Notar zu übergeben und lediglich einmal jährlich zu aktualisieren. In einem Vertrag sollen die Herausgabegründe abschließend festgelegt werden.

Diese Lösung beseitigt zumindest die Befürchtung eines jederzeitigen Zugriffs des Verbandes auf die gespeicherten Klardaten.

22.4.3 Auskünfte durch Versicherungsunternehmen

Zur Verhinderung von Betrug zu Lasten von Versicherungsunternehmen in der Lebensversicherung sind die Unternehmen nach Unterzeichnung der Datenschutzeinwilligungsklausel berechtigt, auch abgelehnte Anträge an ein zentrales Hinweissystem zu melden, wenn bestimmte – im Merkblatt zur Datenverarbeitung aufgeführte – Voraussetzungen vorliegen.

Die Eingabe eines Petenten bei der Aufsichtsbehörde machte deutlich, daß Versicherungen versuchen, diese Tatsache zu verschleiern. Das Verlangen nach Rückgabe der eingereichten Unterlagen wurden von mehreren Versicherern mit den unterschiedlichsten Begründungen verweigert. Es wurde jedoch nie darauf hingewiesen, daß die Daten im Rahmen der Einmeldung in das zentrale Warn- und Hinweissystem der Lebensversicherer weiter benötigt werden.

Auf Anregung der Obersten Aufsichtsbehörden der Länder sagte der Verband der Lebensversicherer zu, ein Rundschreiben zu verfassen, wonach in derartigen Fällen eine

korrekte Antwort erforderlich sei. Nach Auskunft der Versicherungswirtschaft ist das Rundschreiben bereits vorbereitet und sollte schon 1995 versandt werden.

Nunmehr erreichte die Obersten Aufsichtsbehörden der Entwurf eines Rundschreibens, der jedoch noch nicht abschließend abgestimmt werden konnte.

22.5 Krankenhaus-Entlassungsberichte

Einige private Krankenversicherungen sind dazu übergegangen, regelmäßig Krankenhaus-Entlassungsberichte anzufordern. Selbst nach Einschätzung der Versicherungswirtschaft ist die Kenntnis dieser Berichte nicht generell geeignet, Aufschluß über die Leistungsverpflichtung zu geben. Sie dienen vielmehr in Ausnahmefällen, z. B. wenn die medizinische Notwendigkeit einer Operation fraglich ist, dazu, Zweifel am Behandlungsergebnis auszuräumen.

Der Verband der privaten Krankenversicherung e. V. hat ein Rundschreiben an seine Mitgliedsunternehmen vorbereitet, in dem darauf hingewiesen wird, daß nur im Falle ernstlicher Zweifel an der medizinischen Notwendigkeit des stationären Aufenthaltes unter bestimmten Gesichtspunkten diese Berichte angefordert werden dürfen. Ferner wird deutlich gemacht, daß in allen übrigen Fällen die ausdrückliche Zustimmung des Versicherungsnehmers eingeholt werden muß.

Die Obersten Aufsichtsbehörden haben angeregt, die Betroffenen darüber hinaus in jedem Fall zumindest zu informieren, daß ein KrankenhausEntlassungsbericht angefordert wurde.

22.6 Zugriff auf Versichertendaten

Die Versicherungsunternehmen haben die Zugriffsrechte ihrer Mitarbeiter auf die Vertrags- und Leistungsdaten der Kunden unterschiedlich geregelt. Trotz mehrfacher Nachfrage wurde den Obersten Aufsichtsbehörden der Länder bisher weder eine Aufstellung der Möglichkeiten in den Versicherungen noch ein Lösungsvorschlag zur Vereinheitlichung übersandt (vgl. 14. TB, 22.4).

Einzelne Unternehmen erwägen, ihren Mitarbeitern bundesweit zumindest die Vertragsdaten sämtlicher Kunden zugänglich zu machen, eventuell sogar weitergehend die Leistungsdaten zur Verfügung zu stellen. Derart umfassende Möglichkeiten überschreiten bei weitem die Erforderlichkeit der Kenntnisnahme von Kundendaten im Rahmen eines Vertragsverhältnisses. Es mag durchaus sein, daß einzelne Versicherungsnehmer großen Wert darauf legen, unter gewissen Umständen sämtliche Geschäftsstellen eines Unternehmens im Bundesgebiet aufsuchen zu können und dort die notwendigen Informationen vorzufinden. Andere Versicherungsnehmer wenden sich jedoch entschieden gegen eine bundesweite Streuung ihrer Daten.

Dieses Problem ließe sich lösen, indem jedem einzelnen Kunden die Wahlfreiheit im Sinne einer Zugriffsbeschränkung auf eine, mehrere oder sämtliche Geschäftsstellen eingeräumt wird (vgl. 14. TB, 5.3). Darüber hinaus sind auch technisch erweiterte Zugriffe – beispielsweise durch individuelle Kundenpaßwörter – im Einzelfall denkbar.

Ein Gespräch des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) mit betrieblichen Datenschutzbeauftragten von Versicherungsunternehmen hat ergeben, daß in der Mehrzahl der Fälle nach der Art der Daten unterschieden wird:

– Adreßdaten des Kunden sind in jeder Geschäftsstelle abrufbar. Bei Vertragsdaten ist ein regionaler Zugriff, je nach Sparte, für alle zuständigen Mitarbeiter möglich.

– Die Schaden- und Leistungsdaten stehen nur im Rahmen der jeweiligen Organisationseinheiten den berechtigten Schadensachbearbeitern zur Verfügung.

Durch Angaben, die über die Personalien hinausgehen, kann der Versicherungskunde in allen Geschäftsstellen weitere Zugriffe ermöglichen. Gegen diese Ausübung seines Selbstbestimmungsrechts bestehen keine Bedenken. Bei den vorher genannten Zugriffsmöglichkeiten ohne Mitwirkung des Kunden wird jedenfalls nach Sensibilität der Daten differenziert, so daß die Gefährdung des Datenschutzes nicht so ausgeprägt ist wie bei Kreditinstituten mit uneingeschränkten Zugriffsmöglichkeiten in allen Zweigstellen.

22.7 Gruppenversicherungsverträge

Einige Vereine bieten ihren Mitgliedern Gruppenversicherungsverträge mit festgelegten Versicherungsunternehmen zu vergünstigten Tarifen an. Um die Vereinsmitglieder vor unzulässigen Datenübermittlungen zu schützen, wurde mit den Obersten Aufsichtsbehörden ein bestimmtes Verfahren vereinbart. Danach sind die Betroffenen vorab über einen vorgesehenen Vertreterbesuch zu informieren und haben die Möglichkeit, die Datenübermittlung von vornherein zu verhindern (vgl. zuletzt 12. TB, 24.6).

