Bayerischer Landtag
11. Wahlperiode

Drucksache **11/60**
14.11.86

Achter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1985/1986

Der Landesbeauftragte für den Datenschutz
Nr. DSB/ 1 – 510 – 9

München, 14. November 1986

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Achter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident!

In der Anlage übersende ich gemäß Art. 28 Abs. 4 des Bayerischen Datenschutzgesetzes den achten Tätigkeitsbericht.

Mit vorzüglicher Hochachtung

Dr. Konrad Stollreither

Inhaltsübersicht

1. Vorbemerkung

Im Berichtszeitraum beschäftigten mich, stärker noch als in vergangenen Jahren, Fragen des Datenschutzes im Sicherheitsbereich. Dazu trug nicht zuletzt die öffentliche Diskussion über die im Bundestag eingebrachten Sicherheitsgesetze bei. Die Terroranschläge der letzten Zeit bestätigen die Aktualität dieses Themas. Bedauerlicherweise traten dadurch viele andere Fragen des Datenschutzes, die nicht weniger bedeutsam sind, in den Hintergrund.

Im Zusammenhang mit den insbesondere im Jahre 1986 erfolgten Mordanschlägen von Terroristen ist wiederholt die Behauptung erhoben worden, „überzogener Datenschutz" sei mitverantwortlich für Schwierigkeiten bei der Täterermittlung. Ich halte diese Vorwürfe für unberechtigt und betone, daß es seit Beginn meiner Tätigkeit mein Anliegen ist, gerade im Sicherheitsbereich den korrekten Staatsbürger zu schützen. Meine Auffassung in der Frage „Sicherheit und Datenschutz" ergibt sich unmißverständlich aus meinen Ausführungen im 5. Tätigkeitsbericht (1982), die ich im folgenden wiederhole:

> „Die öffentliche Diskussion des Datenschutzes im Sicherheitsbereich ist im Berichtszeitraum durch den meines Erachtens überflüssigen Streit geprägt worden, ob Sicherheit vor Datenschutz oder Datenschutz vor Sicherheit gehen müsse. Gerade aus dem Bereich der Sicherheitsbehörden ist von prominenter Stelle gefordert worden, daß Datenschutz nicht zum Tatenschutz werden dürfe und Sicherheit der Vorrang vor Datenschutzinteressen des Einzelnen zukomme. Diese Diskussion war schon deshalb unglücklich, weil letzten Endes der Anspruch des einzelnen Bürgers, sich frei entfalten zu können, sowohl voraussetzt, daß er sich vor Verbrechen weitgehend sicher fühlen kann, als auch verlangt, daß seine Privatsphäre beachtet wird. Eine generelle Abwägung zwischen Datenschutz und Sicherheit ist daher abwegig und kann zu keinen brauchbaren Ergebnissen führen. Daher kann auch ich als Datenschutzbeauftragter nicht für den Datenschutz einen absoluten Vorrang vor den Erfordernissen der öffentlichen Sicherheit verlangen. Falls die notwendige Balance zwischen den berechtigten Belangen der Bürger und der zu ihrem Schutz tätigen Sicherheitsbehörden nicht gewahrt wird, droht Gefahr sowohl für die Institution des Datenschutzes als auch für die Arbeit der Sicherheitsbehörden. An keinem von beiden kann der Bürger interessiert sein."

2. Gesundheit

2.1. Überblick

Im Gesundheitsbereich hat sich der Datenschutz ganz wesentlich fortentwickelt:

Der Bayerische Landtag beschloß detaillierte Geheimhaltungsvorschriften für den öffentlichen Gesundheitsdienst im Gesetz über die Gesundheits- und Veterinärfachverwaltung (Art. 6). Sie betreffen insbesondere die zweckgebundene Verwendung und Nutzung von personenbezogenen Daten, die den Gesundheitsbehörden im Rahmen freiwilliger Beratung offenbart werden. Besondere Bedeutung dürfte die Vorschrift für Fragen der Organisation von Gesundheitsämtern entwickeln. So wird aus meiner Sicht eine etwaige gemeinsame Führung von Aktenunterlagen aus freiwilligem Beratungsbereich und hoheitlicher Tätigkeit des Gesundheitsamtes sowie eine Einbeziehung personenbezogener Informationen aus diesen Arbeitsbereichen in Zentralkarteien von Gesundheitsämtern zu überprüfen sein.

Der Bayerische Landtag novellierte außerdem die Datenschutzvorschrift des Bayerischen Krankenhausgesetzes. Der bisherige Artikel 13 wird ab 1. Januar 1987 durch einen neuen Artikel 26 ersetzt. Dabei ist nicht nur die Terminologie an die allgemeinen datenschutzrechtlichen Begriffe angepaßt, sondern auch eine Reihe bisher offener Fragen geklärt worden. Genannt seien die Nutzung von Patientendaten des Krankenhauses für Ausbildung und Forschung im Rahmen der Aufgaben des Krankenhauses, Befugnisse zur Auftragsdatenverarbeitung – einschließlich der Mikroverfilmung – und die Offenbarung personenbezogener Daten gegenüber mit- und nachbehandelnden Ärzten. Die Regelung des bisherigen Artikel 13 des Krankenhausgesetzes hatte sich in der Praxis als hilfreich erwiesen. Dies habe ich bei meinen Prüfungen wiederholt festgestellt. Es ist zu hoffen, daß dies in verstärktem Maße auch für die verbesserte Fassung in Artikel 26 BayKrG gilt.

Von besonderer Bedeutung ist schließlich die Entwicklung auf dem Gebiet der Krankheitsregister, insbesondere dem Krebsregister. Erörtert wurde in letzter Zeit ein Projekt der Bayerischen Landesärztekammer und der Bayerischen Kassenärztlichen Vereinigung, die eine zentrale onkologische Dokumentation einrichten wollen. Inhalt der Datensammlung sollen lediglich solche Daten sein, die ohne Zutun des Patienten weder von der Kassenärztlichen Vereinigung, noch von der Ärztekammer auf eine bestimmte Person bezogen werden können. Sie soll primär der Nachsorge dienen. Abzuwarten bleibt, wie die Datenverarbeitungs-Konzeption für den Ausbau der klinischen Krebsregister der bayerischen Hochschulen ausgestaltet werden und wie sie gegebenenfalls mit dem vorgenannten faktisch anonymen onkologischen Nachsorgeregister in Verbindung treten soll.

2.2. Gesetz über den öffentlichen Gesundheitsdienst

Der Bayerische Landtag hat am 12. Juli 1986 das Gesetz über die Gesundheits- und Veterinärfachverwaltung in Bayern beschlossen (Gesetz über den öffentlichen Gesundheitsdienst – GDG, GVBl. S. 120 ff.). Dem Bayerischen Staatsministerium des Innern bin ich für die vorangegangene laufende Unterrichtung über den Gesetzentwurf, sowie für die geduldige Bereitschaft zur Auseinandersetzung mit meinen gewiß nicht immer bequemen Vorstellungen und Argumenten dankbar. Die Erörterungen bezogen sich stets auf die Fragen der Geheimhaltung personenbezogener Daten, die in dem Gesetz zu regeln waren.

Das GDG enthält nunmehr in Art. 6 Vorschriften über die Geheimhaltungspflichten und in Art. 7 über das Zusammenwirken von Dienststellen, die sich ebenfalls auf den Umgang mit personenbezogenen Daten beziehen. Um die zu regelnde Problematik deutlich zu machen, seien die folgenden Ausführungen aus der amtlichen Gesetzesbegründung zitiert (Landtagsdrucksache 10/8972 zu Art. 6):

> „Typischerweise sind die vom öffentlichen Gesundheitsdienst wahrzunehmenden Aufgaben hoheitlicher Natur. Das ärztliche und nichtärztliche Fachpersonal des öffentlichen Gesundheitsdien-

stes wird bei Wahrnehmung der gesundheitspolizeilichen Fachaufgaben (vgl. die Überwachungs- und Aufsichtsaufgaben nach den Artikeln 8, 10 und 14) in der Eigenschaft als Amtsträger (§ 11 Abs. 1 Nr. 2 StGB) tätig und unterliegt somit der Pflicht zur Amtsverschwiegenheit (Art. 30 BayVwVfG, § 203 Abs. 2 StGB, Art. 69 BayBG, § 9 BAT).

Daneben werden die Behörden des öffentlichen Gesundheitsdienstes, insbesondere die Gesundheitsämter und Veterinärämter, im Rahmen ihrer Dienstaufgaben vielfach auch beratend und aufklärend tätig (vgl. Art. 11: Familienberatung, Schwangerenberatung, gesundheitliche Beratung bei Suchtkrankheiten, sowie Art. 13 Abs. 1 Nr. 3). Der Bürger kann diese Beratungs-, Aufklärungs- und Dienstleistungsangebote des öffentlichen Gesundheitsdienstes annehmen, er kann zur Annahme dieser Angebote aber nicht verpflichtet werden. In diesem Bereich der Dienstleistungs-, Aufklärungs- und Beratungsangebote wird das ärztliche und nichtärztliche Fachpersonal der Behörden des öffentlichen Gesundheitsdienstes nicht ausschließlich in der Eigenschaft als Amtsträger tätig, sondern primär in der Rolle als „Arzt", als „Tierarzt" oder als andere gemäß § 203 Abs. 1 oder Abs. 3 StGB zur Wahrung des Berufsgeheimnisses verpflichtete Person. Es entstehen bei Inanspruchnahme der Angebote durch den Bürger die von § 203 Abs. 1 und Abs. 3 StGB geschützten berufsspezifischen Vertrauensverhältnisse. Eben dieses vertrauensvolle Verhältnis (vornehmlich zwischen Arzt und Patient) wird allgemein als das primäre Schutzgut des § 203 StGB angesehen (Lenckner in Schönke/Schröder, Kommentar zum Strafgesetzbuch, RN 1 zu § 203).

Angesichts der vielschichtigen Aufgabenstellung des öffentlichen Gesundheitsdienstes und – dementsprechend – der unterschiedlichen Rolle, in der sich die Bediensteten bei Wahrnehmung von Dienstaufgaben befinden können, angesichts ferner des legitimen Vertrauensanspruchs des Bürgers, dem Berufsgeheimnis unterfallende Tatsachen nicht für anderweitige Verwaltungszwecke zu berücksichtigen (dies ist auch Voraussetzung für die Annahme der einschlägigen Beratungsangebote; vgl. hierzu auch BVerfGE 44, 353, 374 ff.), muß sichergestelltwerden, daß persönliche Geheimnisse, in die der Bürger „aus freien Stücken" Bediensteten einer Behörde des öffentlichen Gesundheitsdienstes Einsicht gewährt hat, nicht in anderem Zusammenhang personenbezogen verwertet werden."

Art. 6 Abs. 1 GDG legt daher fest, daß die Gesundheitsbehörden personenbezogene Daten, die sie aufgrund freiwilliger Mitwirkung des Betroffenen erfahren, nicht für materiell andersartige Aufgaben verwerten dürfen.

Abs. 2 des Art. 6 enthält demgegenüber Ausnahmen von der vorgenannten Grund-Regel. Neben den Fällen der Einwilligung (Abs. 2 Satz 1) läßt Abs. 2 Satz 2 die Mitteilung personenbezogener Daten an die zuständige Behörde in Abweichung von dem oben geschilderten Grundsatz zu, wenn dies „zur Abwehr von Gefahren für Leben oder Gesundheit Dritter erforderlich ist; der Betroffene soll hierauf hingewiesen werden". Nach der amtlichen Begründung zum Gesetzentwurf handelt es sich hier um „anerkannte Melderechte", die dann bestehen, „wenn es um den Schutz höherrangiger Rechtsgüter, also um Leben oder Gesundheit Dritter geht. So ist etwa die Meldung krankheitsbedingter fahruntauglicher Personen an die Verkehrsbehörde auch ohne Einwilligung des Betroffenen zulässig (vgl.BGH, NJW 1968, Seite 2288). Dies entspricht auch § 2 Abs. 4 der Berufsordnung für die Ärzte Bayerns vom 1. Januar 1978 (Bayerisches Ärzteblatt, Sondernummer Dezember 1980). Um hier aber das Vertrauensverhältnis in größtmöglicher Weise zu schonen, soll der Betroffene auf die Möglichkeit der Mitteilung hingewiesen werden, um ihn gegebenenfalls zu bewegen, selbst zur erforderlichen Einsicht zu kommen und vom fraglichen Tun abzusehen."

Auch in Art. 7 sind Durchbrechungen des oben geschilderten Grundsatzes vorgesehen: Danach unterrichten die Gesundheitsbehörden die zuständigen Verwaltungsbehörden, wenn ihnen bei Wahrnehmung ihrer Aufgaben Verstöße gegen Vorschriften des öffentlichen Gesundheitsrechts bekannt werden. Nach der amtlichen Begründung schließt dies die Befugnis zur Weitergabe personenbezogener Daten ein. Im übrigen ist nach Art. 7 Abs. 1 Satz 3 die Weitergabe personenbezogener Daten an die zuständigen Behörden an die Voraussetzung gebunden, daß der Zweck, zu dessen rechtmäßiger Erfüllung die Daten erhoben wurden, sich dadurch nicht ändert, oder die Weitergabe durch Rechtsvorschrift ausdrücklich zugelassen ist.

Die gesetzlich zugelassenen Durchbrechungen des Geheimhaltungsgebots und der Verwendungsbeschränkung von Daten, die Gesundheitsbehörden freiwillig anvertraut wurden, beruhen auf der (politischen) Entscheidung, das Angebot freiwilliger Beratungstätigkeiten der Gesundheitsbehörden gegenüber der Bevölkerung mit der Möglichkeit der genannten – u.U. belastenden – Maßnahmen zu verbinden. Bei einer Beratung durch die Träger der freien Wohlfahrtspflege dürften solche möglichen Beeinträchtigungen für Ratsuchende dagegen ausscheiden. Ich habe deshalb darauf hingewiesen, daß nur ein maßvoller Vollzug dieser Regelungen, der die Mitteilungen personenbezogener Daten aus diesem Bereich auf den im konkreten Einzelfall erforderlichen Inhalt beschränkt, und die strikte Beachtung des Verhältnismäßigkeitsgrundsatzes, vor Schwierigkeiten beim Vollzug dieser Bestimmungen über die Durchbrechung der Geheimhaltung bewahren kann. Ich halte eine stichprobenweise Überprüfung der sich aus dem Gesetz ergebenden Datenübermittlungspraxis für geboten.

2.3. Datenschutz und Schweigepflicht im Krankenhaus

Die Beratung eines zweiten Gesetzes zur Änderung des Bayer. Krankenhausgesetzes eröffnete die Möglichkeit, auch die Schweigepflicht bzw. Datenschutzvorschrift des Art. 13 zu novellieren. Dabei sollten nach Möglichkeit Fragen, die sich in den letzten Jahren bei der Anwendung der geltenden Fassung des Art. 13 ergaben, geklärt und die Terminologie möglichst weitgehend dem allgemeinen Datenschutzrecht angepaßt werden. Den Staatsministerien für Arbeit und Sozialordnung und des Innern bin ich für die frühzeitige Unterrichtung über die Entwürfe und die weitere Beteiligung bei den Ausarbeitungen dankbar. So konnte ich eine Reihe von Anregungen zum neuen Art. 26 Bayer.

Krankenhausgesetz vorbringen. Die nachfolgenden Punkte erscheinen mir in diesem Zusammenhang besonders berichtenswert:

Die Regelungen des neuen Art. 26 des Bayerischen Krankenhausgesetzes, der zum 1.1.1987 in Kraft tritt, betreffen Patientendaten ohne Rücksicht darauf, ob diese in Dateien oder in anderer Form gespeichert oder verarbeitet werden. Der Auslegung des Begriffs „Patientendaten" wurde die Rechtsprechung zur ärztlichen Schweigepflicht zugrunde gelegt, wonach sich die Geheimhaltungspflicht auch auf Angaben über andere Personen als Patienten, die dem Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden, erstrecken kann.

Wie bisher sind Erhebung und Aufbewahrung von Patientendaten im Rahmen der Aufgabenstellung des Krankenhauses zulässig. Diese umfaßt insbesondere die in § 2 Nr. 1 des Bundes-Krankenhaus-Finanzierungsgesetzes näher beschriebenen Aufgaben zur Heilung und Linderung, den Forschungsauftrag bei Hochschulkliniken, sowie sonstige Aufträge aufgrund gesetzlicher Zuweisung. Einen weiteren Erlaubnistatbestand für die Erhebung und Aufbewahrung von Patientendaten stellt im übrigen die Einwilligung des Patienten dar.

Die Regelung zum Anspruch des Patienten auf Auskunft über Daten ist sehr differenziert: Danach hat der Patient Anspruch auf Auskunft

- über die zu seiner Person aufbewahrten Daten,
- über die Personen und Stellen außerhalb des Krankenhauses, an die seine Daten übermittelt wurden, sowie
- darüber, welche Daten zu anderen Zwecken als zur Behandlung und deren verwaltungsmäßiger Abwicklung übermittelt wurden.

Die Auskunft über die Patientendaten, die zur Behandlung oder zu deren verwaltungsmäßiger Abwicklung übermittelt wurden, ist zu erteilen, soweit die Unterlagen des Krankenhauses hierzu Angaben enthalten. Dies soll bewirken, daß in Krankenhäusern für Zwecke der Behandlung und ihrer verwaltungsmäßigen Abwicklung keine zusätzlichen Aufzeichnungspflichten entstehen. Soweit entsprechende Aufzeichnungen jedoch vorhanden sind, ist dem Patienten Auskunft zu gewähren. Zu Datenübermittlungen zu anderen Zwecken als Behandlung und deren verwaltungsmäßige Abwicklung werden jedoch Aufzeichnungen erforderlich um der Auskunftspflicht genügen zu können.

Soweit es mit Rücksicht auf den Gesundheitszustand des Patienten dringend geboten erscheint, soll die Auskunft durch einen Arzt vermittelt werden. Besteht ein Patient auf der vollen Auskunft, kann sie ihm auch der vermittelnde Arzt nicht verweigern. Eine Beschränkung der Auskunft ist lediglich hinsichtlich ärztlicher Beurteilungen oder Wertungen zulässig.

Die neue Regelung ermöglicht beispielsweise also künftig auch Auskünfte zu Datenübermittlungen an Kostenträger. Dies kann für den Betroffenen durchaus von Interesse sein, da gelegentlich fraglich sein kann, ob das Krankenhaus mehr als die zur verwaltungsmäßigen Abwicklung bzw. Kostenerstattung notwendigen Daten übermittelt hat bzw. diese vom Kostenträger angefordert wurden. Erfahrungsgemäß ist es auch nicht selten ein dringendes und wohl auch berechtigtes Anliegen von Patienten, eine, ggf. unzulässige, Weitergabe von Diagnosedaten aufzuklären, weil als deren Folge nachteilige Wirkungen zu befürchten oder schon eingetreten sind.

In Erweiterung der Regelung des bisherigen Art. 13 des Bayerischen Krankenhausgesetzes wird in Art. 26 Abs. 4 Satz 2 nunmehr ausdrücklich festgestellt, daß der Krankenhausarzt Patientendaten nicht nur selbst nutzen darf, sondern damit auch andere Personen im Krankenhaus beauftragen kann, soweit dies zur Erfüllung näher genannter Aufgaben erforderlich ist. Damit soll klargestellt werden, daß der Krankenhausarzt die Patientendaten anderen Personen im Krankenhaus nicht zu deren freien Verfügung überlassen kann, sondern aufgrund einer „Beauftragung" immer noch eine Leitungsfunktion beibehält. Personen im Krankenhaus, die auf diese Weise Patientendaten erfahren, können wohl von den Gerichten eher als „ärztliche Gehilfen" anerkannt werden, so daß durch die Datenweitergabe der Schutzbereich der ärztlichen Schweigepflicht wohl nicht verlassen wird.

Der neue Art. 26 Abs. 4 enthält in Satz 4 und 5 aber auch noch wichtige Bestimmungen über die Verarbeitung von Patientendaten „im Auftrag". Die Zulässigkeit der Offenbarung von Patientendaten gegenüber den Auftragnehmern einer Datenverarbeitung oder zur Mikroverfilmung hatte in der Vergangenheit immer wieder Fragen aufgeworfen. Die neue Regelung enthält eine Erlaubnis zur Verarbeitung von Patientendaten im Auftrag einschließlich der Mikroverfilmung durch andere Personen oder Stellen unter der Voraussetzung,

- daß das Krankenhaus sicherstellt, daß beim Auftragnehmer die besonderen Schutzmaßnahmen technischer und organisatorischer Art gegen unberechtigte Verwendung oder Übermittlung von Patientendaten getroffen werden und
- daß keine Anhaltspunkte dafür bestehen, daß durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden.

Hierzu ist anzumerken, daß Patienten-Datenverarbeitung „außer Haus" mit der Zweifelsfrage belastet ist, ob Stellen, die solche Arbeiten für Krankenhäuser verrichten, von den Gerichten als „ärztliche Gehilfen" anerkannt werden. Die Vorschriften des Strafgesetzbuches über die ärztliche Schweigepflicht und die Schweigepflicht der ärztlichen Gehilfen (§ 203 Abs. 1 Nr. 1 und Abs. 3, sowie § 204 StGB, sowie §§ 53 Abs. 1 Nr. 3, 53 a, 97 Abs. 1, 2 und 4 der Strafprozeßordnung (Zeugnisverweigerungsrecht, Beschlagnahmeverbot)) machen deutlich, daß ärztliche Aufzeichnungen vor jeglicher Zweckentfremdung geschützt werden müssen – auch vor der Inanspruchnahme der Daten für die Strafverfolgung. Die Erlaubnis zur Auftragsdatenverarbeitung darf deshalb rechtlich nicht dazu führen, daß die durch Strafgesetzbuch und Strafprozeßordnung geschützten Daten dieses Schutzes beraubt werden. Solange also keine Anhaltspunkte dafür bestehen, daß durch Auftragsdatenverarbeitung der durch die vorgenannten gesetzlichen Vorschriften vorgesehene Geheimnisschutz gefährdet wird, ist die Auftragsdatenverarbeitung durch andere Personen oder Stellen nach Art. 26 Abs. 4 Satz 4 zulässig. Ergeben sich jedoch Anhaltspunkte dafür, daß dies nicht (mehr) zutrifft, wenn zum Beispiel Gerichte den vorgenannten Schutz bei Auftragnehmern verneinen würden, ist die Auftragsdatenverarbeitung nach der neuen Regelung nicht mehr erlaubt.

Die Regelung des Art. 26 Abs. 4 Satz 4 ist schließlich noch im Zusammenhang mit der Regelung in folgendem Satz 5

zu sehen. Hieraus ergibt sich, daß Art. 26 Abs. 4 Satz 4 und 5 die Verarbeitung einschließlich der Mikroverfilmung von Patientendaten, die nicht ausschließlich der verwaltungsmäßigen Abwicklung der Behandlung der Patienten dienen (also medizinische Daten), nur in anderen Krankenhäusern erlaubt.

Im Interesse der Sicherung des ärztlichen Geheimnisbereiches ist einer Datenverarbeitung im Krankenhaus selbst stets der Vorzug zu geben. Die Praxis ist jedoch für die verwaltungsgemäße Abwicklung der Behandlung von Patienten darüber bereits weit hinausgegangen. Hierfür wird in erheblichem Umfang Datenverarbeitung im Auftrag in Anspruch genommen.

Anders ist die Lage bei rein medizinischer Auftragsdatenverarbeitung wie z.B. bei medizinischer Dokumentation. Diese findet nach hiesiger Erkenntnis im wesentlichen jeweils in (anderen) Kliniken statt. Im Hinblick auf § 97 Abs. 1 und 2 der Strafprozeßordnung, wonach ärztliche Unterlagen einer Beschlagnahme auch dann nicht unterliegen, „wenn sie im Gewahrsam einer Krankenanstalt sind", erschien die Schaffung einer gesetzlichen Erlaubnis zur Datenverarbeitung im Auftrag für rein medizinische Daten bei anderen Krankenhäusern noch vertretbar. Außerdem haben Krankenhäuser ganz allgemein eine lange Tradition in der Wahrung der ärztlichen Schweigepflicht, jedenfalls nach außen hin. Schließlich könnte bei Auftragnehmern, die nicht als Krankenhäuser im wesentlichen nur Patientendaten verarbeiten, auch die Gefahr bestehen, daß aus Rationalisierungsgründen Verknüpfungen von Patientendaten mit anderen Daten derselben Personen aus anderen Arbeitsbereichen vorgenommen würden, was zur (physischen) Herstellung problematischer „Profile" führen könnte.

Da eine Umstellung bereits bestehender „Datenverarbeitung außer Haus" für medizinische Daten nicht kurzfristig möglich ist, räumt Art. 27 Abs. 3 des Gesetzes hierfür eine Übergangsfrist von 5 Jahren ein.

Abs. 5 des Art. 26 regelt die Übermittlung von Patientendaten an Dritte (Behandlungsvertrag, Rechtsvorschrift oder Einwilligung des Patienten). Eine Offenbarung von Patientendaten an Vor-, Mit- oder Nachbehandelnde ist nach der Vorschrift zulässig, soweit das Einverständnis des Patienten anzunehmen ist. Diese Regelung stimmt mit derjenigen in der Berufsordnung für die Ärzte Bayerns in der Fassung vom 1.10.1983 überein.

2.4. Krebsregistrierung

Wie bereits im letzten Tätigkeitsbericht dargestellt, hat der Bayerische Landtag durch Beschluß vom 23.10.1985 die Bayerische Staatsregierung um einen Bericht über den weiteren Ausbau der bestehenden universitären Klinik-Tumor-Register (München, Erlangen-Nürnberg, Würzburg) sowie gegebenenfalls um die Vorlage eines Gesetzentwurfs gebeten, falls sich dies im Zuge des Aufbaues der Klinikregister mit Rücksicht auf die ärztliche Schweigepflicht oder aus anderen Gründen als notwendig erweisen sollte. Da dieser Bericht wegen umfangreicher Erhebungen bei den genannten Universitäten bis zum Abschluß des vorliegenden Tätigkeitsberichts noch nicht erstellt war, kann zu der Problematik vorerst aus der Sicht des Datenschutzes nichts Neues mitgeteilt werden. An dieser Stelle sei lediglich meine Auffassung wiederholt, daß

- die betroffenen Patienten möglichst nicht durch Grundrechtseingriffe, die in der Erhebung von Krankheitsdaten liegen könnten, belastet werden sollten und
- etwaige gesammelte personenbezogene Krankheitsdaten mit allen zur Verfügung stehenden rechtlichen und technisch-organisatorischen Mitteln gegen Änderungen ihres Verwendungszwecks zu sichern sind.

Die Formulierung von Einverständniserklärungen der betroffenen Patienten zur Weiterleitung von Daten zu ihrer Person und über Krankheits- bzw. Heilungsverlauf an erfassende Einrichtungen sowie zur Speicherung und Nutzung dort entstehender Datensammlungen, war Gegenstand wiederholter Besprechungen. Zu berücksichtigen ist dabei, daß die an der Sammlung onkologischer Patientendaten interessierten Stellen aufgrund ärztlicher Erfahrung bei der Aufklärung der Patienten über die Art der Datensammlung (Tumorregister) Zurückhaltung üben wollen. Als Vorbild dient hierfür das „therapeutische Privileg", nach dem unter Umständen die Aufklärung eines Patienten vor seiner Einwilligung in einen körperlichen Eingriff zu Heilungszwecken von schonender Zurückhaltung geprägt sein darf, wenn dadurch beispielsweise die Heilungsaussichten erhöht werden. Demgegenüber werden im Normalfall bei der datenschutzrechtlichen Prüfung von Einwilligungserklärungen nicht unerhebliche Anforderungen an die Klarheit der Information über die Datenverarbeitungsmaßnahme, in die eingewilligt werden soll, gefordert. Es bedarf hier wohl noch erheblicher Bemühungen, um einen tragfähigen Kompromiß zu erreichen. Aus der Sicht des Datenschutzes sei jedoch jetzt schon darauf hingewiesen, daß ein solcher Kompromiß, wie er möglicherweise bei einer Sammlung von Daten über Tumorpatienten hingenommen werden könnte, keinesfalls zum Bezugsfall für die Gestaltung anderer Krankheitsregister werden darf. Dem steht nämlich entgegen, daß eine deutliche Aufklärung über den Charakter eines Krankheitsregisters in anderen Fällen wohl schwerlich mit Hinweis auf das therapeutische Privileg abgelehnt werden könnte.

2.5. Diagnosestatistik der Krankenhäuser – Erstellung außer Haus?

Nach der Bundespflegesatzverordnung sind durch die Krankenhäuser neuerdings Diagnosestatistiken zu erstellen. Hierzu müssen zunächst personenbezogene Patientendaten in den Krankenhäusern ausgewertet werden. Zu klären war, ob solche personenbezogenen Diagnosedaten an eine Stelle außerhalb des Krankenhauses zur Erstellung der Statistik im Wege der „Datenverarbeitung im Auftrag" übermittelt und dort gespeichert werden können.

Aus der Sicht des Datenschutzes habe ich Bedenken gegen eine Auslagerung personenbezogener Diagnosedaten erhoben. Für eine Offenbarung gegenüber dem Auftragnehmer liegt eine gesetzliche Befugnis nicht vor. Die Einholung von Einwilligungen ist mit den bekannten Problemen der Aufklärung der Patienten verbunden. Auch bestehen die in anderem Zusammenhang bereits geschilderten Probleme, daß personenbezogene Daten beim Auftragnehmer möglicherweise nicht der ärztlichen Schweigepflicht unterliegen und auch das ansonsten für Patientendaten im Krankenhaus geltende Beschlagnahmeverbot außerhalb der Krankenhäuser wohl nicht greift.

Ich habe mich deshalb dagegen gewandt, personenbezogene medizinische Einzeldaten für die Statistik vom Krankenhaus auf Vorrat an einen Auftraggeber außer Haus über-

senden zu lassen, um erst später, nach Abschluß der Behandlung, dort die notwendigen Rechenschritte für die Statistik vornehmen zu lassen. Ich habe statt dessen ein Verfahren befürwortet, nach dem die erforderlichen Statistikdaten vom Krankenhaus erst zum Zeitpunkt der „Schlußrechnung" an den Auftragnehmer übersandt werden und die Übernahme der Daten in die anonymisierte Diagnosestatistikdatei in kürzester Zeit erfolgt. Soweit Krankenhäuser unabhängig von den Anforderungen der Bundespflegesatzverordnung darauf Wert legen, Einzeldaten aus mehreren Abteilungen des Krankenhauses (z. B. bei Verlegung des Patienten innerhalb des Krankenhauses) in die Statistik einzubeziehen, müßte jeweils ein Weg gefunden werden, die Diagnosestatistikdaten im Krankenhaus selbst zu sammeln und gesammelt mit den Daten für die Schlußrechnung zum Auftragnehmer weiterzugeben. Meine Gespräche mit dem Bayerischen Staatsministerium für Arbeit und Sozialordnung haben auch keinen Hinweis darauf ergeben, daß zur Erstellung des in § 16 Abs. 4 Nr. 1 Bundespflegesatzverordnung genannten Leistungsnachweises eine andere Lösung erforderlich wäre.

Generell sei darauf hingewiesen, daß eine personenbezogene Speicherung von Diagnosedaten bei Auftragnehmern außerhalb des Krankenhauses über einen längeren Zeitraum auf datenschutzrechtliche Bedenken stoßen würde. Der Datenerhebung zunächst innerhalb des Krankenhauses mit anschließend anonymisierter Weitergabe der Daten an den Auftragnehmer wäre daher stets der Vorzug zu geben.

2.6. Behandlung in psychiatrischen Krankenhäusern – Führerscheinfrage

Von verschiedenen Seiten wird der Landesbeauftragte für den Datenschutz immer wieder auf ein Problem aufmerksam gemacht, das Patienten psychiatrischer Krankenhäuser erheblich belasten kann: Werden Fahrerlaubnisinhaber in psychiatrischen Krankenhäusern nach dem Unterbringungsgesetz untergebracht oder befinden sie sich freiwillig in psychiatrischer Behandlung, machen die zuständigen Verwaltungsbehörden offenbar in vielen Fällen Zweifel an der Eignung zum Führen eines Kraftfahrzeuges geltend. Die Behörden haben nach dem Straßenverkehrsgesetz und der Straßenverkehrs-Zulassungs-Ordnung eine Fahrerlaubnis zu entziehen, wenn sich der Inhaber der Fahrerlaubnis zum Führen von Kraftfahrzeugen als ungeeignet erweist. Sie können die Beibringung eines Gutachtens anordnen, wenn sie Anlaß zu der Annahme haben, daß ein Fahrerlaubnisinhaber ungeeignet oder nur noch bedingt geeignet ist. Möglicherweise wird von machen Behörden auch „routinemäßig" bei solchen Personen eine Überprüfung der Fahrtauglichkeit eingeleitet. Die Betroffenen reagieren darauf überrascht und verärgert. Ärzte und Bezirkskrankenhäuser empfinden diese Maßnahme häufig als unverhältnismäßig, da ein erheblicher Anteil der Patienten bei Entlassung aus dem psychiatrischen Krankenhaus zur Teilnahme am Straßenverkehr geeignet sei. Dies insbesondere im Vergleich zu Patienten nicht-psychiatrischer Krankenhäuser, die beispielsweise nach Behandlung einer Herz-Kreislauferkrankung entlassen werden.

Die Führerscheinstellen bei den Kreisverwaltungsbehörden erfahren von der Behandlung eines Betroffenen in einer psychiatrischen Klinik auf verschiedene Weise:

- Durch das Gericht, das nach dem Unterbringungsgesetz die Unterbringung angeordnet hat, da nach Art. 13 Abs. 1 Nr. 3 des Bayerischen Unterbringungsgesetzes die Unterrichtung der Kreisverwaltungsbehörde über die Anordnung der Unterbringung vorgeschrieben ist. Innerhalb der Kreisverwaltungsbehörde wird diese Mitteilung an die Führerscheinstelle weitergeleitet.
- Vom Vormundschaftsgericht, das eine Pflegschaft einrichtet, aufgrund deren Betroffene in psychiatrische Kliniken aufgenommen werden: Die Mitteilung über die Einrichtung einer Pflegschaft wird aufgrund der Anordnung über Mitteilungen in Zivilsachen (MiZi) an die Gemeinden gerichtet, damit die Wahlämter von entsprechenden gesetzlichen Einschränkungen des Wahlrechts benachrichtigt werden. Jedenfalls in den kreisfreien Gemeinden mit eigenen Führerscheinstellen erreicht die Mitteilung offenbar auch diese Stellen.
- Im Einzelfall können Führerscheinstellen mehr oder weniger zufällig auch auf anderen Wegen von der Aufnahme eines Betroffenen in ein psychiatrisches Krankenhaus erfahren.

Inwieweit nun die Führerscheinbehörden von der Tatsache einer Unterbringung in einem psychiatrischen Krankenhaus oder von der Tatsache einer freiwilligen psychiatrischen Behandlung unterrichtet werden dürfen oder gar müssen, wird seit Jahren diskutiert. Eine solche Datenübermittlung durch die behandelnden Ärzte oder durch die von der Unterbringung unterrichteten Behörden an die Führerscheinstelle bedarf aber jedenfalls als Eingriff in das Recht auf informationelle Selbstbestimmung einer gesetzlichen Ermächtigung. Eine solche gesetzliche Ermächtigung besteht derzeit immer noch nicht. Zwar habe ich Verständnis, daß im Interesse der Verkehrssicherheit bei begründeten Zweifeln auf entsprechende Mitteilungen nicht völlig verzichtet werden kann. Ich bin aber der Auffassung, daß für derartige Datenübermittlungen dringend eine ausreichende Rechtsgrundlage geschaffen werden muß.

Aus der Sicht des Datenschutzes ist aber auch fraglich, ob es überhaupt als verhältnismäßig betrachtet werden kann, ohne Vorprüfung der eingangs zitierten ärztlichen Argumente, also ohne Ansehung des Einzelfalls, Angaben über Behandlungen in psychiatrischen Kliniken an Führerscheinstellen zu übermitteln, weil dies zu einer zu pauschalen Einleitung eines Verfahrens zur Überprüfung der Fahrtauglichkeit führen kann. Dabei darf nicht vergessen werden, daß die oft nicht unerheblichen Kosten der Überprüfung dem Betroffenen angelastet werden können.

Der Verband der Bayerischen Bezirke hat sich deshalb schon vor einiger Zeit an das Bayerische Staatsministerium des Innern mit der Bitte um Abhilfe gewandt. Auch seitens des Landesbeauftragten für den Datenschutz fand im Berichtszeitraum hierzu eine Erörterung mit dem zuständigen Referenten des Bayerischen Staatsministeriums des Innern statt. Soweit bekannt, wurde eine Lösung des Problems noch nicht gefunden.

2.7. Offenbarung von Krankheitsdaten gegenüber Rettungsleitstellen

Die Bekanntgabe von Namen und Anschrift der Wochenenddienst- und Notfall-Ärzte in der Presse – wie früher allgemein üblich – wurde vor einiger Zeit weitgehend eingestellt. Wer im Notfall oder am Wochenende einen Arzt

konsultieren möchte, muß sich daher – wenn er seinen Hausarzt nicht erreichen kann – an die Rettungsleitstellen wenden. Bei entsprechenden Anrufen erheben die Rettungsleitstellen neben Namen und Anschrift des Anrufers auch Krankheitsdaten, um die Dringlichkeit des Anliegens beurteilen zu können.Das Telefongespräch wird zudem auf Tonband aufgezeichnet.

Aus der Sicht des Datenschutzes scheint die Zentralisierung der Notfalldienste über die Rettungsleitstellen auf den ersten Blick keine Probleme aufzuwerfen. Solche ergeben sich allerdings durch die Tatsache, daß Patienten, die sich unter keinen Umständen einer anderen Person als einem Arzt anvertrauen wollen, durch das neue Verfahren gezwungen werden, Angaben über ihre Krankheit gegenüber Mitarbeitern der Rettungsleitstelle zu machen, um überhaupt (im Notfall oder am Wochenende) in Kontakt zu einem Arzt zu kommen. Hinzu kommt, daß personenbezogene Angaben über Krankheiten, Unfälle u. ä. bei den Rettungsleitstellen registriert und für eine gewisse Zeit vorgehalten werden müssen.

Gegen die der geltenden Praxis entsprechenden Richtlinien zur Einsatzvermittlung des kassenärztlichen Notfalldienstes habe ich Bedenken erhoben, die auch durch eine Eingabe erhärtet wurden. Nach diesen Richtlinien hatte der Mitarbeiter in der Rettungsleitstelle anhand eines Formulars vom Anrufer die erforderlichen Angaben für den Einsatz des diensthabenden Notfallarztes zu erfragen. Dem Anrufer mußte dabei klargemacht werden, daß bei unvollständigen Angaben die Versorgung des Patienten nicht vermittelt werden könne. Im Hinblick auf das Verbot der Veröffentlichung der diensthabenden Notfallärzte in der örtlichen Presse sollte entsprechend den Richtlinien zur Einsatzvermittlung der Namen der diensthabenden Notfallärzte von der Rettungsleitstelle nur mitgeteilt werden, wenn der Hilfesuchende

- eine Arztpraxis zu Behandlungszwecken aufsuchen kann, oder
- eine dringende telefonische Beratung durch den Arzt wünscht.

In diesen beiden Fällen wurden dem Betroffenen der notfalldiensthabende Arzt von der Rettungsleitstelle genannt, ohne daß er höchstpersönliche Daten der Rettungsleitstelle offenbaren mußte. Der Anrufer brauchte in diesem Falle also nur dem Arzt Angaben über seine Krankheit zu machen.

Wünschte der Betroffene dagegen einen Hausbesuch, müßte er nach den Richtlinien zunächst gegenüber der Rettungsleitstelle Krankheitsdaten offenbaren. Nach meinem Eindruck wird dies von manchen Betroffenen als peinlich empfunden. Außerdem ist mir bekannt, daß in den letzten Jahren in einer nicht unerheblichen Zahl von Fällen Aufzeichnungen von Rettungsleitstellen zu Beweiszwecken beschlagnahmt wurden, was bei Aufzeichnungen von Ärzten über ihre Patienten nicht zulässig wäre. Das Bayer. Staatsministerium des Innern hat zudem noch mitgeteilt, daß es derzeit kein technisches Verfahren gibt, das das unzulässige Abhören des Funkverkehrs der Rettungsleitstelle mit dem Arzt unter Einsatz vertretbarer wirtschaftlicher Mittel verhindert oder zumindest wesentlich erschwert.

Auf meine deswegen vorgetragenen Bedenken hin änderte die Kassenärztliche Vereinigung Bayerns mit Wirkung vom 1.7.1985 die Richtlinien, die jetzt lauten:

„Macht der Anrufer einen dringenden Fall ärztlicher Behandlung geltend, will aber über Namen und gegebenenfalls Anschrift hinaus keine oder nur unvollständige Angaben machen, ist er zu befragen, ob er einen Hausbesuch, die Behandlung in der Arztpraxis oder eine dringende telefonische Beratung wünscht. Die gewünschte Hilfeleistung ist ihm zu vermitteln.

Wünscht der Anrufer einen Hausbesuch und kann aufgrund fehlender bzw. unvollständiger Angaben nicht ermittelt werden, ob der Hausbesuch vorrangig vor anderen bereits vorliegenden Besuchsanforderungen durchgeführt werden muß, obliegt dem diensthabenden Arzt die Abwicklung der ihm übermittelten Fälle. Dieser entscheidet auch über die Priorität der Abwicklung."

Nach Ansicht der Kassenärztlichen Vereinigung Bayerns soll damit einem Wunsch des Notfallpatienten, sich auch bei Einschaltung der Rettungsleitstelle nur einem Arzt anzuvertrauen, Rechnung getragen werden, wobei auch ein etwaiges Abhör-Risiko des Funkverkehrs mit dem Notfallarzt oder ein Beschlagnahme-Risiko vermieden werde. Mit Ausnahme der vorgenannten beiden Fälle (Behandlung in der Arztpraxis und dringende telefonischer Beratung) sei im übrigen eine Namensnennung des Arztes nicht erforderlich, um dem vorbezeichneten Anliegen des Patienten entsprechen zu können.

Diese neue Regelung räumt, wie ich meine, die datenschutzrechtlichen Bedenken bezüglich der Abwicklung des kassenärztlichen Notfalldienstes weitgehend aus. Mit meiner Bitte an die Kassenärztliche Vereinigung Bayerns, die Mitarbeiter der Rettungsleitstellen entsprechend zu unterrichten, habe ich angeregt zu prüfen, in welcher Weise die Bevölkerung über die möglichen Formen der Hilfeleistung einschließlich der Möglichkeit zum Verzicht auf Krankheitsangaben gegenüber der Rettungsleitstelle in Kenntnis gesetzt werden könnte. Die Kassenärztliche Vereinigung Bayerns beabsichtigt allerdings keine entsprechende Veröffentlichung, da dem Anrufer von der Rettungsleitstelle die in einem Notfall häufig schwer zu treffende Entscheidung, welche Form der ärztlichen Hilfe notwendig und ausreichend sei, abgenommen werden solle. Im Hinblick auf die geschilderte datenschutzrechtliche Problematik vermag dies nicht vollständig zu befriedigen. Die Bewährung der Neuregelung in der Praxis wird daher abzuwarten sein.

2.8. Korrespondenz Krankenhäuser – Betriebskrankenkassen

Eine Betriebskrankenkasse in Bayern hat mich darauf aufmerksam gemacht, daß immer wieder Rechnungen oder anderer Schriftverkehr von Krankenhäusern nicht an die Betriebskrankenkasse, sondern an die Adresse des Arbeitgebers gerichtet werden. Auch bei einem größeren Klinikum in Bayern habe in dieser Hinsicht erschreckende Unkenntnis geherrscht. Die Arbeitgeber als privatrechtliche Einrichtung und die Betriebskrankenkasse als Körperschaft des öffentlichen Rechts wurden von Krankenhäusern anschriften- und organisationsmäßig gleichbehandelt. Die strenge Trennung, auf die die Betriebskrankenkassen besonderen Wert legen müssen, um den Schutz der ihnen anvertrauten Patienten- und Sozialdaten sicherstellen zu können, war nicht einmal bekannt.

Ich habe die Bayerische Krankenhausgesellschaft von dieser Problematik unterrichtet und gebeten, bei der Beseitigung hier offenbar bestehender Unklarheiten mitzuwirken.

2.9. Ärztlicher Fragebogen einer Krankenpflegeschule

Eine Eingabe führte zu Zweifeln an der Zulässigkeit einzelner Fragen eines in einer öffentlichen Krankenpflegeschule benutzten ärztlichen Fragebogens. Der Fragebogen dient der Feststellung der körperlichen und geistigen Eignung von Bewerberinnen für den Krankenpflegeberuf nach dem Krankenpflegegesetz.