Mehreren Eingaben zufolge werden aber entweder die erforderlichen Einwilligungen nicht eingeholt oder die Avis-Schreiben nicht gemäß dem vereinbarten Text abgefaßt.

Unter diesen Umständen ist die Übermittlung von Vereinsmitgliederdaten an Versicherungsunternehmen unzulässig. Zwar handelt es sich um listenmäßig zusammengefaßte Daten, die gemäß § 28 Abs. 2 Nr. 1 b BDSG unter erleichterten Bedingungen übermittelt werden dürfen. Aus folgenden Gründen besteht jedoch Grund zu der Annahme, daß die Betroffenen ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung haben:

– Den Vereinsmitgliedern wird nicht schriftlich ein Angebot des Unternehmens unterbreitet, sondern sie werden von Versicherungsvertretern zu Hause aufgesucht. Damit kann sozialer Druck zum Abschluß eines Vertrages verbunden sein.

– Dies gilt besonders angesichts der Tatsache, daß häufig versucht wird, Abtretungserklärungen für etwaige Überschußbeteiligungen zugunsten des datenübermittelnden Vereins zu erwirken.

– Gruppenversicherungsverträge werden oft von Vereinen angeboten, in denen beispielsweise ältere Menschen organisiert sind, so daß es erfahrungsgemäß zu einer hohen Anzahl von Vertragsabschlüssen kommt.

Ohne daß die Betroffenen Gelegenheit erhalten, zu widersprechen, ist die Datenübermittlung von einem Verband oder Verein an ein Versicherungsunternehmen also nicht zulässig.

Dies wurde mit dem hauptsächlich betroffenen Versicherungsunternehmen noch einmal besprochen. Dessen Aussagen zufolge handelte es sich jedoch um bedauerliche Ausnahmefälle, in denen im Einzelfall von den mit den Aufsichtsbehörden abgesprochenen Verfahrensweisen abgewichen wurde.

23. Schufa

23.1 Mieterdatenschutz und Schufa-Selbstauskunft

Über die Praxis einiger Vermieter, von Mietinteressenten regelmäßig die Vorlage einer Schufa-Selbstauskunft zu verlangen, hatten wir zuletzt im 13. TB (22.1) berichtet und auf datenschutzrechtliche Bedenken gegen ein solches Verfahren hingewiesen. Die Bürgerschaft beschloß daraufhin in ihrer Sitzung vom 8./9. Mai 1996 ein Ersuchen an den Senat, darauf hinzuwirken, daß zukünftig Wohnungsunternehmen nicht von Mietinteressenten und deren Bürgen eine Schufa-Selbstauskunft verlangen. Dabei waren sich die Abgeordneten darüber im klaren, daß eine Einflußnahme nur auf die städtischen Wohnungsunternehmen möglich ist. Diese Wohnungsunternehmen haben entweder bisher keine Schufa-Selbstauskünfte angefordert oder werden zukünftig darauf verzichten.

Da die Bürgerschaft ihr Ersuchen zugleich als Appell an andere Wohnungsunternehmen und Vermieter verstanden wissen wollte, hat sich die Baubehörde im Juli 1996 in diesem Sinne schriftlich an zahlreiche wohnungswirtschaftliche Verbände gewandt. In dem Schreiben wurden die Verbände gebeten, den Beschluß der Bürgerschaft zur Kenntnis zu nehmen und ihre Verbandsmitglieder entsprechend zu informieren, damit in Zukunft auf die Vorlage von Schufa-Selbstauskünften verzichtet wird. Außerdem wurde darauf hingewiesen, daß nach den Schufa-Richtlinien Anfragen bei der Schufa zur Vermietung von Wohn- und Geschäftsräumen unzulässig sind. Diese Richtlinie solle über eine Selbstauskunft nicht umgangen werden.

Die ersten Reaktionen einiger Verbände zeigen, daß zahlreiche Vermieter auch zukünftig die Option haben wollen, Schufa-Selbstauskünfte von Mietinteressenten verlangen zu dürfen. Ein Verband hat seinen Mitgliedern unter Hinweis auf das Schreiben der Baubehörde sogar ausdrücklich empfohlen, nicht auf Schufa-Selbstauskünfte zu verzichten. Deshalb werden wir ergänzend das Gespräch mit den wohnungswirtschaftlichen Interessenvertretern suchen.

Daneben haben wir die Problematik an den Düsseldorfer Kreis herangetragen, um zu erreichen, daß die zuständigen Ressorts in den anderen Bundesländern in gleicher Weise initiativ werden. Dabei war unser Ziel, daß zumindest die kommunalen und städtischen Wohnungsunternehmen bundesweit einheitlich grundsätzlich nicht die Vorlage einer Schufa-Selbstauskunft verlangen. In der Sitzung des Düsseldorfer Kreises vom 19./20. September 1996 wurde unsere Anregung zur Kenntnis genommen und mehrheitlich zugesagt, in diesem Sinne an die Ressorts heranzutreten, sobald entsprechende Eingaben vorliegen.

Eine ähnliche Problematik durch Vorlage von Schufa-Selbstauskünften ergibt sich bei Versicherungsvermittlern (vgl. 22.3).

24. Versandhandel

24.1 Warndatei

Ein Versandhandelsunternehmen in Hamburg führt eine Warndatei, auf die auch andere Versandhäuser des Konzerns zugreifen können. Hierüber hatten wir zuletzt im 14. TB (24.1) berichtet. Unsere Verhandlungen haben wir mit dem Unternehmen im Berichtszeitraum fortgesetzt und dabei einige datenschutzrechtliche Fortschritte erzielen können.

Auf dem Erstbestellschein wird der Besteller vor der Unterschriftszeile darauf hingewiesen, daß auf der Rückseite eine Information über die Verwendung seiner Daten im Rahmen der Auftragsabwicklung abgedruckt ist. Diese Information enthält nunmehr auch einen Hinweis darauf, daß das Versandhandelsunternehmen zum Zwecke der Kreditprüfung einen Datenaustausch mit anderen konzernverbundenen Versandhäusern und den im Kreditgewerbe üblichen Informationsaustausch mit der Schufa durchführt. Dies reicht aus, um für den Personenkreis, der einen Erstbestellschein verwendet, eine Ausnahme von der Benachrichtigungspflicht nach § 33 Abs. 2 Nr. 1 BDSG anzunehmen.

Da das Unternehmen auch zahlreiche andere Bestellmöglichkeiten anbietet – hierbei spielt insbesonders der telefonische und zunehmend auch der multimediale Bestellservice eine wichtige Rolle –, kommt jedoch den Allgemeinen Geschäftsbedingungen (AGB) zusätzlich eine wichtige Bedeutung zu, weil bei diesen Bestellwegen der Erstbestellschein nicht verwendet wird. Deshalb hat das Versandhandelsunternehmen auch dort den Hinweis auf den Datenaustausch in gleicher Formulierung wie auf dem Erstbestellschein aufgenommen. Leider ist dieser Hinweis optisch, drucktechnisch und plazierungsmäßig nicht besonders hervorgehoben. Diesen Aspekt erörtern wir mit dem Unternehmen weiter.

Im übrigen hat sich das Versandhaus wegen des Betriebs der Warndatei zwischenzeitlich nach § 32 Abs. 1 BDSG zum Register der Aufsichtsbehörde gemeldet. Darüber hinaus sind noch Festlegungen nach § 10 Abs. 2 BDSG von den beteiligten Versandhandelsunternehmen wegen des Online-Betriebs

der Warndatei zu treffen. Sie sollen der Aufsichtsbehörde in Kürze vorgelegt werden.

25. Kreditwirtschaft

25.1 Allfinanzkonzepte und Einwilligungserklärung

Banken und Sparkassen arbeiten zunehmend mit anderen Finanzdienstleistungsunternehmen, z. B. Bausparkassen und Versicherungen zusammen, um ihren Kunden umfassende

Finanzdienstleistungen anbieten zu können. Seit Anfang 1994 verhandeln die Obersten Aufsichtsbehörden der Länder und Vertreter der Kreditwirtschaft in der Arbeitsgruppe „Kreditwirtschaft“ über die Formulierung einer Einwilligungserklärung zur Datenweitergabe im Konzern oder Verbund.

Durch Unterzeichnung der Einwilligungserklärung geben die Kunden ihr Einverständnis zur Datenübermittlung an andere Unternehmen im Konzern oder an Kooperationspartner, die die Daten dann für gezielte Kundenwerbung nutzen dürfen. Übermittelt werden dabei neben Namen und Anschrift der Kunden u. a. auch Daten über Bausparverträge, Bankguthaben und Kredite. Die Übermittlung führt daher zur Offenlegung von sensiblen Daten, die dem Bankgeheimnis unterliegen.

Von Beginn der Verhandlungen an haben die Aufsichtsbehörden eine den Erfordernissen des § 4 Abs. 2 BDSG genügende konkrete Einwilligungserklärung gefordert. Da andere Rechtsgrundlagen nach den Vorschriften des BDSG nicht ausreichen, sind derartige Übermittlungen nur zulässig, wenn die Betroffenen gemäß § 4 Abs. 2 BDSG eingewilligt haben.

Eine rechtswirksame Einwilligung setzt neben der umfassenden Information Freiwilligkeit voraus. Die Betroffenen müssen aus der Formulierung der Erklärung klar erkennen können, an wen welche Daten zu welchem Zweck übermittelt werden sollen. Die Nichtunterzeichnung der Erklärung darf auf den Bankvertrag keine Auswirkungen haben. Transparenz und Freiwilligkeit der Einwilligungserklärung stehen daher bei deren Beurteilung durch die Aufsichtsbehörden im Vordergrund.

Die Vertreter der Kreditwirtschaft haben – erstmals 1994 – Klauselentwürfe für die Datenübermittlung im Konzern und Verbund vorgelegt. Die Aufsichtsbehörden haben gefordert, den Datenumfang, den Empfängerkreis sowie die Anlässe der Datenübermittlung zu konkretisieren und die Klausel mit einer Ankreuz- oder Streichmöglichkeit zu kombinieren. Diese Anregungen wurden von der Kreditwirtschaft zum Teil berücksichtigt.

Wegen der in der Praxis unterschiedlich ausgestalteten Zusammenarbeit im Verbund oder Konzern haben die Vertreter der Kreditwirtschaft nun drei Einwilligungsklauseln vorgelegt. Sie haben darauf hingewiesen, daß diese Entwürfe nur den Charakter von Empfehlungen für die den Verbänden angehörenden Mitgliedsunternehmen hätten und die Ausgestaltung der Erklärungen im einzelnen den jeweiligen Unternehmen vorbehalten bleiben müsse.

In der kombinierten Hinweis-/ Einwilligungsklausel für Verträge mit einem Vermittler wird entsprechend der Forderung der Aufsichtsbehörden die weitergehende Nutzung der Daten von der Einwilligung der Kunden abhängig gemacht, wenn der Vermittler die Daten für Beratungen bei anderen Finanzdienstleistungen verwenden will. In der Klausel wird darauf verwiesen, daß die Einwilligungserklärung ohne Einfluß auf den Vertrag jederzeit widerrufen werden kann.

In den Klauselentwürfen über die Datenübermittlung zwischen Kreditinstituten bzw. Bausparkassen und Kooperationspartnern werden neben den Namen der Verbundpartner auch die Daten aufgezählt, die übermittelt werden sollen. Allerdings handelt es sich nicht um eine abschließende Aufzählung, wie sie von den Aufsichtsbehörden gefordert wurde. Durch die Formulierung „insbesondere dürfen übermittelt werden“, ist auch die Übermittlung weiterer Daten nicht ausgeschlossen.

Die Aufsichtsbehörden haben neben einer Änderung dieser Formulierung gefordert, daß die Einwilligungserklärung nach § 4 Abs. 2 Satz 3 BDSG im äußeren Erscheinungsbild hervorzuheben ist. Den gesetzlichen Anforderungen würde am besten durch eine separate Erklärung Rechnung getragen. Gerade weil die Finanzdaten der Betroffenen an Unternehmen übermittelt werden sollen, zu denen die Kunden vielfach keine Geschäftsbeziehungen unterhalten oder nicht unterhalten wollen, kommen der Bestimmtheit und dem Erscheinungsbild der Klauseln große Bedeutung zu.

Die Aufsichtsbehörden regen des weiteren zur Herausstellung der Freiwilligkeit des Erklärenden bei Abgabe der Einwilligungserklärung an, neben dem bereits in den Klauselentwürfen der Kreditwirtschaft enthaltenen Hinweis auf die Widerrufsmöglichkeit den Erklärenden auf die Möglichkeit der Streichung der Klausel hinzuweisen, wenn diese mit anderen Erklärungen in einem Formular zusammengefaßt wird.