Das Bayerische Staatsministerium des Innern hat in einer Stellungnahme hierzu folgendes ausgeführt:

> „Das Krankenpflegegesetz regelt nicht, auf welche Weise die gesundheitliche Eignung für den Krankenpflegeberuf festzustellen ist. Es ist davon auszugehen, daß jeder begutachtende Arzt auch ohne nähere Angaben weiß, welche gesundheitlichen Anforderungen an eine Krankenpflegekraft zu stellen sind. Nach unseren Informationen beschränken sich deshalb die entsprechenden ärztlichen Zeugnisse regelmäßig auf die Feststellung, ob die untersuchte Person für den Beruf gesundheitlich geeignet ist; damit ist den Erfordernissen des Datenschutzes voll Rechnung getragen. Dies gilt auch für den Fall, daß die gesundheitliche Eignung im Rahmen der Ausbildungszulassung durch eine ärztliche Bescheinigung nach den § 32, 39 des Jugendarbeitsschutzgesetzes nachgewiesen wird (vgl. hierzu die Verordnung über die ärztlichen Untersuchungen nach dem Jugendarbeitsschutzgesetz mit Anlagen i. d. F. der ÄndVvom 5.9.1986, BGBl. I, S. 1013). Wir haben das Bezugsschreiben zum Anlaß genommen, die für den Vollzug des Krankenpflegegesetzes zuständigen Regierungen in vorstehendem Sinn zu unterrichten, mit der Bitte, erforderlichenfalls dafür zu sorgen, daß die Schulen entsprechend verfahren."

Der Ansicht des Bayerischen Staatsministeriums des Innern schließe ich mich an. Insbesondere halte ich eine Beschränkung des ärztlichen Zeugnisses auf die Feststellung, ob die untersuchte Person für den Krankenpflegeberuf gesundheitlich geeignet ist, für ausreichend. Darüber hinausgehende Datenerhebungen über den Gesundheitszustand durch die Krankenpflegeschule sind demzufolge nicht erforderlich. Im Hinblick auf die bisher bestehende Rechtsunsicherheit im genannten Bereich erschien es jedoch nicht angebracht, die Krankenpflegeschule formell zu beanstanden. Ich gehe davon aus, daß in Zukunft entsprechend der Weisung des Bayerischen Staatsministeriums des Innern verfahren wird.

2.10. Namensschilder von Patienten oder Heimbewohnern an Zimmertüren

Ein Krankenhausträger hatte bei mir angefragt, ob an Zimmertüren in den Krankenhäusern die Namen von Patienten angebracht werden dürfen. Hierzu habe ich die Ansicht vertreten, daß eine Offenbarung von Patientendaten gegenüber Dritten – die auch durch Namensschilder an Krankenzimmertüren erfolgen kann, beispielsweise gegenüber den Besuchern – nur mit Einwilligung des Patienten erfolgen darf. Ich halte jedoch auch eine Auffassung für vertretbar, wonach regelmäßig davon ausgegangen werden kann, daß der Patient den Besuch am Krankenbett wünscht und damit konkludent in die Auskunft beim Pförtner und die Namensangabe auf den Zimmerschildern einwilligt. Dies gilt nicht, wenn der Patient seinen gegenteiligen Willen kundtut oder Anhaltspunkte dafür bestehen, daß eine Bekanntgabe des Krankenhausaufenthalts untunlich ist. Dies dürfte insbesondere bei einer Unterbringung in psychiatrischen Abteilungen zutreffen oder in anderen Behandlungsbereichen, die auf eine Erkrankung schließen lassen, die Patienten Außenstehenden üblicherweise nicht ohne weiteres bekanntgeben. Der Einholung eines (mündlichen) Einverständnisses des Patienten ist daher der Vorzug zu geben.

2.11. Krankenhauspatienten dem Sozialamt gemeldet

Ein Sachverhalt, über den bereits früher berichtet wurde (4. TB, Nr. 3.4.5, S. 31) ist gleichwohl wiederum aufgetreten: Eine Stadt hat als Krankenhausträger Patienten des Krankenhauses dem Sozialamt gemeldet, obwohl in diesen Fällen Sozialhilfe nicht gewährt wurde und die Patienten die Rechnungen selbst – wenn auch teilweise mit mehr oder minder kurzer Überziehung der Zahlungsfristen – beglichen. Zur Erforderlichkeit dieser Datenweitergabe trug die Krankenhausverwaltung mir gegenüber vor, es gebe Fälle, in denen unklar sei, wer für die Krankenhausbehandlungskosten aufkäme. Bei Kassenpatienten sei dies der Fall, wenn keine Kostenübernahmeerklärung der Krankenkasse vorliege, bei Privatpatienten, wenn ein angeforderter Kostenvorschuß nicht bezahlt oder eine Rechnung nicht in angemessener Frist nach Rechnungsstellung beglichen werde. In diesen Fällen bestehe häufig die Möglichkeit, daß die Krankenkassenbehandlungskosten vom zuständigen Sozialhilfeträger getragen werden (§ 121 BSHG). Zur Ermittlung der Kostenträgerschaft innerhalb des unten dargestellten Zeitraumes würden die Patientendaten vorsorglich an die Sozialämter weitergegeben.

Vorliegend war durch verwaltungsinterne Vorschriften die Erstattung von Aufwendungen beim Krankenhausaufenthalt daran geknüpft, daß der Krankenhausträger seine Ansprüche innerhalb einer Frist von 4 Monaten ab dem Tag der Aufnahme in das Krankenhaus gegenüber dem Sozialamt geltend macht. Das Datum der Rechnungsstellung wurde dabei nicht berücksichtigt. Bei längerem Krankenhausaufenthalt und verzögerter Rechnungsstellung konnte diese Regelung dazu führen, daß dem Betroffenen wenig oder gar keine Zeit verblieb, den Rechnungsbetrag auszugleichen, ohne daß gleichzeitig die Erstattung beim Sozialamt geltend gemacht wurde.

Aufgrund bei mir eingegangener Beschwerden habe ich die Stadt auf die Problematik aufmerksam gemacht. Meines Erachtens gilt es zu verhindern, daß durch verwaltungsinterne Richtlinien und verzögerte Rechnungsstellung das Krankenhaus personenbezogene Daten dem Sozialamt melden muß, bevor der Betroffene überhaupt in üblicher Weise ausreichend Gelegenheit hat, seine Rechnung zu begleichen.

Das oben dargestellte Verfahren wird derzeit geändert. Angestrebt wird dabei, daß zum einen die Frist auf 6 Monate verlängert wird und zum andern, daß als maßgeblicher Zeitpunkt für den Fristbeginn nicht mehr der Tag der Aufnahme, sondern der Tag der Entlassung maßgeblich ist.

Ich werde diese Angelegenheit weiterverfolgen.

2.12. Auskunftsersuchen einer Klinik

Eine Universitätsklinik bat eine Meldebehörde um eine Adreßauskunft. Durch entsprechende Gestaltung des Anfrageformulars offenbarte die Universität gegenüber der Meldebehörde gleichzeitig, daß die Bezugsperson als Patientin im Jahre 1980 bestrahlt worden war.

Die Übermittlung der Meldedaten war nach Art. 31 Abs. 1 Satz 1 des Bayerischen Meldegesetzes zulässig. Als unzulässig erachte ich jedoch die Offenbarung der Krankheits- bzw. Behandlungsdaten, die in dem Anfrageformular enthalten waren. Diese Angaben fallen gemäß Art. 13 des Bayerischen Krankenhausgesetzes (bisherige Fassung) bzw. Art. 26 des Bayerischen Krankenhausgesetzes (neue Fassung) sowie § 203 des Strafgesetzbuches unter die ärztliche Schweigepflicht. Sie sind für die erbetene Auskunft in keiner Weise erforderlich. Ich habe vorgeschlagen, das Auskunftsersuchen künftig in einer neutralen Form zu stellen, die nicht erkennen läßt, in welcher Abteilung der Universitätsklinik die Bezugsperson Patientin war.

Von der Klinik liegt inzwischen ein Vorschlag für ein geändertes Anfragemuster vor.

3. Sozialbehörden

3.1. Überblick

Der Bekanntheitsgrad der immerhin seit 1. Januar 1981 geltenden Bestimmungen zum Schutz der Sozialdaten im 2. Kapitel des 10. Buches zum Sozialgesetzbuch läßt immer noch Wünsche offen. In Gesprächen wird von Mitarbeitern der Sozialleistungsträger immer wieder geltend gemacht, daß eine sehr große Zahl von gesetzlichen Bestimmungen, Verordnungen und Verwaltungsvorschriften, die fortdauernd Änderungen in den Anspruchsvoraussetzungen für Sozialleistungen enthalten, beachtet werden müssen, neben denen die Umsetzung anderer Rechtsvorschriften – und dazu zählt nach Meinung der Beteiligten auch das Datenschutzrecht – nicht zuletzt wegen fehlender unmittelbarer Auswirkungen beim Empfänger von Sozialleistungen zurücktreten müsse. Diese Argumentation gibt zu denken. Im Ergebnis stelle ich bei Mitarbeitern einzelner Behörden vielfach Unkenntnis, häufig aber auch Unsicherheit bei der Anwendung bestehender Vorschriften über den Sozialdatenschutz in der Praxis fest. Dies kann zu durchaus unterschiedlichen Ergebnissen führen.

So habe ich anläßlich einer datenschutzrechtlichen Prüfung bei einem Versorgungsamt (fast mit Bewunderung) festgestellt, daß verwaltungsinterne Weisungen der vorgesetzten Dienstbehörde aus dem Jahre 1955 (im Einzelfall sogar aus dem Jahre 1938) die eine Weitergabe medizinischer Daten an andere Stellen der öffentlichen (Gesundheits-)Verwaltung vorsehen, präzise befolgt werden, obwohl sie nach Erlaß der Bestimmungen zum Schutz der Sozialdaten im X. Buch des Sozialgesetzbuches nicht mehr der Rechtslage entsprechen. So sehr diese Handlungsweise aus der Sicht des einzelnen Sachbearbeiters wegen dessen Weisungsgebundenheit gerechtfertigt erscheinen mag, so sehr muß es jedoch nachdenklich stimmen, wenn die Rechtsentwicklung der vergangenen Jahre nur wenig Spuren in bestehenden Informationsflüssen hinterläßt.

Es gibt aber auch völlig anders geartete Reaktionen auf die Rechtsvorschriften zum Schutz der Sozialdaten. Insbesondere von Mitarbeitern von Sozialleistungsträgern selbst wird gelegentlich beklagt, daß Auskunftsersuchen durch andere Sozialleistungsträger nur sehr schleppend beantwortet werden. Dies gelte auch dann, wenn die Gewährung von Sozialleistungen von anderen Sozialleistungen abhinge, die Entscheidung eilbedürftig sei und rechtliche Hindernisse für den Informationsfluß im Hinblick auf § 69 SGB X nicht erkennbar seien. Wenn eine solche Zurückhaltung im Einzelfall dann noch zu einem längerem Schriftwechsel zwischen den beteiligten Stellen führt und dadurch die Gewährung von Sozialleistungen verzögert wird, verkehren sich die für den Schutz des Betroffenen gedachten Rechtsvorschriften in ihr Gegenteil. Demgegenüber bleibt festzuhalten, daß die Bestimmungen zum Schutz der Sozialdaten bei rechtmäßigen Auskunftsersuchen zwischen Sozialleistungsträgern nicht zu einer Verzögerung bei der Leistungsgewährung führen müssen. Hier ist in eiligen Fällen durchaus auch eine telefonische Auskunft zulässig, wenn der Datengeber sich in geeigneter Weise über die Identität des Fragestellers und die Erforderlichkeit der Anfrage in Kenntnis setzt. Freilich setzt dies voraus, daß die vorhandenen datenschutzrechtlichen Bestimmungen auch auf der Sachbearbeiterebene im Sozialleistungsbereich hinlänglich bekannt sind.

Erfreulicherweise kann ich davon berichten, daß gerade in letzter Zeit bei Fortbildungsveranstaltungen der Sozialleistungsträger den Problemen des Datenschutzes ausreichend Zeit eingeräumt wird.

Im folgenden werden einige Einzelprobleme aus meiner Tätigkeit näher dargestellt.

3.2. Meldung aller Neugeborenen an die Datenstelle der Rentenversicherungsträger

Nach dem Hinterbliebenenrenten- und Erziehungszeiten-Gesetz vom 11.7.1985 (BGBl I S. 1450) müssen die zuständigen Meldebehörden der Datenstelle der Rentenversicherungsträger den Monat und das Jahr der Entbindung, den Familiennamen (jetzigen und früheren Namen mit Namensbestandteilen), den Vornamen, den Tag der Geburt, den Geburtsort und die letzte Anschrift der Mutter mitteilen. Die Änderungsverordnung zur Zweiten Meldedaten-Übermittlungsverordnung des Bundes (2. BMeldDÜV) hat noch festgelegt, daß auch die Anzahl der Kinder bei Mehrlingsgeburten mitzuteilen ist und die Geburtsmitteilung unverzüglich nach Speicherung einer Geburt im Melderegister zu erfolgen hat. Einschränkungen bezüglich des Personenkreises der Mütter sind in dieser Verordnung nicht vorgesehen, obwohl dadurch in Einzelfällen auch Übermittlungen vorgeschrieben werden, die aus Datenschutzsicht problematisch erscheinen. Es müssen nämlich auch Daten übermittelt werden, in Fällen in den ein Leistungsanspruch nicht entstehen wird, etwa bei Erziehung durch Dritte oder wenn die Eltern von der Versicherungspflicht befreit sind (z. B. bei Beamten). Außerdem wird keine Rücksicht auf Fälle genommen, in denen die betroffene Mutter die Datenübermittlung möglicherweise gar nicht wünscht, beispielsweise wenn das Kind unmittelbar nach der Geburt zur Adoption freigegeben wird. Die Übermittlung wird der betroffenen Mutter im Regelfall auch nicht bekanntgemacht. Es ist unverständlich, daß in der Verordnung nicht wenigstens ein Widerspruchsrecht der Betroffenen gegen die Speicherung vorgesehen wurde.

Die „Mitteilung" über die Geburt des Kindes erfolgt an die Datenstelle der Rentenversicherungsträger (§ 1401 c RVO, § 123 c AVG). Für die 2. BMeldDÜV ist demgegenüber der Begriff „Übermittlung" (in § 4 Abs. 2) gewählt worden. Wegen der Begriffsbestimmung in den Datenschutzgesetzen könnte daraus der Schluß gezogen werden, daß die Datenstelle der Rentenversicherungsträger als speichernde Stelle für die übersandten Daten anzusehen wäre. Demgegenüber verarbeitet jedoch die Datenstelle Versichertendaten ausschließlich im Auftrag der Rentenversicherungsträger. Ich habe daher in Schreiben an das Bayerische Staatsministerium des Innern und das Bayerische Staatsministerium für Arbeit und Sozialordnung eine Klarstellung für erforderlich bezeichnet. Gleichzeitig habe ich darauf hingewiesen, daß Daten, die nicht mehr erforderlich sind, bei der Datenstelle und bei den Rentenversicherungsträgern unverzüglich gelöscht werden sollten. § 84 SGB X findet meines Erachtens hier unmittelbar Anwendung.

3.3. Wird die Rentenversicherungsnummer zum allgemeinen Personenkennzeichen?

Der Bund hat einen Gesetzentwurf vorgelegt, der sicherstellen soll, daß die allgemeine Rentenversicherungsnummer nicht aufgrund immer weiterer Verbreitung die Funktion eines allgemeinen Personenkennzeichens übernimmt. Diese Absicht ist sehr zu begrüßen, da die allgemeine Rentenversicherungsnummer zunehmend in weiteren Verwaltungsbereichen Eingang findet und damit eines Tages in der Lage wäre, ein allgemeines Verknüpfungskennzeichen für einen großen Teil der Bevölkerung darzustellen. In meiner Stellungnahme habe ich die Notwendigkeit, die Entstehung eines allgemeinen Personenkennzeichens zu verhindern, betont. Das Recht auf informationelle Selbstbestimmung würde in dem Maße, in dem sich die Rentenversicherungsnummer als allgemeines Verknüpfungskennzeichen durchsetzt, immer stärker berührt, da über Verknüpfungen die Herstellung von problematischen Persönlichkeitsprofilen zunehmend erleichtert würde.

Aus der Sicht des Datenschutzes muß deshalb die Verwendung der Rentenversicherungsnummer auf die Aufgaben der Rentenversicherung, einschließlich der dafür notwendigen Datenflüsse beschränkt bleiben. Der vorliegende Entwurf geht darüber jedoch weit hinaus. Er erweitert die Verwendbarkeit der Rentenversicherungsnummer als Hauptordnungsmerkmal für den gesamten Bereich der gesetzlichen Krankenversicherung, Unfallversicherung und für sämtliche Aufgaben der Bundesanstalt für Arbeit einschließlich der Kindergeldzahlung. Damit wird die überwiegende Mehrheit der Bürger mit Hilfe eines eindeutigen Ordnungsmerkmals erfaßt und gespeichert. Die Versicherungsnummer könnte aufgrund des Gesetzes bedenklich in die Nähe eines allgemeinen Personenkennzeichens rücken, zumal die Speicherung und Verwendung der Nummer kaum auf Sozialversicherungsträger zu beschränken wäre. So ist denkbar, daß z. B. auch Arbeitgeber,Krankenhäuser, Sozialämter und andere beteiligte Stellen die Versicherungsnummer mitverwenden.

Gegen den Entwurf habe ich deshalb grundsätzlich Bedenken erhoben. Seine sorgfältige Überprüfung auch anhand der Ausführungen des Bundesverfassungsgerichts zur Einführung eines allgemeinen Verknüpfungsmerkmals habe ich für geboten erachtet. Ich habe Sorge, daß die vorgeschlagene Regelung die Entwicklung der Versicherungsnummer zum Personenkennzeichen nicht verhindert, sondern eher sanktioniert.

Auf folgende Einzelpunkte des Entwurfs bin ich noch näher eingegangen:

Der Entwurf läßt einen Datenaustausch der in § 35 SGB I genannten Sozialbehörden untereinander mit Hilfe der Versicherungsnummer zu. Diese Verwendung der Nummer zwischen den Behörden hätte zur Folge, daß die Versorgungsämter, Jugendämter, Sozialämter, Wohngeldstellen, Ausgleichsämter und andere die Versicherungsnummer erheben, speichern oder für den Datenaustausch verwenden dürfen, auch wenn ein unmittelbarer oder mittelbarer Bezug zu den Aufgaben der gesetzlichen Rentenversicherung nicht besteht. Zwar wurde in der Gesetzesbegründung dazu ausgeführt, daß der Datenaustausch der genannten Stellen untereinander mit Hilfe der Versicherungsnummer im Hinblick auf das Gebot, die Erforderlichkeit der Verwendung der Versicherungsnummer zu beachten, eine Ausnahme sein würde. Dies vermag jedoch nicht zu überzeugen. Es sollte deshalb konsequenterweise eine Regelung aufgenommen werden, die die Nutzung der Nummer zwischen den genannten Behörden begrenzt.

Die vorgesehene Regelung erlaubt eine Verwendung der Versicherungsnummer für das gesamte Aufgabenspektrum der Bundesanstalt für Arbeit, d. h. auch für den Vollzug des Bundeskindergeldgesetzes. Eine unmittelbare Beziehung zwischen der Kindergeldleistung und den Aufgaben der Sozialversicherung ist meines Erachtens nicht erkennbar. Die Zuweisung der Aufgabe „Kindergeld" zur Bundesanstalt für Arbeit erfolgte aus rein organisatorischen Gründen. Im Hinblick auf das Ziel des Gesetzentwurfs, nämlich die Einschränkung der Verwendung der Rentenversicherungsnummer außerhalb der Rentenversicherung sollte unbedingt davon abgesehen werden,die Verwendung der Nummer im Bereich der Kindergeldkasse zuzulassen.

Es besteht außerdem die Sorge, daß beim praktischen Vollzug der Bestimmungen des Gesetzes der Aufbau eines von der Rentenversicherungsnummer verschiedenen Ordnungsmerkmals regelmäßig als (erheblicher) organisatorischer Aufwand angesehen würde, auf den zugunsten der Nutzung der Rentenversicherungsnummer verzichtet wird. Überdies ist bekannt, daß beim arbeitsmedizinischen Dienst der Berufsgenossenschaften unter Hinweis auf die hohe Fluktuation der Arbeitnehmer Wünsche bezüglich der einheitlichen Verwendung der Versicherungsnummer bestehen. Die arbeitsmedizinischen Dienste vollziehen jedoch Aufgaben nach dem Arbeitssicherheitsgesetz. Ansprechpartner der Betriebsärzte sind die Arbeitgeber, nicht die Berufsgenossenschaften. Das Arbeitssicherheitsgesetz zählt auch nicht zu den besonderen Teilen des Sozialgesetzbuches. Die Einführung der Rentenversicherungsnummer in diesen Bereich würde daher ein Überschreiten des Aufgabenbereichs des Sozialgesetzbuches bedeuten.

Schließlich fehlen dem Entwurf Vorschriften über die Vergabe der Versicherungsnummer. Er beläßt es bei dem geltenden Recht, wonach nur die Träger der Rentenversicherung die Nummer vergeben dürfen. Dabei wird offenbar davon ausgegangen, daß jeweils der Grund für die Vergabe einer Nummer beim Rentenversicherungsträger selbst vorliegt. Die nunmehr in dem Gesetzentwurf enthaltene Befugnis der Nicht-Rentenversicherungsträger zur Erhebung und

Speicherung der Versicherungsnummer läßt befürchten, daß diese Stellen die Vergabe einer Versicherungsnummer auch dann beantragen werden, wenn diese Nummer für andere Aufgaben als für Zwecke der Rentenversicherung benötigt wird. Zu denken wäre etwa an eine Nummernvergabe für freiwillige Mitglieder einer gesetzlichen Krankenversicherung, die nicht gleichzeitig rentenversichert und/oder arbeitslosenversichert sind, an entsprechende Bezieher von Kindergeld o. ä. Eine solche Entwicklung wäre als weiterer Schritt anzusehen, eine Art Ersatz-Personenkennzeichen zu schaffen Ich halte es für geboten, daß Sozialleistungsträger – soweit sie nicht Rentenversicherungsträger sind – verpflichtet sind bzw. werden, zumindestens in den beschriebenen Fällen eigene Ordnungsbegriffe zu vergeben und zu verwenden. Dieses muß jedoch gesetzlich hinreichend klargestellt werden.

Das Bayerischen Staatsministerium für Arbeit und Sozialordnung teilt meine Auffassung nicht inallen Punkten. Der Meinungsaustausch hierüber ist noch nicht abgeschlossen.

3.4. Abgrenzung von Behandlungs- und Pflegefall nach § 184 RVO aufgrund personenbezogener Daten

Die gesetzlichen Krankenkassen sind bei einer Krankenhausbehandlung eines Versicherten nur dann leistungspflichtig, wenn eine Krankenhausaufnahme erforderlich ist, um die Krankheit zu erkennen oder zu behandelnoder Krankheitsbeschwerden zu lindern. In anderen Fällen (Pflegefällen) sind andere Sozialleistungsträger leistungspflichtig. Die gesetzlichen Krankenkassen haben daher grundsätzlich das Recht, sich durch Anforderung ärztlicher Stellungnahmen von ihrer eigenen Leistungspflicht zu überzeugen (§ 184 RVO und Rechtsprechung des Bundessozialgerichts). Mit Wirkung vom 1.1.1985 wurde § 372 Abs. 2 Nr. 1 RVO ergänzt: Danach haben die Landesverbände der Krankenkassen für ihre Mitgliedskassen Verträge mit den Krankenhäusern (oder deren Vereinigungen) zu schließen, um sicherzustellen, daß Art und Umfang der Krankenhauspflege den Anforderungen des § 184 RVO entspricht. Die Verträge haben u. a. Regelungen zu enthalten, die eine Überprüfung der Notwendigkeit und Dauer der Krankenhauspflege in geeigneten Fällen durch den Vertrauensarzt oder andere beauftragte Ärzte ermöglichen.

Es gilt daher ein Verfahren zu finden, in dem die „geeigneten Fälle" festgestellt werden können, Hierzu müssen in der Regel personenbezogene Daten erhoben und verarbeitet werden. Bisher haben einzelne Krankenkassen Fragebögen zur Prüfung der medizinischen Notwendigkeit von Krankenhausbehandlungen verwendet. Hierbei mußte jeweils die Erforderlichkeit der Datenerhebung im Einzelfall überprüft werden. Als Lösungsmöglichkeit wurde aber auch vorgeschlagen, ab einer bestimmten Zeitdauer des Krankenhausaufenthalts die Voraussetzung für eine Überprüfung als gegeben zu betrachten und nur über die Patienten, die dann noch im Krankenhaus behandelt werden, bestimmte Angaben zur Überprüfung der Leistungspflicht von Krankenkassen zu erheben.

Auf meine Bitte hat die Bayerische Krankenhausgesellschaft für den somatischen Bereich und der Verband der Bezirke für den psychiatrischen Bereich Erhebungen über die Verweildauer der Patienten in Krankenhäusern durchgeführt. Es ergab sich, daß bei somatischen Erkrankungen 99,5 % aller Patienten das Krankenhaus nach spätestens 90 Tagen wieder verlassen hatten. Bei einer Aufenthaltsdauer von maximal 60 Tagen hatten etwa 98 % der Patienten das Krankenhaus verlassen. Ich habe daher zunächst vorgeschlagen, eine Krankenhausaufenthaltsdauer von 90 Tagen im somatischen Bereich als Kennwert für den „geeigneten Fall" anzusetzen. Nach den Erhebungen im Bereich der Neurologie in den Nervenkrankenhäusern wird eine vergleichbare Situation bei einer Krankenhausverweildauer von etwa 6 Monaten erreicht. Im Fachbereich Psychiatrie können zwischen 85 % und 95 % der Patienten nach Ablauf eines Jahres aus dem Krankenhaus entlassen werden. Nach Ablauf von 2 Jahren haben zwischen 90 % und 98 % der Patienten das Krankenhaus verlassen. Hier sind auch deutliche Unterschiede entsprechend der Aufgabe und Struktur der einzelnen Nervenkrankenhäuser festzustellen.

Diese Ergebnisse habe ich mit dem Bayerischen Staatsministerium für Arbeit und Sozialordnung, dem Verband Bayerischer Bezirke, der Bayerischen Krankenhausgesellschaft und der Arbeitsgemeinschaft der Bayerischen Krankenkassenverbände erörtert. Übereinstimmung wurde darüber erzielt, daß eine Prüfung der medizinischen Notwendigkeit von Krankenhauspflege bei psychischen Krankheiten im Regelfall nicht vor Ablauf eines Jahres für erforderlich gehalten wird. Dabei kann auch eine Unterschreitung der Einjahresfrist bei Vorliegen konkreter Anhaltspunkte im Einzelfall zulässig sein. Im Beschwerdefall wäre die anfragende Krankenkasse jedoch darlegungspflichtig.

Die Krankenhauspflegebedürftigkeit im Bereich der Psychiatrie wird nach dem bisher in Bayern vereinbarten Prüfverfahren nicht durch den vertrauensärztlichen Dienst überprüft, sondern erfolgt durch paritätisch besetzte Ausschüsse. Diese Ausschüsse tagen in den jeweiligen Bezirkskrankenhäusern und erhalten vor Ort Einblick in die vorhandenen Krankenakten. Eigene Unterlagen entstehen bei den Ausschüssen nicht. Das Verfahren hat sich nach Aussage der Vertragsparteien bewährt. Die Neufassung des § 372 Abs. 2 Nr. 1 RVO läßt nun bei der Überprüfung der Notwendigkeit der Dauer der Krankenhauspflege in geeigneten Fällen neben dem Vertrauensarzt auch die Einschaltung anderer beauftragter Ärzte zu. Zu prüfen ist daher, ob die Mitglieder bestehender Prüfungsausschüsse als „andere beauftragte Ärzte" anzusehen sind. Gegebenenfalls wären Vereinbarungen denkbar, die die Einsichtnahme in Krankenakten durch Nicht-Ärzte ausschließen würden.

Zur Vereinheitlichung der Fragebogen, die nach Ablauf der erörterten Fristen in den hier in Frage stehenden Fällen zu verwenden wären, unterbreitete der Landesbeauftragte für den Datenschutz Vorschläge, über die die Beteiligten noch entscheiden müssen. Für den Bereich der somatischen Krankenhäuser war eine Übereinstimmung über eine Frist im Berichtszeitraum noch nicht zustandegekommen; es fehlen auch die in § 372 Abs. 2 RVO vorgesehenen Verträge.

3.5. Nutzung personenbezogener Daten von Nichtmitgliedern durch Ortskrankenkassen für Werbemaßnahmen

Personen, die nicht Mitglieder von Ortskrankenkassen sind, haben sich bei mir darüber beschwert, daß ihre Daten, die den Ortskrankenkassen für bestimmte eng begrenzte Zwecke anvertraut sind, für Werbemaßnahmen verwendet wurden.

Die Allgemeinen Ortskrankenkassen erhalten vom Arbeitgeber als Einzugsstellen Adreß- und Einkommensdaten auch von solchen Arbeitnehmern, die nicht krankenversicherungspflichtig, wohl aber renten- bzw. arbeitslosenversicherungspflichtig, sind (§ 1399 Abs. 2 Satz 2 RVO, § 121 AVG, § 2 Abs. 3 Satz 2 der 2. DEVO). Die Beitragsdaten von Mitgliedern der Ortskrankenkassen wie von Nichtmitgliedern werden gemeinsam im „Versichertendatenbestand" der AOK für Zwecke der Beitragsüberwachung gespeichert. Möglich wäre daher, daß Bedienstete der Ortskrankenkassen, die berechtigten Zugang zum Versichertendatenbestand haben, Adressen, Einkommensdaten und Daten über den Arbeitgeber von Nichtmitgliedern für Werbemaßnahmen der eigenen AOK nutzen. Dies war insbesondere zu besorgen, wenn „zur Aufrechterhaltung der Wettbewerbsfähigkeit der AOK" die Mitarbeiter verpflichtet werden, neue, insbesondere junge Mitglieder (Risikostruktur) zu gewinnen, wie sich aus dem Schreiben einer Ortskrankenkasse ergibt.

Die fraglichen Daten sind „zwangsweise erhobene Daten" im Sinne der Ausführungen des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983. Solche Daten dürfen nur entsprechend dem gesetzlichen Zweck verwendet werden. Eine Zweckentfremdung müßte gesetzlich zugelassen sein. Die Daten dürfen daher meines Erachtens von der AOK nur zweckgebunden im Rahmen der 2. DEVO genutzt werden.

Macht eine Ortskrankenkasse geltend, daß die Erhebung von Adreßdaten nur im Privatbereich der Mitarbeiter erfolgt, so ist meines Erachtens eine wirkungsvolle Kontrolle nur dann möglich, wenn die Herkunft dieser Daten im Einzelfall nachvollziehbar aufgezeichnet wird.

In einer vorläufigen Stellungnahme hat das Bayerische Staatsministerium für Arbeit und Sozialordnung als Rechtsaufsichtsbehörde der Ortskrankenkassen meine vorgetragenen Bedenken unterstützt.

3.6. Offenbarung von Sozialdaten an eine Vergabestelle für Bauleistungen

Nach einem Beschluß des Bayerischen Landtags sollen öffentliche Aufträge an Unternehmen nur dann vergeben werden, wenn der Bewerber u. a. seiner Pflicht zur Abführung von Sozialversicherungsbeiträgen vollständig nachgekommen ist.

Aufgrund einer Eingabe war die Frage zu klären, ob die zuständige Ortskrankenkasse Auskunft über gezahlte Sozialversicherungsbeiträge und andere Angaben über einen Unternehmer ohne Einwilligung des Betroffenen gegenüber einer Vergabestelle für Bauleistungen geben durfte. Ich habe mich auf den Standpunkt gestellt, daß nach §§ 68 bis 75 SGB X eine solche Offenbarung nicht vorgesehen ist. Da es sich hier um eine abschließende Aufzählung gesetzlicher Offenbarungsbefugnisse und damit -möglichkeiten handelt und auch das BillBG eine derartige Offenbarung an Vergabestellen für Bauleistungen nicht vorsieht, sehe ich keine Möglichkeit, ohne Einwilligung des Betroffenen eine solche Auskunft zu erteilen.

Als datenschutzrechtlich zulässige Möglichkeit kommt jedoch die Ausstellung einer Bescheinigungdurch die gesetzliche Krankenkasse in Frage, die vom Bewerber für den Bauauftrag selbst eingeholt wird. Inhaltlich darüber hinausgehende Rückfragen der Vergabestelle bei der zuständigen Ortskrankenkasse wären nur mit Einwilligung des betroffenen Bewerbers zulässig. Da es sich um die Offenbarung von Betriebs- oder Geschäftsgeheimnissen handelt, gilt für die gesetzlichen Krankenkassen wegen der Gleichstellung solcher Geheimnisse mit personenbezogenen Daten in § 35 Abs. 4 SGB I das Sozialgeheimnis. Dabei wird davon ausgegangen, daß die Auskunft der gesetzlichen Krankenkasse keine personenbezogenen Daten über die versicherungspflichtigen Beschäftigten des Bewerbers enthält.

Dieser Rechtsauffassung hat sich die Oberste Baubehörde im Bayerischen Staatsministerium des Innern angeschlossen und in einem Rundschreiben an die nachgeordneten Behörden festgestellt:

> „Es ist daher von der datenschutzrechtlich zulässigen Möglichkeit Gebrauch zu machen, bei der Anforderung zur Angebotsabgabe zu erklären, daß die Auftragserteilung u. a. von der Vorlage einer gültigen Bescheinigung der allgemeinen Ortskrankenkasse (Beitragsnachweis) abhängig gemacht werden kann."

Nach Mitteilung der Obersten Baubehörde werden weitergehende Auskünfte über den Bewerber von der Krankenkasse seitens der Vergabestelle nicht benötigt.

3.7. Rechnungsprüfer als interner Datenschutzbeauftragter?

Sozialleistungsträger haben bei Vorliegen der in § 28 Abs. 1 BDSG genannten Bedingungen einen internen Datenschutzbeauftragten zu bestellen (§ 79 Abs. 1 SGB X i. V. mit § 28 BDSG). § 28 BDSG beschreibt zwar auch inhaltlich die Bedingungen zur Person des Datenschutzbeauftragten, regelt die Frage etwa bestehender Inkompatibilitäten der Tätigkeit des Datenschutzbeauftragten mit anderen Dienstaufgaben aber nicht näher. Demzufolge kann der Sozialleistungsträger den Datenschutzbeauftragten im Rahmen seiner Organisationshoheit grundsätzlich selbst bestimmen.

Wichtigste Voraussetzung für die Tätigkeit des Datenschutzbeauftragten ist die in § 28 Abs. 2 BDSG geforderte fachliche Kompetenz. Die unmittelbare Unterstellung des Datenschutzbeauftragten gegenüber dem Amtsleiter bzw. Geschäftsführer des Sozialleistungsträgers (§ 28 Abs. 3 BDSG) stellt darüber hinaus sicher, daß Entscheidungen im Bereich des Datenschutzes direkt von der verantwortlichen Stelle getroffen werden. Es bedarf wohl keiner näheren Erläuterung, daß die Aufgaben des Datenschutzbeauftragten am besten von einem Mitarbeiter wahrgenommen werden können, der von anderen Aufgaben freigestellt ist. Wird der Datenschutzbeauftragte aus wirtschaftlichen Gründen auch mit anderen Aufgaben betraut, muß darauf geachtet werden, daß Interessenkonflikte zwischen den verschiedenen Aufgabengebieten ausgeschlossen sind. Dies gilt in besonderer Weise für solche Mitarbeiter, die neben der Aufgabe des Datenschutzbeauftragten verantwortlich mit personenbezogenen Daten umgehen oder Leitungsfunktionen im Bereich der ADV haben sollen.

Als Argument von Gewicht ist auch das vom Bundesrechnungshof in einem Prüfungsbericht zitierte Gebot zu werten, wonach der Leiter der Rechnungsprüfungsstelle der Tätigkeit für die Rechnungsprüfung nicht durch andere Aufgaben entzogen werden darf. Dies muß bei der Entscheidung – bezogen auf die Verhältnisse der einzelnen Dienst-

stelle – berücksichtigt werden. Dem weiteren Argument des Bundesrechnungshofes, nämlich eines gewissen Widerstreites zwischen Erfordernissen des Datenschutzes und dem Ziel der Rechnungsprüfung, nämlich einer sparsamen Verwaltung, vermag ich dagegen nicht zu folgen. Art. 15 BayDSG bzw. § 6 BDSG fordern technische und organisatorische Maßnahmen für den Datenschutz nur, wenn der (finanzielle) Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Eine Interessenkollision zwischen „empfehlenswerten" Datenschutzmaßnahmen und den Grundsätzen der Wirtschaftlichkeit und Sparsamkeit müßte sich daher noch durch ein verantwortungsbewußtes Bemühen um „Konkordanz" beherrschen lassen.

Zusammenfassend vertrete ich die Auffassung, daß Grund zu einer Beanstandung aus datenschutzrechtlicher Sicht nur dann gegeben wäre, wenn der zum Datenschutzbeauftragten bestellte Leiter einer Rechnungsprüfungsstelle die oben zitierten persönlichen Voraussetzungen nicht erfüllen würde oder wegen der Fülle anderer Aufgaben seiner Tätigkeit als Datenschutzbeauftragter nicht ausreichend nachkommen könnte.

3.8. Vorladung wegen Pflegschaft – auf Postkarte

Eine Stadt hatte einen Beschwerdeführer betreffs „Anordnung einer Pflegschaft" auf offener Postkarte gebeten, an einem bestimmten Tag im Amtsgebäude vorzusprechen. Ich bat das Sozialamt der Stadt um Stellungnahme, ob diese Verfahrensweise nach Ansicht des Sozialamts dem gebotenen Schutz der Sozialdaten genüge. Dabei bat ich zu berücksichtigen, daß neben den Postbediensteten auch Mitbewohner des Hauses (z. B. Vermieter oder Untermieter) Kenntnis vom Inhalt der Postkarte erlangen können. Die Stadt meinte dazu, daß die Vorladung nicht eindeutig darauf schließen ließe, daß der Empfänger unter Pflegschaft gestellt werden solle. Es würden auch Bürger vorgeladen,die ausersehen seien, ehrenamtlich eine Pflegschaft zu übernehmen. Die Stadt gestand jedoch zu, daß beispielsweise Mitbewohner des Hauses aus der Postkarte unzutreffende Schlüsse ziehen könnten, die den Empfänger einer solchen Vorladung peinlich berühren. Die Mitarbeiter des Sozialamtes wurden deshalb gebeten, Mitteilungen ähnlichen Inhalts künftig in verschlossenen Briefumschlägen zu versenden.

4. Polizei

4.1. Zur Lage des Datenschutzes

Im letzten Tätigkeitsbericht hatte ich eine vielfach zu weit gehende Speicherung personenbezogener Daten bei der Polizei gerügt, die selbst Kinder und hochbetagte Menschen umfaßt hat. Ein Rückblick auf den Stand des Datenschutzes bei den Sicherheitsbehörden muß deshalb auch die Reaktionen auf diese Kritik des Datenschutzbeauftragten berücksichtigen. Als begrüßenswerte Reaktionen sind hier zunächst verschiedene Weisungen des Bayer. Staatsministeriums des Innern zu erwähnen, die die gröbsten Fehler künftig ausschließen sollen; auf sie wird an anderer Stelle näher eingegangen. Bemerkenswert ist auch die schonungslose Analyse des Polizeipräsidiums Mittelfranken. Neben dem Hinweis, daß das Ergebnis meiner Überprüfungen zum Anlaß von Maßnahmen geworden sei, hat das Polizeipräsidium u.a. folgendes ausgeführt:

> „Die Feststellung, daß die Zahl der bisher vorgenommenen personenbezogenen Speicherungen" (KpS und KAN) zu umfangreich ist, fand auch das Polizeipräsidium bei eigenen Überprüfungen bestätigt. Die Ursache ist darin zu sehen, daß die Sachbearbeiter in ihrer Entscheidung, ob der Vorgang KpS- bzw. KAN-würdig ist, die Bestimmungen schematisch und extensiv ausgelegt haben. In erster Linie wird stets „der Fall" gesehen und offensichtlich nach dem Motto gehandelt: „Lieber zuviel, als zuwenig". Das PP Mittelfranken ist bemüht, durch entsprechende Schulung die Beamten für die Probleme unter dem Gesichtspunkt der Einzelfallprüfung zu sensibilisieren und ihnen den Sinn und Zweck der Erfassung nahe zu bringen. Durch verstärkte Kontrollen vor der Erfassung sollen Fehler künftig vermieden werden."

Eine solche Erkenntnis ist meines Erachtens die Voraussetzung dafür, daß bei der Datenverarbeitung der Polizei nicht nur der notwendige Datenschutz berücksichtigt wird, sondern gleichzeitig auch die für die Effizienz polizeilicher Tätigkeit notwendige Relevanz der verarbeiteten Daten erreicht wird.

Für die Akzeptanz des Datenschutzes bei der Polizei spielen auch Veröffentlichungen in Fachzeitschriften und Verbandsblättern der Polizei eine wichtige Rolle. So wurde in der vom Bayer. Staatsministerium des Innern herausgegebenen Zeitschrift „Polizei Intern" ausgesprochen sachlich zu meinem 7. Tätigkeitsbericht, insbesondere zu dessen Ausführungen zur Datenspeicherung im Kriminalaktennachweis (KAN) berichtet. Ich bin überzeugt, daß diese Berichterstattung dazu beitragen wird, bei den Polizeibeamten im Freistaat Bayern Verständnis für meine Absicht zu wecken, Persönlichkeitsschutz der Bürger unter gleichzeitiger Wahrung der Effizienz der Polizei zu verwirklichen. Beachtlich ist auch die Reaktion des Berufsverbandes, den ich im letzten Tätigkeitsbericht eines gespannten Verhältnisses zum Datenschutz in seinen Publikationen geziehen hatte, der unter der Frage „Was ist los mit uns, der Polizei?" folgendes ausführt:

> „Da sind wir uns doch tatsächlich nicht zu blöd, in Fällen, in denen kindliche Neugier sich für das andere Geschlecht interessiert oder ein Junge dem anderen das Sandschäufelchen auf den Kopf haut, den Anzeigen aufgebrachter Eltern stattzugeben und Ermittlungsverfahren wegen sexuellen Mißbrauchs an Kindern oder Körperverletzung einzuleiten. Da zeigen wir eiskalt ein Kleinkind wegen Mittäterschaft zum schweren Diebstahl aus einen Wohnwagen an, nur weil es den älteren Kindern bei deren diebischen Vorhaben hinterhergelaufen ist. Es hat schon immer Kollegen gegeben, scharfe Hunde, die das Kind im Mutterleib anzeigen, aber sind wir allgemein nicht mehr souverän genug, hier einfach nicht mitzuspielen, unserem gesunden Menschenverstand nachzugeben? Denken wir überhaupt noch bei dem, was wir tun oder lassen wir uns in allem nur noch von Richtlinien leiten?"

Dieser Verband stellt aber noch eine weitere Frage, die an uns, die Gesellschaft gerichtet ist und die uns vor Schadensfreude über die Fehlleistungen der Polizei bei der Datenverarbeitung bewahren sollte. Auf die selbstgestellte

Frage „Was ist los mit unserer Gesellschaft" schreibt der Verband: „Die Polizei greift die Kinder ja kaum von sich aus aus dem Sandkasten, sie werden ihr in der Regel angezeigt. Wird unsere Gesellschaft ihrer Kinder nicht mehr Herr, so daß nur noch der Ausweg zur Polizei bleibt? ... Warum nur findet unsere Gesellschaft eine solch masochistische Lust daran, ihre Kinder und sich selbst mit Strafanzeigen zu überziehen und fortlaufend zu kriminalisieren?"

Bei der Bewertung der Lage des Datenschutzes bei der Polizei sind aus meiner Sicht Fortschritte festzustellen. Ein Indiz dafür ist auch die Tatsache, daß sich Polizeibehörden zunehmend bei Zweifelsfragen an meine Geschäftsstelle wenden. Dies zeigt auch ein gestiegenes Datenschutzbewußtsein. Die Tatsache, daß sich zunehmend Polizeibeamte in eigenen Datenschutzangelegenheiten an mich wenden, ist ein weiterer Beleg dafür, daß Datenschutz zur Selbstverständlichkeit wird.

4.2. Schwerpunkte meiner Tätigkeit

Meine Tätigkeit im Sicherheitsbereich innerhalb des Berichtszeitraums war von drei Schwerpunkten geprägt:

Prüfungen bei der Polizei, Beantwortung von entsprechenden Bürgereingaben und Beratung der Sicherheitsbehörden.