In der letzten Sitzung der „Arbeitsgruppe Kreditwirtschaft“ wurden in den Fragen der Bestimmtheit/Bestimmbarkeit der zur Übermittlung vorgesehenen Daten, der Hervorhebung der Einwilligungserklärung bei Zusammenfassung mit anderen Erklärungen und der Freiwilligkeit/Transparenz der Einwilligungserklärung Annäherungen erzielt. Es bestand Einvernehmen, daß auch bei bereits bestehenden Vertragsverhältnissen eine Datenübermittlung und -nutzung nur bei Vorhandensein einer wirksamen Einwilligungserklärung erfolgen darf.

25.2 Datenerhebung in Kreditkartenanträgen

Im Berichtszeitraum beschäftigte sich die Aufsichtsbehörde mit der Datenerhebung in Kreditkartenanträgen. Einige Kartenherausgeber legen dem Kunden bei Antragstellung umfangreiche Fragebogen vor, mit denen detaillierte Angaben über persönliche Verhältnisse und die Einkommens- und Vermögenssituation erfragt werden. Auf diese Weise erfährt das Kreditinstitut außer Geburtsort, Nationalität und Gültigkeitsdauer der Aufenthaltserlaubnis auch den Familienstand der Antragsteller, die Anzahl der Kinder, den Mädchennamen der Mutter, die Art der Wohnung, den früheren Wohnsitz und ob die Antragsteller im Besitz eines Pkw sind. Es werden Angaben über den

– auch früheren – Arbeitgeber verlangt, über die Beschäftigungsbranche und welche weiteren Kreditkarten die Antragsteller besitzen.

Zusätzlich verlangt der größte Teil der Kartenherausgeber auch ein Einverständnis des Antragstellers zur Einholung bankülicher Auskünfte bei der kontoführenden Bank sowie die Unterzeichnung der Schufa-Klausel. Die Kreditinstitute erhalten so eine umfangreiche Sammlung sensibler personenbezogener Daten der Antragsteller.

Datenschutzrechtlich ist es zweifelhaft, ob die Datenerhebung in dem genannten Umfang mit den Vorschriften des Bundesdatenschutzgesetzes vereinbar ist. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die Speicherung von personenbezogenen Daten im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen zulässig. Die Datenerhebung muß nach Treu und Glauben und auf rechtmäßige Weise erfolgen (§ 28 Abs. 1 Satz 2 BDSG). Mit Einreichung des Antragsformulars entsteht ein vertragsähnliches Vertrauensverhältnis zwischen den Antragstellern und den Kreditkartenherausgebern.

Im Rahmen dieses Vertrauensverhältnisses ist die Erhebung und Verarbeitung von personenbezogenen Daten aber nur in dem Umfang zulässig, in dem sie zur Entscheidung über einen Vertragsabschluß für den Kreditkartenherausgeber erforderlich ist. Danach dürfen nur die Daten erhoben werden, die Rückschlüsse auf die Bonität der Antragsteller und das Ausfallrisiko zulassen. Angaben wie u. a. Einzug in die derzeitige Wohnung, frühere Anschrift, Fahrzeugbesitz, Wohnungsstatus und Beschäftigungsdauer bedürfen daher aus datenschutzrechtlicher Sicht einer kritischen Überprüfung, da sie nicht generell Rückschlüsse auf die Bonität zulassen.

Wegen der grundsätzlichen Bedeutung der Angelegenheit wird das Thema in der Arbeitsgruppe Kreditwirtschaft mit Vertretern der Kreditwirtschaft erörtert.

25.3 Datenerhebung nach dem Wertpapierhandelsgesetz

Durch zahlreiche Eingaben wurden wir darauf aufmerksam, daß Kreditinstitute unter Hinweis auf das Wertpapierhandelsgesetz umfangreiche Daten zu den Vermögens- und Einkommensverhältnissen ihrer Kunden forderten.

Im Zusammenhang mit der Durchführung von Wertpapiergeschäften verlangen Kreditinstitute in einem Fragebogen detaillierte Auskunft über Vermögenswerte, jährliche Einkünfte, monatliche Belastungen, Hypotheken und die Anzahl der unterhaltsberechtigten Kinder ihrer Kunden. Daneben werden Angaben über das bisherige Anlageverhalten und die verfolgten Anlageziele erhoben. Selbst bei risikoarmen Anlagearten, wie dem Kauf von einer geringen Menge festverzinslicher Bundesanleihen, werden auf diese Weise von den Kunden umfassende Daten über ihre finanziellen Verhältnisse verlangt. Einige Kreditinstitute forderten darüber hinaus von Kunden, deren Wertpapiergeschäfte schon längere Zeit zurücklagen, nachträglich den Fragebogen auszufüllen.

Anlaß für die Datenerhebung ist die am 1. Januar 1995 in Kraft getretene Vorschrift des § 31 Wertpapierhandelsgesetz (WpHG). § 31 WpHG enthält allgemeine Verhaltensregeln für Wertpapierdienstleistungsunternehmen. Nach Absatz 2 der Vorschrift haben die Unternehmen von ihren Kunden Angaben über deren Erfahrungen oder Kenntnisse in den jeweiligen Wertpapiergeschäften, über die mit den Geschäften verfolgten Ziele und über die finanziellen Verhältnisse zu verlangen, soweit dies zur Wahrung der Interessen der Kunden und im Hinblick auf Art und Umfang der beabsichtigten Geschäfte erforderlich ist.

Sinn dieser Regelung ist eine ordnungsgemäße Anlageberatung, die unter Beachtung der Schutzbedürfnisse der Kunden sowie unter Berücksichtigung der Risiken der Anlage zu erfolgen hat. Die in § 31 Abs. 2 WpHG erhobenen Kundendaten dienen der Einschätzung der Schutzbedürftigkeit des Kunden, um diesen vor Risiken aus einer geplanten Wertpapieranlage zu schützen und dem Kreditinstitut die ordnungsgemäße Erbringung von Wertpapierdienstleistungen im Interesse der Kunden zu ermöglichen.