Prüfungen habe ich bei folgenden Behörden vorgenommen:

Polizeipräsidium München
Polizeidirektion Erding
Polizeidirektion Kempten
Grenzpolizeiinspektion Pfronten

Außerdem habe ich bei nahezu allen bayerischen Polizeidirektionen eine Nachprüfung zur Datenspeicherung im Kriminalaktennachweis vorgenommen.

Die Zahl der Bürgereingaben im Sicherheitsbereich ist im Berichtszeitraum stark gestiegen. Zwar wird hierdurch die Kapazität meiner Geschäftsstelle besonders stark beansprucht, doch bin ich andererseits für meine Tätigkeit auf die Mitarbeit der Bürger besonders angewiesen und deshalb für die Schilderung von Einzelfällen dankbar. Die auf die Bürgereingaben hin vorgenommenen Einzelfallprüfungen haben in der überwiegenden Zahl keine Verletzung von Datenschutzbestimmungen durch Polizeibehörden ergeben.

Schließlich habe ich mich auch im Berichtszeitraum zu neu einzuführenden und zur datenschutzrechtlichen Verbesserung bestehender Automationsvorhaben sowie zu neuen Rechts- und Verwaltungsvorschriften im Sicherheitsbereich geäußert. In dieser beratenden Tätigkeit sehe ich den Versuch, bereits vorbeugend Datenschutz zu verwirklichen.

4.3. Führung und Auswertung von kriminalpolizeilichen Sammlungen (KpS)

Die Speicherung in Kriminalakten oder polizeilichen Dateien berührt die Bürger stärker als die Speicherung in sonstigen Behördenakten. Tatsächlich kann gerade die Führung von Kriminalakten das verfassungsrechtlich geschützte Persönlichkeitsrecht der in ihnen genannten Personen besonders berühren. Bei Führung dieser Akten und der Speicherung in polizeilichen Dateien sowie bei Datenübermittlungen aus solchen Sammlungen muß daher im besonderen Maße darauf geachtet werden, daß nur richtige, im Einzelfall tatsächlich erforderliche Daten in der jeweils zulässigen Zeitspanne gespeichert und nur den berechtigen Polizeidienststellen zur Verfügung gestellt sowie nur im konkreten erforderlichen Einzelfall übermittelt werden. Hierauf und auf die diesbezügliche Entscheidung des Bayer. Verfassungsgerichtshofes vom 9.7.1985 hatte ich in meinem 7. Tätigkeitsbericht hingewiesen. Diese Grundsätze habe ich deshalb auch dieses Mal bei meinen Prüfungen zugrunde gelegt.

4.3.1. Kriminalaktennachweis (KAN)

Zum besseren Verständnis der nachfolgenden Ausführungen erläutere ich kurz die wesentlichen Grundsätze des Kriminalaktennachweises (KAN).

Der KAN dient dem Nachweis von Kriminalakten, die beim Bund und bei den Ländern geführt werden. Der Kriminalaktennachweis gliedert sich in einen Bundes-KAN, einen Landes-KAN und in den sogenannten regionalen KAN. Der Bundes-KAN soll sich darauf beschränken, Hinweise auf Täter besonders schwerer, katalogmäßig aufgelisteter Straftaten oder von Straftaten mit überregionaler Bedeutungzu geben. Letzteres haben die eingebenden Polizeibeamten zu entscheiden. Im Landes-KAN und im regionalen KAN – einer bayerischen Besonderheit – werden die Kriminalakten bayerischer Polizeidienststellen nachgewiesen. In dem bei den einzelnen Polizeidirektionen geführten regionalen KAN werden weitgehend dezentralisiert die Nachweise über Akten der Personen geführt, die lediglich auf örtlicher Polizeiebene von Bedeutung sind. Nur die übrigen Nachweise zu den bayerischen Kriminalakten werden im Landes-KAN, also landesweit abrufbar, geführt.

Im Berichtszeitraum habe ich der weiteren Entwicklung des KAN ein besonderes Augenmerk gewidmet. Neben einer allgemeinen Nachprüfung auf der Grundlage meiner letztjährigen Erfahrungen habe ich noch zwei Polizeidirektionen näher kontrolliert. Ich habe mich von folgenden Grundsätzen leiten lassen:

Zweck und Umfang kriminalpolizeilicher personenbezogener Sammlungen, zu deren Erschließung der Kriminalaktennachweis dient, ergeben sich aus den der Polizei gesetzlich zugewiesenen Aufgaben. Die Erfassung im Kriminalaktennachweis muß deshalb zur Gefahrenabwehr oder zur Strafverfolgung erforderlich sein. Weil derzeit präzise gesetzliche Regelungen zur polizeilichen Datenverarbeitung fehlen, muß bei der Prüfung der Zulässigkeit der Führung polizeilicher Sammlungen im Einzelfall auf die entsprechenden Richtlinien zurückgegriffen werden.

4.3.1.1. Ergebnis der Nachprüfung

Unmittelbar nach Erscheinen meines letzten Tätigkeitsberichtes hatte das Bayer. Staatsministerium des Innern die Weisung erteilt, daß die Speicherung von Kindern nur in Ausnahmefällen zulässig sein könne und auch über 70 Jahre alte Personen nur in eingeschränktem Maße im KAN geführt werden dürften. Weitere Hinweise betrafen die erkennungsdienstliche Behandlung, die flexible Vergabe der Aussonderungsfristen und einige Formen der Datenübermittlung. Das Staatsministerium des Innern hat damit meine Prüfungsergebnisse klar und deutlich der polizeilichen Praxis vermittelt.

Um zu prüfen, welche Veranlassungen die bayerischen Polizeibehörden aufgrund meiner diesbezüglichen Beanstandungen vorgenommen haben, habe ich von sämtlichen

bayerischen Polizeidirektionen, die am Kriminalaktennachweis angeschlossen sind, abgesehen von zwei Direktionen, die ich kurz zuvor geprüft hatte, Listenausdrucke über

- Kinder
- Personen über 70 Jahre Lebensalter
- Ordnungswidrigkeiten und
- über bestimmte Entscheidungen zur Überörtlichkeit des Delikts und damit Speicherung im Bundes-KAN

angefordert.

Obwohl sich die Auswertung auf einige prägnante Kriterien beschränken mußte und eine tiefergehende Bewertung nur an Hand der dazugehörenden kriminalpolizeilichen Akten hätte erfolgen könnnen, zeigte diese Nachprüfung bereits eine deutliche Verringerung der Datenspeicherungen. Allerdings habe ich auch den Eindruck gewonnen, daß die Anordnungen des Innenministeriums manchmal zu schematisch umgesetzt worden sind. Im einzelnen ist folgendes festzustellen:

- Bei der Erfassung von **Kindern, alten Menschen** und **Ordnungswidrigkeiten** sind Verbesserungen eingetreten. Allerdings ist es meines Erachtens noch verfrüht, bereits von einem datenschutzrechtlich bedenkenfreien Zustand zu sprechen.

  Bei einer Direktion sind mir im Gegensatz zu anderen bayerischen Polizeidirektionen viele Erfassungen wegen vermißter Kinder aufgefallen. Ich gehe davon aus, daß nicht bereits stundenweise „vermißte Kinder" gespeichert werden, die sich nur in ihrem gewohnten Lebensraum verlaufen haben. Bei einer Reihe von Polizeidirektionen war der Bestand an Kindern, alten Menschen und Ordnungswidrigkeiten im Verhältnis zur Bedeutung der Delikte noch zu hoch. Auch die Speicherungsebene (Bundes-KAN, Landes-KAN, regionaler KAN) bei Kindern und alten Menschen war teilweise unrichtig. Aufgefallen ist auch die häufige Speicherung alter Menschen ausschließlich wegen Ladendiebstahls.

  Fehler habe ich auch bei der sogenannten retrograden (rückwärtigen) Erfassung festgestellt. Zum Beispiel sind Ordnungswidrigkeiten bis in die 50er-Jahre zurück erfaßt worden. Zweifel an der Erforderlichkeit für die polizeiliche Aufgabenerfüllung habe ich auch an Speicherungen, die aussagen, daß

  - jemand 1964 als 17jähriger eine Ordnungswidrigkeit nach dem Schulpflichtgesetz begangen hat oder
  - eine Person vor 10 Jahren wegen unzulässigen Lärmens zur Anzeige gebracht worden ist,
  - zu einem 82jährigen die fahrlässige Begehung einer Ordnungswidrigkeit gegen das Landesstraf- und Verordnungsgesetz – Verhütung von Bränden – vermerkt war.

  Auch waren z.B. nach wie vor zu Kindern Sachverhalte erfaßt, die bei einem ordnungsgemäßen Vollzug der Aussonderungsfristen der KpS-Richtlinien nicht mehr hätten bekannt sein dürfen. Gleiches gilt auch für Kriminalakten Erwachsener.

- Nach wie vor scheinen Probleme grundlegender Art bei der Vergabe der **KAN-Merker**, die die Speicherung der Daten im Bundes-KAN veranlassen, und bei der Abgrenzung zwischen Landes-KAN und regionalem KAN zu bestehen.

  Gleichartige Delikte waren teilweise im regionalen KAN, teilweise im Landes-KAN gespeichert, ohne daß ein Grund für die unterschiedliche Sachbehandlung ersichtlich gewesen wäre. Bei einer Direktion war ein Großteil der erfaßten Ordnungswidrigkeiten durch Vergabe eines falschen Steuerungsmerkers in den Landes-KAN gesteuert worden, obwohl diese grundsätzlich nur im regionalen KAN hätten gespeichert werden dürfen.

  Zu dem KAN-Merker „planmäßig und überörtlich" habe ich etwa bei einer Direktion festgestellt, daß sie Sachverhalte mit diesem KAN-Merker speichert, die sich nicht in ihrem Zuständigkeitsbereich zugetragen haben und die sie auch nicht bearbeitet hat. Dadurch ist der gleiche Sachverhalt zu einer Person zweifach im Landes-KAN gespeichert, was zum unzutreffenden Eindruck führen kann, der Betroffene sei zweier Straftaten beschuldigt.

  Ganz generell habe ich festgestellt, daß eine Reihe von Polizeidirektionen einen besonders hohen Bestand an Speicherungen haben, die auch im Bundes-KAN und damit bundesweit abrufbar zur Verfügung stehen. Hier wird die Erforderlichkeit der Speicherungen genau zu prüfen sein.

Wegen der offenkundig bestehenden Unklarheiten über die Vergabe der sogenannten KAN-Merker für den Bundes-KAN sind die vorgesetzten Dienstbehörden aufgefordert, durch entsprechende Schulung den Beamten die notwendigen Kenntnisse zu vermitteln. Mir ist bekannt, daß derzeit eine Arbeitsgruppe die Kriterien für diese Merker überprüft und bereits Konsequenzen gezogen worden sind.

Auch über den Umfang der Erfassung von Straftaten im Kriminalaktennachweis scheint mir vielfach noch Unklarheit zu herrschen. So widerspricht es eindeutig der Errichtungsanordnung zum KAN, wenn sämtliche Straftaten – vielfach das gleiche Delikt –, die am gleichen Tage bzw. innerhalb eines sehr kurzen Zeitraumes begangen worden sind und die darüber hinaus noch unter dem gleichen Aktenzeichen bearbeitet werden, einzeln im KAN aufgeführt werden.

- **Weitere Feststellungen** waren:

  Manchmal hat sich mir die Frage gestellt, ob nach Abschluß des Strafverfahrens die Deliktbezeichnungen im KAN berichtigt worden sind. Diese Berichtigung wäre insbesondere dann wichtig, wenn z.B. die Schlüsselzahl dieses Deliktes darüber entscheidet, ob der Betroffene im Bundes-KAN oder nur im Landes-KAN gespeichert ist. Eine mangelnde Bereinigung kann hier zur Beeinträchtigung schutzwürdiger Belange der Betroffenen führen.

  Die Speicherung von Selbstmordversuchen und das Tätigwerden der Polizei im Rahmen des Unterbringungsgesetzes kann m. E. grundsätzlich nur im regionalen KAN erfolgen. Dies wird erst bei einigen Direktionen so gehandhabt. Eine heute 91jährige war vor 3 Jahren von der Polizei nach dem Unterbringungsgesetz in ein Krankenhaus gebracht worden. Dies war im Landes-KAN erfaßt.

  Außerdem ist bei dieser stichprobenartigen Nachprüfung aufgefallen, daß bei der Erfassung von früheren Vorgängen teilweise Sachverhalte gespeichert werden, die 40 Jahre und mehr zurückreichen. Ich habe Zweifel, ob dies für eine sinnvolle kriminalpolizeiliche Arbeit notwendig ist.

Bei einer Direktion war auffällig, daß weder Daten von Kindern noch über 70 Jahre alten Personen gespeichert waren. Sollten die Daten aller Kinder und alten Menschen ohne nähere Einzelfallprüfung gelöscht worden sein, hielte ich dies für bedenklich.

Ein Problem scheint nach wie vor das richtige Setzen der Aussonderungsfristen zu sein, die teilweise noch zu schematisch vergeben werden. So konnte ich bei Ordnungswidrigkeiten und bei Speicherungen aus Gründen der polizeilichen Gefahrenabwehr feststellen, daß die Regelaussonderungsfristen von 10 Jahren vergeben worden waren. Dies ist grundsätzlich nicht sachgerecht.

Besonders sorgfältig hat das Polizeipräsidium Mittelfranken auf die Ergebnisse meiner Nachprüfung reagiert und in seinem Zuständigkeitsbereich eine eigene Überprüfung durchgeführt, die zu einer weiteren Aktualisierung und Bereinigung des Datenbestandes geführt hat. Dies ist besonders erfreulich.

Um eine Reihe der auch bei der Nachprüfung festgestellten Fehler bei der Bearbeitung des KAN künftig weitgehend auszuschließen, sind im **DV-Programm des Landeskriminalamtes** einige Plausibilitätsprüfungen für die Speicherungen im L-KAN und B-KAN aufgenommen worden. Diese betreffen die Speicherungen von Kindern, Jugendlichen und älteren Menschen. Ich erhoffe mir mit diesen Plausibilitätsprüfungen eine Verbesserung des Datenmaterials.

4.3.1.2. Weitere Prüfergebnisse

Neben der oben erwähnten Nachprüfung bei der Führung des Kriminalaktennachweises habe ich im Berichtszeitraum bei zwei Polizeidirektionen Erding und Kempten Prüfungen durchgeführt.

Vorweg kann ich feststellen, daß deren Ergebnisse bezüglich der Speicherungen im KAN in Anbetracht meiner vorjährigen diesbezüglichen Prüferfahrungen grundsätzlich erfreulich sind. Den beiden überprüften Polizeidirektionen scheint es weitgehend gelungen zu sein, die Datenspeicherung im KAN auf das erforderliche Maß zu beschränken. Diese Polizeidirektionen haben bewiesen, daß ein sachgerechter Umgang mit dem KAN möglich ist. Gleichwohl habe ich bei den nachstehenden Bereichen noch einzelne Schwierigkeiten festgestellt:

Kinder:

Zwar war die vorgefundene Zahl der gespeicherten Kinder an sich nicht hoch, doch war der Anteil der Kinder, die nur wegen sogenannter Antragsdelikte gespeichert waren, zu groß.

Verkehrsdelikte und Ordnungswidrigkeiten:

Verkehrsdelikte und Ordnungswidrigkeiten dürfen nur nach sehr strenger Prüfung in Kriminalakten aufgenommen und somit im Kriminalaktennachweis gespeichert werden. Der Bestand von 696 Ordnungswidrigkeiten bei einer Polizeidirektion erscheint mir deshalb zu hoch. Tatsächlich haben auch Stichproben ergeben, daß Speicherungen dieser Ordnungswidrigkeiten für die Aufgaben Gefahrenabwehr oder Straftatenbekämpfung nicht immer erforderlich waren. Auch bei den vereinzelt vorgenommenen retrograden Erfassungen sind teilweise zeitlich bereits länger zurückliegende Ordnungswidrigkeiten mit in den KAN aufgenommen worden. Eine Speicherung von Ordnungswidrigkeiten lediglich zur Abrundung des Persönlichkeitsbildes, wie es mir in einer Polizeidirektion als Begründung genannt worden ist, reicht meines Erachtens nicht aus. Dies gilt besonders, wenn Ordnungswidrigkeiten gespeichert werden, die bereits einige Jahre zurückliegen.

Zu hoch waren die Bestände der Verkehrsdelikte. Zweifel habe ich auch, ob es tatsächlich erforderlich ist, zeitlich bereits länger zurückliegende Verkehrsdelikte im KAN zu erfassen:

> Beispielsweise waren 2 Bürger erfaßt, die 1967 als 13jähriger, bzw. 1963 als 14jähriger ohne Fahrerlaubnis gefahren waren.

Dies scheint weder für die Gefahrenabwehr noch für die Straftatenverfolgung erforderlich zu sein.

Zweifel an der Erforderlichkeit der Datenspeicherung bestehen auch in folgenden beiden Fällen:

> Ein Jugendlicher hatte in sein Mofa ein größeres Ritzel eingebaut, um die Geschwindigkeit zu erhöhen.

Ein anderer Jugendlicher war lediglich wenige 100 Meter auf öffentlichem Verkehrsgrund ohne Fahrerlaubnis gefahren.

Speicherungsebenen im KAN:

Wie eingangs zum Kriminalaktennachweis ausgeführt, beruht das Konzept des Kriminalaktennachweises auf einer Abschichtung in verschiedenen Speicherungsebenen. Die Speicherung in diesen Ebenen ist entscheidend für die Frage, in welchem Bereich die einzelnen Daten abrufbar sein sollen (z.B. bundesweit, landesweit oder nur im Bereich einer Polizeidirektion). Durch Eingabe sogenannter „KAN-Merker" können Straftaten statt nur im Landes-KAN gespeichert zu sein, zum Bundes-KAN übermittelt werden. Wenn ich hier bei meinen Prüfungen auf weniger Fehlspeicherungen als im vergangenen Jahr gestoßen bin, sind hier trotzdem noch einige zweifelhafte Sachbehandlungen festzustellen:

> Vollrausch und Verletzung der Unterhaltspflicht als „gewohnheitsmäßig" (?) begangene Straftaten im Bundes-KAN. Unterhaltspflichtverletzung ist ein sogenanntes Dauerdelikt. Das Kriterium „gewohnheitsmäßig" könnte allenfalls dann gegeben sein, wenn mehrere verschiedene Unterhaltsberechtigte geschädigt werden.
>
> Einmietbetrug und vorsätzliche Körperverletzung als „gewerbsmäßig" (?) begangene Straftaten im Bundes-KAN.
>
> Jagdwilderei, begangen mit einem Gewehr, in den Bundes-KAN.

Auf ein besonders unerfreuliches Problem bin ich gestoßen:

Bei einer Direktion waren Datenfelder im KAN, die für personengebundene Hinweise vorgesehen waren, für Registratur- und Hinweiszwecke zweckentfremdet worden. Wenn auch im konkreten Fall in diesen Datenfeldern keine datenschutzrechtliche bedenklichen Speicherungen angetroffen worden sind, zeigt der Fall doch, daß die theoretische Möglichkeit besteht – eventuell an Datenschutz- und Dienst-

aufsicht vorbei – Daten in automatisierten Systemen zu speichern, die nicht von dieser Stelle oder überhaupt nicht zulässigerweise gespeichert werden dürften.

4.3.2. Polizeipräsidium München

Vorweg möchte ich bemerken, daß das Ergebnis meiner datenschutzrechtlichen Prüfung beim Polizeipräsidium München recht nachdenklich stimmt. Obwohl die Prüfung wenige Tage gedauert hat und eine derzeit nur sehr geringfügige Automatisierung keine Querschnittsprüfungen, sondern nur Stichproben erlaubt hat, drängt sich der Eindruck auf, daß dem Datenschutz beim Polizeipräsidium München bislang noch nicht der notwendige Stellenwert eingeräumt worden ist. Die Versäumnisse liegen in der Vergangenheit. Nun meine ich Anhaltspunkte zu haben, daß nach einem Personalwechsel die Datenschutzprobleme entschieden angegangen werden sollen. Hierzu wird es jedoch einer erheblichen Anstrengung bedürfen.

Unvollständige Übersicht über die Dateien

Das Problem beginnt bereits damit, daß beim Polizeipräsidium keine aktuelle und vollständige Übersicht über die einzelnen bei dieser Behörde geführten Dateien bestehen. Die vorhandene Übersicht ist einige Jahre alt und lückenhaft. Eine Reihe von Dateien, die bei verschiedenen Dienststellen geführt werden, sind für die Übersicht nicht gemeldet, der Inhalt anderer Dateien entspricht nicht der entsprechenden Errichtungsanordnung. Wer nicht weiß, welche Daten in seinem Zuständigkeitsbereich verarbeitet werden, ist nicht in der Lage, die Verantwortung für die Einhaltung des Datenschutzes in seinem Bereich zu übernehmen.

Fehlende Abstimmung der Dateien

Neben der nach den Richtlinien über die Führung kriminalpolizeilicher Sammlungen (KpS) vorgesehenen Kriminalaktensammlung bestehen im Polizeipräsidium München auf der Ebene von Dezernaten und Kommissariaten Dateien, die miteinander nicht abgestimmt sind. Aussonderungen in der Kriminalaktensammlung werden in diesen Dateien nicht nachvollzogen, weder der Verfahrensausgang noch das Alter der Betroffenen (Kinder, Jugendliche, alte Menschen mit kürzeren Aussonderungsfristen) ist berücksichtigt. Teilweise fehlen die für die Aussonderung notwendigen Erfassungs- und Aussonderungsdaten. Bei dieser Sachbehandlung ist das Polizeipräsidium München auch nur begrenzt in der Lage, die nach den KpS-Richtlinien im bestimmten Umfang vorgesehenen Auskünfte an betroffene Bürger richtig und mit vertretbarem Aufwand zu erteilen. Außerdem verstößt diese Vorgehensweise allein schon wegen der fehlerhaften Aussonderung gegen die KpS-Richtlinien. Bei dieser Sachbehandlung kann der Landesbeauftragte für den Datenschutz seine Kontrolltätigkeit nicht sachgerecht wahrnehmen. Außerdem besteht die Gefahr, daß er aufgrund unvollständiger Informationen an Petenten ggf. falsche Auskünfte erteilt.

Kriminalakten

Obwohl das Polizeipräsidium München nach seinen eigenen Angaben die Kriminalakten seit längerer Zeit bereinigt und den Bestand, der noch im letzten Jahr mit ca. 500.000 Akten angegeben worden war, auf nun ca. 450.000 Akten verringert hat, hat die stichprobenartige Ziehung von Kriminalakten ergeben, daß bei ca. zwei Dritteln der durchgesehenen Akten mehr oder weniger gravierende datenschutzrechtliche Fehler vorliegen. Zum Teil kann dies darin begründet liegen, daß bei der Aufbewahrung von Vorgängen eine notwendige Trennung zwischen Vorgangsverwaltung und kriminalpolizeilichen Unterlagen bislang nicht vorhanden gewesen ist. In meinem 7. Tätigkeitsbericht habe ich diese Problematik bereits angesprochen. Das Polizeipräsidium München ist allerdings bemüht, diese erforderliche Trennung in Zukunft vorzunehmen. Im einzelnen wurden folgende Feststellungen leider auch in bereits „bereinigten" Akten getroffen:

- Kriminalakten werden trotz abgelaufener Aussonderungsfristen geführt.
- Der Vermerk des Aussonderungsdatums auf dem Aktendeckel, der eine zeitgerechte Vernichtung erlauben soll, fehlt in zahlreichen Fällen.
- Soweit Aussonderungsdaten vermerkt sind, sind diese oft nicht nachvollziehbar. In den meisten Akten ist der für die Aussonderung maßgebliche Fristbeginn, dies ist im Regelfall der Zeitpunkt der Tat, falsch festgelegt. Beispiele für solche Fehler sind:
  - Zeitpunkt der Bearbeitung der Anzeige statt des Tatzeitpunktes,
  - der Eingang des Widerrufs der Fahndung nach einem Ausländer durch das Kreisverwaltungsreferat,
  - die Anforderung eines Auszugs aus dem Bundeszentralregister,
  - die nach der Verurteilung eingehende Mitteilung über die Dauer der Bewährungszeit,
  - die Tatsache, daß jemand entmündigt worden ist,
  - Berichtigung der Personalien des Betroffenen,
  - Bekanntwerden des Verfahrensausgangs, um nur einige aus der Vielzahl ähnlich gelagerter Fälle zu nennen.

  Die Festsetzung der Aussonderungsfristen ist zu schematisch gehandhabt worden. Selbst wenn im Einzelfall der Sachverhalt deutlich von der Norm abweicht, wird nicht genügend flexibel auf dessen Besonderheiten eingegangen.
- Sogar die Tatsache, daß jemand Geschädigter einer Straftat geworden ist, hat zur Anlage eines Kriminalaktes zu seiner Person oder zur Aufnahme in bereits bestehende Akten geführt. Fast schon amüsant ist der folgende Fall, der zu einer Eintragung in einer Kriminalakte geführt hat:

  > Eine Ehefrau war samt Hund zu einem Bekannten gezogen, um freiwillig mit diesem Mann für einige Tage zusammenzuleben und auch das Bett zu teilen. Der betrogene Ehemann ging zur Polizei, meldete seine Frau als vermißt und, da ihm der Aufenthalt seiner Ehefrau wohl bekannt war, gab er den derzeitigen Liebhaber seiner Frau als möglichen „Entführer" an. Die Polizei stellte daraufhin fest, daß die Ehefrau freiwillig ihrem Mann fernblieb, womit für sie die Sache grundsätzlich erledigt war. Gleichwohl wurde der ganze Vorgang aktenkundig in der Kriminalakte des „Entführers".
- Obwohl Kriminalakten grundsätzlich nur zur Erfüllung der polizeilichen Aufgaben, Gefahrenabwehr und zur künftigen Verfolgung von Straftaten anzulegen sind, finden

sich auch Vorgänge, die hierunter nicht subsumiert werden können. So werden wegen Verkehrsdelikten Kriminalakten angelegt. Auch die Tatsache, daß Personen kurzzeitig vermißt waren, führt zur Anlage von Kriminalakten.

Unter die für die Aufgabenerfüllung der Polizei nicht erforderliche weitergehende Führung von Kriminalakten zählt auch folgender Fall:

> Ein amerikanischer Student setzte sich des Nachts auf die Mauer vor dem Bayer. Landtag, um von dort oben einen schönen Überblick über München zu erhalten. Die Polizei nahm den Studenten vorläufig fest, führte eine erkennungsdienstliche Behandlung durch und nahm Ermittlungen wegen Verdachts des Hausfriedensbruchs auf. Vom Landtagspräsidenten wurde der für eine eventuelle Strafverfolgung notwendige Strafantrag nicht gestellt. Die Ermittlungen der Polizei schlossen mit dem Vermerk, daß keinerlei politischer Hintergrund bei dem Sitzen auf der Landtagsmauer festgestellt werden konnte. Gleichwohl blieb die Kriminalakte bestehen, wurde der Betroffene in die automatisierte Datei der bekannten Täter mit dem personengebundenen Hinweis des „politischen Täters" aufgenommen und wurde eine Meldung an das Bayer. Landesamt für Verfassungsschutz weitergegeben.

- Obwohl die Aufnahme von Kindern in Kriminalakten allenfalls unter strengen Voraussetzungen zulässig sein kann, haben auch meine Stichproben auf Kriminalakten zu Kindern geführt. Unter Führung eines schon etwas älteren Kindes waren 3 sieben- bis achtjährige Kinder in einen Kindergarten eingestiegen und hatten dort Spielzeug entwendet. Ein Teil der Spielsachen fand sich bereits in der nächsten Umgebung des Kindergartens wieder. Zu diesen einzelnen Kindern waren jeweils Kriminalakten angelegt worden und dies, obwohl der Vorfall sich erst vor kurzer Zeit zugetragen hat und die diesbezüglichen neuen Anordnungen des Innenministeriums (zur eingeschränkten Zulässigkeit der Speicherung von Kindern, vgl. 4.3.1.1) allen Polizeidienststellen bekannt sein mußten.

Erkennungsdienstliche Behandlung (ed-Behandlung)

In der Kartei der ed-Behandlungen (insbesondere Anfertigungen von Lichtbildern und Fingerabdrücken) sind derzeit ca. 76.500 Personen erfaßt. Stichproben haben auch hier die bereits im letzten Tätigkeitsbericht gerügte Tatsache bestätigt, daß ein nicht geringer Anteil von ed-Behandlungen die sogenannte Bagatellkriminalität betrifft, also z.B. Fälle von Beleidigung, Beförderungserschleichung und Sachbeschädigung, für die eine ed-Behandlung im Hinblick auf die gesetzlichen Anforderungen grundsätzlich nur in Ausnahmefällen gerechtfertigt ist.

Außerdem fehlt ein Nachweis über den Verbleib der im Rahmen der erkennungsdienstlichen Behandlung gefertigten sieben Lichtbilder. Somit besteht keine Gewähr, daß im Falle der notwendigen Vernichtung erkennungsdienstlicher Unterlagen auch tatsächlich alle gefertigten Lichtbilder vernichtet werden.

Dateien und Karteien

Die Kriminalakten des Polizeipräsidiums München sind derzeit noch nicht im Kriminalaktennachweis erfaßt. Dies ist für die nächste Zeit vorgesehen. Derzeit sind grundsätzlich die Personen automatisiert erfaßt, die erkennungsdienstlich behandelt worden sind. Bei dieser Datei ist aufgefallen, daß die im Rahmen der ed-Behandlung vergebenen personengebundenen Merkmale nur in einem Teil der Fälle tatsächlich zugetroffen haben. Stichprobenartig überprüft habe ich Merkmale wie Polit, Mongo (mongoloid), Zigeuner, Rocker, geistesschwach sowie Prostitution. Meine schon an anderer Stelle geäußerten Bedenken gegen die personengebundenen Hinweise wegen ihrer vielfach mangelnden Aktualität sind auch hier bestätigt worden:

> Ein Österreicher, der unerlaubt in das Bundesgebiet eingereist war und auf dem Oktoberfest Brezeln verkauft hat und deshalb nach dem Ausländergesetz und der Gewerbeordnung angezeigt worden ist, hatte ohne ersichtlichen Grund den Hinweis: „Rocker".
>
> Eine Person wurde offenbar wegen der Einnahme von zwei Valium-Tabletten mit dem Hinweis „geistesschwach" belegt.

Durch die Vergabe falscher personengebundener Hinweise entsteht eine unzulässige Brandmarkung der Betroffenen. Aber auch die polizeiliche Recherche nach möglichen Straftätern wird durch die Vergabe unzutreffender Kriterien unnötig erschwert.

Alkoholikerkartei

Bei einer Münchner Polizeiinspektion werden dort bekannte Alkoholiker im Stadtstreicher- und Bettlermilieu durch besondere Kennzeichnung als Alkoholiker ausgewiesen.

„Penner"-Kartei

Unter der Bezeichnung „Pennerpack" führt eine Münchner Polizeiinspektion eine Kartei der Personen, die gegen die Benutzungsordnung für die Verkehrsflächen des Stachusbauwerks verstoßen. Da die Ausübung des Hausrechts für diese Verkehrsflächen der Polizei übertragen worden ist, werden dort alle diejenigen Personen erfaßt, die die Flächen nicht vorwiegend zum Fußgängerverkehr, sondern beispielsweise zum Herumstehen, Herumsitzen, Bier trinken oder anderem benutzen. Daß in dieser Kartei offenbar auch Personen erfaßt werden, die die betroffenen Flächen keineswegs in dem nicht zugelassenen Umfang benutzen, hat eine Stichprobe bestätigt:

> So fand sich eine Karteikarte über einen im Stachusgeschoß kontrollierten jungen Soldaten einer Gebirgsjägerkompanie in Mittenwald, der verheiratet und Vater von Kindern ist.

Ich habe grundsätzliche Bedenken, ob dadurch bei der Polizei nicht „sozial auffällige" Minderheiten registriert werden, ohne daß dies in der vorliegenden Sachbehandlung aus Gründen der polizeilichen Aufgabenerfüllung erforderlich ist.

Transvestiten-, Homo- und Stricherkarteien

Bei der Anlage von Karteien für den sexuellen Bereich läßt sich die Polizei offenbar von eigenen Gesetzmäßigkeiten leiten. Bei der datenschutzrechtlichen Bewertung habe ich allerdings die gesetzlichen Aufgaben und Befugnisse der

Polizei heranzuziehen. Dies führt zu erheblichen Zweifeln an Art und Inhalt dieser Dateien. So vermag ich grundsätzlich keinen Grund zu erkennen, weshalb die Polizei die Tatsache, daß jemand Transvestit ist, als Anlaß zur Aufnahme in eine eigenständige **Transvestitenkartei** nimmt.

Im Gegensatz zur Transvestitenkartei ist die **Homokartei** sehr groß. In ihr sind nicht nur die Personen aufgenommen, die Straftaten nach § 175 Strafgesetzbuch oder nach anderen Bestimmungen des 13. Abschnitts des Strafgesetzbuches begangen haben, soweit sie homosexuelle Handlungen betreffen, sondern auch solche Personen, zu denen die Polizei aufgrund sonstiger Informationen zu der Annahme gelangt, daß die Betroffenen homosexuell veranlagt sein könnten oder in homosexuellen Kreisen verkehren. Hierbei werden auch Personen erfaßt, die als Opfer von Straftaten möglicherweise Homosexuelle sind, die bei Razzien in einschlägigen Lokalen angetroffen oder die in der Nähe von öffentlichen Bedürfnisanstalten kontrolliert worden sind. Außerdem gibt es sogenannte vorsorgliche Erfassungen, die offenbar auf Informationen beruhen, die die Polizei auf sonstigen Wegen über die sexuellen Eigenschaften erhält. Diese Kartei ist nach Bekundungen der Polizei bislang weder überarbeitet, noch sind Aussonderungen vorgenommen worden. Auch die schon Jahre zurückliegende Änderung der entsprechenden strafrechtlichen Bestimmungen hat zu keiner Bereinigung der Kartei geführt. Ich habe das Polizeipräsidium München dringend zur Überarbeitung dieser Kartei aufgefordert. Die Polizei hat die ihr gesetzlich zugewiesenen Aufgaben und Befugnisse zu achten.

Auch in der **Stricherkartei** wurden bislang offensichtlich keine Aussonderungen vorgenommen, obwohl die Polizei selbst dies bei über 25jährigen eigentlich vorsieht. Im übrigen habe ich Zweifel, ob alle hier erfaßten Personen tatsächlich der männlichen Prostitution nachgehen, da beispielsweise eine Kontrolle im Stachus-Untergeschoß allein für die entsprechende Annahme meines Erachtens nicht ausreicht.

Sonstiges

Meine grundsätzlich positiven Erkenntnisse aus der Überprüfung des Staatsschutzdezernates finden sich unter der entsprechenden Gliederungsnummer (4.11.1). An dieser Stelle sei nur darauf hingewiesen, daß es sehr begrüßenswert ist, daß der ursprünglich ca. 60.000 Karteikarten umfassende Bestand auf etwa 11.000 Karteikarten verringert worden ist.

Eine Antwort des Polizeipräsidiums München auf meine Prüfungsfeststellungen steht noch aus. Im übrigen wird auf die Ausführungen zur Übermittlung von Sozialdaten (4.8.2) hingewiesen.

4.3.3. Polizeibeamte im Kriminalaktennachweis

Es ist allgemein bekannt, daß Polizeibeamte im Vollzugsdienst häufig Ziel von Strafanzeigen werden. Wie die Erfahrung gezeigt hat, sind in der weit überwiegenden Zahl dieser Fälle die Polizeibeamten zu Unrecht beschuldigt und die gegen sie eingeleiteten Ermittlungsverfahren eingestellt worden. Die Gefahr, mit unberechtigten Strafanzeigen überzogen zu werden, gehört quasi zum Berufsrisiko des Polizeibeamten, mit dem sich der einzelne abfinden muß. Die Einführung des Kriminalaktennachweises und die damit verbundene Möglichkeit, landes- oder bei bestimmten Delikten sogar bundesweit die Tatsache des Vorhandenseins von Kriminalakten abrufen zu können, hat auch für die Polizeibeamten selbst zu einer zusätzlichen Beeinträchtigung ihrer schutzwürdigen Belange geführt. Dies hat eine Eingabe eines Polizeibeamten deutlich gemacht. War ohne den automatisierten Kriminalaktennachweis bislang die Tatsache eines gegen einen Polizeibeamten gerichteten Ermittlungsverfahrens nur im engsten dienstlichen Umkreis des Polizeibeamten bekannt, ist diese Tatsache nun grundsätzlich jedem für den Kriminalaktennachweis abfrageberechtigten Polizeibeamten zugänglich. Weil manche Straftaten, deren die Polizeibeamten in ihrer dienstlichen Ausübung bezichtigt werden, sogenannte Amtsdelikte und damit teilweise Verbrechen sind, besteht diese Zugänglichkeit dann bundesweit.

Selbstverständlich steht auch einem Polizeibeamten das verfassungsrechtlich geschützte Persönlichkeitsrecht und die daraus abzuleitende Wahrung seiner schutzwürdigen Belange zu. Die Tatsache jedenfalls, daß Polizeibeamte in rechtmäßiger Ausübung ihres Dienstes bereits aufgrund ihrer Befugnisse und Tätigkeiten in erhöhtem Maße Ziel von Anzeigen und strafrechtlichen Ermittlungsverfahren werden können, muß bei der Entscheidung über die Speicherung im Kriminalaktennachweis und deren Dauer berücksichtigt werden.

4.4. Neuordnung der polizeilichen Meldewege

Zur Verbesserung der Information der einzelnen Polizeidienststellen, zum Erkennen überörtlicher Täter, zur Aufklärung von Straftaten, zum rechtzeitigen Handeln in Gefährdungssituationen und zur Konzentrierung polizeilicher Tätigkeit sind in den vergangenen Jahrzehnten eine Reihe von polizeilichen Meldewegen eingerichtet worden. Im letzten Tätigkeitsbericht hatte ich in diesem Zusammenhang festgestellt, daß die Einführung von automatisierten polizeilichen Dateien weitgehend ohne Auswirkungen auf die bisherigen Meldedienste geblieben ist, obwohl deren Funktionen weitgehend durch Dateien und entsprechende Abfragemöglichkeiten ersetzt worden sind. Dies führt teilweise zu unnötigen Mehrfachübermittlungen von Daten, die datenschutzrechtlich bedenkliche Doppelspeicherungen zur Folge haben können. Zum Teil werden mit diesen Meldewegen schlicht überflüssige Informationen übermittelt.

Auch zu den sogenannten **„Lage- oder Tagesmeldungen"** hatte ich darauf hingewiesen, daß mit dieser Übermittlung von personenbezogenen Informationen das Konzept der Abschottung, wie es mit dem „Informationssystem Bayer. Polizei", insbesondere mit dem automatisierten Kriminalaktennachweis vorgesehen ist, umgangen werden kann. Dies gilt jedenfalls dann, wenn Informationen auf diesem Wege übermittelt werden, deren Inhalt einen sinnvollen Bezug zu effektiven polizeilichen Tätigkeiten vermissen läßt und zur Erfüllung der Ziele „Erhebung der Sicherheitslage" und der „Fahndung und Ermittlung überörtlicher Täter" nicht geeignet ist. Als Beispiel für solche überflüssigen Übermittlungen hatte ich folgenden Fall beschrieben:

> Eine Polizeidienststelle hatte dem Landeskriminalamt, vier Polizeidirektionen und dem zuständigen Polizeipräsidium mitgeteilt, daß der Bürger H. wegen Volltrunkenheit in Schutzgewahrsam genommen und der Rentner A. zwei Schachteln Zigaretten im Wert von DM 7,– im Supermarkt entwendet hat.

Aufgrund meiner Prüfergebnisse hatte das Bayer. Staatsministerium des Innern zunächst angeordnet, daß die Übersendung der Lagemeldungen an das Landeskriminalamt ab sofort einzustellen sei.

Leider hat das Ministerium diese Weisung inzwischen revidiert und die Polizeibehörden aufgefordert, dem Bayer. Landeskriminalamt die Lage- und Tagesmeldungen in dem bis Oktober 1985 üblichen Umfang weiterhin zuzuleiten.

Sollten nun wieder unabhängig von der Bedeutung des Meldungsinhaltes für die Aufgabenerfüllung des Landeskriminalamtes personenbezogene Daten übermittelt werden, muß ich meine im letzten Tätigkeitsbericht geäußerten Bedenken wiederholen. Dies gilt insbesondere für Übermittlungen solcher Informationen, die nach dem KAN-Konzept nur im regionalen KAN zu speichern wären. Diese Informationen sollten wegen ihrer geringen Bedeutung gerade nicht dem Landeskriminalamt und den anderen Polizeidirektionen zugänglich sein. Ich habe das Bayer. Staatsministerium des Innern über meine Bedenken unterrichtet.

4.5. Bedeutungswandel der Spurendokumentationssysteme

Spurendokumentationssysteme (SPUDOK) sollen, wie ich bereits in früheren Tätigkeitsberichten vorgetragen habe, die Ermittlungsbehörden bei der Bearbeitung umfangreicher Ermittlungsverfahren unterstützen. Der Einsatz von Spurendokumentationssystemen soll es der Polizei erlauben, einen Überblick über eine Vielzahl von Hinweisen und Spuren jeder Art zu erhalten, die im Rahmen der polizeilichen Ermittlungstätigkeit angefallen sind.

Während Spurendokumentationssysteme zunächst nur für einzelne konkrete Ermittlungsverfahren eingesetzt worden sind, werden sie nun auch für

- Katastrophenfälle/Gefahrenabwehr (Einsatzdatei), zur
- Bewältigung und Vereinfachung von Verwaltungsaufgaben und als
- polizeiliches Führungsmittel eingesetzt.

Außerdem zeichnet sich eine nicht unproblematische Entwicklung ab. Spurendokumentationssysteme werden zunehmend zur Aufklärung sämtlicher Verfahren einer ganzen, bestimmten Deliktsgruppe herangezogen. Damit verschärfen sich aber die bisherigen Probleme, die in der Speicherung vieler nicht Tatverdächtiger und der prinzipiellen Möglichkeit liegen, daß Unschuldige aufgrund der Nutzung der umfangreichen Speicher- und Verknüpfungsmöglichkeiten sowie des Datenabgleichs mit anderen Datenbeständen durch eine „Verdachtsverdichtung" zu Verdächtigen werden. Wenn eine Vielzahl von Verfahren über einen längeren Zeitraum auf Spurendokumentationssystemen geführt werden, können prinzipiell sämtliche in einem Spurendokumentationssystem gespeicherte Personen, auch sogenannte dritte Personen wie Zeugen, Hinweisgeber, Geschädigte, Gefährdete, miteinander abgeglichen und verknüpft werden. Auch dies fördert das Risiko, daß Unschuldige zu Unrecht in Verdacht geraten.

Weil derzeit die gesetzlichen Regelungen für die polizeilichen Spurendokumentationen noch fehlen und damit die zum Schutz der Betroffenen notwendigen Schranken nicht festliegen, sehe ich die derzeitige Ausweitung der Spurendokumentationssysteme aus datenschutzrechtlicher Sicht mit Sorge.

4.6. Personengebundene Hinweise

Im polizeilichen Informationssystem, wie z. B. in der Datei „Kriminalaktennachweis" oder im INPOL-Verbund-System werden personengebundene Hinweise verwendet. Dies können Hinweise auf eventuelle Gewalttätigkeit, Geisteskrankheit, Fürsorgeerziehung oder Prostitutionsausübung sein, um nur einige zu nennen. Auf das grundsätzliche Problem bin ich insbesondere im letzten Tätigkeitsbericht eingegangen. Einzelprobleme habe ich auch im Zusammenhang mit meinen Überprüfungen (vergl. z. B. 4.3.2) angesprochen. Das Bayer. Staatsministerium des Innern hat erfreulicherweise diese Thematik noch einmal aufgegriffen und darauf hingewirkt, daß diese Probleme im zuständigen Arbeitskreis der Chefs der Landeskriminalämter erörtert werden. Ergebnisse liegen mir derzeit noch nicht vor.

Aufgefallen ist mir bei der Prüfung einer Polizeidirektion, die ungewöhnlich häufige Vergabe von sogenannten personengebundenen Hinweisen (PHW). Wie ich früher schon festgestellt habe, kann die Speicherung derartiger Hinweise die Ergreifung polizeilicher Maßnahmen nur aufgrund des Feldinhaltes veranlassen und ganz allgemein zu einer sozialen Abstempelung der Betroffenen führen. PHW stellen nur bruchstückhafte Informationen dar, deren Aktualität ohnehin häufig nichtgewährleistet ist. So war mir insbesondere die hohe Anzahl der PHW „geistesschwach" und „geisteskrank" aufgefallen. Die Tatsache des Tätigwerdens der Polizei im Rahmen des Unterbringungsgesetzes scheint mir allein nicht ausreichend zu sein für die Vergabe eines solchen Hinweises. Der Polizei dürfte in der Regel das notwendige ärztliche Wissen fehlen, um entsprechende Bewertungen anzustellen.