Mit dieser Zielsetzung ist die standardisierte und detaillierte Datenerhebung in den Fragebögen aber nicht vereinbar. Die Formulierungen „soweit“ und „erforderlich“ in § 31 Abs. 2 WpHG schränken die Datenerhebung auf solche Angaben ein, die für ein konkretes Anlagegeschäft im Einzelfall erforderlich sind. Angaben über das bisherige Anlageverhalten und die genauen Einkommens- und Vermögensverhältnisse sind daher von der Art des

Wertpapiergeschäfts und der Höhe der Transaktion abhängig. Darüber hinausgehende Angaben dürfen von den Kunden nur unter deutlichem Hinweis auf die Freiwilligkeit dieser Angaben erhoben werden. Eine Praxis der Banken, Fragebögen mit umfangreichen Fragen bei jedem Anlagegeschäft zu verwenden, ohne auf die Erfordernisse des Einzelfalles abzustellen, ist mit § 31 Abs. 2 WpHG nicht vereinbar. Eine gewisse Standardisierung der Datenerhebung mit Hilfe von Fragebögen kann allerdings mit den gesetzlichen Vorgaben im Einklang stehen.

Die Aufsichtsbehörden haben angeregt, die Möglichkeiten des Einsatzes von unterschiedlichen Fragebögen zu überprüfen, die den Unterschieden im Hinblick auf die Schutzbedürftigkeit und den Erfahrungs- und Wissenstand der Kunden im Einzelfall Rechnung tragen können.

Das Bundesaufsichtsamt für den Wertpapierhandel hat gemäß § 35 Abs. 2 WpHG inszwischen einen Richtlinienentwurf bezüglich der Anforderungen nach §§ 31 und 32 WpHG aufgestellt. Der Entwurf geht auf die Einholung von Kundenangaben und die Mitteilung zweckdienlicher Informationen ein. Nach dem Richtlinienentwurf ist der Umfang der von Kunden einzuholenden Angaben am Interesse des Kunden und an Art und Umfang der beabsichtigten Geschäfte auszurichten. Der Kunde ist vorher darauf hinzuweisen, wenn Angaben im Hinblick auf die beabsichtigten Geschäfte nicht erforderlich sind, sondern nur zur Vereinfachung im Rahmen der Gesamtgeschäftsbeziehung eingeholt werden.

Die Aufsichtsbehörden haben begrüßt, daß der Richtlinienentwurf die in der Praxis bei Befragungen nach § 31 Abs. 2 WpHG aufgetretenen datenschutzrechtlichen Probleme aufgegriffen hat. Vor dem Hintergrund ihrer Erfahrungen haben sie jedoch noch weitere differenzierende datenschutzrechtliche Regelungen in der Richtlinie gefordert. Es wurde angeregt, deutlicher zum Ausdruck zu bringen, daß nach dem Wertpapierhandelsgesetz für den Kunden keine gesetzliche Auskunftspflicht für die verlangten Angaben dem Kreditinstitut gegenüber besteht. Der Kunde muß freiwillig selbst entscheiden können, ob und welche Angaben er zu machen bereit ist.

Die Aufsichtsbehörden haben außerdem Konkretisierungen des Richtlinienentwurfs zur Erforderlichkeit der Kundenangaben im Einzelfall und zur Zweckbindung dieser Angaben gefordert. Es wurden Präzisierungen bei den Aufzeichnungs- und Aufbewahrungspflichten angeregt, wenn Dokumentationspflichten auch für weitere als die in § 34 Abs. 1 WpHG genannten Daten bestehen sollten.

Die Aufsichtsbehörden werden sich an der weiteren Entwicklung der Richtlinie gemäß § 35 Abs. 2 WpHG beteiligen.

25.4 Beschränkung des Zugriffs auf Kontoinformationen

Im 13. TB hatten wir unter 26.1 dargestellt, daß die Obersten Aufsichtsbehörden der Länder eine Eingrenzung der Zugriffsmöglichkeiten auf Kontoinformationen für erforderlich halten. Die Zugriffsmöglichkeiten sollen auf eine oder wenige Zweigstellen eines Kreditinstitutes beschränkt werden, um Mißbräuche von vornherein auszuschließen. Bei den Gesprächen zwischen den Obersten Aufsichtsbehörden und der Kreditwirtschaft konnte in diesem Punkt noch kein Ergebnis erzielt werden. Die Gespräche werden fortgeführt.

26. Arbeitnehmerdatenschutz

26.1 Telefondatenverarbeitung

26.1.1 Verarbeitung von Telefonverbindungsdaten

Im Rahmen der datenschutzrechtlichen Beratung von Unternehmen und Betriebsräten ist die Aufsichtsbehörde Hamburg beim Betrieb von Telekommunikations-Anlagen (TK-Anlagen) auf folgendes Verfahren gestoßen, das bereits in einigen Betriebsvereinbarungen auf der Grundlage des § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) festgeschrieben worden ist:

In der TK-Anlage werden bei jedem Anruf aus dem Unternehmen zunächst die kompletten Verbindungsdaten, darunter auch die vollständige Telefonnummer des Angerufenen, gespeichert. Verbindungsdaten eingehender Gespräche werden nicht erfaßt. In regelmäßigen Abständen – in der Regel täglich – werden die Verbindungsdatensätze aus der TK-Anlage programmgesteuert auf einen separaten Gebührenrechner übertragen und anschließend in der TK-Anlage gelöscht. Damit wird erreicht, daß die Verbindungsdaten über ausgehende Telefongespräche maximal für die Dauer von 24 Stunden in der TK-Anlage verfügbar sind.

Auf dem Gebührenrechner werden die Zielrufnummern grundsätzlich um 3 bis 4 Ziffern gekürzt gespeichert. Ein Programm auf diesem Rechner wählt einmal monatlich nach einem Zufallsprinzip 5 Prozent der Nebenstellen aus, für die die Verbindungsdatensätze für die nachfolgende Dauer eines Monats in kontrollierbarer ungekürzter Form gespeichert werden. Diese Nebenstellennummern werden in eine spezielle Datei geschrieben.

Die im Gebührenrechner gespeicherten Verbindungsdaten werden höchstens zwei Monate aufbewahrt und danach gelöscht. Darüber hinaus sind eine Reihe von zusätzlichen Regelungen getroffen worden (Geheimhaltungsverpflichtung der mit der Auswertung befaßten Personen, Protokollierung aller Zugriffe in einer Log-Datei, Einsichtsrecht des Betriebsrats in die Log-Datei, Herausnahme des Anschlusses des Betriebsrats aus der Zielnummernerfassung usw.).

Da eine datenschutzrechtlich problematische Vollspeicherung nur vorübergehend erfolgt, dürfte das beschriebene Verfahren der Verbindungsdatenverarbeitung noch zulässig sein. Im Düsseldorfer Kreis soll die Angelegenheit weiterbehandelt werden.