4.7. Berichtigung der Deliktbezeichnung

Nach Abschluß des Ermittlungsverfahrens oder nach Ausgang des gerichtlichen Verfahrens kann sich die rechtliche Beurteilung eines Sachverhaltes vielfach anders darstellen, als dies zum Zeitpunkt der Einleitung der polizeilichen Ermittlungen der Fall gewesen ist. Dies kann zur Folge haben, daß eine Straftat beispielsweise statt als Verbrechen „nur noch" als Vergehen zu bewerten ist und sich somit beispielsweise bei der polizeilichen Speicherung Auswirkungen auf die Speicherungsebene (Bundes-KAN oder Landes-KAN) ergeben können. Eine Berichtigung und ggf. Löschung von Daten sind insbesondere dann erforderlich, wenn das Verfahren eingestellt worden ist oder mit Freispruch geendet hat.

Die Löschung unrichtiger oder zumindest zu Unrecht belastender personenbezogener Daten ist ein wesentliches Datenschutzrecht. Wegen dessen besonderer Bedeutung bei Sicherheitsbehörden besteht neben der Regelung im Bayer. Datenschutzgesetz auch eine entsprechende Verwaltungsvorschrift in den Richtlinien für kriminalpolizeiliche Sammlungen. Es genügt freilich nicht, wenn eine Polizeibehörde nur die bei ihr gespeicherten Daten löscht. Waren diese Daten zuvor an andere Behörden übermittelt worden, muß auch bei diesen gelöscht werden. Nicht hinnehmbare Folgen, wenn dies nicht geschieht, zeigt der nachfolgende Fall:

> Gegen einen Petenten wurde wegen Verdachts des Raubes von einer Polizeibehörde ermittelt. Nachdem sich bei der Gegenüberstellung mit dem Opfer herausgestellt hatte, daß der Petent nicht

der Täter sein konnte, wurde das Ermittlungsverfahren von der zuständigen Staatsanwaltschaft nach § 170 Abs. 2 Strafprozeßordnung eingestellt. Die ermittelnde Polizeibehörde hat angesichts dieser Sachlage die zum Petenten angelegten Kriminalakten zu Recht vernichtet und dies dem Petenten auf Anfrage auch mitgeteilt.

Weil der Petent bei einer Routinekontrolle „Schwierigkeiten" hatte, wandte er sich mit der Bitte um Prüfung an mich, ob aus dem eingestellten Ermittlungsverfahren noch Daten bei der Polizei vorhanden sind. Dabei habe ich festgestellt, daß beim Bayer. Landeskriminalamt, dem die ermittelnde Polizeibehörde die Tatsache des Ermittlungsfahrens gegen den Petenten im Wege einer Erkenntnisanfrage mitgeteilt hatte, diese Informationen noch gespeichert waren. Tatsächlich hatte es die ermittelnde Polizeibehörde bei Vernichtung der bei ihr zum Petenten angelegten Kriminalakte versäumt, dem Landeskriminalamt über den Verfahrensausgang nachzuberichten. Aufgrund meiner Prüfung ist dies nun geschehen und sind die den Petenten belastenden Daten auch beim Landeskriminalamt vernichtet worden.

Aus datenschutzrechtlicher Sicht ist es grundsätzlich erforderlich, bei Veränderungen wesentlicher Gesichtspunkte den Stellen nachzuberichten, die vom Verdacht gegen einen Betroffenen unterrichtet worden sind, um dadurch der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken. Dies gilt insbesondere dann, wenn belastende Unterlagen über einen Betroffenen vernichtet werden. Es genügt nicht, daß in einer Dienststelle nur die eigenen Unterlagen bereinigt werden, wenn andere Stellen, insbesondere Zentralbehörden, die unrichtigen Daten weiter verarbeiten. Die datenschutzrechtliche Löschung von Daten ginge andernfalls zumindest teilweise ins Leere. Auch für den Betroffenen würde, insbesondere wenn ihm die Vernichtung der ihn betreffenden Unterlagen bestätigt worden ist, zu Unrecht ein Vertrauenstatbestand geschaffen.

Gleiches muß immer dann gelten, wenn die ermittelnde Polizeibehörde erfährt, daß der Betroffene rechtskräftig freigesprochen worden ist. Auch hier ist den Stellen, denen zuvor der Verdacht mitgeteilt worden war, der Freispruch nachzuberichten.

4.8. Weitere Einzelfragen

4.8.1. Freiwillige Fingerabdrücke

In einer niederbayerischen Ortschaft ist eine Frau ermordet worden. Der Täter war über eine Leiter in das Zimmer seines Opfers gestiegen. Weil die Leiter aus der Ortschaft stammte, vermutete die Kriminalpolizei den Täter unter den männlichen Dorfbewohnern. Nach Diskussionen im örtlichen Gemeinderat und im Lehrerkollegium eines nahegelegenen Gymnasiums wurden alle männlichen Bewohner der Ortschaft (zwischen 16 und 60 Jahre) zur freiwilligen Abgabe von Finderabdrücken aufgefordert. Den Männern war zugesichert worden, daß nach Beendigung der Überprüfung die entstandenen erkennungsdienstlichen Unterlagen entweder vernichtet oder dem Betroffenen ausgehändigt würden. Diese Aktion, die leider nicht zur Ergreifung des Täters geführt hat, ist, wie mir versichert worden ist, inzwischen abgeschlossen. Weder beim Landeskriminalamt noch bei der zuständigen Kriminalpolizeiinspektion befinden sich noch erkennungdienstliche Unterlagen.

Es gibt keinen Zweifel, daß die Polizei zur Aufklärung einer so schweren Straftat wie die eines Mordes ihre Befugnisse ausschöpfen muß. Gerade weil die Polizei andererseits für die Aufklärung solcher Straftaten umfangreiche Befugnisse besitzt, sollte mit „freiwilligen" Datenerhebungen besonders vorsichtig umgegangen werden. Auch Beschlüsse im Gemeinderat und Besprechungen in einem Lehrerkollegium dürfen nicht zu einer faktischen Ausweitung der der Polizei für erkennungsdienstliche Behandlungen gesetzlich zugewiesenen Befugnisse führen.

4.8.2. Übermittlung von Sozialdaten

Sozialdaten sind durch das Sozialgeheimnis besonders geschützt. Ihre Offenbarung ist nur aufgrund der in den §§ 68 ff SGB X genannten Fällen oder mit Einwilligung des Betroffenen zulässig. Nach § 68 SGB X können der Polizei Name, Geburtsdaten, Anschrift sowie bestimmte Arbeitgeberdaten übermittelt werden, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Das Polizeipräsidium München und die AOK München haben für die rechtmäßige Abwicklung dieser Amtshilfe eine Vereinbarung getroffen. Der Landesbeauftragte für den Datenschutz hat wie schon in früheren Jahren, auch im Berichtszeitraum bei mehreren Dienststellen des Polizeipräsidums München Kontrollen durchgeführt, um die Zulässigkeit der Datenanfrage durch Polizeibeamte des Polizeipräsidiums München bei der AOK München strichprobenartig zu überprüfen. Hierbei hat sich in keinem Fall ein Anlaß zu einer Beanstandung ergeben. Alle Anfragen haben, soweit erkennbar, den Grundsatz der Verhältnismäßigkeit berücksichtigt und sind bei der AOK erst erfolgt, nachdem bei anderen Stellen die erforderlichen Auskünfte nicht zu erhalten waren. Die AOK hat in diesen Fällen nur die vom Gesetz zugelassenen Auskünfte erteilt.

Mit der AOK München und dem Polizeipräsidium München besteht Einvernehmen bei der Auslegung von § 68 SGB X dahingehend, daß im Hinblick auf den Grundsatz der Verhältnismäßigkeit zur Verfolgung einfacher Ordnungswidrigkeiten grundsätzlich keine Anfragen an die AOK gerichtet werden. Dies geschieht in der Praxis auch grundsätzlich nicht und wäre etwa im Hinblick auf die über 1 Million Verkehrsordnungswidrigkeiten, die im Bereich des Polizeipräsidiums München zu erledigen sind, auch gar nicht möglich. Das Polizeipräsidium München wird durch geeignete Maßnahmen sicherstellen, daß auch künftig Anfragen bei geringfügigen Ordnungswidrigkeiten grundsätzlich vermieden werden.

4.9. Novellierung des Polizeirechts

Die Notwendigkeit der Novellierung des Polizeirechts und insbesondere die Aufnahme präziser Regelungen für die polizeiliche Datenverarbeitung in das Polizeiaufgabengesetz sind allenthalben unbestritten. Zwischenzeitlich liegt auch ein neuer „Vorentwurf zur Änderung des Musterentwurfes eines einheitlichen Polizeigesetzes des Bundes und der Länder" (Stand 12.3.1986) vor. Die weiteren Arbeiten an diesem Entwurf scheinen jedoch im Hinblick auf einen Beschluß der Innenministerkonferenz zu ruhen, mit dem der Bundesminister der Justiz zu einer entsprechenden Novellierung der Strafprozeßordnung aufgefordert worden ist. Diese zweifelsohne notwendige Abstimmung der entsprechenden gesetzlichen Regelungen im Polizeirecht und der Strafprozeßordnung darf meines Erachtens nicht dazu führen, daß sich die Novellierung des Polizeirechts über

Gebühr verzögert. Dies gilt in ganz besonderem Maße für Bayern, weil der Bayer. Verfassungsgerichtshof in seiner Entscheidung vom 9.7.1985 ausdrücklich festgestellt hat, daß die Führung und Auswertung von kriminalpolizeilichen Sammlungen durch den Gesetzgeber geregelt werden müsse. Zwar hat auch der Verfassungsgerichtshof festgestellt, daß die derzeit bestehende Regelungslücke für eine gewisse Übergangszeit hingenommen werden müsse. Die vom Gericht damit eingeräumte Frist dürfte jedoch nach den Grundsätzen, die von der Verfassungsrechtsprechung hier üblicherweise angelegt werden, wohl mit Ende der nun begonnenen Legislaturperiode ablaufen. Gegebenenfalls wird sich der bayerische Gesetzgeber genötigt sehen, bereits vor einer an sich notwendigen Abstimmung mit den entsprechenden Regelungen in der Strafprozeßordnung in das Polizeiaufgabengesetz Bestimmungen zur polizeilichen Datenverarbeitung aufzunehmen.

Musterentwurf

Für die bevorstehende Novellierung des Bayer. Polizeiaufgabengesetzes stellt der derzeit vorliegende Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes eine wesentliche Grundlage dar. Deshalb gebe ich eine kurze datenschutzrechtliche Bewertung dieses Entwurfes:

Als datenschutzrechtlicher Bewertungsmaßstab kann nach wie vor der von den Datenschutzbeauftragten der Länder und des Bundes am 24.1.1985 gefaßte Beschluß zu den „Anforderungen an Datenschutzregelungen im Polizeirecht" gelten. Hiernach ist zweifelsfrei festzustellen, daß der neueste Entwurf aus datenschutzrechtlicher Sicht zum Teil erhebliche Verbesserungen gegenüber den früheren Formulierungen enthält. Dies betrifft z. B. die Regelungen zur Aufnahme der Zweckbindung bei der Datenverarbeitung, die Regelungen zur Datenerhebung und zur Datenübermittlung sowie die Aufnahme auch der Datenverarbeitung in Akten in den Entwurf.

Allerdings ist neben der noch ausstehenden Harmonisierung mit den entsprechenden Änderungen der Strafprozeßordnung auch festzustellen, daß eine Reihe von Regelungen noch wesentlich präziser gefaßt werden sollte. So bleibt bei der Festlegung des zulässigen Umfangs der Datenverarbeitung beispielsweise noch offen, welche Personengruppen in welcher Weise gespeichert werden dürfen, inwieweit personengebundene Hinweise aufzunehmen sind und unter welchen Voraussetzungen Kriminalakten angelegt werden dürfen. Diskussionsbedürftig sind nach wie vor die Regelungen zur „vorbeugenden Bekämpfung von Straftaten" sowie zur „Vorsorge zur Gefahrenabwehr". Ohne sämtliche Kritikpunkte nennen zu wollen, sei noch auf Probleme hingewiesen bei Bild- und Tonaufzeichnungen im Zusammenhang mit der Beobachtung von Versammlungen, bei der Datenerhebung über Kontakt- und Begleitpersonen im Wege der Observation und bei den Voraussetzungen zur polizeilichen Beobachtung. Das Recht auf informationelle Selbstbestimmung fordert in stärkerem Maße als bisher vorgesehen, den Bürger über ihn betreffende Datenerhebungen, etwa bei der polizeilichen Beobachtung, spätestens nach Beendigung der Maßnahmen grundsätzlich zu unterrichten. Auch dürfen die von mir an sich begrüßten Regelungen zu Vorgangsverwaltung und Dokumentation durch eine fehlende enge Zweckbestimmung nicht zu einer andere Regelungen umgehenden Datenauswertung führen.

Im Hinblick auf die in den letzten Jahren festzustellende Entwicklung der Entwürfe zum Musterentwurf eines einheitlichen Polizeigesetzes bin ich optimistisch, daß das künftige Polizeirecht die datenschutzrechtlichen Belange weitgehend berücksichtigen wird.

4.10. Grenzpolizei

4.10.1. Personenkontrollen durch die Bayer. Grenzpolizei

Auch in diesem Berichtszeitraum haben sich wiederum zahlreiche Bürger an mich gewandt, die von der Bayer. Grenzpolizei beim Überschreiten der Grenze oder im Zollgrenzbezirk kontrolliert worden sind. Dabei werden immer wieder Befürchtungen geäußert, Ausweisdaten würden maschinell gelesen und dann möglicherweise gespeichert oder auf andere Weise notiert und festgehalten. Teilweise wird auch bei gründlicheren Kontrollen im Einzelfall der Verdacht geäußert, daß möglicherweise unrichtige Daten der Anlaß hierzu gewesen sein könnten.

Hierzu ist folgendes festzustellen:

Rechtsgrundlagen für die polizeiliche Kontrolle des grenzüberschreitenden Verkehrs an allen Auslandsgrenzen Bayerns sind das Bundesgrenzschutzgesetz, das Bayer. Polizeiorganisationsgesetz und das Polizeiaufgabengesetz. Die polizeiliche Kontrolle des grenzüberschreitenden Verkehrs umfaßt hierbei neben der Prüfung etwa erforderlicher Grenzübertrittspapiere auch die Grenzfahndung sowie die Beseitigung von Störungen und die Abwehr von Gefahren, die ihren Ursprung außerhalb des Bundesgebietes haben. Grenzpolizeiliche Maßnahmen im Rahmen der oben angeführten Bestimmungen können auch eine fahndungsmäßige Überprüfung einzelner Bürger umfassen. Hierzu kann es im Einzelfall erforderlich sein, daß sich die Polizeibeamten die fahndungsrelevanten Daten – in der Regel sind dies die Personalien – für die Anfrage an den Datensichtgeräten in ihren Dienststellen auf Notizzetteln vormerken. An manchen Grenzübergängen werden im Rahmen der Grenzkontrolle die Personalpapiere auf Kontrollgeräte aufgelegt, die zu Unrecht mit Kopierautomaten verwechselt werden.

Meine Ermittlungen haben in allen Fällen ergeben, daß handschriftliche Notizen nach erfolgter Überprüfung durch die Grenzpolizeibeamten stets vernichtet worden sind. Eine Speicherung derartig erhobener Fahndungsdaten findet nicht statt. Auch die zum Fahndungsabgleich mit dem Lesegerät gelesenen Daten sind nicht abgelichtet oder sonst gespeichert worden. Soweit im Einzelfall intensivere Kontrollen durchgeführt worden sind, war dies nicht auf unrichtige Daten zur Person des Kontrollierten zurückzuführen, sondern beruhte auf anderen im Einzelfall nicht zu rügenden polizeitaktischen Erwägungen.

4.10.2. Prüfung einer Grenzpolizeiinspektion

Die Zulässigkeit der Speicherung personenbezogener Daten war Gegenstand einer Prüfung bei einer Grenzpolizeiinspektion. Zwar habe ich dabei keine bedeutsamen Verletzungen des Datenschutzrechts festgestellt. Allerdings mußte ich auch hier rügen, daß Sachverhalte personenbezogen in kriminalpolizeilichen Sammlungen erfaßt werden, deren Speicherung nicht erforderlich war oder die allenfalls über einen kürzeren Zeitraum hätten gespeichert werden dürfen. Auffallend war auch hier die doch umfangreiche Speicherung von Ordnungswidrigkeiten als alleiniger Sachverhalt zu einer Person. Als Beispiele können dienen:

- Ein Bürger hatte vergessen, den im Zuständigkeitsbereich der Grenzpolizeiinspektion liegenden Zweitwohnsitz anzumelden.
- Finnische Staatsbürger hatten beim Grenzübertritt Ordnungswidrigkeiten begangen. Weil bei diesen Personen anzunehmen ist, daß sie diesen Grenzübergang wohl nicht mehr überschreiten, war eine Speicherung etwa zur „Gefahrenabwehr" nicht erforderlich.

Auch die Vergabe der Aussonderungs-Prüffristen ist nach dem Ergebnis der durchgeführten Stichproben bisher zu schematisch und an den Regelfristen orientiert erfolgt. Die Aussonderung als solche war im Rahmen der selbst gesetzten Fristen im übrigen korrekt.

Das Präsidium der Bayer. Grenzpolizei hat mir mitgeteilt, daß es alle Dienststellen der Grenzpolizei darauf hingewiesen hat, die Aussonderungsfristen flexibler und in Fällen geringerer Bedeutung grundsätzlich kürzer festzulegen.

Zu den Staatsschutzangelegenheiten siehe Punkt Staatsschutz.

4.11. Polizeilicher Staatsschutz

4.11.1. Führung der Vorgänge

Im Berichtszeitraum habe ich bei drei Staatsschutzdienststellen der Polizei und bei einer Grenzpolizeiinspektion, soweit sie Staatsschutzangelegenheiten erledigt, kurze datenschutzrechtliche Prüfungen durchgeführt. Bei derartigen Prüfungen lasse ich mich von folgendem Grundsatz leiten: Informationen und Daten, die von Staatsschutzdienststellen verarbeitet werden, bedürfen wegen ihrer besonderen Sensibilität und der aus der Natur der Sache vergleichsweise engen Beziehung zum Verfassungsschutz vor einer personenbezogenen Erfassung in Kriminalakten oder auf Karteikarten einer besonders kritischen Prüfung hinsichtlich Richtigkeit und Erforderlichkeit der Speicherung. Ich verkenne andererseits nicht, daß dem polizeilichen Staatsschutz eine wichtige Bedeutung zukommt, die auch eine ausreichende, an den Aufgaben des Staatsschutzes orientierte Datenspeicherung verlangt.

Wie in den zurückliegenden Jahren habe ich die bekannt unerfreulichen Feststellungen treffen müssen:

- Karteikarten gehen noch auf weit zurückliegende Zeiten zurück und sind bislang noch nicht überarbeitet worden.
- Vorgänge sind personenbezogen verkartet, die mit der eigentlichen Aufgabenerfüllung des Staatsschutzes nichts zu tun haben.
- Gleiches gilt für Vorgänge, die lediglich dem Nachweis der Tätigkeit der Behörde dienen.
- Auch ist eine sachgerechte Aussonderung der von den Staatsschutzkommissariaten verwahrten Unterlagen anhand der Suchkarteien vielfach nicht möglich, weil auf den Karteikarten teilweise die Wiedervorlagedaten fehlen; eine erfreuliche Ausnahme ist hier die Staatsschutzkartei des Polizeipräsidiums München.
- Die Wiedervorlagefristen werden starr und schematisch vergeben. Vielfach wird auch für Sachverhalte Erwachsener zu unkritisch eine Überprüfungsfrist von 10 Jahren vergeben, so bei Verfahrenseinstellungen nach § 170 Abs. 2 StPO, bei betagten Mitbürgern oder Ausländern, die sich als Touristen in München aufgehalten haben. Im übrigen sind die eingetragenen Wiedervorlagedaten häufig falsch. So wird der Beginn der Frist falsch berechnet oder wird für Heranwachsende statt der vorgeschriebenen 5 Jahre regelmäßig eine 10-Jahres-Frist vergeben. Dabei ist gerade die richtige Vergabe von Aussonderungsdaten Voraussetzung für eine effektive Aussonderung.
- Auch fehlt es teilweise an der Abstimmung der Karteien mit den zugehörigen Kriminalakten. So finden sich bei Staatsschutzdienststellen noch Karteikarten, obwohl die zugehörige Akte bereits ausgesondert ist. Noch bestehende Kriminalakten sind wegen fehlender Karteikarten nicht zugänglich.
- Beim Staatsschutz wurden Vorgänge festgestellt, die lediglich allgemeine kriminalpolizeiliche Erkenntnisse enthalten. Hier besteht die Gefahr, daß trotz Löschung dieser Daten in den allgemeinen kriminalpolizeilichen Sammlungen, was ich auch tatsächlich festgestellt habe, diese beim Staatsschutz unzulässig bestehenden Informationen auf Anfrage hin noch weiter verbreitet werden können.

Folgende Beispiele mögen meine Kritik belegen:

- Eine Person, die der Häftlingsüberwachung im Terrorismusbereich unterliegt, hatte bei einem Versandhaus Textilien bestellt. Nun ist das Versandhaus in der Staatsschutzkartei erfaßt.
- Vor vielen Jahren stand ein Auto vor einem Überwachungsobjekt. Obwohl die Erkenntnismitteilung über den Kraftfahrzeughalter negativ war, also keine Erkenntnisse erbracht hatte, ist der Halter nach wie vor in der Kartei erfaßt.
- Gegen eine Person bestand vor 7 Jahren der Verdacht nachrichtendienstlicher Tätigkeit. Obwohl die Ermittlungen längst ergeben hatten, daß der Verdacht haltlos war, ist die Person weiterhin gespeichert. Selbst eine Anfrage des Bundeskriminalamts nach dem Verfahrensausgang zum Zwecke der Aktenbereinigung war für dieses Kommissariat kein Anlaß, die eigene Speicherung kritisch zu überdenken.
- Außerhalb Bayerns brannte ein Reisebüro nach Brandstiftung aus. Im Zuge der Täterermittlung wurden auch die Kunden des Reisebüros überprüft. Über einen im Zuständigkeitsbereich eines bayerischen Staatsschutzkommissariats wohnhaften Kunden wurde an die sachbearbeitende außerbayerische Dienststelle mitgeteilt, daß keine Erkenntnisse über ihn vorliegen. Gleichwohl wurde wegen dieses Vorgangs eine Karteikarte beim Staatsschutz personenbezogenen angelegt.
- Regelmäßig werden Personen verkartet, zu denen auf eine polizeiliche Anfrage hin keine Erkenntnisse festgestellt und mitgeteilt worden sind. Hier wären allenfalls Nachweise in einer sogenannten Vorgangsverwaltung über die Erledigung der Anfrage vertretbar.
- Eine Person ist gespeichert, weil sie im Hause eines Verlages gegen die übertriebene Darstellung von Frauen in Pornomagazinen protestiert hatte.
- Gerade im Staatsschutzbereich ist eine sorgfältige Arbeit besonders notwendig. Dieses Gebot ist von einem Staatsschutzkommissariat in einem auch in der Öffentlichkeit bekanntgewordenen Fall verletzt worden, weil zu einem Stadtrat, der Mitglied in einer demokratischen Partei ist, völlig zu Unrecht der Hinweis „DKP-Sympathisant" eingetragen worden war.

Ich habe die geprüften Staatsschutzdienststellen aufgefordert, die festgestellten Mängel zu beheben, die Unterlagen, soweit erforderlich, dringend zu überprüfen und insbesondere darauf zu achten, daß bloße Tätigkeitsnachweise allenfalls in einer Vorgangsverwaltung registriert werden, die lediglich Verwaltungszwecken dient.

Das Bayer. Staatsministerium des Innern hat auf meine Kritik die Bayer. Polizeidienststellen aufgefordert, die bestehenden Staatsschutzkarteien zu bereinigen und, abgestimmt auf die Bedeutung der Angelegenheit im Einzelfall, unterschiedliche Aufbewahrungs- und Überprüfungsfristen festzulegen. An die Staatsschutzdienststellen ist die Weisung ergangen, Verwaltungsvorgänge nicht in die Staatsschutzkartei aufzunehmen, sondern gesondert zu verwahren, ferner wurde die Empfehlung ausgesprochen, exakte Feststellungsanordnungen für bereits bestehende Staatsschutzkarteien zu erlassen.

Ich begrüße diese Weisungen des Bayer. Staatsminsteriums des Innern und gehe davon aus, daß künftig die Datenschutzbelange auch beim Staatsschutz ausreichend berücksichtigt werden. Inzwischen haben eine Reihe von Polizeipräsidien auf der Grundlage der vom LKA bereits vor Jahren herausgegebenen Anordnung detaillierte Feststellungsanordnungen erlassen.

4.11.2. Informationsaustausch

Für den Staatsschutzbereich bestehen mehrere Richtlinien, die den Informationsaustausch zwischen den einzelnen Staatsschutzbehörden, zu Zentralbehörden wie Landes- und Bundeskriminalamt und zum Verfassungsschutz regeln. Solange diese Datenübermittlungen allerdings nicht in Gesetzen und präziser als bisher geregelt sind, muß dafür Sorge getragen werden, daß im Wege dieses Informationsaustausches allenfalls solche Staatsschutzerkenntnisse an andere Stellen übermittelt werden, die für die von den bestehenden Richtlinien verfolgten Zwecke und für die Aufgabenerfüllung der Datenempfänger im Einzelfall unbedingt erforderlich sind. Soweit in diesen Richtlinen lediglich generalklauselartig formulierte Bestimmungen anordnen, daß alle jene Straftaten und Sachverhalte von Staatsschutzbehörden weiter übermittelt werden müssen, die im weitesten Sinne einen Zusammenhang mit politischen Themen aufweisen und deren Sachbearbeitung deshalb von den Staatsschutzdienststellen wahrgenommen wird, bestehen derzeit für derartige Eingriffe keine ausreichenden Rechtsgrundlagen. Bis diese Rechtsgrundlagen geschaffen sind, müssen derartige Übermittlungsregelungen in Staatsschutzrichtlinien so eng gefaßt werden, daß nur die zur Aufrechterhaltung einer ordnungsgemäßen Arbeit des Staatsschutzes unbedingt erforderlichen Sachverhalte übermittelt werden. Andernfalls würde in bedenklicher Weise ohne Rechtsgrundlage unverhältnismäßig in das Recht auf informationelle Selbstbestimmung der Betroffenen durch Staatsschutzbehörden eingegriffen.

Ich begrüße es, daß das Bayer. Staatsministerium des Innern meine Vorbehalte gegen generalklauselartige Übermittlungsregelungen in den Staatsschutzrichtlinien (z. B. Kriminalpolizeilicher Meldedienst in Staatsschutzsachen) teilt und meiner Auffassung ausdrücklich zustimmt, daß keineswegs alle Straftaten und Sachverhalte unter einem Auffangtatbestand subsumiert werden können, nur weil sie einen „politischen" Hintergrund haben. Es ist auch erfreulich, daß sich ein Arbeitskreis der Innenministerkonferenz mit diesem Problem befaßt und eine Neufassung für diese Regelung ausgearbeitet hat. Allerdings wird meines Erachtens auch diese Neuformulierung den Umfang der Sachverhalte, die unter den Auffangtatbestand eingeordnet werden und somit den Melde- und Erfassungspflichten dieses Meldedienstes unterliegen, nicht im beabsichtigten Maße beschränken. Auch habe ich Zweifel, ob die Neuregelung den Sachbearbeitern vor Ort – und dies scheint mir besonders wichtig zu sein – wirklich klare Hinweise zur Behandlung des Einzelfalls an die Hand geben kann. Grundsätzlich ist die Neufassung lediglich eine etwas umfangreicher gefaßte Wiedergabe der schon bisher bestehenden Kriterien für eine Datenübermittlung. Wesentliche Fragen bleiben meines Erachtens nach wie vor offen: Welche Anhaltspunkte sind beispielsweise zur Beurteilung des Motivs des Täters erforderlich? Wie muß die Verbindung zu einer Organisation aussehen, damit die Voraussetzungen für eine Meldung erfüllt sind? Auch das angegriffene Objekt allein kann kein genügendes Entscheidungskriterium sein, um zwischen Gegnern der freiheitlich demokratischen Grundordnung und anderen sich im politischen Rahmen legal bewegenden Personen zu unterscheiden.

Außerdem ist noch folgendes zu bedenken: Besteht neben präzisen Übermittlungsregelungen für Täter schwerwiegender Staatsschutzdelikte eine Übermittlungsregelung für sonstige Fälle, so muß gerade diese besonders klar und detailliert sein. Andernfalls kann die Bereitschaft gefördert werden, die Zulässigkeit von Datenübermittlungen nicht an Hand der strengen Einzelregelungen, sondern auf der Grundlage der allgemeinen Regelung zu prüfen.

Folgender Fall, über den bereits mehrfach in der Presse berichtet worden ist, mag meine Bedenken gegen den derzeitigen Vollzug der Staatsschutzmeldedienste belegen:

> In einer bayerischen Stadt hatte eine Heldengedenkfeier der NPD stattgefunden. 8 Personen hatten eine Gegendemonstration abgehalten, ohne diese beim zuständigen Landratsamt angemeldet zu haben. Über diese Tatsache hat das zuständige Staatsschutzkommissariat personenbezogene Meldungen im Rahmen eines Meldedienstes in Staatsschutzangelegenheiten über das Bayer. Landeskriminalamt an das Bundeskriminalamt gesandt. Das Bundeskriminalamt hat die Daten in NADIS (Nachrichtendienstliches Informationssystem) eingespeichert. Abgesehen von der Tatsache, daß die Teilnahme einiger Betroffener an der Veranstaltung nicht erwiesen war, und somit falsche Informationen übermittelt und gespeichert worden sind, stellt sich hier bereits die Frage, ob in so einem Fall tatsächlich eine Berichterstattung im Wege eines Meldedienstes in Staatsschutzangelegenheiten für die Aufgabenerfüllung des Landes- und Bundeskriminalamtes erforderlich war. Ich jedenfalls vermochte eine Erforderlichkeit im vorliegenden Fall nicht zu erkennen. Zwar sind die entsprechenden Daten mittlerweile bei den mit der Angelegenheit befaßten und bei den in Kenntnis gesetzten Behörden gelöscht, doch waren Beeinträchtigungen schutzwürdiger Belange der Betroffenen während der Speicherungsdauer nicht auszuschließen.

Ich habe diesen Fall zum Anlaß genommen, das Bayer. Landeskriminalamt zu bitten, darauf hinzuwirken, vor der Weiterleitung derartiger Meldungen deren Erforderlichkeit besonders sorgfältig zu prüfen. Dies gilt gerade im Hinblick auf die seit Anfang dieses Jahres betriebene Datei APIS (siehe dort).

4.11.3. Errichtung einer Arbeitsdatei PIOS – Innere Sicherheit (APIS)

Zur Datei APIS hatte ich im 7. Tätigkeitsbericht einige Bedenken angemeldet. Diese beruhen in der Zusammenführung bisher getrennter Datenbestände zur Terrorismusbekämpfung und zum polizeilichen Staatsschutz, der aufgrund seiner Zuständigkeit auch viele Taten von vergleichsweise geringfügiger Bedeutung zu verfolgen hat. Außerdem werden durch den Einsatz dieses Verfahrens erheblich erweiterte Möglichkeiten der Aktenerschließung einschließlich der Möglichkeit zur Speicherung sogenannter „anderer Personen" eröffnet, also von Personen, die nicht Verdächtige sind.

Der Bundesminister des Innern hat sich mit meinen Bedenken detailliert auseinandergesetzt. Obwohl ich mich einer Reihe seiner Argumente etwa über die fachliche Notwendigkeit, Informationen aus dem Terrorismus- und dem Extremismusbereich bzw. aus dem Bereich der Staatsgefährdung unter bestimmten Voraussetzungen zusammenzulegen, nicht verschließen möchte, habe ich gegen die derzeitige Handhabung der Datei APIS dennoch einige Bedenken. Sie betreffen die parallele Führung weiterer Dateien neben APIS, die fehlende Abstimmung der Datei APIS mit den Meldediensten im Staatsschutzbereich und die nicht geklärten Fragen des Zugangs des Verfassungsschutzes zu Staatsschutzdaten. Derzeit fehlen überdies noch ausreichende Rechtsgrundlagen für diesen Bereich. Nach wie vor wird bei der Führung der Datei APIS nicht genügend zwischen Straftaten im Terrorismusbereich sowie schweren Staatsschutzdelikten einerseits und weniger schwerwiegenden Straftaten aus dem Staatsschutzbereich wie z. B. Farbschmierereien, Beleidigungen, Hausfriedensbruch andererseits unterschieden. Dies gilt sowohl hinsichtlich der Tatsache der Erfassung dieser Delikte als auch hinsichtlich des Umfangs der im Einzelfall zu speichernden Daten. Bei einer schweren Straftat mögen zur Aufgabenerfüllung mehr Daten erforderlich sein als bei Straftaten geringerer Bedeutung. Auch eine Abschottung zwischen Straftaten von örtlicher und überörtlicher Bedeutung ist derzeit nicht vorgesehen, so daß in die Datei APIS eingestellte Straftäter, unabhängig von der Bedeutung der Straftat, bundesweit abrufbar sind. Auch die Speicherung von anderen Personen wie Geschädigten, Gefährdeten oder Kontaktleuten ist aus datenschutzrechtlicher Sicht noch nicht befriedigend gelöst. Nach wie vor vertrete ich die Auffassung, daß beispielsweise Geschädigte und Gefährdete vor ihrer Einspeicherung in die Datei APIS um ihre Einwilligung gefragt werden sollten. Sollte die Einholung der Einwilligung im Einzelfall unpraktikabel sein, müßten diese Betroffenen zumindest nachträglich von der Tatsache der Speicherung unterrichtet werden. Meines Erachtens stellen die Speicherung in APIS und die Übermittlung aus APIS auch für Geschädigte und Gefährdete ein Risiko wegen einer nicht auszuschließenden Gefährdung ihrer schutzwürdigen Belange dar. Bereits eine Fehlinterpretation der Tatsache, daß ein Betroffener in APIS gespeichert ist, kann zu einer solchen Beeinträchtigung schutzwürdiger Belange führen.

Derzeit ist m. E. noch nicht hinreichend sichergestellt, daß über die verschiedenen Meldewege im polizeilichen Staatsschutz nur solche personenbezogenen Informationen an das Landeskriminalamt und an das Bundeskriminalamt mit der Folge einer Speicherung in die Datei APIS gelangen, die hinreichend auf ihre Richtigkeit und ihre Bedeutung überprüft sind. Aus datenschutzrechtlicher Sicht ist wegen der oben bereits genannten Mehrfachspeicherung von Daten in verschiedenen Dateien weiterhin kritisch zu beachten, daß somit für möglicherweise gleiche Informationen unterschiedliche Zugriffsberechtigungen und unterschiedliche Aussonderungsfristen bestehen. Dies läßt sich weder mit der auch für die Polizeibehörden notwendigen Überschaubarkeit der Datenflüsse und Datensammlungen vereinbaren noch mit den Grundsätzen des Rechts auf informationelle Selbstbestimmung, nach denen der Bürger wissen können muß, wer was wann über ihn weiß. Die Probleme können sich grundsätzlich noch verschärfen, wenn in die Datei APIS Bürger bereits aufgrund bloßer Erkenntnisanfragen bei Beginn von Ermittlungen gespeichert werden, obwohl möglicherweise nur erste vage Verdachtsmomente abgeklärt werden sollen. Die Richtigkeit der in APIS gespeicherten Informationen ist auch dann nicht gewährleistet, wenn der Ausgang von Ermittlungs- oder Strafverfahren nicht berücksichtigt wird. Gerade bei einer Staatsschutzdatei können im besonderen Maße schutzwürdige Belange durch unvollständige oder unrichtige Daten beeinträchtigt werden.

Es gibt keinen Zweifel, daß die Polizei gerade auch im Staatsschutzbereich wichtige Aufgaben zu erfüllen hat und hierfür die notwendigen Informationstechniken einsetzen muß. Ich kann mich jedoch des Eindruckes nicht erwehren, daß im Bundesgebiet für den Staatsschutzbereich eine geschlossene Konzeption des Meldeverfahrens, der Speicherungen und der Auskünfte derzeit noch fehlt und damit nicht nur möglichen Gefährdungen für den gesetzestreuen Bürger mangels dieser Konzeption nicht ausreichend begegnet werden kann, sondern auch die Effizienz polizeilicher Dateien leidet.

5. Verfassungsschutz

5.1. Prüftätigkeit beim Bayer. Landesamt für Verfassungsschutz

Meine Prüftätigkeit beim Bayer. Landesamt für Verfassungsschutz hat sich wie in den vorausgegangenen Jahren auf die Beantwortung von Bürgereingaben und eine kurze generelle Prüfung beschränkt:

Wenden sich Bürger mündlich oder schriftlich mit der Befürchtung an mich, daß beim Verfassungsschutz möglicherweise unrichtige Daten über sie gespeichert werden, die zu Nachteilen für sie geführt hätten, gehe ich diesen Einzelfällen nach. Soweit es mir notwendig erscheint, nehme ich auch Einblick in die zugrundeliegenden Personen- und Sachakten. Diese Einsicht hat mir das Bayer. Landesamt für Verfassungsschutz in den von mir erbetenen Fällen gewährt. Differenzen über die datenschutzrechtliche Bewertung dieser Fälle hat es mit dem Landesamt für Verfassungsschutz nicht gegeben. Soweit erforderlich hat das Amt Daten und Bewertungen berichtigt. Dies begrüße ich.

Im Berichtszeitraum habe ich wiederum das Landesamt für Verfassungsschutz zu einer kurzen generellen Prüfung aufgesucht. Schwerpunkte waren Feststellungen bezüglich der Rechtmäßigkeit und Richtigkeit der Speicherungen in NADIS, der Informationsfluß von der Polizei an das Landesamt für Verfassungsschutz, die Behandlung der Anfragen des Landesamts für Verfassungsschutz an Sozialbehörden im Rahmen des § 72 SGB X und an Meldebehörden im Rahmen von Art. 31 Abs. 2 Bayer. Meldegesetz sowie die Einsichtnahme in einige weitere Dateien. Außerdem habe ich Feststellungen über die erfreuliche Bereinigung und Aussonderung von Vorgängen in diesem Amt getroffen.

Als **Ergebnis** meiner Prüfungen kann ich den Eindruck wiedergeben, daß das Bayer. Landesamt für Verfassungsschutz zunehmend erfolgreich die datenschutzrechtlichen Anforderungen bei der Datenverarbeitung berücksichtigt. Diese Feststellung scheint mir besonders wichtig zu sein, weil durch die folgende Darstellung einzelner Problemfälle nicht der falsche Eindruck entstehen darf, als ob das Landesamt den Datenschutz nicht beachtet. Tatsächlich waren die durchgesehenen Vorgänge im überwiegenden Maße datenschutzrechtlich nicht zu beanstanden und ist die Bewertung der nachfolgenden Fälle zwischen dem Staatsministerium des Innern und mir nicht unbestritten.

Im folgenden nun einige kritische Anmerkungen zur Prüfung:

In einigen Fällen hat die stichprobenartige Prüfung aufgrund des mir vorgelegten Materials aus meiner Sicht ergeben, daß das Bayer. Landesamt für Verfassungsschutz Bürger personenbezogen gespeichert hat, obwohl dies nach den bei der Prüfung vorliegenden Erkenntnissen zur Erfüllung der dem Landesamt gesetzlich zugewiesenen Aufgaben nicht erforderlich war. Fälle solcher Speicherungen waren zum Beispiel:

- Die Teilnahme einer Person an zahlreichen Veranstaltungen gegen ein Kernkraftwerk, die in Gasthäusern, Pfarrzentren, Räumen des DGB und anderswo abgehalten worden sind. Aus den Unterlagen hat sich kein Anhaltspunkt ergeben, daß sich die betroffene Person bei dem Besuch der Veranstaltungen außerhalb des grundgesetzlich vorgegebenen Rahmens verhalten hätte.
- Das Landesamt für Verfassungsschutz war über den Ausgang eines Strafverfahrens (hier ein Freispruch), dessen Einleitung ihm mitgeteilt worden war, von der zuständigen Polizeibehörde nicht unterrichtet worden. Damit waren die beim Landesamt für Verfassungsschutz gespeicherten Daten insoweit objektiv unrichtig.

Sicher ist es gerade Aufgabe des Verfassungsschutzes, Vorfeldarbeit zu leisten. Deshalb sind auch in Bereichen Beobachtungen anzustellen, in denen zunächst noch nicht klar erkennbar ist, ob die Betroffenen sich im Rahmen des Grundgesetzes bewegen oder deren Handlungen verfassungsfeindlichen Charakter entwickeln. Auch unter Respektierung dieser Aufgaben meine ich, daß das Bayer. Landesamt für Verfassungsschutz Personen, die ihre verfassungsrechtlich garantierten Rechte wahrnehmen und bei denen es zunächst unklar bleibt, ob sie hierbei die Schwelle zur verfassungsfeindlichen Handlung überschreiten und in bestimmten Organisationen lediglich als „Idealisten" oder „Bekenner" auftreten, nicht ebenso behandeln darf wie solche Personen, die die Ziele einer als verfassungsfeindlich bekannten Organisation durchsetzen wollen.

Die Notwendigkeit der Beachtung meiner schon im letzten Jahr erhobenen Forderungen bezüglich des Verfahrens der Sicherheitsüberprüfungen hat sich im Berichtszeitraum bestätigt. Die von mir nachvollzogenen Sicherheitsüberprüfungen haben erneut gezeigt, daß allen am Verfahren beteiligten Stellen bewußt sein muß, daß die Durchführung von Sicherheitsüberprüfungen für die Betroffenen wesentliche Auswirkungen haben kann und deshalb mit besonderer Genauigkeit erfolgen muß. Ich hoffe, daß das Verfahren der Sicherheitsüberprüfung spätestens in der nächsten Legislaturperiode möglichst präzise gesetzlich geregelt wird (vgl. hierzu auch 5.2).

5.2. Bereichsspezifische Datenschutzregelungen bei Nachrichtendiensten

Die Datenverarbeitung der Verfassungsschutzbehörden greift in besonderem Maße in das informationelle Selbstbestimmungsrecht der Bürger ein, weil sie von der Natur der Sache her fast vollständig im Geheimen und somit unter Ausschluß der Öffentlichkeit und der Kontrolle durch die Betroffenen stattfindet. Deshalb sind nach allgemeiner Überzeugung präzise gesetzliche Regelungen für die Datenverarbeitung der Verfassungsschutzbehörden notwendig. Derzeit liegen Entwürfe für ein Bundesverfassungsschutzgesetz, ein Zusammenarbeitsgesetz und ein MAD-Gesetz vor.

Ziel des **Bundesverfassungsschutzgesetzes** ist, wie sich aus seiner ausführlichen Bezeichnung ergibt, die Regelung der Zusammenarbeit des Bundes und der Länder in Angelegenheit des Verfassungsschutzes und der Tätigkeit des Bundesamtes für Verfassungsschutz. Das **MAD-Gesetz** soll die gesetzliche Grundlage für die Anwendung nachrichtendienstlicher Mittel sowie die Verarbeitung personenbezogener Daten durch den militärischen Abschirmdienst schaffen. Das **Zusammenarbeitsgesetz (ZAG)** soll die notwendigen Rechtsgrundlagen für die Übermittlung personenbezogener Informationen zwischen Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder auf dem Gebiet des Staats- und Verfassungsschutzes und nachrichtendienstlicher Tätigkeiten schaffen. Zwar fallen die beabsichtigten Gesetze in die Gesetzgebungskompetenz des Bundes, doch werden auch die Länder in doppelter Weise durch sie betroffen. Zum einen sollen diese Gesetze die Datenübermittlungen zwischen Bundes- und den unterschiedlichen Landesbehörden regeln und zum anderen werden die beabsichtigten Regelungen auch Auswirkungen auf eine notwendige Novellierung der Landesverfassungsschutzgesetze haben. Deshalb bin auch ich als Landesbeauftragter für den Datenschutz zur Stellungnahme gefordert:

Bei der Schaffung neuer gesetzlicher Regelungen für die Datenverarbeitung von Verfassungsschutzbehörden und ihrer Zusammenarbeit mit sonstigen Sicherheitsstellen kann es nicht allein darum gehen, die derzeitige Praxis gesetzlich festzuschreiben. Vielmehr muß der Umfang zulässiger Informationsverarbeitung dieser Behörden auf der Grundlage des Volkszählungsurteils des Bundesverfassungsgerichts überprüft und durch spezielle Aufgaben- und Befugnisnormen konkretisiert und ggf. begrenzt werden. Mit den anderen Datenschutzbeauftragten bin ich mir darüber einig, daß hierbei folgende Grundsätze berücksichtigt werden sollten:

- Die Regelungen zur Informationsverarbeitung durch den Verfassungsschutz müssen den Anforderungen der Normenklarheit entsprechen. Der Bürger muß in der Lage

sein, den gesetzlichen Bestimmungen zumindest dem Grundsatz nach entnehmen zu können, aus welchem Anlaß, in welcher Weise und zu welchem Zweck der Verfassungsschutz personenbezogene Daten verarbeiten darf.