26.1.2 Aufzeichnung von Telefongesprächen in Unternehmen

Im Zuständigkeitsbereich der Aufsichtsbehörde Hamburg sind einige Unternehmen bereits seit längerem auf Anraten der zuständigen Polizeidienststellen dazu übergegangen, sämtliche Anrufe aufzuzeichnen, die in der Telefonzentrale auflaufen. Die Anlagen sind so gestaltet,

daß Gespräche, die von außen direkt mit Nebenstellen geführt werden, nicht aufgezeichnet werden können. Es handelt sich in aller Regel um digitale Dokumentationssysteme, die es ermöglichen, sowohl digitalisierte Aufzeichnungen über Verbindungsdaten als auch über Gesprächsinhalte vorzunehmen. Nachfolgend geht es um die Problematik der automatischen Aufzeichnung von Gesprächsinhalten.

In den hier bekanntgewordenen Fällen setzen die Unternehmen solche Anlagen ein, um Drohanrufe festzuhalten. Die digitalen Aufzeichnungsgeräte verfügen über eine Speicherkapazität von jeweils ca. vier Minuten. Ist diese Kapazität erreicht, wird die vorhergehende Aufnahme überschrieben. Sofern sich darunter ein Drohanruf befindet, wird der Gesprächsinhalt auf ein analoges Tonband überspielt, um die Ernsthaftigkeit der Drohung überprüfen zu können.

Da die Installierung und der Betrieb einer solchen Anlage den Bestimmungen des § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz unterliegt, haben die Unternehmen entsprechende Betriebsvereinbarungen geschlossen. Insoweit ist den Grundsätzen über den Persönlichkeitsschutz des Arbeitnehmers im Arbeitsverhältnis Rechnung getragen worden. Problematisch bleibt die Aufzeichnung der Gesprächsinhalte jedoch hinsichtlich der Persönlichkeitsrechte der Anrufer.

Nach § 201 Abs. 1 StGB wird mit Freiheits- oder Geldstrafe bestraft, wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt (Nr. 1) oder eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht (Nr. 2). Die Praxis der Unternehmen, jeden in der Telefonzentrale eingehenden Anruf zumindest für wenige Minuten aufzuzeichnen, erfüllt objektiv die Voraussetzungen der Aufnahme nach § 201 Abs. 1

Nr. 1 StGB, weil auch telefonische Äußerungen zum Schutzbereich dieser Regelung gehören. Auf die Gesprächsinhalte kommt es nicht an, sondern auch die Vermittlungsphase eines eingehenden Telefonats ist umfaßt.

Für die Strafbarkeit kommt es darauf an, ob die jeweilige Aufzeichnung unbefugt erfolgt. Hierzu muß folgende Differenzierung vorgenommen werden:

Die gezielte Aufzeichnung „auf Knopfdruck“ eines Drohanrufs ist ohne weiteres durch Notwehr nach § 32 StGB oder bei „notwehrähnlicher Lage“ aus § 34 StGB gerechtfertigt. Dasselbe wird man wohl auch bei der zufälligen Aufnahme eines Drohanrufes durch eine automatische Anlage annehmen müssen.

Problematisch ist hingegen die Aufzeichnung von Anrufen Unbeteiligter. Da von einer mutmaßlichen Einwilligung dieses Personenkreises nicht ausgegangen werden kann, kommt als Befugungsnorm allenfalls der rechtfertigende Notstand des § 34 StGB in Betracht. Dessen Anwendung hängt allerdings von zahlreichen Voraussetzungen ab, deren Erfüllung bei einer automatischen Aufzeichnung von Gesprächsinhalten höchst zweifelhaft sein dürfte.

Auch das neue Telekommunikationsgesetz (TKG) hilft hier nicht weiter. Zwar regelt § 86 Abs. 3 bis 5 TKG die Verarbeitung von Nachrichteninhalten und erfaßt auch den Fall der Wortaufzeichnung. Die Bestimmung sieht in ihrer abschließenden Aufzählung von Erlaubnistatbeständen aber die Ermittlung von Nachrichteninhalten zum Zwecke der Aufzeichnung von Drohanrufen nicht vor. Insbesondere gehören Drohanrufe im Sinne des § 86 Abs. 2 Nr. 3 b TKG nicht zu den Ausnahmefällen.

Im Ergebnis ist somit festzustellen, daß die beschriebene Praxis der Aufzeichnung von Telefongesprächen sowohl nach § 201 StGB als auch nach § 86 TKG Rechtsprobleme aufwirft. Die Aufsichtsbehörde Hamburg rät deshalb regelmäßig davon ab, ein System zur automatisierten Gesprächsaufzeichnung einzusetzen. Vielmehr sollten sich die Unternehmen darauf beschränken, lediglich in begründeten Einzelfällen, in denen Drohanrufe zu besorgen sind, Gesprächsinhalte „auf Knopfdruck“ aufzuzeichnen. Solche Einzelfälle sind nicht nur einzelne Anrufe, sondern es kann sich auch um begrenzte Zeiträume handeln, in denen vorübergehend sämtliche Anrufe wegen einer konkret bestehenden Bedrohungslage festgehalten werden müssen. Eine dauernde Bedrohungslage mit ständiger Aufzeichnung der Telefonate ist allerdings für keinen Wirtschaftsbereich anzunehmen; vergleichsweise gibt es auch in staatlichen Bereichen mit fortdauernder latenter Bedrohung keine ständige Aufzeichnung.

Der Düsseldorfer Kreis hat sich in seiner Sitzung am 19./20. September 1996 dieser Auffassung angeschlossen.

In der rechtswissenschaftlichen Literatur wird andererseits auch die Meinung vertreten, daß durch die Einführung eines sogenannten „Treuhandmodells“, das eine Reihe von Sicherheitsvorkehrungen gegen die mißbräuchliche Nutzung der aufgezeichneten Gespräche beeinhaltet, eine Rechtsgutsbeeinträchtigung und somit eine Strafbarkeit nach § 201 StGB im Ergebnis ausgeschlossen werden kann. Ein solches Modell kann zwar die tatsächliche Gefährdung der Rechte der Betroffenen minimieren. Dies ändert jedoch nichts am Vorliegen der tatbestandsmäßigen Voraussetzungen des § 201 Abs. 1 Nr. 1 StGB. Deshalb halten wir auch in diesem Fall eine Daueraufzeichnung von Telefonaten nicht für vertretbar.