- Die Regelungen müssen auch in sich differenziert sein und auf die unterschiedlichen Aufgaben der Verfassungsschutzbehörden abstellen.
- Der Grundsatz der Zweckbindung gilt auch für Verfassungsschutz- und Sicherheitsbehörden im Verhältnis zueinander.
- Jede Art der Datenverarbeitung und Datenverwendung einschließlich der Datenerhebung ist in die Regelungen aufzunehmen. Weil der zunehmende Einsatz der elektronischen Datenverarbeitung manche Risiken für den Bürger verstärken kann, sind gerade auch für den Verfassungsschutz wesentliche neue Automatisierungsschritte gesetzlich zu regeln.

Unter Berücksichtigung der tragenden Elemente des Volkszählungsurteils des Bundesverfassungsgerichts und der eben genannten Grundsätze ist zu den vorliegenden Gesetzentwürfen aus der Sicht des Datenschutzbeauftragten noch folgendes zu bemerken:

Die Beschreibung der gesetzlich zugewiesenen Aufgaben und Befugnisse hinsichtlich der Datenverarbeitung von Verfassungsschutz- und Sicherheitsbehörden muß m. E. präziser werden. Die bisher verwendeten Begriffe wie etwa „Bestrebungen gegen die freiheitlich demokratische Grundordnung", „die Sicherheit des Bundes oder eines Landes" oder „sicherheitsgefährdende oder geheimdienstliche Tätigkeiten" oder „Schutz auswärtiger Belange der Bundesrepublik Deutschland" sind für die Beschreibung der Aufgaben und Befugnisse der Verfassungsschutzbehörden nicht ausreichend präzise. Die zweifelsohne umfangreiche Rechtsprechung zu diesen Begriffen kann eine präzisere Beschreibung im Gesetz nicht ersetzen. Das Staatsministerium des Innern vertritt hier eine andere Auffassung, die zweifelsohne beachtenswerte Argumente für sich in Anspruch nehmen kann, der ich aber insoweit nicht folgen möchte. Meines Erachtens müßten sich aus den Erfahrungen der Tätigkeit der Verfassungsschutzbehörden in den vergangenen Jahrzehnten deren Aufgaben näher beschreiben lassen. Gerade für den einzelnen Bürger erscheint mir zum Beispiel besonders wichtig, unter welchen Voraussetzungen „beeinflußte" Organisationen beobachtet werden dürfen und wie weit hierbei die Beobachtung auf Einzelpersonen ausgedehnt werden darf. Für den Einzelnen muß aus dem Gesetz feststellbar sein, wann er die Schwelle von der rechtmäßigen Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Den Anforderungen an die notwendige Präzision bei der Festlegung der Voraussetzungen für die einzelnen Phasen der Datenverarbeitung werden auch nicht Begriffe wie „Aufgaben des Verfassungsschutzes" und „Zwecke des Verfassungsschutzes" gerecht.

Ein besonderes Anliegen ist mir eine klare Regelung der Sicherheitsüberprüfungen. Detaillierter als bisher vorgesehen sind die Mitwirkung des Verfassungsschutzes an solchen Überprüfungen, die Befragung dritter Personen, die Unterrichtung des Betroffenen sowie Art und Weise der Verarbeitung der hierbei angefallenen Daten zu regeln. Gleiches gilt für die Voraussetzungen, unter denen überhaupt Sicherheitsüberprüfungen durchgeführt werden dürfen.

Der bisher vorgesehene Informationsaustausch der Verfassungsschutzbehörden untereinander ist meines Erachtens zu umfassend. Er greift in besonders hohem Maße in das verfassungsrechtlich verbürgte Recht auf informationelle Selbstbestimmung ein. Das Bundesverfassungsgericht hat hierzu erneut festgestellt, daß eine Einschränkung dieses Rechtes nicht weiter gehen darf „als es zum Schutze öffentlicher Interessen unerläßlich ist" (E 67, 100 (143). Demnach dürfen nur die Informationen übermittelt werden, die zur jeweiligen Aufgabenerfüllung tatsächlich erforderlich sind. In ganz besonderem Maße gilt dies für die im Zusammenarbeitsgesetz vorgesehenen Datenübermittlungen zwischen Polizeibehörden und Verfassungsschutz. Zwar wirkt das Trennungsgebot zwischen Polizei und Verfassungsschutz nicht absolut. Durchbrechungen des Trennungsgebotes durch Datenübermittlungen zwischen diesen beiden Bereichen sind aber auf äußerst eng begrenzte Fälle durch präzise und normenklare Regelungen zu beschränken. Dies muß auch für die Datenübermittlung von Grenzpolizeibehörden an Nachrichtendienste gelten.

Der Einsatz nachrichtendienstlicher Mittel ist aus datenschutzrechtlicher Sicht jeweils als Datenerhebung zu werten. Weil diese Datenerhebung durch nachrichtendienstliche Mittel verdeckt, also ohne Kenntnis des Betroffenen, erfolgt, stellt sie einen besonders belastenden Eingriff dar. Die Voraussetzungen des Einsatzes nachrichtendienstlicher Mittel und die wichtigsten nachrichtendienstlichen Mittel sind zumindest im Gesetz zu nennen, dabei ist mir bewußt, daß dies aus der Natur der Sache nicht abschließend geschehen kann. Weiterhin sind – vergleichbar den Regelungen über die Post- und Telefonüberwachung – Verwertungsbeschränkungen und eine Verpflichtung zur grundsätzlichen nachträglichen Unterrichtung des Betroffenen vorzusehen.

Die wesentlichen Regelungen zur Datenverarbeitung dürfen sich nicht nur auf die Datenverarbeitung in Dateien beschränken, sondern müssen auch Akten und sonstige Unterlagen umfassen, zumal bei Verfassungsschutzbehörden ein Großteil der das Persönlichkeitsrecht der Bürger maßgeblich berührenden Daten derzeit noch in Akten geführt werden. Außerdem können komplexe Aktensammlungen bereits heute gezielt und mit Hilfe bestimmter automatisierter Verfahren erschlossen werden.

Besonders präzise müssen m. E. auch die Vorschriften gefaßt werden, mit denen sonstige Verwaltungsbehörden zur Mitteilung von Wahrnehmungen an den Verfassungsschutz verpflichtet werden. Aus dem Recht auf informationelle Selbstbestimmung folgt, daß der Bürger, der in Kontakt mit einer Verwaltungsbehörde tritt, grundsätzlich erkennen können muß, was diese wann und bei welcher Gelegenheit an Verfassungsschutzbehörden zu übermitteln hat.

Angesichts des weitreichenden Auftrages der Verfassungsschutzbehörden zur Sammlung von Informationen bedürfen die dabei angefallenen personenbezogenen Erkenntnisse einer besonders strengen Abschottung nach außen. Dies gilt insbesondere deshalb, weil gerade beim Verfassungsschutz einliegende Informationen vielfach auf nicht abschließend gesicherten Erkenntnissen beruhen und zumindest teilweise auf Wegen erlangt werden, die den anderen Verwaltungsbehörden verschlossen sind.

Die Trennungslinie zwischen den Aufgaben des Verfassungsschutzes einerseits und den Aufgaben des polizeilichen Staatsschutzes andererseits ist bislang viel zu wenig

deutlich erkennbar. Staatsschutzbehörden sind grundsätzlich keine Außenstellen des Verfassungsschutzes. Die notwendige Trennung zwischen Staatsschutz und anderen Polizeibehörden einerseits und Nachrichtendiensten andererseits kann sich nicht nur auf die organisatorische Schaffung unterschiedlicher Behörden beschränken. Ein zu weit gehender Informationsaustausch zwischen beiden Bereichen würde letztlich auch die im Hinblick auf die anders gestalteten Aufgaben unterschiedlich zugemessenen Befugnisse unterlaufen.

Die Gesetzentwürfe berücksichtigen in ihrer letzten vorliegenden Fassung bereits eine Reihe meiner Anregungen. Ich bin deshalb überzeugt, daß eine sachliche Fortsetzung der Diskussion in der nächsten Legislaturperiode zu einer sachgerechten Lösung dieser zweifelsohne besonders komplizierten Materie führen wird.

6. Justiz

6.1. Überblick

Das Verhältnis zwischen dem Landesbeauftragten für den Datenschutz und dem Bayer. Staatsministerium der Justiz ist zeitweise etwas spröde. Dies mag seinen Grund in der unterschiedlichen Beurteilung des Umfangs meiner Prüfungskompetenz haben. Während das Staatsministerium der Justiz den Standpunkt vertritt, daß ich meine Tätigkeiten auf Dateien zu beschränken habe, vertrete ich hingegen die Auffassung, daß Datenschutz grundsätzlich für jede personenbezogene Datenverarbeitung gilt. So erhalte ich von Justizbehörden vielfach Auskünfte, die ich zur Beantwortung von Bürgereingaben benötige, nur mit dem ausdrücklichen Hinweis auf meine angeblich fehlende Zuständigkeit.

Ich habe immer anerkannt, daß die verfassungsrechtlich garantierte richterliche Unabhängigkeit und die Selbständigkeit des Rechtspflegers auch bei Fragen des Datenschutzes im Justizbereich zu berücksichtigen sind. Auch ist mir bekannt, daß derzeit noch ein großer Teil der personenbezogenen Daten im Justizbereich in Akten geführt wird, für die das Bayer. Datenschutzgesetz grundsätzlich nur mittelbar anwendbar ist. Allerdings sind die vom Bundesverfassungsgericht seit Jahren entwickelten Grundsätze zum Schutz des Persönlichkeitsrechts und die neuerdings zum Recht auf informationelle Selbstbestimmung erarbeiteten Vorgaben – hierauf habe ich bereits in früheren Tätigkeitsberichten hingewiesen – auch im Bereich der Rechtspflege zu beachten. Diese Grundsätze machen nicht nur den Bedarf an der Schaffung neuer und die Überarbeitung bestehender Rechtsvorschriften deutlich: sie sind auch bei der alltäglichen Verarbeitung personenbezogener Daten im Justizbereich zu berücksichtigen. Meine Kontrollkompetenz für den Geschäftsbereich des Bayer. Staatsministeriums der Justiz leite ich aus Art. 28 BayDSG ab, der mir die Überwachung der Einhaltung des „Datenschutzes" schlechthin zuweist.

Wie die folgenden Ausführungen im Tätigkeitsbericht zeigen, bewegen mich im Justizbereich nahezu immer die gleichen Themenkreise. Dennoch wäre der Eindruck falsch, daß im Justizbereich der Datenschutz noch keine deutlichen Spuren hinterlassen hat. So sind etwa für die Mitteilungen in Strafsachen und die Mitteilungen in Zivilsachen Übergangslösungen gefunden worden, die bereits zahlreiche Datenschutzanliegen berücksichtigen. Weiter sind Gesetzgebungsverfahren etwa zum Persönlichkeits- und Datenschutz im Prozeßkostenhilfeverfahren oder zum Opferschutz im Strafverfahren zu nennen; letzteres geht auf eine begrüßenswerte Initiative des Bayerischen Staatsministeriums der Justiz zurück. Das Schwergewicht künftiger, zur stärkeren Berücksichtigung des Persönlichkeitsschutzes notwendiger Gesetzgebungsverfahren wird im Bereich der Strafprozeßordnung, des Gerichtsverfassungsgesetzes und der Zivilprozeßordnung liegen.

Daneben hatte ich mich vor allem mit zahlreichen Bürgeranfragen zum Persönlichkeitsschutz im Gerichtsverfahren (Öffentlichkeit, Presseberichterstattung, Ladungen, Zustellungen, Namensnennung in Terminbestimmungen), mit der sogenannten Fremddatenerfassung von Justizdaten, mit Datenübermittlungen zur Strafverfolgungsstatistik sowie mit zahlreichen Fragen aus dem Strafvollzug zu befassen.

Im folgenden stelle ich einige Probleme aus meiner Tätigkeit etwas näher dar.

6.2. Reform des Strafprozeßrechts

In meinem 7. Tätigkeitsbericht habe ich bereits darauf hingewiesen, daß die derzeit geltende Strafprozeßordnung die Informationsverarbeitung in Ermittlungs- und Strafverfahren nach heutigem Datenschutzverständnis nur unvollkommen regelt. So sind etwa die bisherigen Regelungen in der Strafprozeßordnung zur Aufklärung und Verfolgung strafbarer Handlungen (z. B. §§ 152 Abs. 2, 160 Abs. 1, 161 Satz 1 und 163 Abs. 1 StPO) keine ausreichende Rechtsgrundlage für sämtliche Formen der bei dieser Tätigkeit anfallenden Datenverarbeitung. Das Fehlen ausreichender Rechtsgrundlagen wird insbesondere im Hinblick auf die neuen, im Rahmen der Strafverfolgung verwendeten Fahndungsmethoden – wie polizeiliche Beobachtung, Rasterfahndung, Einsatz von V-Leuten und verdeckten Ermittlungen – deutlich. Die Strafprozeßordnung kennt keine Generalklausel zum Eingriff in Individualrechtsgüter. Daher werden neben Regelungen für neue Fahndungsmethoden auch Befugnisnormen für den gesamten Bereich der Erhebung von Informationen, für die Speicherung und die Verwendung der Daten im Strafverfahren sowie Vorschriften für die Akteneinsicht zu schaffen sein, um nur einige Bereiche anzusprechen. Diese Auffassung wird offensichtlich nunmehr auch im Justizbereich geteilt. So hat der Bundesminister der Justiz vor einiger Zeit ein Problempapier erarbeitet, das sich für ergänzende gesetzliche Regelungen im Bereich der Fahndungsmaßnahmen, der Fahndungshilfsmittel und des Akteneinsichtsrechts im Strafverfahren ausspricht. Das Papier wurde mittlerweile in einen ersten Arbeitsentwurf umgesetzt, der Gegenstand weiterer Beratungen sein wird. Weiter ist auf den Entwurf eines Ersten Gesetzes zur Verbesserung der Stellung des Verletzten im Strafverfahren hinzuweisen, der u. a. das Ziel verfolgt, die Persönlichkeitsrechte des Tatopfers im Prozeß durch eine stärkere Einschränkung des Öffentlichkeitsgrundsatzes besser als bisher zu schützen. Schließlich darf ich an dieser Stelle auch noch die Einführung einer bereichsspezifischen Rechtsgrundlage für die Nutzung des neuen maschinenlesbaren Personalausweises im strafrechtlichen Ermittlungsverfahren erwähnen (Schleppnetzfahndung; § 163 d StPO; siehe unter Nr. 6.8 dieses Tätigkeitsberichts).

Viele der hier in aller Kürze angesprochenen Überlegungen der Justiz zur Reform der Strafprozeßordnung kann ich aus meiner Sicht grundsätzlich begrüßen. Vor allem der vom Bundesminister der Justiz vorgelegte Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren enthält beachtenswerte Anregungen, mit denen man sich noch gründlich auseinanderzusetzen haben wird. Gemeinsam mit den übrigen Datenschutzbeauftragten in Bund und Ländern bin ich jedoch der Auffassung, daß durch nur punktuelles Herausgreifen einiger weniger Problembereiche den Anforderungen der verfassungsgerichtlichen Rechtsprechung zum Umgang mit personenbezogenen Daten, die auch für den Strafprozeß gelten müssen, insgesamt nicht genügt werden kann. Es bedarf vielmehr, wie bereits in meinem letzten Tätigkeitsbericht angedeutet, einer umfassenden und einheitlichen, von den gleichen Leitgedanken getragenen Gesamtlösung. Die Datenschutzbeauftragten haben deshalb damit begonnen, in einem Arbeitskreis zur Reform der Strafprozeßordnung einen Forderungskatalog zu erarbeiten, der eine Zusammenstellung aller Themenbereiche enthalten soll, in denen die Schaffung geeigneter Rechtsgrundlagen zum Schutz des Persönlichkeitsrechts der Betroffenen geboten erscheint. Zugleich sollen inhaltliche Kriterien bestimmt werden, an denen die neuen Vorschriften zu messen sein werden.

Im Rahmen meiner Mitarbeit im Arbeitskreis habe ich mich insbesondere mit den Problemen des Datenverkehrs zwischen Staatsanwaltschaften und Polizei befaßt. Ich bin dabei zu dem Ergebnis gelangt, daß die Polizeiorgane bei ihrer strafverfolgenden Tätigkeit auch im Falle des sogenannten ersten Zugriffs nach der vom Gesetzgeber getroffenen Grundkonzeption als Justizbehörden im funktionellen Sinne tätig werden. Die von der Polizei erhobenen Daten müssen als Justizdaten angesehen werden. Hieraus ergeben sich wichtige Konsequenzen für die Zulässigkeit der weiteren Verarbeitung dieser Daten, insbesondere auch für die Frage eines direkten Zugriffs der Staatsanwaltschaften auf automatisierte polizeiliche Informationssysteme. Weiter habe ich mich näher befaßt mit Problemen des internen Datenverkehrs zwischen den Staatsanwaltschaften unter Berücksichtigung von Überlegungen für den Aufbau eigener automatisierter Informationssysteme sowie mit den Anforderungen an normenklare gesetzliche Regelungen für die Ausschreibung von Beschuldigten und Zeugen zu Fahndungszwecken. Auch hier reichen die bestehenden Vorschriften im Lichte neueren Verfassungsverständnisses nicht mehr aus. Ich beabsichtige, meine Mitarbeit im Arbeitskreis Strafprozeßordnung fortzusetzen, wobei mein besonderes Augenmerk künftig auch der Abstimmung der Ermittlungsbefugnisse im strafrechtlichen Ermittlungsverfahren mit den entsprechenden Überlegungen zur Reform des Polizeirechts gelten wird. Die schwierige und bisweilen undankbare Tätigkeit der Polizeibeamten vor Ort darf nach meiner Überzeugung nicht durch eine mangelnde Koordinierung der für sie maßgebenden Rechtsgrundlagen noch weiter unnötig erschwert werden. Gerade die notwendige Abstimmung zwischen den Novellierungen des Polizeirechts und der Strafprozeßordnung zeigt die Eilbedürftigkeit auch der Novellierung der Strafprozeßordnung auf. Der Bayer. Verfassungsgerichtshof hat in der schon mehrfach zitierten Entscheidung vom 9.7.1985 zur derzeitigen Speicherung personenbezogener Daten durch die Polizei in Kriminalakten ausdrücklich deren gesetzliche Regelungsbedürftigkeit festgestellt. Wenn dem Gesetzgeber auch eine gewisse Zeitspanne für die Schließung dieser Gesetzeslücke eingeräumt ist, sollte die Novellierung der Strafprozeßordnung gerade im Hinblick auf das Polizeirecht mit besonderem Nachdruck betrieben werden.

6.3. Mitteilungen in Zivilsachen (MiZi)

Die Gerichte haben in Zivilverfahren aufgrund der bundeseinheitlichen Anordnung über Mitteilungen in Zivilsachen (MiZi) Mitteilungen an andere Gerichte oder andere Behörden zu machen. Wegen der zahlreichen in diesen Mitteilungen übermittelten sensiblen personenbezogenen Daten Betroffener hat sich ein Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder intensiv mit den einzelnen Regelungen der MiZi befaßt und Vorschläge für eine Bereinigung unterbreitet; hierüber hatte ich im 7. Tätigkeitsbericht berichtet. Die Justizverwaltungen haben im Hinblick auf das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ihrerseits geprüft, welche Auswirkungen diese Entscheidung im einzelnen auf die Mitteilungen in Zivilsachen hat. Das Staatsministerium der Justiz hat mit Bekanntmachung vom 24. Oktober 1985 in Abstimmung mit dem Bundesminister der Justiz und den anderen Landesjustizverwaltungen die Mitteilungspflichten in Zivilsachen in wesentlichen Punkten eingeschränkt. Diese schnelle Reaktion der Justizverwaltung ist zu begrüßen.

Ein Vergleich mit den Änderungsvorschlägen der Datenschutzbeauftragten mit der nun in Kraft getretenen Änderungsbekanntmachung zeigt, daß diese Bekanntmachung in der Tat bereits vielen datenschutzrechtlichen Anliegen in erfreulicher Weise Rechnung trägt. Die Bekanntmachung ist zweifelsohne aus der Sicht des Datenschutzes ein Schritt in die richtige Richtung. Allerdings sind eine Reihe meiner Vorschläge noch unberücksichtigt geblieben. Das Staatsministerium der Justiz hat mir hierzu mitgeteilt, daß diese noch einer eingehenden Überprüfung unter Beteiligung der Empfänger der Mitteilungen bedürfen. Zum Teil setze ihre Verwirklichung auch die Änderung oder Ergänzung gesetzlicher Vorschriften voraus, was noch einige Zeit in Anspruch nehmen werde. Das Bayer. Staatsministerium der Justiz hat mir in diesem Zusammenhang jedoch die erfreuliche Mitteilung gemacht, daß sich die Justizminister und -senatoren des Bundes und der Länder anläßlich einer Konferenz auf Initiative Bayerns mit der Frage der rechtlichen Grundlagen für die Mitteilungen in Zivilsachen befaßt und den Bundesminister der Justiz gebeten haben, noch im Jahre 1986 Vorschläge für eine gesetzliche Regelung vorzulegen. Das Staatsministerium der Justiz hat außerdem erklärt, daß es sich weiterhin für ein zügiges Voranschreiten der Gesetzgebungsarbeiten einsetzen und hierbei auch die Auffassung der Datenschutzbeauftragten in seine Überlegungen einbeziehen werde.

Der Bundesminister der Justiz hat dem Ersuchen der Ministerkonferenz jetzt Rechnung getragen und den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz) vorgelegt. Der Entwurf sieht gesetzliche Grundlagen für die für erforderlich gehaltenen Mitteilungen vor, die in das Gerichtsverfassungsgesetz eingestellt werden sollen. Eine erste Bewertung des Entwurfs werde ich baldmöglichst abgeben.

6.4. Mitteilungen in Strafsachen (MiStra)

Derzeit erfolgen die Mitteilungen in Strafsachen auf Grundlage der vom Bundesminister der Justiz und den Justizministern und -senatoren der Länder bundeseinheitlich zum 1.4.1985 in Kraft getretenen Neufassung der Anordnung über Mitteilungen in Strafsachen. Es besteht allgemein Einverständnis darüber, daß diese Neufassung nur für eine Übergangszeit gelten kann und die Schaffung einer eindeutigen Rechtsgrundlage für diese Mitteilungen dringend geboten ist. Meine Hoffnung, daß möglicherweise noch in der gegenwärtig laufenden Legislaturperiode eine gesetzliche Grundlage geschaffen werden könnte, hat sich leider nicht erfüllt. Immerhin liegt jetzt aber der bereits oben unter Nr. 6.3 aufgeführte erste Entwurf eines Justizmitteilungsgesetzes vor, der auch die Mitteilungen in Strafsachen umfaßt.

Augenblicklich ist gegen die Anordnung über Mitteilungen in Strafsachen eine Verfassungsbeschwerde beim Bundesverfassungsgericht anhängig. Auf die Bitte des Gerichts hin habe ich eine schriftliche Stellungnahme abgegeben. Ich gehe davon aus, daß die Entscheidung des Bundesverfassungsgerichts im Gesetzgebungsverfahren berücksichtigt werden wird.

Mit einem Einzelproblem der MiStra, nämlich der Mitteilung der Staatsanwaltschaft an die Polizei über den Ausgang des Strafverfahrens, in dem die einzelne Polizeibehörde Ermittlungen angestellt hat, befasse ich mich seit längerem. Bei Prüfungen polizeilicher Kriminalakten oder automatisierter Sammlungen habe ich immer wieder festgestellt, daß der Verfahrensausgang nicht vermerkt ist und die Polizei deshalb die daraus folgenden Schlüsse für die weitere Führung der polizeilichen Unterlagen nicht gezogen hat. Als Begründung für diese mangelnde Berichtigung ist mir vielfach vorgetragen worden, daß von seiten der Staatsanwaltschaft die nach der MiStra notwendige Rückmeldung über den Verfahrensausgang nicht erfolge. Um diesen Mißstand zu beseitigen und es den speichernden Polizeidienststellen außerdem zu ermöglichen, Rückschlüsse aus dem Verfahrensausgang für die weitere Verarbeitung polizeilicher Daten zu ziehen, wurden Überlegungen zur Reform der verschiedenen hier in der Praxis verwendeten Formblätter angestellt. Allerdings wird dadurch selbstverständlich das grundsätzliche Problem der Zuständigkeitsabgrenzung zwischen polizeilicher und staatsanwaltschaftlicher Datenverarbeitung nicht gelöst. Dies wird der Novellierung der Strafprozeßordnung und des Polizeirechts vorbehalten bleiben müssen.

6.5. Schuldnerverzeichnis

Probleme des Schuldnerverzeichnisses beschäftigen mich ständig seit dem 3. Tätigkeitsbericht. Wie bekannt, werden in das beim Amtsgericht geführte Schuldnerverzeichnis Personen eingetragen, die die eidesstattliche Versicherung über ihr Vermögen abgegeben haben oder gegen die wegen Nichtabgabe der eidesstattlichen Versicherung Haft angeordnet ist.

Der Bundesminister der Justiz hat mittlerweile den Entwurf zur Änderung gesetzlicher Vorschriften über das Schuldnerverzeichnis sowie den Entwurf einer Verordnung über die Erteilung von Abdrucken aus den Schuldnerverzeichnissen vorgelegt. Insbesondere der Entwurf zur Änderung gesetzlicher Vorschriften enthält aus datenschutzrechtlicher Sicht einige wesentliche Verbesserungen gegenüber dem geltenden Recht. Hervorzuheben sind in diesem Zusammenhang vor allem die neue Regelung der Löschungsbestimmungen, insbesondere der Verzicht auf das Erfordernis, einen Antrag zu stellen, und die Verankerung einer datenschutzrechtlichen Auskunftssperre. Allerdings sind einige Probleme im Zusammenhang mit der Weitergabe von Daten aus dem Schuldnerverzeichnis an Dritte noch nicht völlig zufriedenstellend gelöst.

Offensichtlich haben die von seiten des Datenschutzes wie auch von seiten der Wirtschaft zu den Entwürfen vorgetragenen Bedenken den Bundesminister der Justiz entmutigt. Jedenfalls hat er mitgeteilt, daß er derzeit keine Chance mehr sehe, in der jetzigen Legislaturperiode noch eine gesetzliche Regelung durchzusetzen. Ich bedauere es außerordentlich, daß die Diskussion um das Schuldnerverzeichnis noch keinen Abschluß gefunden hat und die auch im Hinblick auf das Recht auf informationelle Selbstbestimmung dringend notwendigen Rechtsvorschriften immer noch nicht erlassen sind. Der Bundesjustizminister hat nun in Aussicht gestellt, die notwendigen gesetzlichen Regelungen, nämlich Änderung des § 915 Zivilprozeßordnung und die Aufnahme ergänzender Bestimmungen, im Rahmen einer umfassenden Novellierung des Zwangsvollstrekkungsrechts zu verwirklichen.

Erfreulicher Lichtblick ist in diesem Zusammenhang die vom Bayer. Staatsministerium des Innern an die für den Datenschutz im privaten Bereich zuständigen Aufsichtsbehörden geäußerte Bitte, bei Prüfungen von Handelsauskunfteien darauf zu achten, daß die Löschungsfristen gem. § 915 Abs. 2 Zivilprozeßordnung eingehalten werden.

Automatisierte Führung des Schuldnerverzeichnisses

In Bayern wird bereits an mehreren Amtsgerichten das Schuldnerverzeichnis automatisiert geführt. Probeweise geschieht dies an einem Amtsgericht auch für das Vollstrekkungsregister. Die Umstellung des Schuldnerverzeichnisses auf EDV-Verfahren läßt eine geänderte gesetzliche Regelung des Schuldnerverzeichnisses nunmehr noch dringlicher erscheinen. Die für die bisherige Praxis herangezogenen Allgemeinen Vorschriften des Bundesministers der Justiz (in Verbindung mit § 915 Abs. 4 ZPO) stellen weder eine materiell befriedigende noch eine formell ausreichende Rechtsgrundlage dar. Das Verfahren sieht, wie bisher, eine regelmäßige Datenübermittlung der Neueintragungen und der Löschungen an die Industrie- und Handelskammer vor. Nicht zuletzt durch die „Schuldnerliste" der Industrie- und Handelskammer erhalten wiederum eine Vielzahl von Institutionen und Personen Abschriften aus dem Schuldnerverzeichnis, weshalb die Einhaltung der diesbezüglichen gesetzlich vorgesehenen Löschungsfristen in der Praxis teilweise nicht gewährleistet ist. Hinzu kommt, daß das Vollstreckungsgericht vielfach die zur einwandfreien Identifikation eines Schuldners notwendigen Daten nicht kennt und diese deshalb auch nicht in das Schuldnerverzeichnis eintragen kann. Somit ist den Empfängern der Abschriften aus dem Schuldnerverzeichnis ebenfalls eine sorgfältige Identitätsprüfung hinsichtlich dieser Personen nicht möglich. Damit kann das Risiko von Verwechslungen und damit eine Beeinträchtigung schutzwürdiger Belange Dritter nicht ausgeschlossen werden. Zwar sind diese Probleme nicht erst mit der Automatisierung des Schuldnerverzeichnisses eingetreten; ihre Auswirkungen können sich aber im Einzelfall verschärft zeigen.

6.6. Datenschutz im Notariat

Bereits seit einiger Zeit befasse ich mich mit der Datenverarbeitung im Bereich des Notariatswesens. Kernpunkt einer bundesweit geführten Diskussion ist hier die Frage nach der Anwendbarkeit der Bestimmungen des jeweils maßgebenden Landesdatenschutzgesetzes auf die Tätigkeit der Notare. Im einzelnen geht es insbesondere um die Meldepflicht der Notare zum Datenschutzregister, aber auch um die Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz. Ich habe mich zu diesen Fragen in einer Stellungnahme gegenüber dem Bayer. Staatsministerium der Justiz und der Landesnotarkammer Bayern schon zu Jahresbeginn umfassend geäußert. Dabei habe ich die Auffassung vertreten, daß die bayerischen Notare als Träger eines öffentlichen Amtes grundsätzlich als öffentliche Stellen im Sinne des Bayer. Datenschutzgesetzes angesehen werden müssen und deshalb den Bestimmungen dieses Gesetzes unterliegen, soweit sie personenbezogene Daten in Dateien verarbeiten. Die Bundesnotarordnung als maßgebendes Berufsrecht der Notare steht dem nicht entgegen, da das Bayerische Datenschutzgesetz keine weitergehenden spezifisch berufsrechtlichen Regelungen enthält, sondern sich mit einer Querschnittsmaterie eigener Art befaßt. Bereichsspezifische Vorschriften über den Datenschutz im Notariat gehen selbstverständlich den Bestimmungen des Bayerischen Datenschutzgesetzes im Einzelfalle vor, berühren die Geltung des Gesetzes aber im übrigen nicht. Es besteht daher keine Veranlassung, die bayerischen Notare aus der umfassenden Kontrollbefugnis des Datenschutzbeauftragten zu entlassen oder von einer Registrierung etwaiger anmeldepflichtiger Dateien im Datenschutzregister abzusehen, auch wenn mir bisher aktuelle Fälle einer mißbräuchlichen Datenverarbeitung in bayerischen Notariaten nicht bekanntgeworden sind.

Meine Rechtsauffassung wird im Ergebnis von allen anderen Datenschutzbeauftragten, aber auch vom Bundesminister der Justiz geteilt. Demgegenüber beharrt die Landesnotarkammer Bayern nach wie vor darauf, daß das Bayer. Datenschutzgesetz auf die Tätigkeit der bayerischen Notare keine Anwendung finden soll. Sie bestreitet dem Landesgesetzgeber u. a. die Kompetenz, datenschutzrechtliche Regelungen mit Wirkung für den Bereich des Notariats zu erlassen.

Unbeschadet der unterschiedlichen Bewertung dieser grundsätzlichen Rechtsfragen habe ich mich im Berichtszeitraum bemüht, mit freundlicher Unterstützung der Landesnotarkammer Bayern abzuklären, inwieweit die von den Notaren nach der geltenden Dienstordnung zu führenden Bücher, Verzeichnisse und Karteien überhaupt den Dateibegriff erfüllen können. Nach meinen bisherigen Feststellungen kommen hier vor allem das Namensverzeichnis, das in Karteiform geführte Massenbuch (Verzeichnis von Verwahrungsmassen) und das in Karteiform geführte Erbvertragsverzeichnis der Notare in Betracht. Weitere Datensammlungen müssen in die Überlegungen miteinbezogen werden, wenn sie automatisiert geführt und damit möglicherweise technisch gesehen jederzeit umgeordnet und ausgewertet werden können. Meine Bemühungen gehen deshalb jetzt dahin, einen genaueren Überblick über den Einsatz der elektronischen Datenverarbeitung im bayerischen Notariatswesen zu gewinnen. Zu diesem Zweck hat im August 1986 bereits ein erster Informationsbesuch bei einem Notar in Landshut stattgefunden.

Ich beabsichtige, mich auch weiterhin mit datenschutzrechtlichen Problemen im Notariatswesen zu beschäftigen und meine Gespräche mit der Landesnotarkammer Bayern fortzusetzen. Auch das Bayerische Staatsministerium der Justiz als oberste Aufsichtsbehörde für die bayerischen Notare ist bemüht, in der Auseinandersetzung über die streitigen Fragen neue Vorschläge zu entwickeln, die eine pragmatische und für alle Seiten akzeptable Verfahrensweise ermöglichen sollen. Dies begrüße ich grundsätzlich.

6.7. Kriminologische Zentralstelle

Auf die Vorbereitungen zur Einrichtung einer Kriminologischen Zentralstelle in Wiesbaden und die damit zusammenhängenden Fragen datenschutzrechtlicher Art habe ich zuletzt in meinem 5. Tätigkeitsbericht hingewiesen. Ausweislich ihrer bereits im Jahre 1981 vereinbarten Satzung handelt es sich bei der Zentralstelle um einen eingetragenen Verein des bürgerlichen Rechts mit der Aufgabe, die kriminologische Forschung in der Bundesrepublik Deutschland zu fördern und kriminologische Erkenntnisse für die Forschung, Gesetzgebung, Rechtspflege und Verwaltung zu vermitteln und zu erarbeiten. Ordentliche Mitglieder des Vereins sind die Bundesrepublik Deutschland und alle Bundesländer.

Aus datenschutzrechtlicher Sicht hatte ich Bedenken gegen die Einrichtung der Kriminologischen Zentralstelle als eingetragener Verein geltend gemacht, weil diese Zentralstelle damit den Kontrollinstanzen des Datenschutzes entzogen wird, die für die Justizbehörden zuständig sind. Wegen des Bezugs zu Straftaten sind an die kriminologische Zentralstelle zu übermittelnde personenbezogene Daten besonders sensibel. Bei der Bewertung der schutzwürdigen Belange der Betroffenen ist das auch vom Bundesverfassungsgericht anerkannte Interesse an der Wiedereingliederung des Straftäters in die Gesellschaft zu berücksichtigen. Ich hatte daher das Bayer. Staatsministerium der Justiz um Prüfung gebeten, inwieweit sichergestellt werden kann, daß die Kriminologische Zentralstelle einer ausreichenden Datenschutzkontrolle unterzogen wird.

Mit großer zeitlicher Verzögerung hat die Kriminologische Zentralstelle nunmehr am 13.6.1986 offiziell ihre Arbeit aufgenommen. Ihre Tätigkeit wird nach mir vorliegenden Informationen zunächst auf die Dokumentation laufender Forschungsarbeiten oder einzelner praktischer Modellversuche beschränkt bleiben. Diese Aufgaben sollen, ebenso wie in naher Zukunft anstehende Beratungs- und Kooperationsvorhaben, im wesentlichen ohne die Verarbeitung personenbezogener Daten erledigt werden. Unbeschadet dessen werde ich die Zusammenarbeit insbesondere der bayerischen Justizbehörden mit der Kriminologischen Zentralstelle selbstverständlich sorgfältig im Auge behalten. Zu klären bleibt überdies noch die Frage nach einer sinnvollen datenschutzrechtlichen Überwachung für die Zentralstelle selbst. Offensichtlich besteht dort Bereitschaft, mit dem Hessischen Datenschutzbeauftragten zusammenzuarbeiten. Dieser hat sich erboten, die Aufgabe bei allseitigem Einverständnis in Anwendung des Sitzlandprinzips wahrzunehmen. Eine Entscheidung steht noch aus.

6.8. Schleppnetzfahndung – § 163 d Strafprozeßordnung

Unter dem Schlagwort „Schleppnetzfahndung" ist die im Zusammenhang mit der Novellierung von Paß- und Personalausweisgesetz vorgesehene Einführung eines § 163 d in

die Strafprozeßordnung heftig diskutiert worden. Statt der ursprünglich vorgesehenen Fassung des § 163 d StPO ist eine die Datenschutzbelange in stärkerem Maße berücksichtigende Regelung Gesetz geworden.

Bürgeranfragen zur Schleppnetzfahndung zeigen mir, daß vielfach nicht bekannt ist, daß § 163 d StPO in der ursprünglich vorgesehenen Fassung des Entwurfs nicht in Kraft getreten ist und damit die damals gelten gemachten Bedenken zu einem erheblichen Teil nicht mehr zutreffen. Deshalb will ich über die Diskussion aus datenschutzrechtlicher Sicht kurz nachberichten:

Die Speicherung personenbezogener Daten in Dateien, die beim automatischen Lesen des maschinenlesbaren Personalausweises oder eines maschinenlesbaren Passes anfallen, ist nur aufgrund besonderer gesetzlicher Regelung zulässig (§ 3 a Abs. 2 ff Personalausweisgesetz, § 16 Abs. 2 ff Paßgesetz). § 163 d StPO gestattet nun eine solche ausnahmsweise Speicherung für bestimmte Zwecke der Strafverfolgung. Allerdings beschränkt sich die Anwendung von § 163 d StPO nicht nur auf den Einsatz maschinenlesbarer Identitätspapiere, sondern erfaßt auch vergleichbare Vorgänge, bei denen Daten über die Identität einer Vielzahl von Personen erhoben werden.

Aus datenschutzrechtlicher Sicht hatte ich gegen die ursprüngliche Fassung des Entwurfs zu § 163 d StPO Bedenken geäußert und die am Verfahren beteiligten bayerischen Stellen darauf hingewiesen, daß ich die geplante Regelung aus meiner Sicht für in wesentlichen Teilen mißglückt halte. Im einzelnen habe ich dabei folgende Gesichtspunkte geltend gemacht:

- Der Entwurf greift von seiner Rechtsfolge her tief in das informationelle Selbstbestimmungsrecht unverdächtiger Bürger ein, ohne daß bisher hinreichend geklärt wäre, ob die vorgeschlagene Form der Datenspeicherung überhaupt geeignet ist, die Aufklärung der im Entwurf genannten Straftaten (Katalogdaten) zu fördern.
- Der Entwurf grenzt die vorgesehene Datenerfassung weder in räumlicher noch in zeitlicher oder personeller Hinsicht hinreichend normenklar ein. Die vorgeschlagenen Zulässigkeitsvoraussetzungen bleiben insoweit viel zu vage.
- Der Katalog der Straftaten, der zu einer Datenspeicherung berechtigen soll, ist zu weit gefaßt. Angemessen erschien mir eine Anlehnung an § 111 StPO, der ebenfalls Maßnahmen gegen Unbeteiligte vorsieht.
- Der Entwurf macht nicht hinreichend deutlich, an welche der rechtlich zulässigen Formen von Personenkontrollen er anknüpfen will.
- Wegen des Gewichts, das der Anordnung und der Datenspeicherung hier zukommt, erscheint allein eine richterliche Anordnungskompetenz angemessen.
- Die vorgesehene Löschungsregelung ist unzureichend. Es bedarf der Feststellung einer Höchstfrist, nach deren Ablauf die gespeicherten Daten Unbeteiligter zumindest regelmäßig zu löschen sind.
- Auch die vorgesehenen Verwertungsregelungen sind unbefriedigend. Eine Verwertung der Daten zu einem anderen als dem ursprünglich vorgesehenen Zweck wird nur dann zulässig sein können, wenn es um die Verfolgung einer Straftat geht, der zumindest gleiches Gewicht wie der Tat zukommt, deretwegen die Daten ursprünglich gespeichert worden sind (Katalogdaten).
- Das Grundrecht der Betroffenen auf informationelle Selbstbestimmung erfordert regelmäßig die Benachrichtigung der Betroffenen von der erfolgten Datenspeicherung.

Die nun verabschiedete Regelung berücksichtigt einen wesentlichen Teil der aus der Sicht des Datenschutzes gegen die ursprüngliche Fassung geltend gemachten Bedenken. Das habe ich mit Befriedigung zur Kenntnis genommen. Der Kreis der Straftaten, derentwegen eine sogenannte Schleppnetzfahndung durchgeführt werden kann, ist eingeschränkt worden. Auch dürfen nur noch die anläßlich einer grenzpolizeilichen Kontrolle oder die bei einer Personenkontrolle nach § 111 StPO (Einrichtung von Kontrollstellen) angefallenen Daten und nicht mehr die anläßlich irgendeiner Personenkontrolle angefallen Daten in einer Datei gespeichert werden. Außerdem ist nun vorgesehen, daß die Anordnung derartiger Maßnahmen grundsätzlich durch den Richter zu erfolgen hat. Auch die Anforderungen an den Inhalt einer derartigen Anordnung sind wesentlich präziser. Ebenso ist die Zeitdauer der Speicherung nun begrenzt. Nach wie vor ist allerdings die Verwendung der zunächst zur Aufklärung ganz bestimmter sehr schwerer Straftaten gespeicherten Daten für andere Strafverfolgungszwecke zulässig, ohne daß der Gesetzgeber ausdrücklich Schranken gesetzt hätte, die von vornherein eine Beachtung des Grundsatzes der Verhältnismäßigkeit garantieren. Die Verwendung solcher durch Personenkontrollen erlangten personenbezogenen Daten zu anderen Zwecken wird daher in Zukunft besonders sorgfältig zu beobachten sein.

6.9. Strafvollzug

6.9.1. Novellierung des Strafvollzugsrechts

Im Rahmen des Strafvollzuges werden zahlreiche personenbezogene Daten der Gefangenen erhoben, gespeichert, an andere Stellen übermittelt oder auf sonstige Weise verarbeitet. Wegen dieser in der Natur der Sache liegenden umfangreichen Verarbeitung personenbezogener Daten im Strafvollzug sind die den Strafvollzug regelnden Vorschriften im Hinblick auf die vom Bundesverfassungsgericht im Volkszählungsurteil erarbeiteten Grundsätze um entsprechende Normen zu ergänzen.

Der Bundesminister der Justiz hat zwischenzeitlich eine entsprechende Entwurfsskizze zur Änderung des **Strafvollzugsgesetzes** vorgelegt. Ich begrüße es, daß sich die Justizverwaltungen nunmehr anschicken, auch für den Bereich des Strafvollzugs die erforderlichen Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts zu ziehen. Der „erste Versuch" einer entsprechenden Regelung scheint mir im Ansatz durchaus datenschutzfreundlich ausgefallen zu sein. Er enthält in vielen Punkten Vorschläge, die meine Zustimmung finden können. Bei der Weiterentwicklung dieses Entwurfs wird zu beachten sein, daß manche Regelungen noch einer Präzisierung bedürfen. Die Befugnisse, Daten von Gefangenen zu erheben und zu speichern, sollten noch konkretisiert und auf das Datenvolumen begrenzt werden, das zulässigerweise für die rechtmäßige Erfüllung der den Justizvollzugsanstalten gesetzlich zugewiesenen Aufgaben erforderlich ist. Gleiches gilt für einige Datenübermittlungsvorgänge. Im Hinblick auf das Gewicht, das das Bundesverfassungsgericht ausreichenden gesetzlichen Regelungen zur Datensicherung beigemessen hat, werden auch in einem Strafvollzugsgesetz die

notwendigen technisch-organisatorischen Maßnahmen näher beschrieben werden müssen. Ich habe zu der mir vorliegenden Entwurfsskizze eine umfangreiche Stellung1nahme mit zahlreichen Anregungen abgegeben und hoffe, daß sie im weiteren Gesetzgebungsverfahren berücksichtigt werden.

Zwischenzeitlich hat mir das Staatsministerium der Justiz auf meine Bitte hin auch den Entwurf eines **Jugendstrafvollzugsgesetzes** vorgelegt. Bereits eine erste Durchsicht hat allerdings ergeben, daß sich der Gesetzentwurf in weiten Bereichen an den Wortlaut des geltenden Strafvollzugsgesetzes anlehnt und damit bedauerlicherweise die neuere Rechtsprechung des Bundesverfassungsgerichts zum Persönlichkeitsrecht im allgemeinen und zum informationellen Selbstbestimmungsrecht im besonderen weitgehend außer Betracht läßt. Daß Belange des Persönlichkeitsschutzes und der Datenschutz in diesem Entwurf bislang völlig unbeachtet geblieben sind, verwundert mich um so mehr, als zum Strafvollzugsgesetz selbst, wie oben dargelegt, bereits konkrete Überlegungen für eine Berücksichtigung des Rechts auf informationelle Selbstbestimmung angestellt werden. Es dürfte wohl unbestreitbar sein, daß die vom Bundesverfassungsgericht im Volkszählungsurteil erarbeiteten Grundsätze auch im Bereich des Jugendstrafvollzuges entsprechende gesetzliche Regelungen für die Verarbeitung personenbezogener Daten erforderlich macht.

6.9.2. Überprüfung der Urlaubsanschriften von Strafgefangenen

Wird Strafgefangenen Urlaub gewährt, so wird häufig über die Person, bei der der Gefangene den Urlaub verbringen will, mit Einverständnis des Betroffenen eine Überprüfung durchgeführt. Das Problem der Überprüfung von Bezugspersonen Gefangener habe ich bereits im letzten Tätigkeitsbericht kurz angeschnitten. Weil mich gerade zu dieser Frage eine Reihe von Eingaben von Strafgefangenen erreicht hat, will ich jedoch hierauf noch einmal kurz eingehen:

Die Überprüfung der Bezugspersonen ist aus datenschutzrechtlicher Sicht als „Datenerhebung" zu werten. Im Bayer. Datenschutzgesetz ist die Zulässigkeit einer Erhebung personenbezogener Daten nicht ausdrücklich festgelegt. Jedoch wird man aus diesem Gesetz folgern können, daß eine Datenerhebung mit Sicherheit immer dann erfolgen kann, wenn der Betroffene sein Einverständnis zu dieser Maßnahme erteilt. Die für diese Zwecke erstellten Vordrucke einer Justizvollzugsanstalt sehen nun eine entsprechende Einverständniserklärung der Betroffenen vor. Wenn der Betroffene im Einzelfall mit der Erholung von Auskünften über ihn nicht einverstanden ist, steht es ihm frei, die vorgelegte Erklärung nicht abzugeben. Diese Vorgehensweise vermag ich datenschutzrechtlich im Grundsatz nicht zu beanstanden. Natürlich verkenne ich nicht, daß auf dem Betroffenen, der zumeist in einer mehr oder weniger engen Beziehung zum Gefangenen stehen dürfte, ein gewisser Druck lastet, die von der Anstalt gewünschte Erklärung abzugeben. Er muß befürchten, daß eine Verweigerung des Einverständnisses im Ergebnis zu einer Ablehnung des Urlaubs- oder Besuchsantrages für den Gefangenen führen kann. Dies kann jedoch letztlich die Freiwilligkeit der Erklärung nicht durchgreifend beeinträchtigen. Es gehört nämlich grundsätzlich zu den legitimen Aufgaben einer Justizvollzugsanstalt, sich zu vergewissern, daß ein Gefangener während seines Urlaubs oder sonstigen Ausgangs oder durch einen Besuch nicht in ein soziales Umfeld gerät, das einen schädlichen Einfluß auf ihn ausüben könnte. In diesem Zusammenhang kann es auch erforderlich sein, nähere Auskünfte über die Bezugsperson einzuholen, zu der der Gefangene in Kontakt treten möchte. Ist der Justizvollzugsanstalt in diesen Fällen die Erhebung der erforderlichen Daten nicht möglich, muß der Gefangene mit einer Ablehnung seines Antrages rechnen. Dies ist eine vom Gesetz vorgesehene Rechtsfolge, die den freien Willen der betroffenen Bezugsperson unberührt läßt. Für eine willkürliche Vorgehensweise der Justizvollzugsanstalten bei Urlaubs- oder Besuchsanträgen habe ich keine Anhaltspunkte gewinnen können.

Bei fehlendem Einverständnis des Betroffenen kann die Justizvollzugsanstalt im übrigen Auskünfte von Sozialleistungsträgern, die dem Sozialgeheimnis unterliegen, regelmäßig nicht erhalten.

7. Städte und Gemeinden

7.1. Überblick

Bemerkenswert erscheint mir die stetige Verstärkung des DV-Einsatzes im kommunalen Bereich. Sie betrifft sowohl die Übernahme bewährter DV-Verfahren für bestimmte Verwaltungsaufgaben auf immer mehr Städte und Gemeinden als auch die Automatisierung weiterer, bisher noch nicht automatisierter Verwaltungsverfahren und die Verbreitung des Einsatzes von Personal-Computern in bisher nicht für automationswürdig gehaltenen Bereichen.

Aus der Sicht des Datenschutzes beobachte ich nicht ganz ohne Sorge vereinzelt eine Tendenz, die Speicherung und Abrufbarkeit personenbezogener Daten aus sehr unterschiedlichen Arbeitsbereichen einer Kommune so zu gestalten, daß alle Daten von einem einzigen Terminal aus abrufbar sind. Es bedarf noch gründlicher Prüfung, ob und inwieweit mit solchen Terminals ein Querschnittsüberblick, wie er sich durch den Zugriff auf personenbezogene Daten eines Einwohners aus verschiedenen Verwaltungsbereichen der Kommune ergeben kann, überhaupt rechtmäßig genutzt werden kann. Dabei ist zu klären, ob hier Ansätze zur Entstehung und Nutzung rechtlich problematischer Persönlichkeitsprofile vorliegen.

Anfragen von Kommunen beim Landesbeauftragten für den Datenschutz, die sich auf die datenschutzrechtliche und -technische Bewertung von Automationsvorhaben oder Datenspeicherungen bzw. -übermittlungen beziehen, begrüße ich. Erfahrungsgemäß muß ich aber davon ausgehen, daß trotz der Freigabevorschrift des Art. 26 Abs. 2und 4 BayDSG durchaus nicht alle Datenverarbeitungskonzeptionen mitgeteilt werden, obwohl sie jeweils die betreffende Datenverarbeitung für die nächsten zehn bis zwanzig Jahre festlegen. In diesen Fällen habe ich keine Gelegenheit, zusätzliche datenschutzrechtliche Gesichtspunkte in die Konzeption einzubringen, was letztendlich auch zu Beanstandungen führen kann.

Häufig ist es bei Anfragen aus dem kommunalen Bereich geboten, die jeweiligen Aufsichtsbehörden über die Fragestellung zu unterrichten. Soweit die Kommunen diesen Weg nicht von sich aus eingeschlagen haben, verständige ich die Aufsichtsbehörden in solchen Fällen zumindest durch Abdruck meines Schreibens. Wiederholt habe ich auch anfragende Stellen gebeten, sich unmittelbar an Aufsichtsbehörden zu wenden, z. B. wenn Datenschutzaspekte eines Problems nur eine untergeordnete Rolle spielen.

Aus meiner Sicht begrüße ich auch, daß in einer Reihe von Fortbildungsveranstaltungen sachkundige Mitarbeiter meiner Geschäftsstelle für Referate und Diskussionen eingeschaltet wurden. Auf diese Weise kann ich nicht nur meine Erfahrungen Sachbearbeitern aus Kommunalbehörden mitteilen, sondern auch von dort unmittelbar Sorgen, Probleme und Erfahrungen kennenlernen und um Verständnis für das Anliegen des Datenschutzes werben.

7.2. Unzulässige Verwendung von Steuerdaten für andere Zwecke der Gemeinde

Wie bekannt, verwenden Gemeinden personenbezogene Daten, wie Namen, Anschrift und Objekt (Grundstück) eines Steuerpflichtigen nicht nur im gemeindlichen Steuerverfahren, sondern auch für andere gemeindliche Zwecke, beispielsweise für die Erhebung von Müllabfuhr- und Straßenreinigungsgebühren sowie für die Erstellung von „Objektlisten". Die Einzelheiten des Sachverhalts wurden im letzten Tätigkeitsbericht unter Nr. 8.1, Seite 39, dargestellt. Trotz wiederholter Hinweise seitens des Landesbeauftragten für den Datenschutz hat sich noch keine Änderung der rechtlichen Situation ergeben.

Die Nutzung von Daten aus dem gemeindlichen Steuerbereich für den Bereich der sonstigen Kommunalverwaltung widerspricht nach wie vor der geltenden Rechtslage. Es sei erneut im Rahmen des Tätigkeitsberichts auf die Notwendigkeit einer Rechtsänderung hingewiesen. Die Alternative, nämlich eine Änderung in der Verfahrensweise der Gemeinden, würde einen erheblichen Mehraufwand an Datenerhebung sowie die völlige Änderung einer Vielzahl von EDV-Programmen im Bereich des gemeindlichen Steuer- und Abgabewesens erfordern. Ich gehe davon aus, daß meine diesbezüglichen Anregungen gegenüber den Bayerischen Staatsministerien des Innern und der Finanzen und nicht zuletzt die Unterrichtung des Beirats beim Landesbeauftragten für den Datenschutz über das Problem, eine Beanstandung vorläufig entbehrlich machen.

Das Bayerische Staatsministerium des Innern hat mitgeteilt, daß erfolgversprechende Verhandlungen zur Änderung der Abgabenordnung laufen.

7.3. Bei Einsichtnahme in Planfeststellungsverfahren Namen registriert

Eine Stadt hatte Unterlagen für ein Planfeststellungsverfahren zur gesetzlich vorgesehenen Einsichtnahme der Bürger ausgelegt. Ein Beschwerdeführer, der sich an mich wandte, war vor der Einsichtnahme aufgefordert worden, Namen und Adresse in eine Liste einzutragen, die dort auflag. Er trug sich zunächst ein, löschte die Angaben jedoch wieder. Ein städtischer Bediensteter hob die Löschung mit Tipp-Ex wieder auf und setzte Namen und Adresse wieder ein. Zur Begründung wurde vorgetragen, man wolle wissen, wieviele Einsichtnehmende es seien und woher sie kämen. Nach dieser Auswertung würden die ausgelegten Listen vernichtet.

Der Petent befürchtete, von den zuständigen Stellen wegen der Einsichtnahme in den Plan eines in der Öffentlichkeit umstrittenen Planfeststellungsverfahrens für einen Gegner des Projektes gehalten zu werden. Dies hielte er für einen Mißbrauch von möglicherweise unerlaubt gesammelten Daten.

Das zuständige Staatsministerium hat auf meine Bitte zu diesem Sachverhalt Stellung genommen und mitgeteilt, das Festhalten identifizierender Personalien erscheine für den Zweck der öffentlichen Auslegung nicht erforderlich, sondern allenfalls zweckmäßig. Keinesfalls bestand eine Pflicht zur Angabe von Daten für die Einsichtnehmenden. Die Angabe von Namen und Anschrift war daher rechtlich gesehen freiwillig.

Die Stadt hat im vorliegenden Fall ohne den in Art. 16 Abs. 2 BayDSG gebotenen Hinweis auf die Freiwilligkeit Daten der Einsichtnehmenden erhoben. Art. 16 Abs. 2 BayDSG ist auch dann zu beachten, wenn im Zeitpunkt der Erhebung der Daten beim Betroffenen noch nicht feststeht, ob die Daten anschließend in einer Datei gespeichert werden sollen bzw. auch dann, wenn zum Zeitpunkt der Datenerhebung positiv feststeht, daß die Daten nicht in einer Datei gespeichert werden (vgl. Schweinoch/Geiger/Weigert, Kommentar zum Bayerischen Datenschutzgesetz, Art. 16 Rd.Nr. 13).

Darüber hinaus war die Datenerhebung auch geeignet, in Einzelfällen Betroffene von der Wahrnehmung ihrer gesetzlichen Rechte abzuhalten. Es ist nicht auszuschließen, daß Bürger von der Einsichtnahme Abstand nehmen, wenn die Einsichtnahme – unzulässigerweise, noch dazu ohne Hinweis auf die Freiwilligkeit – von der Angabe von Name und Adresse abhängig gemacht wird und sie dadurch Nachteile befürchten.

Die Registrierung von Namen und Anschrift der Einsichtnehmenden durch die Stadt wurde daher beanstandet.

7.4. Weitergabe personenbezogener Daten aus Bautenverzeichnissen

Nach Erhebungen des Bayer. Staatsministeriums des Innern werden bei Gemeinden „Bautenverzeichnisse" in sehr unterschiedlicher Form geführt. So geschehe dies in Büchern, manuellen Karteien oder Listen In einem Fall sei eine automatisierte Speicherung festgestellt worden. Erfaßt würden in der Regel Angaben aus einzelnen Bauanträgen, wie Eingangsdatum, Namen und Anschrift des Bauherrn, genaue Bezeichnung des Bauvorhabens, Angaben über das Baugrundstück, Name des Entwurfsverfassers sowie Angaben zum weiteren Verlauf des Baugenehmigungsverfahrens wie Datum der Genehmigung, Versagung der Genehmigung, Beginn und Ende der Baumaßnahme. In einzelnen Fällen würden darüber hinaus noch weitere verfahrensbezogene Daten vorgehalten. Eine Weitergabe von Daten aus diesen „Bautenverzeichnissen" an Baustelleninformationsdienste und an lokale Zeitungen erfolge grundsätzlich nur mit Zustimmung der Bauherren. Private Dritte erhielten Einsicht allenfalls, wenn sie ein berechtigtes Interesse geltend machten; vereinzelt würden Daten auch an Sparkassen und Banken übermittelt.

Hierzu habe ich auf folgendes hingewiesen:

- Soweit die Daten des gemeindlichen Bautenverzeichnisses aus anderen Dateien der Gemeinde stammen, muß eine solche innergemeindliche Datenübermittlung an den Voraussetzungen des Art. 17 Abs. 1 i.V. m. Art. 17 Abs. 3 BayDSG geprüft werden. Im Hinblick auf das informationelle Selbstbestimmungsrecht ist insbesondere darauf zu achten, daß mit der Datenweitergabe keine unverhältnismäßige Änderung des Nutzungszweckes verbunden ist. Einer Weitergabe von Daten aus der gemeindlichen Grundsteuerdatei steht nach der derzeitigen Rechtslage § 30 AO entgegen.

- Soweit Daten aus dem gemeindlichen Bautenverzeichnis weitergegeben werden, ist zu unterscheiden, ob die Datenweitergabe an öffentliche Stellen oder an Personen oder Stellen außerhalb des öffentlichen Bereichs erfolgt. Eine Weitergabe an öffentliche Stellen ist ebenfalls an Art. 17 BayDSG zu messen.
- Wird das Verzeichnis nicht in Dateiform geführt, kann gleichwohl zur Klärung der Frage, ob eine Weitergabe mit dem informationellen Selbstbestimmungsrecht des Betroffenen in Widerspruch steht, Art. 17 BayDSG herangezogen werden. Änderungen des Nutzungszwecks, die hierbei eintreten, werden dabei auf Verhältnismäßigkeit zu prüfen sein.

  Soweit Daten an Personen und Stellen außerhalb des öffentlichen Bereichs weitergegeben würden, bzw. diesen Einsicht gewährt würde, beurteilt sich die Zulässigkeit nach Art. 18 BayDSG. Hierbei ist bei dateimäßiger Führung des Verzeichnisses Art. 18 direkt anzuwenden. Bei nichtdateimäßiger Führung kann der Grundgedanke des Art. 18 BayDSG anerkanntermaßen ebenfalls herangezogen werden. Danach kommt es darauf an, inwieweit schutzwürdige Belange der betroffenen Bauherren durch die Datenübermittlung beeinträchtigt werden. Alleine die Geltendmachung eines berechtigten Interesses an einer Auskunft aus dem Bautenverzeichnis rechtfertigt noch keine Datenweitergabe. Dies gilt auch für die Datenweitergabe an Banken oder Kreditinstitute. Für diese Empfängerkreise halte ich die Einwilligung der Betroffenen zur Datenweitergabe für erforderlich.

Das Bayerische Staatsministerium des Innern hat in diesem Zusammenhang darauf hingewiesen, daß Art. 84 BayBO nur auf die Veröffentlichung von Baudaten im dort näher genannten Umfang anzuwenden ist. Voraussetzung ist in diesem Zusammenhang, daß der Betroffene der Veröffentlichung nicht widersprochen hat. Erfaßt ist die allgemeine listenmäßige oder sonstige regelmäßige und systematische Heraus- oder Weitergabe von Daten eines Bauvorhabens durch die Behörde zum Zwecke der Veröffentlichung. Die Weitergabe von Daten aus dem Bautenverzeichnis an Einzelpersonen oder die Presse richtet sich jedoch nicht nach Art. 84 BayBO sondern nach Art. 30 Bayer. Verwaltungsverfahrensgesetz bzw. bei der Speicherung der Baudaten in einer Datei nach Art. 18 BayDSG. Die Behörde hat dabei nach den zu dieser Vorschrift entwickelten Maßstäben zu überprüfen, ob sie zur Auskunftserteilung befugt ist. Dabei kann eine Güterabwägung erforderlich sein, insbesondere mit dem grundsätzlich der Presse gem. § 4 Abs. 1 Satz 1 des Bayer. Pressegesetzes zustehenden Auskunftsrecht (vergl. aber auch § 4 Abs. 2 Satz 2 BayPrG).

Die Bekanntgabe der vorstehenden Grundsätze an die nachgeordneten Behörden durch das Bayerische Staatsministerium des Innern begrüße ich.

7.5. Automatisierte Verarbeitung von Melde- und Steuerdaten bei einer Privatfirma

Eine bayerische Gemeinde ließ Teile ihrer Aufgaben nach dem Bayerischen Meldegesetz durch eine Privatfirma erledigen. Dies war mit Art. 36 Abs. 1 BayMeldeG nicht vereinbar und verstieß daher gegen die datenschutzrechtliche Vorschrift des Art. 6 BayMeldeG.

Nach Art. 36 BayMeldeG können die Meldebehörden im Bereich des Bayerischen Meldegesetzes andere Gemeinden oder die Anstalt für Kommunale Datenverarbeitung in Bayern zur Abwicklung automatischer Verfahren beauftragen. Im Umkehrschluß hierzu ist – im Hinblick auf die Sensibilität der Daten des Melderegisters – eine Auftragsdatenverarbeitung durch private Stellen als nicht zugelassen anzusehen. Eine andere rechtliche Beurteilung ergibt sich auch nicht aus der amtlichen Begründung zum Bayerischen Meldegesetz. In der Landtagsdrucksache 10/164 vom 21.12.1982 ist zu Art. 36 ausgeführt: „Abs. 1 schließt die Möglichkeit nicht aus, einzelne Datenverarbeitungsaufträge, wie etwa die Erfassung von Daten an private Service-Rechenzentren zu übertragen, soweit dabei die Voraussetzungen dieses Gesetzes und des Bayerischen Datenschutzgesetzes für die Auftragsdatenverarbeitung beachtet werden. Die vollständige Übertragung aller mit der automatisierten Führung des Melderegisters zusammenhängenden Aufgaben an private Auftragnehmer schließt Abs. 1 jedoch aus." Die Meldedaten unterliegen in ihrer Gesamtheit der besonderen Amtsverschwiegenheit des Meldegeheimnisses und gelten als sensibel (vgl. Ziff. 3.3 der Vollzugsbekanntmachung zum Bayerischen Datenschutzgesetz).

Die Gemeinde hatte aber nicht nur Meldedaten, sondern auch im Bereich Abgabenerhebung und Besteuerung Auftragsdatenverarbeitung mit der Privatfirma vereinbart. Ich habe dies für nicht vereinbar mit § 30 der Abgabenordnung (Steuergeheimnis) erachtet. Auch Steuer- und Abgabedaten gelten, da sie dem Steuergeheimnis unterliegen, als besonders sensible und schutzwürdige Daten, die grundsätzlich nicht zur Datenverarbeitung an Private abgegeben werden dürfen (vgl. Ziff. 3.3 VollzBekBayDSG). Damit soll einer unzulässigen Offenbarung steuerlicher Daten entgegengewirkt werden (§ 30 Abs. 4 AO).

Die Auftragsdatenverarbeitung der Gemeinde durch eine private Firma mußte wegen Verletzung der vorgenannten Vorschriften über den Datenschutz beanstandet werden. Ich habe die Gemeinde aufgefordert, eine Änderung umgehend in Angriff zu nehmen und datenschutzgerechte Alternativen vorzustellen. Eine entsprechende Änderung hat die Gemeinde in Aussicht gestellt.

8. Einwohnermelderegister

8.1. Anpassung des Melderegisters an den gesetzlichen Rahmen

Art. 43 Abs. 1 des Bayerischen Meldegesetzes schreibt die Löschung von Daten, die über den in Art. 3 des Meldegesetzes festgelegten Datenrahmen hinausgehen bis zum 31.12.1984 vor. Ich habe im Berichtszeitraum daher verschiedene Gespräche, u. a. mit der Anstalt für Kommunale Datenverarbeitung in Bayern, über die Anpassung der früheren Datenspeicherungen an den nunmehr gesetzlich vorgeschriebenen Rahmen für das Melderegister geführt. Dabei konnte ich jedenfalls bei der AKDB, die für eine Vielzahl bayerischer Meldeämter die Melderegister automatisiert führt, feststellen, daß vorgesehen ist, sensiblere Daten, wie z. B. Wahlausschlußgründe, mit einer eigenen Routine zu löschen und (von der AKDB) für weniger sensibel erachtete Felder dann zu löschen, wenn der Datensatz aus anderen Gründen verarbeitet wird. Es werde gleichzeitig sichergestellt, daß die über Art. 3 MeldeG hinausgehenden Daten nicht mehr genutzt werden können.

Allerdings legte die AKDB auf die Feststellung Wert, daß es in der Verantwortung der Meldebehörden liege, nur melderechtlich zulässige Daten beispielsweis ein Bemerkungsfeldern zu speichern.

Bei anderen Städten und Gemeinden, die ihr Meldewesen selbst automatisiert haben, konnte ich im Wege der Beratung eine Anpassung der Datensätze an das geltende Melderecht erreichen.

8.2. Weitergabe des Ordnungsmerkmals aus dem automatisierten Einwohnermeldewesen

Gemäß Art. 4 des Bayerischen Meldegesetzes darf bei der Übermittlung von Meldedaten das bei der Automatisierung des Melderegisters verwendete Ordnungsmerkmal für registrierte Einwohner nur für diese Übermittlungen, nicht jedoch für sonstige Zwecke der Stelle verwendet werden. Wie bereits früher berichtet, wird diese Verwendungsbeschränkung vom Landesbeauftragten für den Datenschutz kontrolliert. Sie soll nach dem Willen des Meldegesetzes sicherstellen, daß das Ordnungsmerkmal nicht zu einem allgemeinen, das Meldewesen überschreitenden, Verknüpfungsmerkmal wird.

Im Rahmen dieser Überprüfung wurde bei einer Stadt festgestellt, daß immer noch regelmäßig an ein Finanzamt in einer Liste Ordnungsmerkmale zusammen mit anderen Daten von Einwohnern übermittelt wurden. Gegen die Übermittlung der übrigen Daten bestand kein Einwand. Die Weitergabe des Ordnungsmerkmals war jedoch nicht „erforderlich" im Sinne der vorgenannten Vorschrift. Die Stadt hat nun bei Weitergabe der Daten (aus den Lohnsteuerkarten) den Ausdruck des Ordnungsmerkmals auf der Liste entfallen lassen.

8.3. Fehlerhaftes Antragsformular auf Einrichtung melderechtlicher Datenübermittlungssperren

Auch im Berichtszeitraum wurde festgestellt, daß Meldebehörden für die Eintragung von Übermittlungssperren nach dem Bayer. Meldegesetz (Art. 32, 34, 35) Vordrucke eines bayerischen Formularverlags verwenden, die dem geltenden Recht zuwiderlaufen.

So wird beispielsweise eine vom Gesetz nicht vorgesehene Begründung des Bürgers verlangt, weshalb er der Weitergabe seiner Daten an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung nach Art. 35 Abs. 1 Satz 3 MeldeG widersprechen will (siehe Nr. 9.1 meines 7. Tätigkeitsberichts).

Obgleich ich den Verlag und verschiedene Gemeinden, von denen ich erfuhr, daß sie das fehlerhafte Formular verwenden, auf die Unrechtmäßigkeit dieser Begründungspflicht sowie auf vorhandene weitere Mängel hingewiesen habe, ist es mir aus folgenden Gründen nicht gelungen, den generellen Verzicht auf dieses Formblatt in ganz Bayern zu erreichen:

1. Viele Gemeinden gehen im Vertrauen auf die fachliche Erfahrung ihres Formularverlags von der Rechtmäßigkeit des Inhalts angebotener Vordrucke aus.
2. Der Bürger vertraut seinerseits der Verwaltung und beanwortet – weil ihm vielfach präzise Rechtskenntnisse fehlen – die gestellten Fragen in der Annahme, daß sie rechtmäßig sind.
3. Der Landesbeauftragte für den Datenschutz erfährt nur in Einzelfällen (Anfragen von Meldebehörden oder Bürgern, bzw. durch Datenschutzkontrollen), daß fehlerhafte Formulare verwendet werden. Mangels Zuständigkeit für den nichtöffentlichen Bereich kann er vom Verlag die Information, an welche Gemeinden das Formular verkauft worden ist, nicht verlangen.

Es bleibt zu hoffen, daß die Meldebehörden bei Auswertung dieses Tätigkeitsberichts das besagte Formular bei Feststellen der Unrechtmäßigkeit aus dem Verkehr ziehen und vom Verlag durch ein der Rechtslage angepaßtes ersetzen lassen.

Ich darf in diesem Zusammenhang zum wiederholten Male daran erinnern, daß alle bayerischen öffentlichen Stellen verantwortlich und verpflichtet sind, Datenerhebungen – insbesondere mit Vordrucken und Formularen – nur unter den in Art. 16 Abs.2 BayDSG vorgesehenen Voraussetzungen vorzunehmen.

Besonders begrüßenswert ist insoweit die unter Nr. 16.2 meines 7. Tätigkeitsberichts angesprochene und inzwischen erfolgte Ergänzung der „Staatlichen Vordruckrichtlinien" um datenschutzrechtliche Anforderungen an Erhebungsvordrucke (MABl. Nr. 8/1986, Seite 161), an denen sich auch nichtstaatliche bayerische Behörden orientieren sollten.

9. Personalwesen

9.1. Überblick

Die automatisierte Verarbeitung von Personaldaten wird bei Behörden künftig immer mehr Bedeutung erlangen - das zeigen eine Reihe von Anfragen sowie Mitteilungen über Datenverarbeitungskonzepte. In verschiedenen Behörden laufen Vorarbeiten für automatisierte Verfahren zur Verarbeitung von Personaldaten. Sie reichen von der automatisierten Abwicklung einzelner Verwaltungsaufgaben der Personalstellen bis zu Bemühungen um die Einrichtung dialogunterstützter Personal- und Stellenverwaltungssysteme. In Teilbereichen liegen praktische Erfahrungen mit der Verarbeitung von Personaldaten vor. Auch einzelne Meldungen über die Freigabe automatisierter Verfahren zur Verarbeitung von Personaldaten haben mich erreicht. Für Personalverwaltungen, die erstmalig solche Verfahren planen, sei daher auch an Artikel 26 Abs. 2 und 4 BayDSG erinnert. Danach ist der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, durch die oberste Dienstbehörde schriftlich freizugeben. Der Landesbeauftragte für den Datenschutz ist hiervon zu unterrichten.

Eine größere Zahl von Anfragen bezog sich auf die Registrierung und Nutzung von Telefongesprächsdaten. Nachdem ich im letzten Tätigkeitsbericht hierzu ausführlich Stellung genommen hatte, seien nachfolgend (siehe unten 9.3) die für den staatlichen Bereich nunmehr aufgestellten Grundsätze der Telefongesprächsdatenverarbeitung zusammengefaßt.

Wesentlich schwieriger als bei den bisher anzutreffenden ADV-Verfahren wird sich die Analyse und Bewertung automatisierter Verarbeitung von Personaldaten jedoch dann gestalten, wenn der Bereich einzelner Verwaltungsaufgaben und der hierfür speziell erforderlichen Automation

verlassen wird und zusammengefaßte Daten zur Abwicklung verschiedener Aufgaben der Personalverwaltung dienen sollen. Durch umfangreiche Zusammenfassungen könnten Informationen mit neuer Qualität und zusätzliche Möglichkeiten zur Auswertung der Personaldaten geschaffen werden, die bei isolierten, untereinander nicht verbundenen automatisierten Verfahren kaum bestehen. Hieraus könnten sich auch – gegenüber der herkömmlichen Verarbeitung von Personaldaten – neue Belastungen für die Betroffenen ergeben.

9.2. Zur künftigen Entwicklung der automatisierten Verarbeitung von Personaldaten bei öffentlichen Stellen

Ausgangspunkt der Auseinandersetzung mit Neuentwicklungen auf dem Gebiet der Personaldatenverarbeitung ist die Frage nach deren Rechtsgrundlagen. Hierzu ist festzustellen, daß das Personaldatenrecht des öffentlichen Dienstes nur lückenhaft gesetzlich geregelt ist. Es wird weitgehend von hergebrachten und durch die Rechtsprechung bestätigten ungeschriebenen Rechtsgrundsätzen bestimmt. Auf Bundesebene sind inzwischen Vorarbeiten zur Neuregelung des Personalaktenrechts eingeleitet, um den Problembereich umfassend auf eine gesetzliche Grundlage zu stellen. Es ist damit zu rechnen, daß auch das Bundes-Rahmenrecht eine entsprechende Ergänzung erfährt.

Normiert ist bisher in Art. 100 BayBG die Pflicht zur Personalaktenführung im Beamtenverhältnis. Für die Angestellten des öffentlichen Dienstes setzt dagegen § 13 BAT ein Recht des Dienstherrn auf Führung von Personalakten offensichtlich voraus. Beide Vorschriften lassen aber offen, was Inhalt der Personalakten ist, bzw. sein darf. Letztlich folgt das Recht und die Pflicht einer Behörde zur Führung von Personalakten aber auch zwingend aus der Natur des öffentlichen Dienstverhältnisses als solches. Nach der Rechtsprechung sind Personalakten eine Sammlung von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse eines Beamten betreffen, sofern sie in einem inneren Zusammenhang mit dem Beamtenverhältnis stehen. Dieser Grundsatz des materiellen Personalaktenbegriffs wird ergänzt durch den Grundsatz der Vollständigkeit der Personalakten. Danach sind sämtliche einmal in die Personalakten gelangten Vorgänge dort zu belassen, um den dienstlichen Werdegang des Beamten lückenlos festzuhalten. Begrenzt wird dies durch die in Art. 86 BayBG verankerte Fürsorge- und Schutzpflicht des Dienstherrn und das informationelle Selbstbestimmungsrecht der Betroffenen.

Das BVerfG hat im Volkszählungsurteil gerade auch im Hinblick auf die moderne Entwicklung der Datenverarbeitung ausgeführt: „Eine freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 GG i.V.m. Art.1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Grundsätzlich muß der Einzelne Einschränkungen dieses Rechts im überwiegenden Allgemeininteresse – nach Maßgabe einer verfassungsmäßigen gesetzlichen Grundlage hinnehmen. Dementsprechend beeinflußt das Recht auf informationelle Selbstbestimmung auch die rechtliche Bewertung automatisierter Verarbeitung von Personaldaten.

Werden Personaldaten in automatisierten Dateien geführt, finden die Vorschriften des Bayer. Datenschutzgesetzes Anwendung, da das Personaldatenrecht bereichsspezifische Vorschriften über den Datenschutz bisher nicht enthält. Aus der Sicht des Datenschutzes ist damit im Ergebnis die Speicherung personenbezogener Daten in einem automatisierten Verfahren zulässig, wenn und soweit – unter Berücksichtigung des Personalaktengeheimnisses und der wesentlichen Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil – die Daten zur „rechtmäßigen Erfüllung der durch Rechtsnorm der speichernden Stelle zugewiesenen Aufgaben erforderlich" sind.

Bei der Prüfung der Erforderlichkeit einer Datenspeicherung zur rechtmäßigen Aufgabenerfüllung ist daher auch auf den oben näher erläuterten Begriff der Personalakte abzustellen. Wie erwähnt, handelt es sich um Angaben, die die persönlichen und dienstlichen Verhältnisse eines Beamten betreffen, sofern sie in einem inneren Zusammenhang mit dem Beamtenverhältnis stehen. Der „Zusammenhang mit dem Beamtenverhältnis" stellt jedenfalls eine äußerste Grenze für die Einbeziehung personenbezogener Daten in die automatisierte Verarbeitung und damit auch für die Zulässigkeit einer Datenspeicherung dar. Weitere einschränkende Anforderungen können sich anhand der dem jeweiligen Dienstherren im konkreten Fall zugewiesenen Aufgaben und der für das jeweilige Datum vorgesehene Nutzungen ergeben.

Die Prüfung der Erforderlichkeit zur rechtmäßigen Aufgabenerfüllung muß sich aber auch darauf erstrecken, ob sich nicht bereits bei der Übernahme von Daten aus der Personalakte in ein bestimmtes automatisiertes Verfahren die Frage nach der Verhältnismäßigkeit neu stellt. Gerade bei Personaldaten kann die Aufnahme eines Datums in einen Personalbogen bzw. das Vorhandensein im Personalakt zur gesetzlichen Aufgabenerfüllung völlig ausreichend sein. Dies vor allem dann, wenn eine daneben geführte automatisierte Personaldatei dazu bestimmt ist, die herkömmlichen Personalakten zu ergänzen. Die Prüfung der Verhältnismäßigkeit bezieht sich demnach auf die Frage, ob das jeweilige automatisierte Verfahren gegenüber der herkömmlichen Verarbeitung der Daten in den Personalakten weitere ADV-spezifische Wirkungen – insbesondere belastender Art für die Betroffenen – auslösen könnte.

Zunächst einmal sei – ganz ohne Wertung – festgestellt, daß Automatisierung eine erhöhte Verfügbarkeit und damit Verwertbarkeit der betreffenden Angaben bewirkt. Das heißt z.B., daß Angaben über eine bestimmte Person im automatisierten Verfahren wesentlich schneller auffindbar und nutzbar sind, als in einer evtl. umfangreicheren Akte. Dasselbe gilt auch für die Suche nach den gleichen Angaben bei einer größeren Gruppe von Betroffenen (z.B. bei allen Bediensteten der Behörde bzw. des Bereichs auf den sich das ADV-Verfahren bezieht). Das jeweilige Datum ist also im Hinblick auf die einzelne Person schneller greifbar. Es ist aber im automatisierten Verfahren auch „in Sekundenschnelle" mit den entsprechenden Daten einer großen Zahl anderer Bediensteter vergleichbar. Bei der Aufbewahrung der Daten in Akten wäre dies nur mit unverhältnismäßigem Zeitaufwand möglich. Außerdem können verschiedene Daten, die aus unterschiedlichen Teilen der Personalakten

stammen, wenn sie automatisiert gespeichert sind, als Such- oder Auswahlkriterien nutzbar sein, so daß u. U. maschinell einzelne oder Untergruppen der gesamten gespeicherten Personenzahl nach kombinierten Gesichtspunkten herausgesucht werden können. Schließlich wäre auch eine evtl. Verknüpfbarkeit von Daten mit anderen im gleichen ADV-System oder Datenbanksystem gespeicherten Daten in die Bewertung einzubeziehen.

Diese ADV-spezifischen Wirkungen kann man als erhöhte Verfügbarkeit und breitere Nutzbarkeit der Daten zunächst einmal objektiv feststellen, ohne daß dies bereits eine kritische Bewertung aus Datenschutzsicht zu enthalten braucht. Es ist jedoch Aufgabe des Datenschutzbeauftragten, darauf zu achten, daß sich aus solchen ADV-spezifischen Möglichkeiten bei den einzusetzenden Verfahren keine bedenklichen, belastenden Konsequenzen ergeben. Bei den einfachen, gegenwärtig eingesetzten Personalverwaltungs-Verfahren sind mir bisher derartige Probleme nicht bekannt geworden. Bei künftig denkbaren umfassenderen Verfahren zur Verarbeitung von Personaldaten ist dagegen zu prüfen, ob sie etwa zu schablonenartigen, dem tatsächlichen Fall nicht hinreichend gerecht werdenden Entscheidungen verleiten könnten, weil Inhalte der Personalakte nur auszugsweise und verkürzt übernommen würden, oder ob neue Informationen durch Kombination von Daten aus verschiedenen Arbeitsbereichen der Personalverwaltung hergestellt würden, die im herkömmlichen Verfahren nicht oder nur durch erheblichen Aufwand aufbereitbar wären. Eine Schwierigkeit bei der Bewertung solcher von der Automationstechnik gegebener Möglichkeiten liegt darin, daß die möglichen Kombinationen einer Vielzahl von Daten schwerlich alle zuverlässig von vorneherein abschätzbar sind.

Maßnahmen zur Verhinderung oder Abschwächung etwaiger belastender Wirkungen könnten dann ein Gebot der Verhältnismäßigkeit und damit der „Erforderlichkeit zur rechtmäßigen Aufgabenerfüllung" sein. Maßnahmen gegen unerwünschte Wirkungen einer Automation müßten sich möglicherweise gegen Projekte mit allzu umfangreichem Speicherungsdatensatz und gegen die Beliebigkeit von Verknüpfungs- und Auswahlmöglichkeiten, also gegen eine unbegrenzte Nutzung spezifischer ADV-Möglichkeiten richten. Selbstverständlich muß sich die Prüfung daneben auch auf die Sensibilität der Einzeldaten und deren Erforderlichkeit zur Erfüllung bestimmter einzelner Verwaltungsaufgaben beziehen. Außerdem sind hier auch Mitbestimmungsfragen angesprochen.

Bei der Bewertung typischer Automationsfolgen der Personaldatenverarbeitung wird man in nächster Zeit noch einige Erfahrungen sammeln müssen. Bisher stand – wie erwähnt – die Beurteilung von Automationsverfahren, die in ihrer Auswirkung beschränkt waren, weil sie nur einzelne Teile der Personalverwaltungsarbeit unterstützten, im Vordergrund. Dabei wurden im wesentlichen Datensätze und Feldbeschreibungen im Verhältnis zu den betreffenden abgegrenzten Verwaltungsaufgaben im einzelnen überprüft.

9.3. Telefongesprächsdatenerfassung

Zunächst sei auf die ausführliche Wiedergabe meiner Überlegungen zum Thema „Telefongesprächsdatenerfassung" im 7. Tätigkeitsbericht unter Nr. 11.3 (S. 49/51) verwiesen. Mitte 1986 hat nun das Bayerische Staatsministerium der Finanzen in einem Schreiben an die Staatskanzlei und alle Staatsministerien Grundsätze zur Wahrung der Belange des Datenschutzes und der berechtigten Interessen sowohl des Dienstherrn wie der Bediensteten bei der Registrierung und Nutzung von Telefongesprächsdaten mitgeteilt. Da es sich um datenschutzrechtlich sehr bedeutsame Festlegungen für den Einsatz von Einrichtungen zur selbsttätigen Gebührenerfassung handelt, seien nachfolgend die mir besonders wichtig erscheinenden Punkte wiedergegeben:

1. Allgemeines

Zweckbindung: Erfaßte und gespeicherte Gesprächsdaten dürfen nur zur Abrechnung von Gebühren, zur Wirtschaftlichkeitsüberprüfung der Fernmeldeanlagen und für Aussagen über die Verkehrsleistung und Betriebsweise der Anlagen ausgedruckt oder in anderer Weise abgerufen werden.

Sicherungsmaßnahmen: Zur Sicherstellung der Zweckbindung müssen technische und organisatorische Maßnahmen gemäß Art. 15 BayDSG getroffen werden.

2. Orts- und Nahgespräche

Summarische Erfassung: Soweit möglich, können abgehende Orts- und Nahgespräche summarisch nach der Zahl der Gebühreneinheiten je Nebenstelle und Monat erfaßt werden.

Zweckbindung: Wenn die Führung privater Orts- und Nahgespräche eingeschränkt ist, können private Gespräche zusätzlich gekennzeichnet werden. Ein Ausdruck der dabei gewonnenen Daten ist wiederum auf die oben unter 1 genannten Zwecke beschränkt.

3. Ferngespräche

Einrichtungen zur selbsttätigen Gebührenerfassung erlauben in der Regel die Erfassung folgender Daten:

- Telefonnummer der rufenden Nebenstelle,
- Vorwahl und Telefonnummer des angewählten Gesprächsteilnehmers (Zielnummer),
- Datum und Uhrzeit,
- Gebühreneinheiten und Gebührenbetrag,
- Nummer der Amtsleitung,
- sonstige betriebliche Kennzeichnungen,
- Kennzeichnung als Privatgespräch.

Dienstliche Ferngespräche: Hier kann von den technischen Möglichkeiten zur selbsttätigen Gebührenerfassung ohne Einschränkung Gebrauch gemacht werden. Ein Ausdruck der Daten ist grundsätzlich ebenfalls uneingeschränkt zulässig. Dies schließt nicht aus, daß in besonders gelagerten Fällen (z. B. bei Drogenberatern eines Gesundheitsamts) aus rechtlichen oder sachlichen Gründen Abweichungen geboten sein können (siehe auch Anmerkung am Ende der Wiedergabe dieser Grundsätze).

Erfassung privater Ferngesprächsdaten: Zum Schutze des informationellen Selbstbestimmungsrechts müssen die Bediensteten in geeigneter Weise darauf hingewiesen werden, daß sie durch das Führen eines privaten Ferngesprächs darin einwilligen, daß die oben aufgeführten Gesprächsdaten erfaßt, zumindest teilweise ausgedruckt und für Abrechnungszwecke verwertet werden. Andernfalls dürfen private Ferngespräche über dienstliche Fernmeldeanlagen nicht zugelassen werden.

Ausdruck/Zweckbindung: Für Abrechnungszwecke sind in der Regel auszudrucken oder sonst abzurufen und zu verwerten

- Telefonnummer der rufenden Nebenstelle,
- Datum und Uhrzeit,
- Gebühreneinheiten und Gebührenbetrag,
- Name des Inhabers der Nebenstelle.

Eine Verwertung dieser Daten für andere als Abrechnungszwecke ist ausgeschlossen.

Ausdruck der Zielnummer: Hat ein Bediensteter Zweifel an der Abrechnung, so ist auf seinem Antrag auch der Ausdruck der übrigen erfaßten Gesprächsdaten zulässig; dies gilt insbesondere für die Zielnummer.

Sicherung der Ausdrucke:

- Ausdrucke ohne Zielnummer dürfen nur der für die Gebührenabrechnung zuständigen Stelle und dem betroffenen Bediensteten zugänglich gemacht werden.
- Ausdrucke mit Zielnummer dürfen ausschließlich den betroffenen Bediensteten zugänglich gemacht werden.

Versendung und Aufbewahrung in verschlossenem Umschlag ist in beiden Fällen geboten.

Löschung der Daten: Nach Einziehung der Gebühren (wenigstens vierteljährlich) sind die Daten zu löschen und die Ausdrucke zu vernichten, soweit sie nicht den Bediensteten ausgehändigt wurden. Die Löschung bzw. Vernichtung hat innerhalb von 2 Monaten nach Ende des Abrechnungszeitraumes zu erfolgen. Können einzelne Abrechnungen nicht rechtzeitig erledigt werden, darf die Frist für die Löschung der Daten und die Vernichtung der Ausdrucke ausnahmsweise überschritten werden. Die Gründe hierfür sind schriftlich festzuhalten.

Aus der Sicht des Datenschutzes begrüße ich den Erlaß dieser Grundsätze ausdrücklich. Anzumerken bleibt, daß die grundsätzlich uneingeschränkte Zulässigkeit eines Ausdruckes von dienstlichen Ferngesprächsdaten nichts über den Umfang zulässiger Auswertung solcher dienstlicher Daten aussagt. Hier können sich noch personalvertretungsrechtliche Fragen (Mitarbeiterüberwachung) stellen.