27. Register nach § 32 BDSG und Prüftätigkeit

27.1 Register und Meldepflicht

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach § 32 BDSG der Meldepflicht. Derzeit sind zu diesem Register 199 Unternehmen gemeldet. Unterteilt nach der Art der meldepflichtigen Tätigkeit ergibt sich folgendes Bild:

Speicherung zum Zwecke der Übermittlung

Auskunfteien/Warndienste 13

Direktmarketing/Adreßhändler 23

Speicherung zum Zwecke der anonymisierten Übermittlung

Markt- und Meinungsforschung 13

Auftragsdatenverarbeitung

Servicerechenzentren 22

Akten- und Datenträgervernichter 13

Mikroverfilmer 7

Datenerfasser 24

sonst. Auftragsdatenverarbeitung 84

27.2 Prüfungen

Der folgenden Übersicht sind die Zahlen der Überprüfungen im Berichtszeitraum zu entnehmen, die gem. § 38 Abs. 2 BDSG regelmäßig vor Ort stattfinden:

Auskunfteien / Warndienste 3

Direktmarketing / Adreßhändler 5

Markt- und Meinungsforschung 1

Servicerechenzentren –

Akten- und Datenträgervernichter 2

Mikroverfilmer –

Datenerfasser 12

sonstige Auftragsdatenverarbeitung 29

gesamt 52

Anhang

Ergebnisse der Konferenzen der Datenschutzbeauftragten des Bundes und der Länder von 1996

EG-Datenschutzrichtlinie und Bundesdatenschutzgesetz (zu 1.1 und 1.4)

Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten
2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung
3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz
4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität
5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen
6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung
8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist
9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren
10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z.B.

durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen
12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung
13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing
14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau

Datenvermeidung durch Technik (zu 1.1, 1.3 und 3.1)

Datensparsamkeit durch moderne Informationstechnik (Datenvermeidung, Anonymisierung und Pseudonymisierung)

Die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von Informations- und Kommunikationstechnik bringt mit sich, daß jeder Benutzer immer mehr elektronische Spuren hinterläßt. Das wird dazu führen, daß er über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der vielen über ihn gespeicherten Daten keine Kontrolle mehr hat, so daß die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen Persönlichkeitsprofilen ständig zunimmt.

Dieser Gefahr kann dann begegnet werden, wenn in Zukunft die Frage nach der Erforderlichkeit personenbezogener Daten im Vordergrund steht, wobei Datensparsamkeit bis hin zur Datenvermeidung angestrebt werden muß. Durch die Nutzung neuer Möglichkeiten der modernen Informations- und Kommunikationstechnik (IuK-Technik) ist es in vielen Anwendungsfällen möglich, den Umgang mit personenbezogenen Daten zu reduzieren bis hin zur vollständigen Vermeidung. Auf diese Weise kann das Prinzip **„Datenschutz durch Technik“** umgesetzt werden. Datensparsamkeit und Datenvermeidung werden sich dabei auch zunehmend als Wettbewerbsvorteil erweisen.

Ausgehend von einer Untersuchung des niederländischen und der kanadischen Datenschutzbeauftragten zum sogenannten **Identity Protector** beschäftigen sich derzeit die Datenschutzbeauftragten des Bundes und der Länder intensiv mit der Formulierung von Anforderungen zur datenschutzfreundlichen Ausgestaltung von IuK-Technik. Schon die Sommerakademie in Kiel zeigte unter dem Motto „Datenschutz durch Technik - Technik im Dienste der Grundrechte“ Wege zur Wahrung der Persönlichkeitsrechte der Bürger auf. Einige datenvermeidende Technologien wie die anonyme, vorausbezahlte Telefonkarte, sind bereits seit längerer Zeit allgemein akzeptiert. Erste Ansätze der Datenvermeidung auf gesetzgeberischer Ebene sind im Entwurf zum Teledienstegesetz und zum Mediendienstestaatsvertrag enthalten.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" erarbeitet im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Bericht mit Vorschlägen und Empfehlungen, wie unter Nutzung der modernen Datenschutztechnik das Prinzip der Datenvermeidung umgesetzt werden kann. Dabei werden Begriffe wie

Anonymisierung und Pseudonymisierung eine zentrale Rolle spielen. Bei der Erarbeitung des Berichtes werden Experten aus Wissenschaft und Forschung hinzugezogen, um den aktuellen Stand der Technik berücksichtigen zu können. Auch Vertreter der Wirtschaft werden einbezogen, damit die Umsetzung der Vorschläge der Datenschutzbeauftragten als zukünftiger Wettbewerbsvorteil erkannt wird.

Während der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" ein Zwischenbericht zum Thema vorgelegt. Der umfassenden Darstellung des gesamten Problemkreises wird eine so große Bedeutung beigemessen, daß noch weitere Recherchen und die intensive Einbeziehung externer Fachleute erforderlich sind, um zukunftsweisende und realistische Empfehlungen geben zu können.

Parlamentsspezifischer Datenschutz (zu 4.)

Empfehlungen Datenschutzregelungen für Parlamente

Personenbezogene Daten werden von den Parlamenten in zunehmendem Maße auch unter Einsatz moderner Informations- und Kommunikationstechnik verarbeitet und einem breiteren Kreis von Interessenten erschlossen. Die Rahmenbedingungen hierfür sind in bereichsspezifischer Weise datenschutzrechtlich zu regeln. Die besondere Schutzwürdigkeit sensibler personenbezogener Daten (z.B. im Falle von Petitionen oder Anfragen von Abgeordneten) ist dabei zu berücksichtigen. Die Datenschutzbeauftragten vertreten hierzu - im Anschluß an die von den Konferenzen der Direktoren der Landesparlamente verabschiedeten Ergebnisse - folgende Auffassung:

1. Die Verarbeitung personenbezogener Daten zur Wahrnehmung parlamentarischer Aufgaben darf, soweit sie Außenwirkung gegenüber den Bürgerinnen und Bürgern entfaltet, nicht durch bloße Geschäftsordnungsbestimmungen geregelt werden. Eine umfassende bereichsspezifische Regelung durch formelles Gesetz trägt der informationellen Selbstbestimmung und der Parlamentsautonomie Rechnung. Eine anderweitige Regelungsform bildet die in einigen Ländern bereits verwirklichte Datenschutzordnung des Parlaments, die auf gesetzlicher Ermächtigung beruht, für die Fraktionen und Abgeordneten sowie deren Mitarbeiter verbindlich und im Gesetzblatt veröffentlicht ist.

2. Die nähere Ausgestaltung der Datenschutzkontrolle im Parlamentsbereich bestimmt sich nach den Besonderheiten des Landesrechts. Dabei muß das zuständige Kontrollorgan nach seiner Stellung, seinen Befugnissen und seinem Verfahren eine sachgerechte, substantielle datenschutzrechtliche Prüfung gewährleisten, die den besonderen verfassungsrechtlichen Status des Abgeordneten, insbesondere die Freiheit seines Mandats, zu berücksichtigen hat.