9.4. Beihilferecht

In mehreren Eingaben haben sich Beamte mit der Bitte um datenschutzrechtliche Überprüfung des Antragsverfahrens auf Anerkennung der Beihilfefähigkeit von Psychotherapie an mich gewandt. Sie wandten sich vor allem dagegen, daß in einem „Bericht an den Gutachter" unter vollständiger Namensnennung Aussagen über Psychogenese und Psychodynamik der neurotischen Entwicklung und über die Prognose der Therapie gefordert werden.

Im einzelnen wurde kritisiert, daß die Angabe der identifizierenden Daten des Patienten im Berichtsformular für die Begutachtung irrelevant und daher sachlich nicht erforderlich sei. Es wurde darauf verwiesen, daß die Krankenkassen nicht ohne Grund bei ihren Einsendungen an Gutachten Chiffren verwenden. Dies schütze den Patienten davor, daß ein ihm nicht namentlich bekannter Gutachter seine psychiatrische Krankengeschichte inklusive Namen und Personaldaten erfährt.

Außerdem wurde kritisiert, daß das Beihilfeformular, das mit Namen und Geburtsdatum des Patienten sowie gegebenenfall des beihilfeberechtigten Ehepartners oder Elternteils versehen ist, mit an den Gutachter übersandt werde, obwohl damit keine für die Begutachtung erforderlichen Informationen übermittelt würden. In einer Eingabe wurde vorgeschlagen, es sollten für den Gutachter die für seine Beurteilung relevanten Daten zur Behandlung und Beurteilung auf dem Berichtsformular, die für die Beihilfestelle erforderlichen identifizierenden Daten auf dem Antragsformular enthalten sein. Das Berichtsformular sollte offen nur beim Gutachter, das Antragsformular offen nur bei der Beihilfestelle eingesehen werden können. Zu klären wäre auch, wo das Berichtsformular letztendlich aufzubewahren wäre, um eine Kenntnisnahme anderer Personen als des Gutachters auszuschließen.

Schließlich wurde kritisiert, daß das Antragsformular gegenwärtig in III 1. die Aufforderung zu „vollständiger wissenschaftlicher Diagnose" enthält. Gleichwohl sei hier nur eine allgemeine Diagnose erforderlich, da dieses Blatt offen bei der Beihilfestelle liege.

In den Eingaben wurde betont, daß Verbesserungen im Interesse des Schutzes sehr sensibler personenbezogener Daten ohne jeden Verlust für die fachgerechte Abwicklung des Verfahrens möglich erschienen.

Das Bayer. Staatsministerium der Finanzen, das in Bayern für das Beihilferecht federführend ist, hat mir hierzu mitgeteilt, die Bund- und Länderkommission für das Beihilferecht habe Mitte des Jahres 1986 eine Unterkommission beauftragt, die mögliche Verbesserungsvorschläge erarbeiten solle. Ein Ergebnis wurde mir bislang nicht mitgeteilt.

10. Statistik

10.1. Allgemeines

Das Volkszählungsurteil des Bundesverfassungsgerichts hat Novellierungsarbeiten an vielen Statistikgesetzen in Gang gesetzt. So wurden das Volkszählungsgesetz und das Mikrozensusgesetz geändert. Von beiden dürfte eine erhebliche Vorbildwirkung ausgehen. Sie sind durch sehr konkrete Regelungen über die Durchführung der Statistiken sowie durch erhebliche Vorsicht im Umgang mit erhobenen Daten gekennzeichnet. Auch Entwürfe zur Änderung des Bundesstatistikgesetzes, das mit seiner allgemeinen Regelung grundsätzlich bei allen Statistiken zu beachten ist, wurden vorgelegt. Der Bundestags-Innenausschuß führte im September 1986 eine Anhörung zum Gesetzentwurf der Bundesregierung (Drucksache 10/5345) durch, bei der ich Gelegenheit hatte, mich als Sachverständiger zu äußern. Aus dem Fragenkatalog für diese Anhörung will ich im folgenden auf zwei Fragen eingehen:

Der Bundestagsinnenausschuß stellte das Problem „Befragung ohne oder mit Auskunftspflicht als Grundsatzregelung" zur Debatte. Diese Frage muß unter Berücksichtigung des Eingriffs in das informationelle Selbstbestimmungsrecht geklärt werden, der durch eine Befragung mit Auskunftspflicht ausgelöst wird. Nach den Ausführungen des Bundesverfassungsgerichts im Urteil über das Volkszählungsgesetz 1983 (E 65/1 ff, 52 ff) ist ein solcher Eingriff in das informationelle Selbstbestimmungsrecht nur zulässig,

wenn er im überwiegenden Interesse der Allgemeinheit erfolgt und den Geboten der Normenklarheit und der Verhältnismäßigkeit entspricht. Dieser Grundsatz bedeutet meines Erachtens, daß bei der Anordnung jeder statistischen Erhebung, also auch von Bundesstatistiken zu prüfen ist, ob diese Voraussetzungen im jeweiligen Einzelfall gegeben sind. Ob die für eine statistische Erhebung angeordnete Auskunftspflicht erforderlich und verhältnismäßig ist, kann zuverlässig erst festgestellt werden, wenn bekannt ist, welche Daten für eine bestimmte Statistik erhoben werden sollen. Diese Frage ist meiner Ansicht nach daher vom Gesetzgeber für jede statistische Erhebung einzeln zu prüfen. Dabei muß der Gesetzgeber auch prüfen, ob eine freiwillige Erhebung, als der möglicherweise geringere Eingriff ausreichen würde. Ich habe mich daher dagegen ausgesprochen, bereits im Bundesstatistikgesetz die Auskunftspflicht als Regelfall festzulegen. Das Gesetz sollte für die Möglichkeit der freiwilligen Erhebung oder der Befragung mit Auskunftspflicht zumindestens offen sein. Auch wenn sich in der Praxis die Auskunftpflicht als Regelfall erweisen sollte, dürfte dies nicht dazu führen,daß freiwillige Erhebungen im Bundesstatistikgesetz nur den Charakter von Ausnahmefällen hätten. Wäre nämlich bereits im Bundesstatistikgesetz die Auskunftspflicht als Regel festgelegt, ohne daß deren Verhältnismäßigkeit im Einzelfall geprüft sein könnte, bestünde die Gefahr, daß der Gesetzgeber später, beim Erlaß der einzelnen Statistikgesetze, nicht mehr gründlich prüft und damit in seinen Willen aufnimmt, ob für die einzelne Datenerhebung wirklich eine Auskunftspflicht bestehen sollte.

Ein Zugang zu statistischen Einzelangaben wird mit Entwurf des Bundesstatistikgesetzes für Zwecke der Wissenschaft sowie in einer Stellungnahme des Bundesrates für ausschließlich statistische Zwecke für Statistikämter bei obersten Landesbehörden, Gemeinden oder Gemeindeverbänden vorgesehen. Die Weitergabe von Daten an wissenschaftliche Einrichtungen soll nur erfolgen, wenn sie nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft bestimmten einzelnen Personen zugeordnet werden könnten – wenn also eine faktische Anonymisierung gegeben wäre. Dies kann aus der Sicht des Datenschutzes wohl nur dann als ausreichende Sicherung angesehen werden, wenn auch im übrigen rechtlich und technisch-organisatorisch zuverlässig sichergestellt ist, daß die Empfänger wissenschaftlicher Daten diese an keine anderen Personen, Stellen oder Behörden zu keinem anderen Zweck – auch nicht für Zwecke der Strafverfolgung – weitergeben bzw. weitergeben müssen. Dies halte ich für eine sehr wichtige Frage, weil andere als wissenschaftliche Nutzer aufgrund anders gearteter Motivation oder Aufgabenstellung bereit sein könnten, einen höheren Aufwand für eine Reidentifizierung von Daten zu treiben, der für Wissenschaftler gleichwohl „unverhältnismäßig" wäre. Die Übermittlung für wissenschaftliche Zwecke an wissenschaftliche Einrichtungen muß eine Übermittlung in eine „Sackgasse" sein. Die ausschließlich wissenschaftliche Nutzung muß mit allen verfügbaren Mitteln gesichert werden. Anders als bei der Übermittlung für wissenschaftliche Zwecke halte ich eine Regelung über den Zugang zu Einzelangaben für oberste Landesbehörden und kommunale Statistische Ämter im Bundesstatistikgesetz selbst für problematisch. Der Gesetzgeber kann nämlich zum Zeitpunkt des Erlasses des Bundesstatistikgesetzes nicht unter gewissenhafter Überprüfung der Sensibilität der Daten, die übermittelt werden sollten, bewerten, ob ihre Übermittlung unter dem Gesichtspunkt der Verhältnismäßigkeit problematisch wäre. So werden beispielsweise Mikrozensusdaten nach dem Mikrozensusgesetz nicht an oberste Landesbehörden, Gemeinden oder Gemeindeverbände übermittelt. Die ausschließliche Nutzung der Mikrozensusdaten im Statistischen Landesamt ist nach meiner Erfahrung das einzige überzeugende Argument, mit dem den immer wieder anfragenden Betroffenen verständlich gemacht werden kann, daß der wirklich zuverlässige Schutz der beim Mikrozensus sehr sensiblen Daten sichergestellt ist. Mit anderen Worten: Erst beim Erlaß des einzelnen Statistikgesetzes wird deutlich, welche Daten mit welcher Sensibilität als Einzelangaben sinnvollerweise an oberste Landesbehörden, Gemeinden oder Gemeindeverbände weitergeleitet werden könnten. Darüber hinaus fehlt bisher eine Definition der abgeschotteten statistischen Stellen bei obersten Landesbehörden, Gemeinden oder Gemeindeverbänden, die nach dem Vorschlag des Bundesrates Empfänger von Einzeldaten sein sollten, so daß sich auch aus diesem Grunde nicht recht abschätzen läßt, ob und inwieweit hier ein Restrisiko in Kauf genommen würde. Ich habe daher vorgeschlagen, eine Vorschrift, die die Übermittlung von Einzeldaten an die vorgenannten Stellen erlauben würde, nicht ins Bundesstatistikgesetz aufzunehmen, sondern über eine solche Übermittlung beim Erlaß der einzelnen Statistikgesetze anhand der unterschiedlichen Sensibilität der Daten zu entscheiden. Gleichzeitig müßte die landesrechtliche Definition und gesetzliche Festlegung der vorgenannten Statistischen Ämter erfolgen, damit auch die erwähnte Frage eines Restrisikos aus der Sicht des Datenschutzes bewertet werden könnte.

10.2. Volkszählung 1987

Die Volkszählung ist eine statistische Erhebung, die als Totalerhebung mit Auskunftspflicht durchgeführt wird. Die Frage, ob das Mittel der Totalerhebung gerechtfertigt ist, wurde vom Bundesverfassungsgericht im Volkszählungsurteil eindeutig beantwortet: „Es ist derzeit nicht zu beanstanden, wenn der Gesetzgeber davon ausgegangen ist, daß Erhebungen aufgrund von Stichproben auf ausnahmslos freiwilliger Basis oder eine Kombination von Voll- und Stichprobenerhebung die Volkszählung als Totalerhebung nicht zu ersetzen vermögen." Diese Beurteilung gilt im Hinblick auf die letztlich kurze Zeitspanne, die seit dem Urteil vergangen ist, auch für die Volkszählung 87.

Zu diesem nun wiederum aktuellen Thema sei vorweg festgestellt:

- Das Volkszählungsgesetz 1987 erfüllt insgesamt die Anforderungen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil an statistische Erhebungen gestellt hat.
- Die Unterrichtung der Bürger über Zweck, Art und Umfang der Erhebung ist auf Betreiben der Datenschutzbeauftragten durch Textänderungen im Haushaltsmantelbogen sowie in den „Informationen zur Volkszählung 1987" noch verbessert worden.
- Gegen den Einsatz automatisierter Datenverarbeitung in der gemeindlichen Erhebungsstelle – zur Unterstützung des Erhebungsverfahrens – bestehen keine durchgreifenden Bedenken, sofern die erforderlichen organisatorischen und technischen Maßnahmen zur Datensicherung getroffen werden und die Abschottung gegenüber anderen Verwaltungsstellen sichergestellt ist. Dies wird Gegenstand von Prüfungen sein.

Vergleicht man die Vorgaben für die Volkszählung 87 mit denen, die für die Zählung 83 vorgesehen waren, so kann die kürzlich in der Presse vertretene Meinung, die Volkszählung 87 entspreche der Volkszählung 83, nur beschränkt Gültigkeit beanspruchen. Diese Aussage trifft nur für den **Umfang** der zu erhebenden Daten zu, nicht aber für die **Nutzung** der Daten.

Aus der Sicht des Datenschutzes ist zur Erhebung folgendes zu bemerken:

Der **Kreis der zu erhebenden Daten** wurde vom Bundesverfassungsgericht im Volkszählungsurteil nicht als bedenklich oder gar unzulässig angesehen. Gegenüber den 1983 zur Erhebung vorgesehenen Daten ist der Wohnungs- und Personalbogen nicht wesentlich verändert. Erwähnenswert ist vielleicht, daß gegenüber 1983 nun auch nach islamischer Religionszugehörigkeit, nach fünf weiteren einzeln aufgeführten Staatsangehörigkeiten und nach der Eigenschaft „Hausmann" gefragt wird. Weggefallen gegenüber 1983 ist die Angabe des Geburtstages und des genauen Geburtsmonats sowie die Frage nach der Zugehörigkeit zu Anstaltspersonal.

Entsprechend dem Volkszählungsurteil besteht mit den zu erhebenden Daten nicht die Gefahr der Erhebung eines Persönlichkeitsprofils oder eines Teilprofils.

Die rechtliche Situation zur **Nutzung** der zu erhebenden Daten hat sich gegenüber 1983 wesentlich verändert:

a) Nutzung in und durch die Erhebungsstellen

- Die Verknüpfung von Volkszählungsdaten mit Verwaltungsdaten in den Erhebungsstellen ist gesetzlich als unzulässig festgelegt worden.

- Nach den rechtlichen Vorgaben muß auch organisatorisch, räumlich und personell Vorsorge gegen eine Vermischung von Verwaltung und Statistik getroffen werden. § 9 Abs. 1 VZG 87 bestimmt, daß die Erhebungsstellen räumlich, organisatorisch und personell von anderen Verwaltungsstellen zu trennen sind. Es ist also eine Abschottung der Bereiche, die die Volkszählungserhebungen durchführen, von anderen Verwaltungstätigkeiten aufgrund gesetzlicher Vorgaben erforderlich.

  Aus datenschutzrechtlicher Sicht ist der Organisation der Erhebungsstelle wesentliche Bedeutung zuzumessen (§ 9 Abs. 1 VZG 87). Die Bestimmung der Erhebungsstellen und das Nähere zur Ausführung dieses Abschottungsgebotes obliegt den Ländern.

  Zur **räumlichen Abschottung** sieht § 5 Abs. 3 der Bayerischen Verordnung zur Durchführung des Volkszählungsgesetzes 1987 (DVVZG) vor, daß die Räume der örtlichen Erhebungsstellen, in denen Unterlagen für die Durchführung der Zählung bearbeitet oder aufbewahrt werden, gegen unbefugten Zugriff zu sichern sind. Regelungsgehalt dieser Vorschrift ist zweierlei: Zum einen sind für die Erhebungsstellen eigene Räume einzurichten, die nur dieser Dienststelle „Erhebungsstelle" zur Verfügung stehen; zum anderen sind Sicherungsmaßnahmen zu treffen, die die Daten aus der Volkszählung vor mißbräuchlicher Nutzung schützen und somit das Recht der befragten Bürger auf informationelle Selbstbestimmung sichern.

  Zur **organisatorischen Abschottung** bestimmt § 5 Abs. 1 in Verbindung mit § 1 Abs. 2 (DVVZG), daß Erhebungsstellen als eigene Dienststellen einzurichten sind. Nur in einer Dienststelle, die von den übrigen Stellen der kommunalen Verwaltung getrennt ist, sah das Bundesverfassungsgericht das verfassungsrechtlich verbürgte Recht des Einzelnen auf informationelle Selbstbestimmung gesichert (BVerfGE 65, 1 (69)).

  Zur **personellen Abschottung** verlangt § 5 Abs. 3 DVVZG die Ausstattung der Erhebungsstelle mit eigenem Personal. An die Mitarbeiter der Erhebungsstelle werden hohe Anforderungen gestellt: Sie müssen die Gewähr für Zuverlässigkeit und Verschwiegenheit bieten. Sie sind auf die Wahrung des Statistikgeheimnisses und zur Geheimhaltung auch solcher Erkenntnisse über Auskunftspflichtige schriftlich zu verpflichten, die gelegentlich ihrer Tätigkeit gewonnen werden. Des weiteren sieht § 5 Abs. 2 DVVZG ein Verbot vor, Einzelangaben aus Erhebungsvordrucken anunbefugte Personen bekanntzugeben. Ausdrücklich aufgenommen ist auch ein Verwertungsverbot, wonach Einzelangaben nicht für andere Zwecke als die zugelassenen der Zählung verwendet werden dürfen. Mit § 5 Abs. 2 Satz 4 DVVZG, wonach die in den Erhebungsstellen tätigen Personen, soweit sie statistische Einzelangaben in den Erhebungsvordrucken bearbeiten, nicht mit anderen Aufgaben des Verwaltungsvollzugs betraut werden dürfen, hat der Verordnungsgeber dem Abschottungsgebot des § 9 Abs. 1 VZG 87 Rechnung getragen. Ich darf an dieser Stelle nochmals darauf hinweisen, daß der Bundesgesetzgeber bewußt die strikte personelle Trennung vorgeschrieben hat. Die Fraktionen der CDU/CSU, SPD und FDP haben sich auf der Grundlage dieser Erörterungen dafür entschieden, es in Bezug auf die personelle Trennung bei der strikten Vorgabe des Regierungsentwurfs zu belassen. Damit wird jede Ausnahmemöglichkeit ausgeschlossen. Namentlich ist es nicht möglich, daß Personal während des Zeitraums, in dem Bedienstete den Erhebungsstellen zugeteilt sind, zeitweise sowohl in den Erhebungsstellen als auch in anderen Bereichen der Verwaltung arbeitet. Zur Begründung wurde von diesen Fraktionen darauf hingewiesen, daß es gerade in § 9 keine problematische Regelung geben dürfe, da die Ausgestaltung dieser Regelung unter Akzeptanzgesichtspunkten eine äußerst wichtige Rolle spiele (Bundestags-Drucksache 10/3843, S. 36).

  Das Gebot der **personellen Trennung** verbietet generell eine Parallelbeschäftigung, untersagt aber auch, Mitarbeiter einzelne Tage oder Stunden aus der Erhebungsstelle abzuziehen, um sie nach eiliger Erledigung ihrer „laufenden Verwaltungsaufgaben" erneut in der Erhebungsstelle einzusetzen. Um allzu große Personalengpässe in der Verwaltung aufgrund des personellen Trennungsgebotes zu vermeiden, wird derzeit ein „Rotationsverfahren" diskutiert. Soweit dieses vorsieht, die kommunalen Bediensteten „der Reihe nach" für einen festgelegten Zeitraum in der Erhebungsstelle einzusetzen, bestehen aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken. Ziel eines wie immer gearteten Verfahrens muß es sein, zu verhindern, daß Kenntnisse aus der Volkszählung anderweitig verwendet werden können.

Dieser Anforderung würde ein Rotationsverfahren, das für den einzelnen Bediensteten einen einmaligen, relativ kurzen Einsatz in der Erhebungsstelle vorsieht, genügen.

Das Abschottungsgebot kann insbesondere kleinen Gemeinden Schwierigkeiten bereiten. Die Bayerische Verordnung zur Durchführung des Volkszählungsgesetzes sieht deshalb ausdrücklich vor, daß das Landratsamt prüft, ob die Abschottungsanforderungen von den einzelnen kreisangehörigen Gemeinden erfüllt werden können. Spätestens 6 Monate vor dem Zählungsstichtag entscheidet das Landratsamt, ob diese Voraussetzungen vorliegen. Mit dieser Verfahrensweise soll den Anforderungen des § 9 Abs. 1 VZG 87 Rechnung getragen werden. Andere Bundesländer stellen, um die Einhaltung des Abschottungsgebots sicherzustellen, auf die Einwohnerzahl einer Gemeinde ab (unter einer bestimmten Einwohnerzahl wird eine Abschottung als nicht möglich unterstellt).

Das Abschottungsgebot gilt für jede kommunale Erhebungsstelle. Auch durch Beauftragung des Statistischen Amtes einer Kommune mit den Aufgaben der Erhebungsstelle könnte unter Umständen eine Interessenkollision geschaffen werden: Auf den ersten Blick erscheinen die Statistischen Ämter als Erhebungsstelle besonders geeignet, da sie ja regelmäßig nicht mit Vollzugsaufgaben betraut sind. Die Abschottung zu den für den Verwaltungsvollzug zuständigen Stellen ist hier auch nicht problematisch. Fragen können sich vielmehr dann ergeben, wenn ein Statistisches Amt neben seinen kommunalstatistischen Aufgaben die Aufgaben der Erhebungsstelle wahrnimmt. Als Erhebungsstelle hätte das Statistische Amt die ausgefüllten Erhebungsvordrucke zusammenzuführen und die Erhebungsvordrucke und die sonstigen Erhebungsunterlagen auf Vollständigkeit und formale Richtigkeit hin zu prüfen. Das Statistische Amt besitzt damit vorübergehend Volkszählungs-Daten, die ihm vom Statistischen Landesamt auch bei Vorliegen eines entsprechenden Landesgesetzes in diesem Umfang nicht übermittelt würden: Nach § 14 Abs. 1 VZG 87 dürfen den zur Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände vom Statistischen Landesamt für ausschließlich statistische Aufgaben Einzelangaben für ihre Zuständigkeitsbereiche nur ohne Hilfsmerkmale und unter weiteren Einschränkungen übermittelt werden. Auf Anforderung der zur Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände erfolgt die Übermittlung auf der Grundlage von Blockseiten.

Um einer evtl. Interessenkollision entgegenzuwirken, halte ich daher eine räumliche, organisatorische und personelle Abschottung der Erhebungsstelle auch innerhalb des kommunalen Amtes für Statistik für erforderlich, die sicherstellt, daß die Daten, die im Zuge der Erhebung bekannt werden, nicht für Aufgaben der kommunalen Statistik genutzt werden.

- Im Rahmen der organisatorischen Vorsorge müssen auch jeweils angemessene Lösungen für die möglichen Interessenkollisionen gefunden werden, die sich beim Leiter und den Mitarbeitern der Erhebungsstelle ergeben können.

  Die **Leitung der örtlichen Erhebungsstelle** obliegt nach § 6 DVVZG grundsätzlich dem Behördenvorstand. Dieser kann jedoch die Aufgaben des Leiters der Erhebungsstelle auf einen Bediensteten übertragen. Von dieser Delegationsmöglichkeit ist lediglich der Erlaß einer Dienstanweisung zur Volkszählung gemäß § 6 S. 5 DVVZG ausgenommen. Bei einer Delegation sowie bei der **Mitarbeiterorganisation** für die Erhebungsstelle gilt es, Interessenkonflikte zu vermeiden. Das Personal der Erhebungsstelle sollte nicht aus Bediensteten aus sensiblen Bereichen der Kommunalverwaltung bestehen. Für die Zähler hat der Bundesgesetzgeber in § 10 Abs. 5 VZG 87 eine Regelung getroffen, die deren Einsatz verbietet, soweit eine Interessenkollision zu besorgen ist. Für den Leiter und die Mitarbeiter der Erhebungsstelle sieht § 9 VZG 87 ein entsprechendes Verbot nicht vor. Ohne auf die rechtliche Diskussion hierzu näher einzugehen, meine ich, schon im Hinblick auf die Akzeptanz der Bürger müßte davon abgesehen werden, Bedienstete, für die möglicherweise durch die Arbeit in der Erhebungsstelle ein Interessenkonflikt entsteht, dort einzusetzen. Nicht unproblematisch wäre es, Bedienstete aus den Meldeämtern in der Erhebungsstelle oder als Zähler einzusetzen. Das Bundesverfassungsgericht hat ja gerade den im Volkszählungsgesetz 1983 vorgesehenen Vergleich der Angaben der Volkszählung mit den Melderegistern als unzulässig angesehen.

b) Nutzung durch das Landesamt für Statistik und Datenverarbeitung und durch die Statistischen Ämter der Gemeinden

aa) Nutzung durch das Bayer. Landesamt für Statistik und Datenverarbeitung

- Im Statistischen Landesamt ist eine Verknüpfung der Volkszählungsdaten mit anderen statistischen Einzeldaten nicht erlaubt und daher aber auch nicht vorgesehen.
- Übermittlungen von Einzeldaten an Landes- oder Bundesbehörden sind im Gegensatz zum Volkszählungsgesetz 83 nicht zugelassen.

bb) Nutzung durch die Statistischen Ämter der Gemeinden

Die Statistischen Ämter der Gemeinden können, wie bereits dargelegt, für ausschließlich statistische Zwecke Angaben in aggregierter Form (Blockseite) vom Bayer. Landesamt für Statistik und Datenverarbeitung erhalten, wenn weitere einengende Voraussetzungen eingehalten sind. Insbesondere läßt das Volkszählungsgesetz 87 eine Übermittlung an die zur Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände nur zu, wenn durch ein Landesgesetz eine Trennung der Stellen von anderen kommunalen Verwaltungsstellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist (§ 14 Abs. 1 Satz 3 VZG 87).

Volkszählung – Alternativen

Schon 1983, aber erst recht 1987 ist aus der Sicht des Datenschutzes der Durchführung einer Volkszählung bei weitem der Vorzug vor einer eventuellen Alternative zu geben,

die in der Aufbereitung und Verfügbarmachung von entsprechenden Daten aus der Vollzugsverwaltung bestehen würde. Wie auch vom Bundesverfassungsgericht im Volkszählungsurteil aufgegriffen, wäre die Herstellung einer Datenübermittlungs- und Verknüpfungsinfrastruktur, die die Gewinnung von Volkszählungsdaten aus dem Verwaltungsvollzug zum Ziel hätte, äußerst problematisch. Es würde mit den damit geschaffenen Datenübermittlungs- und Verknüpfungsmöglichkeiten nämlich die Zusammenführung von weit mehr Daten als nur denjenigen, die für Volkszählungszwekke gesammelt werden müßten, ermöglicht. Auch würden Datenflüsse vorbereitet, die bisher zwischen Behörden nicht bestehen. Es würde mit der Infrastruktur für solche Datenflüsse und Verknüpfungen der Boden für umfassendere Datensammlungen bereitet, als sie bisher bestehen. Sie wären für die Betroffenen keineswegs akzeptabler als eine mit den möglichen Sicherheitsvorkehrungen ausgestattete Volkszählung. Zu möglichen Folgen intensiver Sammlung von Daten hat das Bundesverfassungsgericht im Zusammenhang mit der Geheimhaltung von steuerlichen Angaben in der Entscheidung über Untersuchungsausschüsse des Bundestages folgendes ausgeführt:

> „Die Angaben, die ein Steuerpflichtiger aufgrund des geltenden Abgabenrechts zu machen hat, ermöglichen weitreichende Einblicke in die persönlichen Verhältnisse, die persönliche Lebensführung (bis hin beispielsweise zu gesundheitlichen Gebrechen, religiösen Bindungen, Ehe- und Familienverhältnissen oder politischen Verbindungen) und die beruflichen, betrieblichen, unternehmerischen oder sonstigen wirtschaftlichen Verhältnisse. Über ihre zeitlich kontinuierliche Erfassung, Speicherung und ständige Abrufbarkeit ermöglichen sie demjenigen, der über diese Daten verfügt, ein Wissen außerordentlichen Ausmaßes über die Betroffenen, das unter den gegenwärtigen Lebensverhältnissen in entsprechende Macht über die Betroffenen umschlagen kann." (BVerfGE 67, 100 (142/43)).

Welchen Beitrag leistet der Datenschutzbeauftragte?

Die Aktivität des Datenschutzbeauftragten konzentriert sich im Verhältnis zur Volkszählung derzeit auf Fragen

- der Datensicherung in den Erhebungsstellen, im Statistischen Landesamt und bei Zählern,
- der räumlichen und organisatorischen Abschottung von Statistik und Verwaltung sowie
- der personellen Abschottung.

10.3. Handels- und Gaststättenzählung 85

Die Handels- und Gaststättenzählung 1985 war die erste Bundesstatistik, die nach dem Urteil des Bundesverfassungsgerichts zur Volkszählung als Totalerhebung stattfand. Sie war deshalb ein aufschlußreiches Beispiel dafür, wie Zählungen aufgrund bestehender Gesetze durchgeführt werden, die den Grundsätzen des Bundesverfassungsgerichts zu statistischen Erhebungen nun nicht mehr voll entsprechen. Die Datenschutzbeauftragten der Länder und des Bundes haben sich mit der Erhebung im Rahmen der Handels- und Gaststättenzählung 1985 befaßt und dazu festgestellt:

- Die Datenschutzbeauftragten der für die Durchführung der Statistik zuständigen Länder hatten bis zu Beginn der Erhebung weder die Fragebogen noch die Verwaltungsvorschriften zur Kenntnis erhalten, die zur Sicherung der Rechte der Betroffenen in der Übergangszeit bis zur Anpassung des Handelsstatistikgesetzes an die Anforderungen des Grundgesetzes erforderlich sind. Dies stellten die Datenschutzbeauftragten bedauernd fest.

- Die Datenschutzbeauftragten sind, wie auch das Statistische Bundesamt, der Ansicht, daß das Handelsstatistikgesetz in Teilen nicht den Anforderungen des Volkszählungsurteils entspricht und daher einer Novellierung bedarf.

- Für verschiedene in den Erhebungsbogen enthaltene Fragen (z. B. über gewerblichen Umsatz, unternehmensinterne Dienstleistungen, Zweigniederlassungen, Auszeichnung der Waren mit Brutto- oder Nettopreisen) ist die gesetzliche Grundlage zumindest zweifelhaft. Die Hilfsmerkmale werden im Gesetz überhaupt nicht bestimmt. Ferner fehlen präzise gesetzliche Regelungen über die Trennung der Hilfsmerkmale von den Erhebungsmerkmalen und ihre Löschung.

- Die Datenschutzbeauftragten hielten es daher für erforderlich, Namen und Anschriften sowie weitere Hilfsmerkmale unverzüglich nach Abschluß der maschinellen Plausibilitätskontrolle, spätestens bis zum Ablauf einer zu bestimmenden, möglichst kurzen Frist, von den Erhebungsbogen abzutrennen und zu vernichten. Bis zur Änderung des Handelsstatistikgesetzes müssen die Verpflichtung zur unverzüglichen Trennung von Hilfsmerkmalen und Erhebungsdaten und Löschung der Hilfsmerkmale sowie die Frist, nachderen Ablauf die Löschung abgeschlossen sein muß, durch die zuständigen Behörden festgelegt werden. Eine Aufbewahrung bis zum Abschluß der folgenden Handels- und Gaststättenzählung hielten die Datenschutzbeauftragten nicht für vertretbar.

- Bis zu einer anderweitigen gesetzlichen Regelung dürfen die von den Finanzbehörden für die Durchführung der Zählung im Handwerk und im Gaststättengewerbe gelieferten und mit Hilfe der Angaben der Unternehmen und Arbeitsstätten korrigierten und ergänzten Adreßdateien nach Auffassung der Datenschutzbeauftragten nur für Zählungen nach dem Handelsstatistikgesetz, nicht aber für andere statistische Zwecke verwendet werden.

Die Datenschutzbeauftragten haben bei dieser Gelegenheit betont, daß die vom Bundesverfassungsgericht im Volkszählungsurteil dargelegten Grundsätze nicht nur auf Bevölkerungsstatistiken, sondern auch auf Wirtschaftsstatistiken, wie die Handels- und Gaststättenzählung, anzuwenden sind. Soweit bei Wirtschaftsstatistiken Daten natürlicher Personen erhoben werden, haben diese Betroffenen Anspruchauf den gleichen Schutz wie die Betroffenen im Rahmen von Bevölkerungsstatistiken.

Zu der vorstehend dargestellten Ansicht der Datenschutzbeauftragten haben das Bayerische Staatsministerium des Innern und das Bayerische Landesamt für Statistik und Datenverarbeitung mitgeteilt, die Fragebogen der Handels- und Gaststättenzählung 1985 seien so gestaltet, daß sich

die Namen, Anschriften und weitere Hilfsmerkmale der Unternehmen und Arbeitsstätten auf gesonderten Deckblättern befinden. Diese würden nach Abschluß der maschinellen Plausibilitätskontrollen von den Datenteilen abgetrennt und vernichtet. Die Plausibilitätskontrollen seien entsprechend dem Arbeits- und Zeitplan der Zählung bis Mitte 1986 abgeschlossen. Die Datenteile der Erhebungsvordrukke würden nach Beendigung der Aufbereitungsarbeiten im Herbst 1986 vernichtet. Das auf maschinelle Datenträger übernommene Material sei nach den für die Zählung bundeseinheitlich festgelegten Richtlinien bis zum Abschluß der nächsten Handels- und Gaststättenzählung aufzubewahren, wobei die Adreßdateien von den Erhebungsmerkmalen getrennt geführt würden. Die Daten seien für die Durchführung von nachfolgenden bundesstatistischen Stichprobenerhebungen, z. B. Monats-Jahres- und Ergänzungserhebungen im Handel- und Gastgewerbe, Kostenstrukturstatistiken, Lohn- und Gehaltserhebungen, notwendig.

10.4. Auswertung der Todesursachenstatistik zu Forschungszwecken

Nach der gegenwärtigen Rechtslage ist eine Auswertung der der amtlichen Todesursachenstatistik zugrunde liegenden Daten zu Forschungszwecken ohne entsprechende Einwilligungen nicht möglich. Das Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes sieht vor, daß die Leichenschauscheine über das Gesundheitsamt an das Landesamt für Statistik und Datenverarbeitung geleitet werden. Eine Übermittlung an andere Stellen zu Forschungszwecken ist im Gesetz nicht vorgesehen. Auch eine Datenübermittlung durch das Gesundheitsamt stößt an diese rechtliche Grenze.

Dem wohl berechtigten Interesse der Forschung an Mortalitätsdaten könnte Rechnung getragen werden, wenn eine entsprechende gesetzliche Befugnis zur Offenbarung geschaffen würde. Eine Regelung, die die Übermittlung bestimmter personenbezogener Einzelangaben zuließe, müßte sich allerdings in den Grenzen des für wissenschaftliche Zwecke Erforderlichen halten. Nach den Ausführungen des Bundesverfassungsgerichts zu § 9 Abs. 4 Volkszählungsgesetz 1983 ist auch zu berücksichtigen, daß für die meisten Untersuchungsbereiche ein direkter Personenbezug nicht erforderlich ist, „denn der Wissenschaftler ist regelmäßig nicht an der einzelnen Person interessiert, sondern an dem Individuum als Träger bestimmter Merkmale".

Datenschutzrechtliche Belange müßten daher vor allem im Hinblick auf den Grundsatz der Zweckbindung „Medizinische Forschung" insbesondere im Interesse von Angehörigen berücksichtigt werden. Ein Bekanntwerden von Todesursachen, die einem gesellschaftlichen Negativurteil unterliegen, könnte nämlich nicht nur das Andenken Verstorbener, sondern – je nach Krankheitsart – auch den Ruf oder gar die Kreditwürdigkeit von Abkömmlingen oder anderen noch lebenden Angehörigen beeinträchtigen.

10.5. Übermittlung bestimmter landwirtschaftlicher Betriebsdaten von Gemeinden an Finanzämter

Auf Bitte einer Stadt hatte ich mich mit der datenschutzrechtlichen Frage zu befassen, ob die Stadt vom Finanzamt erbetene Auskünfte über die Aufgabe von landwirtschaftlichen Betrieben sowie über Betriebsveränderungen durch Verpachtung, Zupachtung u. ä. erteilen darf, wenn die hierfür nutzbaren Daten der Stadt aus Erhebungen zu statistischen Zwecken und aus Rentenversicherungsanträgen bekannt sind.

Zu den Statistikdaten ergibt sich, daß nach § 13 Abs. 1 Satz 3 des Gesetzes über Agrarberichterstattung eine Weiterleitung oder Auswertung der aufgrund dieses Gesetzes erhobenen Daten zu steuerlichen Zwecken ausdrücklich ausgeschlossen ist. Dementsprechend hatte auch das Bayerische Landesamt für Statistik und Datenverarbeitung in den Erhebungsunterlagen darauf hingewiesen, daß die Weiterleitung und Auswertung von Einzelangaben für steuerliche Zwecke nicht zulässig sei. Eine Auswertung der Statistik-Daten für steuerliche Zwecke würde daher in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung eingreifen (so auch das Bundesverfassungsgericht im Urteil zum Volkszählungsgesetz 1983).

Bei den Daten aus Rentenversicherungsanträgen war auf § 93 Abs. 1 Satz 1 der Abgabenordnung abzustellen, wonach die Beteiligten und andere Personen der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes erforderlichen Auskünfte zuerteilen haben. Andere Personen als die Beteiligten sollen jedoch von den Finanzämtern erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht (§ 93 Abs. 1 Satz 2 AO). Diese Einschränkung ist eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes. Demnach könnten zwar die Namen der Betroffenen dem Finanzamt bekanntgegeben werden. Das Finanzamt müßte sich jedoch unter Hinweis auf die Auskunftspflicht zunächst an die Betroffenen selbst wenden. Nur in den Einzelfällen, in denen dieses Vorgehen nicht zum Erfolg führt, dürfte die Gemeinde die Daten in dem gewünschten Umfang dem Finanzamt bekanntgeben. Im Gegensatz zu einer solchen Übermittlung im Einzelfalle würde eine regel- und routinemäßige Übermittlung sämtlicher Daten im gewünschten Umfang durch die Gemeinde eine unverhältnismäßige Änderung des Nutzungszwecks der Daten bedeuten.

Auch aus § 71 Abs. 1 Nr. 3 SGB X ergibt sich meines Erachtens keine andere rechtliche Beurteilung. Diese Vorschrift ist hier zwar nicht, jedenfalls nicht unmittelbar, anwendbar, da sie sich nur an die durch das Sozialgeheimnis Verpflichteten wendet, zu denen die Gemeinden nach der abschließenden Regelung des § 35 Abs. 1 SGB I nicht gehören. Nach den Ausführungen des Bayerischen Staatsministeriums für Arbeit und Sozialordnung macht es die gesetzgeberische Intention gleichwohl nötig, auch die Gemeinden, die hinsichtlich der Antragstellung in § 16 SGB I zuständigen Leistungsträgern gleichgestellt werden, zur Geheimhaltung zu verpflichten. § 35 SGB I ist danach auf die Gemeinden entsprechend anwendbar. Dieses ergebe sich daraus, daß die in § 35 SGB I genannten Stellen, wenn sie Dritte in den Vollzug ihrer Aufgaben einschalten, die Verantwortung dafür tragen, daß das Sozialgeheimnis gewahrt bleibt. Auch bei einer Anwendung des § 71 SGB X ist jedoch die Einhaltung der oben genannten Regeln des § 93 der Abgabenordnung zwingend.

10.6. Unzulässige Nutzung von Statistikdaten durch Bauaufsichtsbehörden

Im Rahmen eines baurechtlichen Widerspruchs- und Petitionsverfahrens hat sich eine Bezirksregierung mit der Bitte um Mitteilung von Art und Anzahl des örtlichen Viehbestandes einer Gemeinde an das zuständige Landratsamt gewandt. Das Landratsamt erfragte die Angaben bei der Gemeinde telefonisch und gab sie in einem Aktenvermerk an die Regierung weiter. Die einzelnen Landwirte wurden darin namentlich aufgeführt und Anzahl und Art des Viehbestandes genannt. Die Regierung arbeitete die Daten in ihre Stellungnahme ein, die in dem anschließenden verwaltungsgerichtlichen Verfahren Verwendung fand. Dazu teilte die Regierung mit, die Verwaltungsgerichte erwarteten von Immissionsschutzsachverständigen in Streitsachen im Zusammenhang mit landwirtschaftlichen Betrieben Aussagen über den vorhandenen Tierbestand, um daraus Rückschlüsse ziehen zu können, ob sich eine betriebliche Veränderung noch im Rahmen des Ortsüblichen hielte. In der Regel würden hierzu Daten der Viehzählung herangezogen.

Die Datenerhebung bzw. -übermittlung war nach dem Viehzählungsgesetz zu beurteilen, da dieses als Sondervorschrift den allgemeinen Datenübermittlungsvorschriften des Bayerischen Datenschutzgesetzes vorgeht. § 8 des Viehzählungsgesetzes gestattet eine Verwendung der Einzelangaben der Viehhalter und der Feststellungen bei der allgemeinen Viehzählung und bei der Zwischenzählung im Juni nur für behördliche Maßnahmen zur Durchführung des Tierzuchtgesetzes und des Viehseuchengesetzes, für die Berechnung der Beiträge zur öffentlichen Viehseuchenentschädigungskasse und für die Berechnung der öffentlichen Dasselbekämpfungsgebühren durch die zuständigen Behörden oder die von ihnen beauftragten Stellen. Dieser Verwendungszweck war weder im baurechtlichen noch im Petitionsverfahren gegeben. Die Weitergabe der Daten aus der Viehzählung mit Personenbezug stellte daher eine Verletzung der datenschutzrechtlichen Vorschrift des § 8 des Viehzählungsgesetzes dar. Die Abgabe der Viehzählungsdaten durch die Gemeinde sowie die Erhebung der Daten und Weitergabe durch die Bauaufsichtsbehörden war daher zu beanstanden.

10.7. Zuverlässige Vernichtung von statistischem Datenmaterial

Eine mit der Vernichtung von statistischen Unterlagen des Landesamts für Statistik und Datenverarbeitung betraute Altpapierfirma hatte – offenbar versehentlich – Reste der Unterlagen in einem Container gelassen. Die Papiere wurden dann bei einer anderen Firma, bei der der Container aufgestellt wurde, gefunden. Aus diesem Anlaß habe ich festgestellt, daß es im Hinblick auf das Statistikgeheimnis und die Akzeptanz der amtlichen Statistik durch den Bürger für erforderlich angesehen werden muß, künftig die Vernichtung der Unterlagen mit personenbezogenen Daten grundsätzlich nur noch im eigenen Haus des Landesamtes für Statistik und Datenverarbeitung „in eigener Regie" abzuwickeln. Soweit für eine Übergangszeit eine Entsorgung personenbezogener Unterlagen über Fremdfirmen nicht vermeidbar erscheint, ist neben den entsprechenden vertraglichen Absicherungen eine überaus sorgfältige Auswahl des zu beauftragenden Unternehmens zu treffen sowie eine sofortige Vernichtung des Materials im Beisein von Bediensteten des Bayer. Landesamt für Statistik und Datenverarbeitung zu vereinbaren. Ich habe darum gebeten, mich vor Festlegung des künftigen Entsorgungskonzepts über die beabsichtigte Neukonzeption zu unterrichten.

11. Schule und Hochschule

11.1. EDV-Einsatz in der Schulverwaltung

Die automatisierte Personalverwaltung im Geschäftsbereich des Staatsministeriums für Unterricht und Kultus ist im Umbruch begriffen. Bislang stand für die Personalverwaltung automatisiert nur die beim Staatsministerium für Unterricht und Kultus geführte Lehrerdatei zur Verfügung. Nun ist beabsichtigt, auch bei den Regierungen zur Verwaltung der Lehrerdaten ein automatisiertes Personalverwaltungssystem einzuführen. Außerdem werden auf der Ebene der staatlichen Schulämter neue EDV-Personalverwaltungssysteme errichtet.

Die Einrichtung automatisierter Dateien zur rationellen Aufgabenerledigung liegt selbstverständlich in der grundsätzlichen Entscheidungsbefugnis der für die jeweiligen Aufgaben zuständigen Stellen. Insoweit bestehen gegen die Einführung von automatisierten Personalverwaltungssystemen auf der Ebene der Regierungen und der Schulämter keine grundsätzlichen Einwände, wenn die dann jeweils beabsichtigten Datenspeicherungen in ihrem Umfang in den Grenzen erfolgt, die durch die personalrechtlichen Kompetenzen der jeweiligen speichernden Stellen (Staatsministerium für Unterricht und Kultus, Regierungen, staatliche Schulämter) vorgegeben sind (zur generellen Problematik von Personalinformationssystemenvgl. 9.2). Dabei wird insbesondere darauf zu achten sein, daß überflüssige Doppelspeicherungen vermieden werden. So ist die Speicherung sämtlicher Personaldaten zu den einzelnen Lehrern auf verschiedenen Ebenen grundsätzlich unzulässig, weil zur Aufgabenerfüllung nicht erforderlich. Eine solche umfassende Speicherung kommt grundsätzlich nur der personalaktenverwaltenden Dienststelle zu. Die Speicherungsbefugnis für ein automatisiertes Personalverwaltungssystem ergibt sich im übrigen aus Art. 16 Abs. 1 BayDSG i.V.m. Art. 100 Bayer. Beamtengesetz (für Beamte) und § 13 BAT (für Angestellte).