3. Bei der inhaltlichen Konkretisierung des parlamentsspezifischen Datenschutzes sind Besonderheiten zu berücksichtigen, die sich daraus ergeben, daß personenbezogene Daten dem Parlament oder einzelnen Abgeordneten ausdrücklich oder ihrer Natur nach zweckgebunden übermittelt worden sind (z.B. im Falle von Petitionen oder Anfragen). Die Transparenz personenbezogener Datenverarbeitung im Parlamentsbereich sollte gewährleistet werden. Ferner sollte im Einzelfall sorgfältig geprüft werden, ob das Informations- und Kontrollrecht der Abgeordneten auch durch anonymisierte Weitergabe von Daten innerhalb

des Parlaments gewahrt oder die personenbezogene Weitergabe nach sachgerechten Maßstäben auf einen engeren Kreis von Abgeordneten begrenzt bleiben kann.

4. Bei Übermittlung personenbezogener Daten des Abgeordneten an Stellen außerhalb des Parlaments ist der Tatsache Rechnung zu tragen, daß der Abgeordnete nach dem Grundgedanken der repräsentativen Demokratie sein Mandat öffentlichkeitsbezogen ausübt. Dem berechtigten Interesse der Öffentlichkeit, sich umfassend über parlamentarische Aktivitäten einzelner Abgeordneter zu informieren, können im Einzelfall überwiegende Gesichtspunkte des Persönlichkeitsschutzes entgegenstehen. DieÜbermittlungsregelungen sollten so flexibel gestaltet werden, daß mögliche Auswirkungen auf die Persönlichkeitssphäre des Abgeordneten in die Prüfung der datenschutzrechtlichen Zulässigkeit einer Übermittlung angemessen einbezogen werden können.

Digitales Fernsehen (zu 5.1)

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Femsehens eröffnen sich für die Anbieter - neben einem deutlich ausgeweiteten Programmvolumen - neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten - Chipkarten - nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

Anlage zur Entschließung (vorgelegt vom Arbeitskreis Medien)

Grundsätzlich werden auch Pay-per-View-Programme - wie das traditionelle Abonnenten-Fernsehen - verschlüsselt übertragen. Der Kunde braucht einen Decoder, um die Programme empfangen zu können (die sog. „Set-Top-Box“). Die Sendesignale werden von dem Decoder nur entschlüsselt, wenn er „freigeschaltet“ wurde. Die Freischaltung kann mit verschiedenen technischen Verfahren realisiert werden:

1. Zentrale Freischaltung aus dem Netz

Mit dem Sendesignal gekoppelt werden die Benutzernummern sämtlicher Kunden übertragen, die eine bestimmte Sendung sehen wollen. Der Decoder wird auf diese Weise aus dem Netz nur für die betreffende Sendung „freigeschaltet“. Dieses Verfahren setzt voraus, daß die Kunden entweder telefonisch oder über einen Rückkanal beim Sender die Freischaltung für eine Sendung verlangen. Damit wird das vom Kunden gewünschte Programmangebot grundsätzlich zunächst registriert.

Zudem werden mit dem über Kabel oder Satellit verteilten Signal für die Sendung auch die Nutzernummern der Interessenten - unverschlüsselt - übertragen, deren Decoder freigeschaltet werden soll; sie könnten im gesamten Netz mit verhältnismäßig geringem Aufwand mitgelesen und ausgewertet werden. Im Unterschied zur periodischen Freischaltung von Decodern im Abonnenten-Fernsehen ist damit eine sendungsspezifische Registrierung des Nutzungsverhaltens möglich.

Nur durch zusätzliche organisatorische Maßnahmen - etwa die Einschaltung eines neutralen Dritten, der die Freischaltung im Auftrag des Anbieters übernimmt, jedoch keinen direkten Kundenkontakt hat - läßt sich bei diesem Verfahren eine direkt personenbezogene Speicherung des Nutzungsverhaltens vermeiden.

2. Lokale Freischaltung durch den Nutzer

Jede Sendung wird mit einer elektronischen Entgeltinformation (Token) versehen. Die Kunden, die das Programmangebot sehen wollen, teilen dies per Fernbedienung dem Decoder mit. Das Guthaben auf der Chipkarte, die in den Decoder eingeführt ist, wird entsprechend verringert und der Decoder lokal freigeschaltet.

Das Token-System läßt sich mit vorhandener Technik so gestalten, daß beim Anbieter keinerlei personenbezogene Informationen über die Inanspruchnahme einzelner Sendungen entstehen. Eine vollständig anonyme Nutzung kann insbesondere durch den Einsatz von Wertkarten realisiert werden. Selbst bei Einsatz personalisierter wiederaufladbarer Wertkarten besteht die Möglichkeit, daß lediglich der Ladevorgang (z.B. durch Einzahlung eines Guthabens an einem Automaten oder bei Aufladung aus dem Netz), nicht jedoch die einzelne Programmnutzung durch den Anbieter oder einen zwischengeschalteten Dritten registriert wird.

Allerdings besteht die Gefahr, daß auch bei Token-Verfahren auf der Chipkarte Informationen über die einzelnen Programmabrufe gespeichert und - per Rückkanal - an den Anbieter für Zwecke seiner Abrechnung mit Programmlieferanten übermittelt bzw. von diesem abgerufen werden.

Dem datenschutzrechtlichen Gebot, technische Verfahren so zu gestalten, daß möglichst wenige personenbezogene Daten entstehen und auch eine anonyme Nutzung gewährleistet ist, kann durch das Token-Verfahren bei Pay-per-View besser entsprochen werden als durch

Verfahren mit individueller zentral gesteuerter Freischaltung. Eine anonyme Nutzung ist jedoch auch bei dem Token-Verfahren nur dann zu gewährleisten, wenn der Abruf der Daten über die einzelnen gesehenen Sendungen durch den Anbieter unterbleibt.

Auskünfte über den Fernmeldeverkehr (zu 16.1)

Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks geht einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das

Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z. B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Öffentliche Fahndung im Strafverfahren (zu 17.2)

Grundsätze für die öffentliche Fahndung im Strafverfahren

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15.12.1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

   Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

   Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen.

   Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahndung nach unbekannten Tatverdächtigen, Beschuldigten, Angeschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten ; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen.

Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt, bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

   Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

   - eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und

   - der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeu tung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs. 2 StrEG aufgenommen werden.

   Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

   Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über die Entschädigungspflicht öffentlich bekanntzumachen ist.

Stichwortverzeichnis