Sollten die einzelnen Personalverwaltungssysteme nicht den Kompetenzen entsprechend aufeinander abgestimmt werden, hätte ich hiergegen erhebliche datenschutzrechtliche Bedenken. Voraussetzung für die Einführung neuer Personalverwaltungssysteme auf den Ebenen Regierung und Schulamt ist deshalb meines Erachtens die Erstellung eines einheitlichen und abgestimmten Konzeptes, das datenschutzrechtlich unerwünschte Doppelspeicherungen, soweit möglich, vermeidet. Ich verkenne nicht, daß ein solches abgestimmtes Automatisierungskonzept gerade im Bereich des Staatsministeriums für Unterricht und Kultus wegen der unterschiedlichen Regelungen bezüglich der Personalverwaltungszuständigkeiten nicht einfach ist. So liegen die entsprechenden Kompetenzen für Gymnasien und Realschulen originär beim Staatsministerium selbst. Die Berufsschulen unterstehen den Regierungen. Für die Sonder- und Volksschulen liegt das Schwergewicht der Zuständigkeit ebenfalls bei den Regierungen. Diese sind die Anstellungsbehörden; ihnen obliegen insbesondere Voll-

zugsaufgaben, wie Einstellung, Beförderungen oder Versetzung. Teilbereiche sind allerdings ausgeklammert und den staatlichen Schulämtern oder sogar den einzelnen Schulen übertragen. Für den betroffenen Lehrerkreis ist auch noch das Staatsministerium zumindest insoweit mit Personalführungsaufgaben befaßt, als es für den entsprechenden Erlaß von Richtlinien zuständig ist. Das Kompetenzgefüge wird dadurch noch unübersichtlicher, daß manche Teilaufgaben im Wege der Delegation oder auch der Rückdelegation von anderen als den zunächst durch Rechtsvorschrift bestimmten Stellen vorgenommen werden. So wird zum Beispiel das Staatsministerium für Unterricht und Kultus bei der Führung der Lehrerdatei teilweise im Auftrag der ihm nachgeordneten Stellen tätig. Ich begrüße, daß das Staatsministerium für Unterricht und Kultus zur Erarbeitung einer einheitlichen EDV-Konzeption für die Personalverwaltung eine Arbeitsgruppe gebildet hat. Mir ist zugesagt, daß ich künftig ausreichend an der Erstellung der Neukonzeption beteiligt werde.

Zur Lehrerdatei

Die Lehrerdatei des Staatsministeriums für Unterricht und Kultus wurde bereits in den Jahren 1969 und 1970 aufgebaut mit dem Ziel, die personenbezogenen Arbeiten bei der Personalverwaltung der Lehrer zu rationalisieren, Informationen für Verwaltungs- und Planungszwecke zur Verfügung zu stellen und als Hilfsmittel für die amtliche Statistik zu dienen. Die Daten der Lehrerdatei werden aus den Personalakten entnommen. Bei der Prüfung der datenschutzrechtlichen Zulässigkeit der Datenspeicherung in der Lehrerdatei, dem derzeit umfassendsten Personalverwaltungssystem der Kultusverwaltung, wurde als Maßstab für die Erforderlichkeit der Datenverarbeitung auf die entsprechenden Regelungen für die Personalaktenführung abgestellt. In die Personalakte dürfen nach herrschender Meinung zulässigerweise die Urkunden und Vorgänge aufgenommen werden, welche die persönlichen und dienstlichen Verhältnisse eines Beamten betreffen, sofern sie in einem inneren Zusammenhang mit dem Beamtenverhältnis stehen (vergl. BVerwGE 36,138). Damit ist auch für die Zulässigkeit einer Datenspeicherung in einer Lehrerdatei der „innere Zusammenhang mit dem Beamtenverhältnis" eine äußerste Grenze. Daneben müssen im Einzelfall weitere einschränkende Anforderungen aufgestellt werden.

In Anwendung dieser Grundsätze haben sich bei einer Durchsicht des Datensatzes der Lehrerdatei grundsätzliche Bedenken gegen Art und Umfang der gespeicherten Daten nicht ergeben. Vielmehr scheinen nach vorläufiger Bewertung die Daten jeweils in einem deutlichen und engen Zusammenhang mit dem Dienstverhältnis der betroffenen Lehrer zu stehen und in ihrer überwiegenden Mehrzahl ganz offensichtlich zur Gewährleistung einer ordnungsgemäßen Personalverwaltung erforderlich zu sein. Lediglich bei einigen wenigen Datenfeldern (z.B. Umfang der Angaben zur Religionszugehörigkeit) habe ich Zweifel an der derzeitigen Speicherung geäußert. Diesen will das Staatsminsterium für Unterricht und Kultus Rechnung tragen.

Größere Probleme wirft meines Erachtens die bereits oben grundsätzlich besprochene Frage auf, welche Stelle eigentlich zulässigerweise als personalaktenverwaltende Dienststelle und damit als „speichernde Stelle" im Sinne des Datenschutzrechts anzusehen ist. Wegen der oben dargestellten Gemengelage bei den Kompetenzen für die einzelnen Schultypen ist diese nicht einfach zu beantworten. Grundsätzlich sind meines Erachtens die verschiedenen für die Personalverwaltung zuständigen Stellen auch jeweils für die Speicherung ihrer Daten in der Lehrerdatei verantwortlich. Dies ist bislang vom Staatsministerium für Unterricht und Kultus zu wenig präzise herausgearbeitet worden. Derzeit werden in der Meldung zum Datenschutzregister das Staatsministerium für Unterricht und Kultus und die jeweiligen Regierungen pauschal für alle gespeicherten Lehrer gemeinsam als speichernde Stelle bezeichnet. Allerdings, dies möchte ich an dieser Stelle ausdrücklich feststellen, entstehen dadurch für den einzelnen Lehrer keine Risiken für seine schutzwürdigen Belange.

In diesem Zusammenhang stellt sich auch noch das Problem der Zugriffsberechtigung auf die gesamten in der Lehrerdatei gespeicherten Daten. Auch diese hat sich nach der jeweiligen Aufgabenzuweisung zu richten und darf nur die Datensätze und auch nur den Teil der Datensätze betreffen, die zur Aufgabenerfüllung im Einzelfall erforderlich sind.

Eine unklare Kompetenzabgrenzung kann grundsätzlich dazu führen, daß auch die Verantwortung für die Überwachung der Richtigkeit der gespeicherten Daten unklar ist. Das Staatsministerium für Unterricht und Kultus hat mir allerdings in diesem Zusammenhang zugesichert, daß sowohl das Staatsministerium als auch die Regierungen im Rahmen ihrer Zuständigkeit eigenverantwortlich für die Richtigkeit der in der Lehrerdatei gespeicherten Daten sorgen.

Um die Richtigkeit der Lehrerdaten in der Lehrerdatei zusätzlich zu garantieren, habe ich den Vorschlag unterbreitet, den Lehrern einmal jährlich einen Auszug ihres sie betreffenden Datensatzes auszuhändigen. Die Lehrer könnten dann selbst die Richtigkeit ihrer eigenen Daten überprüfen und ggf. eine Berichtigung veranlassen. Allerdings ist mein Vorschlag auf wenig Gegenliebe gestoßen, weil diese Unterrichtung wegen der großen Anzahl der Lehrer zu aufwendig wäre. Die diesbezüglichen Argumente des Staatsministeriums für Unterricht und Kultus lassen mich zwar nicht unbeeindruckt, doch sollte meine Anregung im Hinblick auf die für den einzelnen Bürger immer weniger überschaubaren Speicherungen weiter im Auge behalten werden. Meines Erachtens könnten auch Wege gefunden werden, die einen übermäßigen Verwaltungsaufwand bei einer solchen Benachrichtigung der Lehrer vermeiden würden.

Bei der Prüfung der regelmäßigen Datenübermittlungen aus der Lehrerdatei habe ich im übrigen festgestellt, daß die in der an mich gerichteten Datenschutzregistermeldung genannten Rechtsgrundlagen teilweise unrichtig sind. Das Staatsministerium für Unterricht und Kultus hat inzwischen eine Änderungsmeldung abgegeben.

11.2. EDV-Einsatz für die Hochschulverwaltung

An der Universität Erlangen-Nürnberg wird derzeit noch im Testeinsatz ein dialogorientiertes Stellen- und Personalverwaltungssystem für die Personalverwaltung eingesetzt. Wie bereits zum EDV-Einsatz in der Schulverwaltung dargelegt, darf ein automatisiertes Personalverwaltungssystem grundsätzlich nur die personenbezogenen Daten der Mitarbeiter speichern, die zur gesetzlichen Aufgabenerfüllung erforderlich sind. Eine erste Durchsicht des vorgesehenen Datensatzes hat grundlegende Bedenken gegen Art und Umfang der gespeicherten Daten bei dieser Anwendung nicht ergeben. Allerdings habe ich bei einzelner Datenfeldern Zweifel an ihrer Erforderlichkeit vorgetragen. Dies betrifft bei-

spielsweise ins einzelne gehende Speicherungen zur Behinderteneigenschaft von Mitarbeitern, die in einem automatisierten Personalverwaltungssystem nicht unbedingt erforderlich sind, oder sehr detaillierte Angaben zur rechtlichen Stellung des Kindes (z. B. die Eigenschaft als Adoptivkind) oder etwa eine Jahresübersicht der Krankheitstage pro Mitarbeiter mit genauen Kalenderangaben. Das Staatsministerium für Unterricht und Kultus hat mir mittlerweile eine erläuternde Stellungnahme der Universität Erlangen-Nürnberg zugeleitet. Eine abschließende Klärung steht hier noch aus.

11.3. Einsatz von Kleincomputern an der Schule

Neben der Verwendung von Kleincomputern im Unterricht werden an bayerischen Schulen Kleincomputer auch zur Unterstützung der an den Schulen anfallenden Verwaltungsarbeiten eingesetzt. Selbstverständlich muß verhindert werden, daß eine etwaige gleichzeitige Verwendung der Kleincomputer zu Unterrichts- und Verwaltungszwekken einen mißbräuchlichen Zugriff auf die Schulverwaltungsdaten eröffnet. Hierzu hat das Bayer. Staatsministerium für Unterricht und Kultus klare Hinweise zum Datenschutz gegeben, worauf ich bereits im 7. Tätigkeitsbericht hingewiesen hatte.

In Einzelfällen können noch Schwierigkeiten oder Fragen zum Datenschutz auftreten:

- So sind an einer Realschule die für die automatische Erstellung der Zwischenzeugnisse erforderlichen Disketten im Sekretariatsfach des Lehrerzimmers der Schule offen aufgelegen. Meiner Ansicht nach entspricht dieses Verfahren nicht den datenschutzrechtlichen Anforderungen. Disketten mit Programmen und Daten für die Zeugniserstellung müssen stets vor dem Zugriff Unberechtigter geschützt werden. Hierzu wäre zumindest die Unterbringung der Datenträger in einem geschlossenen Behältnis erforderlich. Das Bayer. Staatsministerium für Unterricht und Kultus teilt meine Auffassung.
- Die Eingabe der Zeugnisnoten in den Kleincomputer hat ein Lehrer in einem Unterrichtsraum in Anwesenheit von Schülern vorgenommen, die der Lehrer zu beaufsichtigen hatte. Zwar hätten die Schüler weder Zugang noch Einblick in die einzugebenden Zeugnisnoten gehabt, doch halte ich diese Vorgehensweise für datenschutzrechtlich bedenklich. Meines Erachtens sollten Datenverarbeitungssysteme, die zu Schulverwaltungszwecken genutzt werden, stets in einem verschlossenen Raum installiert sein, zu dem Schüler keinen Zugang haben. Nur so kann mit hinreichender Sicherheit ein Zugriff Unbefugter ausgeschlossen werden.
- Ein Lehrer hat die für die Eingabe der Zeugnisnoten erforderlichen Programme kopiert und die Noteneingabe unter Verwendung dieser Programme auf seinem privaten Kleincomputer zu Hause vorgenommen. Auch diese Vorgehensweise ist aus der Sicht des Datenschutzes unzulässig, weil durch die Verwendung schulischer Programme im häuslichen Bereich ein Zugriff Unbefugter – das können Familienangehörige sein – nicht von vornherein völlig ausgeschlossen ist. Selbst wenn im Einzelfall eine gesicherte Aufbewahrung der Datenträger im privaten Bereich gewährleistet erscheinen mag, würde sich eine solche Verfahrensweise zumindest jeglicher effektiven Datenschutzkontrolle entziehen. Damit wäre faktisch die Möglichkeit einer Überprüfung der Einhaltung datenschutzrechtlicher Vorschriften nicht mehr gegeben. Allein schon deswegen halte ich generell die Verarbeitung dienstlicher Daten mit Personenbezug auf häuslichen Privatrechnern für bedenklich.
- Soweit Lehrer Zugang zu automatisierten Schulverwaltungssystemen in der Schule haben, sind sie bei der Aufnahme dieser Tätigkeit auf das Datengeheimnis zu verpflichten. Der Verpflichtung, die schriftlich erfolgt, hat eine entsprechende Belehrung vorauszugehen. Eine weitergehende informationstechnische oder datenschutzrechtliche Grundausbildung solcher Lehrkräfte verlangt das Bayer. Datenschutzgesetz nicht. Die Verpflichtung auf das Datenschutzgeheimnis entbindet nicht von der Beachtung der gesetzlich gebotenen technischen und organisatorischen Sicherheitsvorkehrungen.
- Fallen bei der automatisierten Erstellung von Zeugnissen Fehldrucke an, so sind diese vollständig und zuverlässig zu vernichten. Gleiches würde selbstverständlich auch bei der herkömmlichen Erstellung von Zeugnissen gelten. Sollte es häufiger bei der automatisierten Zeugniserstellung zu Fehldrucken kommen, wäre die Anschaffung eines handelsüblichen Papiervernichters zu überlegen.
- Staatliche Schulen, die personenbezogene Daten in automatisierten Verfahren verarbeiten, sind nach Art. 7 BayDSG i.V.m. § 7 Datenschutzregisterverordnung dem Landesbeauftragten für den Datenschutz zur Aufnahme in das Datenschutzregister zu melden. Auch Änderungen registerpflichtiger Angaben sind meldepflichtig.

Einem Lehrer, der mich zu Fragen des Einsatzes von Kleincomputern an der Schule um eine datenschutzrechtliche Stellungnahme gebeten hatte, waren dienstliche Schwierigkeiten durch seinen Schulleiter erwachsen. Meiner Auffassung nach ist ein Lehrer wie jeder andere Bürger grundsätzlich berechtigt, sich unmittelbar an den Landesbeauftragten für den Datenschutz zu wenden, wenn durch die Verarbeitung personenbezogener Daten schutzwürdige Belange gefährdet werden können. Dienstliche Schwierigkeiten dürften einem Lehrer daraus nicht erwachsen.

11.4. Datenschutzrechtliche Prüfung eines Gymnasiums

Im Berichtszeitraum habe ich ein Städt. Gymnasium datenschutzrechtlich überprüft. Hierzu wurden aus den automatisierten Schüler- und Kollegstufendateien Kontrollausdrucke erholt und mit den Meldungen zum Datenschutzregister verglichen. Prüfgegenstand waren auch eventuelle regelmäßige Übermittlungen aus diesen Dateien und die weiteren an diesem Gymnasium geführten manuellen Dateien. Besondere Datenschutzrechtsverletzungen habe ich nicht festgestellt. Im einzelnen ergab die Prüfung folgendes:

Die stichprobenartige Durchsicht zeigte keine Abweichungen von gemeldeten Datensätzen, keine Verstöße gegen Löschungsbestimmungen und auch keine Anhaltspunkte dafür, daß inhaltlich unrichtige Daten gespeichert sind. Allerdings habe ich Anregungen zu einigen Datenfeldern gegeben. So bin ich der Auffassung, daß Daten, die lediglich unter ganz außergewöhnlichen Umständen für die Erledigung der Dienstgeschäfte benötigt werden, grundsätzlich nicht in einem automatisierten System geführt werden sollten; sie können im Bedarfsfalle den herkömmlichen Unterlagen entnommen werden. Auch müssen Daten grundsätzlich nach Erreichung ihres Speicherungszwecks gelöscht oder

zumindest gesperrt werden. Auffällig war, daß die beiden automatisierten Dateien je ein nicht näher definiertes Datenfeld aufgewiesen haben. Bei einer der beiden Dateien wird das Feld überhaupt nicht belegt, in der anderen Datei werden hier Angaben über eine Befreiung des betroffenen Schülers vom Sportunterricht eingestellt. Zwar ist im konkreten Fall diese Handhabung nicht zu beanstanden. „Offene" Datenfelder der vorliegenden Art bergen aber generell die Gefahr einer mißbräuchlichen Speicherung von zur Aufgabenerfüllung nicht unbedingt erforderlichen Daten in sich. Ich habe deshalb die Leitung der überprüften Schule gebeten, der Nutzung dieser Felder verstärkte Aufmerksamkeit zu widmen.

Als weitere Dateien habe ich eine Schülerkartei, eine Datei „Notenbogen" und eine Lehrerkartei festgestellt. Die Schülerkartei dient dem Zweck, Verwaltungsarbeiten ohne Zugriff auf die automatisierte Datei durchführen zu können. Damit wird der Kreis der zur automatisierten Datei Zugriffsberechtigten klein gehalten. Dies begrüße ich als wirksame Form der Datensicherung. Bei der Lehrerkartei haben die bislang an diesem Gymnasium verwendeten Karteikarten eine Reihe von Daten enthalten, deren Erforderlichkeit zur Erfüllung schulischer Aufgaben nach meiner Auffassung zweifelhaft ist. Dies gilt insbesondere für den Familienstand des Lehrers, die Zahl seiner Kinder und seine Krankenkasse. Während der Prüfung ist mir mitgeteilt worden, daß für die Lehrerkartei neue Karteikarten verwendet werden sollen, die die von mir als nicht erforderlich angesehenen Datenfelder nicht mehr enthalten. Grundsätzlich gehe ich bei Lehrerkarteien davon aus, daß das Feld „Dienstbezeichnung" nicht zu einer historischen Dokumentation des beruflichen Werdegangs eines Lehrers mit den einzelnen Beförderungsdaten genutzt wird.

11.5. Datenerhebung an Schulen

Von Schülern und Erziehungsberechtigten dürfen nur die Daten erhoben werden, die für die Aufgabenerfüllung der Schulen erforderlich sind. Diese Selbstverständlichkeit wird in der Praxis nicht immer beachtet.

Ein Bürger hat mir geschrieben, daß er sich immer wieder darüber wundere, „welcher Erfindungseifer bei der Weiterentwicklung von Formblättern, Antragsformularen etc. entwickelt" werde. Dem kann ich nur zustimmen. So wird etwa auf dem Anmeldeformblatt für eine Berufsfachschule für Kinderpflege nicht nur nach Namen und Anschrift von Vater und Mutter gefragt, sondern auch nach deren jeweiliger Bankverbindung einschließlich Kontonummer. Eine Unterscheidung zwischen volljährigen Fachschülern und Minderjährigen fehlt. Ebensowenig enthält das Anmeldeformular den nach dem Bayer. Datenschutzgesetz ausdrücklich vorgeschriebenen Hinweis auf die Rechtsgrundlage oder die Freiwilligkeit der Angaben. Im konkreten Fall ist der Schule kein Vorwurf zu machen, weil hier das Formblatt vom Städt. Schulreferat zur Verfügung gestellt worden ist. Trotz Mahnung habe ich bislang von der um Stellungnahme gebetenen städtischen Behörde noch keine Antwort erhalten.

Durch einen Bürger bin ich auf ein Anmeldeblatt für eine Volksschule gestoßen, in dem nach dem Namen der Krankenversicherung gefragt wird. Die Erhebung dieser Angabe ist für Schulzwecke nicht erforderlich und meines Erachtens unzulässig. Seit 1.4.1971 ist für alle Unfälle von Schülern während des Besuchs allgemein bildender Schulen der Schutz der gesetzlichen Unfallversicherung gegeben. Dies gilt auch für damit zusammenhängenden Wege. In Bayern sind der Bayerische Gemeinde-Unfall-Versicherungsverband oder die Staatliche Ausführungsbehörde für Unfallversicherung zuständig. Das Bayer. Staatsministerium für Unterricht und Kultus teilt meine Auffassung.

Bemerkenswert ist in diesem Zusammenhang, daß das amtlich festgestellte Meldeblatt für die Volksschule (in der Anlage zur Volksschulordnung) die Erhebung des Datums nicht vorsieht, das zu beanstandende Anmeldeblatt aber den Aufdruck „nach amtl. Muster" trägt. Zwar kann ich aufgrund der entsprechenden Regelung in der Volksschulordnung davon ausgehen, daß Angaben über die Krankenversicherung eines Schülers von öffentlichen Volksschulen in Bayern normalerweise nicht erhoben werden, doch zeigt der vorliegende Fall, daß teilweise Vordrucke verwendet werden, die den Vorschriften nicht entsprechen und unzulässige Datenerhebungen mit sich bringen.

Die Personaldaten für die an einem von mir überprüften Gymnasium geführte Schülerdatei werden mittels eines Anmeldebogens erhoben. Neben einem meines Erachtens nicht erforderlichen Datenfeld habe ich dabei festgestellt, daß der notwendige Hinweis auf die Freiwilligkeit der Angaben der Erziehungsberechtigten zu einigen Datenfeldern fehlt. Hierauf habe ich die zuständigen Stellen hingewiesen.

11.6. Praktische Ausbildung und Berufsgeheimnisse

Fachschulstudenten und Fachoberschüler haben ein Praktikum zu absolvieren. Die praktische Ausbildung findet teilweise bei Sozialleistungsträgern statt, weshalb sich die Frage stellt, ob § 203 Strafgesetzbuch möglicherweise einem solchen Praktikum wegen der damit verbunden Offenbarung von Berufsgeheimnissen entgegensteht. Meiner Ansicht nach ist hierbei folgendes zu bedenken:

Ein unbefugtes Offenbaren, das nach § 203 Strafgesetzbuch unter Strafandrohung steht, liegt nicht vor, wenn durch Rechtsnorm eine berufsorientierte oder berufspraktische Ausbildung angeordnet ist und das Ausbildungsziel ohne die Mitteilung von Geheimnissen aus dem persönlichen Lebensbereich Dritter nicht erreicht werden kann. Allerdings stellt sich hierbei die weitere Frage, wie konkret die berufspraktische Ausbildung im Hinblick auf die in Betracht kommender Ausbildungsstellen durch die Rechtsnorm umschrieben sein muß. Zwar läßt sich hier kein allgemein gültiger Maßstab entwickeln, doch muß die Rechtsnorm sowohl Prüfung als auch Entscheidung ermöglichen, welche Arten von Stellen zur Erreichung des Ausbildungszieles in Frage kommen oder geeignet sind. Zwar wird die ausdrückliche Nennung aller in Betracht kommender Ausbildungsstellen nicht gefordert werden können, doch muß jedenfalls bei vernünftiger Auslegung der die berufspraktische Ausbildung regelnden Vorschriften erkennbar sein, daß eine Ausbildung bei der fraglichen Stelle ihrer Art nach gewollt sein könnte.

Bei einer Prüfung habe ich festgestellt, daß z. B. für die praktischen Studiensemester des Fachhochschulstudiengangs „Sozialwesen" die entsprechende Rahmenstudienordnung hinreichend konkretisiert und die fachpraktische Ausbildung der Fachoberschüler in der Fachoberschulordnung geregelt ist.

Bei der Frage, ob diese Regelungen nun eine Offenbarung von Berufsgeheimnissen z. B. des Arztes, Rechtsanwalts und Sozialarbeiters im Rahmen der fachpraktischen Ausbildung zulassen, ist nach den verschiedenen Ausbildungsrichtungen zu unterscheiden. Bei der Ausbildungsrichtung Sozialwesen ergibt sich aus dem Begriff „Sozialwesen" m. E. hinreichend konkret, daß die Ausbildung bei Stellen des Sozialwesens erfolgen kann, auch soweit diese üblicherweise mit Daten zu tun haben, die einer besonderen beruflichen Schweigepflicht unterliegen. Offen bleibt allerdings die Frage, inwieweit innerhalb des weiten Aufgabenbereichs der Sozialstellen eine Ausbildung in Bereichen mit besonders sensiblen Daten erforderlich ist. In jedem Fall ist eine Offenbarung im Rahmen der Ausbildung nur zulässig, soweit dem Ausbildungsbedürfnis nicht auch ohne Preisgabe von Berufsgeheimnissen Rechnung getragen werden könnte. Bei der Ausbildungsrichtung „Wirtschaft, Verwaltung und Rechtspflege" wird eine sachgerechte Ausbildung im Teilbereich „Rechtspflege" wohl bei Einrichtungen der Rechtspflege erfolgen können. Insoweit müßte man wohl etwa die Offenbarung des Berufsgeheimnisses eines Rechtsanwalts im Rahmen dieser fachpraktischen Ausbildung als vom Willen des Normengebers umfaßt ansehen. Für den Teilbereich „Verwaltung" fehlt allerdings ein solch enger Bezug zur Schweigepflicht z. B. des Arztes oder Sozialarbeiters. Es gibt viele Stellen im großen Bereich der Verwaltung, die in der Regel nichts mit diesen besonderen Berufsgeheimnissen zu tun haben. Hier wird im Einzelfall zuprüfen sein, ob die fachpraktische Ausbildung bei der „Verwaltung" alle denkbaren Zweige der Verwaltung umfaßt, also auch solche bei Sozialleistungsträgern, die eine Offenbarung von Berufsgeheimnissen des Arztes oder Sozialarbeiters mit sich bringt.

11.7. Weitere Einzelfragen

11.7.1. Klassentreffen

Immer wieder erreichen mich Anfragen von Bürgern, die viele Jahre nach Verlassen der Schule ein Klassentreffen ausrichten möchten. Hierzu benötigen sie Namen und aktuelle Anschriften ihrer ehemaligen Mitschüler. Dies gestaltet sich nach der derzeitigen Rechtslage schwierig:

Der Schule ist nach dem Bayerischen Gesetz über das Erziehungs- und Unterrichtswesen die Weitergabe von Daten und Unterlagen über Schüler und Erziehungsberechtigte an außerschulische Stellen grundsätzlich untersagt, falls nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird. Einen solchen Anspruch kann der Veranstalter eines Klassentreffens zweifelsohne nicht geltend machen. Eine manchmal gewünschte Ausnahmegenehmigung von dieser Bestimmung kann selbstverständlich der Landesbeauftragte für den Datenschutz nicht erteilen. Zwar mag die entsprechende Regelung in diesem Gesetz unnötig eng erscheinen. Sie hat aber die wichtige Funktion, die zahlreichen Datenanforderungen von den verschiedensten Stellen abzuwehren, die für geschäftliche, ideelle oder ideologische Zwecke Schülerdaten verwenden möchten. Es ist gerade ein wesentliches Anliegen des von der Verfassung garantierten Persönlichkeitsschutzes, zwangsweise – hier bei Schülern und deren Eltern – erhobene Daten nur für den Zweck zu verwenden, zu dem sie erlangt worden sind. Deshalb dürfen Schülerdaten nur für schulische Zwecke genutzt werden.

Die Schule darf dem Veranstalter eines Klassentreffens allerdings diejenigen Daten über frühere Mitschüler übermitteln, die in einem Jahresbericht enthalten sind. Hierzu gehören insbesondere Name, Geburtsdatum, Jahrgangsstufe und Klasse der Schüler. Mit diesen Daten ist bei dem Einwohnermeldeamt der Wohnsitzgemeinde der ehemaligen Mitschüler im Wege der Melderegisterauskunft die derzeit aktuelle Anschrift zu erfahren.

Bei einer der nächsten Novellierungen des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen könnte geprüft werden, ob für die Veranstaltung von Klassentreffen die Angabe der früheren Heimatadressen der Schüler – die aktuellen Anschriften sind der Schule ohnehin nicht bekannt – gestattet werden könnte.

11.7.2. Erstellung eines Stammbaumes

Die von Schülern erbetene Anfertigung von Stammbäumen führt immer wieder zu datenschutzrechtlichen Fragestellungen. Hierüber hatte ich bereits im 7. Tätigkeitsbericht berichtet und bemerkt, daß das Staatsministerium für Unterricht und Kultus die Hinweise für die Lehrplangestaltung eventuell überarbeiten müsse, um dem auf erfreuliche Weise gestiegenen Datenschutzbewußtsein der Eltern gerecht zu werden. Daß meine Bitte an das Staatsministerium für Unterricht und Kultus nicht gänzlich unberechtigt war, zeigt die Tatsache, daß die Erstellung von Stammbäumen an Schulen immer wieder Eltern beunruhigt. Sie befürchten, daß in kleineren Orten die privaten Familienverhältnisse bekannt werden könnten. Die Lehrer sollten bemüht sein, beim Anfertigen von Stammbäumen nicht zu sehr ins Detail zu gehen und die Gefühle des Schülers zu achten. Das „freiwillige" Mitarbeiten der Kinder rechtfertigt ins einzelne gehende Stammbäume und deren Erörterung vor der Klasse nicht. Im übrigen habe ich es begrüßt, daß ein Lehrer es akzeptiert hat, wenn Schüler die Aufgabe der Stammbaumerstellung nicht erledigt haben. Besonders bedenklich ist es, wenn – wie geschehen – ein Schulbuchverlag in einem zugelassenen Lernmittel diese Grundsätze nicht beachtet. Das Staatsministerium für Unterricht und Kultus hat mir zugesagt, daß der in Frage kommende Schulbuchverlag die Auflage erhalten habe, die die Erstellung von Familienstammbäumen betreffenden Fragen künftig entfallen zu lassen oder unter Einschaltung des Kultusministeriums so zu überarbeiten, daß den Belangen des Persönlichkeitsschutzes Rechnung getragen wird.

11.7.3. Installation von Wechselsprechanlagen

Ein Lehrer hat mich unterrichtet, daß an seiner Realschule eine Wechselsprechanlage installiert sei, mit deren Hilfe es möglich sein soll, vonjedem beliebigen Zimmer der Schule aus jedes andere Schulzimmer abzuhören.

Das Bayer. Staatsministerium für Unterricht und Kultus hat mir hierzu mitgeteilt, daß die fragliche Wechselsprechanlage in jeder Sprechstelle über eine Abhörsperre verfügt. Jeder Teilnehmer hat die Möglichkeit, durch Betätigung der Abhörsperre seine Sprechstelle entsprechend zu blockieren. Ist die Abhörsperre nicht betätigt, ertönt für ankommendes Gespräch als Aufmerksamkeitszeichen ein lauter Anrufgong.

Damit ist aus der Sicht des Datenschutzes gegen die Einrichtung einer solchen Wechselsprechanlage keine Einwendung zu erheben. Ein unbemerktes Abhören von privaten Gesprächen dürfte mit einer derartigen Anlage grundsätzlich nicht möglich sein, weil jeder Lehrer die Möglichkeit hat, eine Abhörsperre zu betätigen und damit die Sprechstelle von vornherein für Außenstehende zu blockieren, und andernfalls ein laut hörbares Signal die Aufnahme der Verbindung zum Klassenzimmer deutlich macht. Eine Verletzung der Persönlichkeitsrechte von Lehrern oder Schülern erscheint angesichts dieser Umstände ausgeschlossen.

11.8. Datenerhebung für Forschungszwecke

Ein Lehrstuhl einer Universität hat eine Langzeituntersuchung zum Problem der Nachwuchsentwicklung in einer bestimmten Sportart durchgeführt. Die für die Untersuchung notwendigen Daten wurden mittels eines Fragebogens bei den Studenten erhoben. Durch den schriftlichen Hinweis auf die „Anonymität" wurde bei den betroffenen Befragten der Eindruck erweckt, daß die Verarbeitung der Daten ohne Personenbezug, also anonym erfolge. Tatsächlich wurden jedoch auf dem Fragebogen-Deckblatt Name, Vorname, Wohnort, Straße und Geburtsdatum sowohl des befragten Studenten wie seines Trainers erhoben. Da es sich um eine sich über mehrere Jahre erstreckende Langzeituntersuchung handelte, wurde der Personenbezug nach Abschluß der Erhebung auch zum Zwecke der Zusammenführung der Daten aus den jährlichen Befragungen aufrechterhalten. Außerdem wurden die Antworten der ebenfalls befragten Trainer mit den Angaben der Studenten verknüpft. Die Studenten hätten daher statt der Zusage der tatsächlich nicht eingehaltenen „Anonymität" auf die Tatsache der personenbezogenen Nutzung und der Verknüpfung ihrer Daten mit den Antworten der Trainer hingewiesen werden müssen. Nur so hätten die befragten Studenten bei ihren freiwilligen Antworten von zutreffenden Voraussetzungen ausgehen können. Diese Datenerhebung war daher insoweit unzulässig. Außerdem fehlte auf dem Erhebungsbogen der gesetzlich vorgeschriebene Hinweis auf die Freiwilligkeit der Angaben.

Um das Ergebnis jahrelanger Arbeit letztendlich nicht zu gefährden, habe ich eine Lösung zur weiteren Durchführung des Forschungsprojektes mit der Universität besprochen, die einerseits zur weitest möglichen Wahrung schutzwürdiger Belange der befragten Studenten führt und andererseits einen sinnvollen Abschluß des Forschungsprojekts gestattet. Über die Einhaltung meiner vorgeschlagenen Sicherungsmaßnahmen habe ich mich unterrichtet.

Den Vorgang habe ich zum Anlaß genommen, das Bayer. Staatsministerium für Unterricht und Kultus zu bitten, für die Durchführung von wissenschaftlichen Untersuchungen mit Personenbezug durch Universitäten verbindliche Regeln zu entwickeln, die eine datenschutzgerechte Abwicklung gewährleisten.

12. Archive und Forschung

12.1. Datenschutz und Forschungsfreiheit

Zwischen Datenschutz und wissenschaftlicher Forschung besteht ein Spannungsverhältnis. Die Stimmen der Forscher werden lauter, die den Datenschutzbehörden eine Beeinträchtigung der Forschungsfreiheit vorwerfen. Datenschutz wird von diesem Personenkreis zwar als durchaus wichtig eingeschätzt, doch wird nur teilweise ein Bedürfnis für die Beachtung des Persönlichkeitsschutzes auch bei wissenschaftlicher Forschung anerkannt; zumindest wird es als der Forschungsfreiheit nachrangig eingeordnet.

Hierzu ist folgendes deutlich festzustellen:

Das allgemeine Persönlichkeitsrecht, aus dem das Recht auf informationelle Selbstbestimmung und damit auch der Datenschutzgedanke abgeleitet werden, wird durch Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 Grundgesetz garantiert. Art. 1 Abs. 1 Grundgesetz sichert die Würde des Menschen, die inhaltlich vornehmlich in der freien Entfaltung seiner Persönlichkeit besteht. Art. 2 Abs. 1 Grundgesetz schließt Wertschutzlücken in Bereichen, die die im Grundgesetz einzeln aufgeführten Freiheitsrechte inhaltlich nicht erfassen. Das Grundgesetz gewährt also dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung. Eingriffe in das Persönlichkeitsrecht und hier speziell in das Recht auf informationelle Selbstbestimmung sind nur aufgrund normenklarer, den Verhältnismäßigkeitsgrundsatz beachtender gesetzlicher Regelungen zulässig.

Auch das Recht auf Wissenschaftsfreiheit ist verfassungsrechtlich durch Art. 5 Abs. 3 Satz 1 Grundgesetz gewährleistet. Diese Norm beruht auf der Schlüsselfunktion, die einer freien Wissenschaft für die Selbstverwirklichung des einzelnen als auch für die gesamtgesellschaftliche Entwicklung zukommt. Zwar sind Begrenzungen der Wissenschaftsfreiheit durch Gesetz ausgeschlossen, doch kann die Wissenschaftsfreiheit nicht grenzenlos sein. Auch ein Forscher darf sich bei seiner wissenschaftlichen Tätigkeit nicht über die verfassungsrechtlich verbürgten Rechte seiner Mitbürger hinwegsetzen. Weil die Wissenschaftsfreiheit aber nicht durch Gesetz eingeschränkt werden kann, können etwaige Einschränkungen nur aus der Verfassung selbst hergeleitet werden. Hierbei kommt der Wissenschaftsfreiheit jedoch nicht schlechthin Vorrang zu. Auch die Wissenschaftsfreiheit ist der in Art. 1 Abs. 1 GG garantierten Würde des Menschen zugeordnet, die als oberster Wert das ganze grundrechtliche Wertsystem beherrscht. Diese Verpflichtung endet im übrigen auch nicht mit dem Tode, was für die Archivverwaltung bedeutsam ist. Zwar ist es zunächst Aufgabe des Gesetzgebers, einen Ausgleich zwischen diesen teilweise in Konflikt zueinander stehenden Grundrechtspositionen des Persönlichkeitsschutzes und der Wissenschaftsfreiheit zu finden. Solange derartige Entscheidungen des Gesetzgebers fehlen – die anstehende Archivgesetzgebung soll diese Lücke zumindest für einen Teilbereich schließen – kann die mit Rücksicht auf kollidierende Verfassungswerte notwendige Grenzziehung nur im Einzelfall durch eine entsprechende Güterabwägung vorgenommen werden. Dies ist von den Stellen zu beachten, die, wie beispielsweise die Archive, den Forschern Daten zur Verfügung stellen, aber auch von den Forschern selbst.

Übergangslösung

Unter Beachtung der vorgenannten Gesichtspunkte und unter Berücksichtigung der Tatsache, daß ein Archivgesetz, auf dessen Entwurf weiter unten eingegangen wird, noch nicht vorliegt, hatte ich in meinem 7. Tätigkeitsbericht Vorschläge unterbreitet, wie in einer Übergangszeit bei der Einsichtnahme durch zeitgeschichtliche Forscher in archiviertes Material verfahren werden könnte. Zur möglichen

Überwachung von dem Schutze des Persönlichkeitsrechts dienenden Auflagen hatte ich unter anderem angeregt, daß sich die Generaldirektion der Staatlichen Archive rechtzeitig ein Pflichtstück der beabsichtigten Veröffentlichung vorlegen läßt. Denn unbeschadet der eigenen Verantwortung des Archivbenutzers kann und muß die Einhaltung der von der Generaldirektion erteilten Auflagen gerade in den Fällen, in denen besonders sensibles Archivgut verwendet wird, natürlich durch die anordnende Behörde in geeigneter Form überwacht werden. Im Falle eines Verstoßes sind Konsequenzen zu ziehen.

Mit meinem Vorschlag einer Vorlage von Pflichtstücken habe ich mir zum einen die grundsätzliche Möglichkeit von Stichprobenkontrollen durch die Generaldirektion versprochen und ganz generell eine präventive Wirkung bei Veröffentlichungen über besonders sensible Daten erhofft. Im übrigen war ich davon ausgegangen, daß die Generaldirektion der Staatlichen Archive von der Anforderung von Pflichtstücken grundsätzlich nicht in allen Fällen Gebrauch machen würde. Außerdem war ich mir bewußt, daß die Generaldirektion allein schon wegen ihrer beschränkten Personalkapazität nicht sämtliche angeforderten Pflichtstücke im Detail auf die eventuelle Beeinträchtigung schutzwürdiger Belange Betroffener überprüfen kann.

Das Bayer. Staatsministerium des Innern hat meine diesbezüglichen Vorschläge erfreulicherweise aufgegriffen und die Zustimmung zur Nutzung von archivierten Akten aus seinem Geschäftsbereich von der Erhebung entsprechender Auflagen zum Schutze der Persönlichkeitsrechte abhängig gemacht. Leider steht die Generaldirektion der Staatlichen Archive meinen Überlegungen reserviert gegenüber. Dieses Problem dürfte sich aber, wie ich hoffe, durch das Inkrafttreten von Bundes- und Landesarchivgesetzen lösen.

12.2. Archivgesetzgebung

In Archiven werden große Mengen personenbezogener Daten erfaßt, verwahrt, ausgewertet und insbesondere für wissenschaftliche und rechtliche Zwecke nutzbar gemacht. Auf die Notwendigkeit, für die archivarische Verarbeitung personenbezogener Daten gesetzliche Regelungen zu schaffen, habe ich seit Jahren hingewiesen. Zwischenzeitlich liegen nun die Entwürfe zu einem Bayerischen Archivgesetz und zu einem Bundesarchivgesetz vor. Dies begrüße ich außerordentlich. Ich hoffe, daß in der jeweils nächsten Legislaturperiode nicht nur das Bayer. Archivgesetz, dem auch der Bayer. Senat besondere Dringlichkeit zuerkannt hat, sondern auch das Bundesarchivgesetz verabschiedet wird. Weil ein nicht unerheblicher Teil des zu archivierenden personenbezogenen Datenmaterials unter dem Schutz bundesrechtlicher Geheimhaltungsbestimmungen steht (z. B. Sozialgeheimnis, Steuergeheimnis), bedarf eine auch weiterhin effektive Tätigkeit bayerischer Archive auch der Verabschiedung der entsprechenden bundesgesetzlichen Regelungen.

Der vorliegende Entwurf zum Bayer. Archivgesetz ist ein erster wichtiger Schritt, um Aufgaben und Benutzung der Archive zu regeln und damit deren Funktion auch in Zukunft zu sichern. Auch für den Schutz des Persönlichkeitsrechts der Betroffenen wird in einer Reihe von Bestimmungen Vorsorge getroffen. Außerdem gibt es klare Regelungen über den Zugang zu den Archiven. In meiner Stellungnahme zu dem Entwurf habe ich aus datenschutzrechtlicher Sicht noch eine Reihe von Änderungsvorschlägen vorgelegt. Diese sollen an dieser Stelle nicht sämtlich wiedergegeben werden. Im folgenden weise ich nur auf einige wesentliche Punkte hin:

- Die Umschreibung der den staatlichen Archiven zugewiesenen Aufgaben scheint mir zu weit gefaßt. Insbesondere die Nutzbarmachung des Archivgutes kann zu einer, dem Grundsatz der Verhältnismäßigkeit widersprechenden Zweckänderung der gespeicherten personenbezogenen Daten führen. Ganz generell sollte deutlicher als bisher zum Ausdruck gebracht werden, daß entgegenstehende Belange Dritter für die Tätigkeit der Archive nicht unbeachtlich sind.
- Die Archivverwaltung darf keinen unbeschränkten Zugang zu sämtlichen Unterlagen öffentlicher Stellen des Freistaates Bayern erhalten und dadurch „allwissend" werden. Die Anknüpfung an Verwaltungsvorschriften zur Begründung von Rechtsfolgen, die letztlich einen Eingriff in das informationelle Selbstbestimmungsrecht betroffener Bürger bewirken können, ist bedenklich.
- Zwischen Archivgut, das aus wissenschaftlichen Gründen aufbewahrt wird, und solchen Unterlagen, die aus Rechtsgründen auf Dauer aufzubewahren sind, ist stärker zu unterscheiden.
- Die vorgesehene Anbietungsregelung berücksichtigt nicht, daß beispielsweise geltendes Bundesrecht einer Übernahme von Unterlagen, für die das Sozial- oder das Steuergeheimnis gilt, entgegenstehen kann. Gelangen Unterlagen in Akten, die dem Steuer- oder Sozialgeheimnis unterliegen, so verhindert dies grundsätzlich die Anbietung und Übernahme des vollständigen Aktenmaterials.
- Das den Vertretern der Staatlichen Archive eröffnete Einsichtsrecht in das gesamte Registraturgut der abgebenden Stelle geht über das Maß des Erforderlichen hinaus und würde eine wohl nicht mehr verhältnismäßige Zweckänderung gespeicherter Daten zur Folge haben. Im übrigen werfen die Einsichtsbefugnisse des Archivpersonals auch in Unterlagen, die besonderen Geheimhaltungsbestimmungen unterliegen, die Frage nach einer gesetzlich hervorgehobenen Verschwiegenheitspflicht für diesen Personenkreis auf.
- Eine nicht unproblematische Zweckänderung würde auch die Möglichkeit eröffnen, archivierte Unterlagen u. a. für „amtliche Zwecke" aller Art zu nutzen. Hier wäre eine deutlich enger gefaßte Formulierung wünschenswert.
- Auch die Regelungen zu den Sperrfristen, vor deren Ablauf eine Einsichtgewährung in das Archivgut grundsätzlich ausgeschlossen ist, müßten noch einmal überdacht werden. So dürfte m. E. nicht die Sperrfrist bereits vor Übernahme der Unterlagen durch die Archive ablaufen. Auch erscheint angesichts der heutigen durchschnittlichen Lebenserwartung der Bevölkerung eine Sperrfrist von 100 Jahren ab Geburt des Betroffenen zu kurz. Damit würde das Archivgut in vielen Fällen früher als 30 Jahre nach dem Tod des Betroffenen für die Nutzung eröffnet sein.

  Für alle Daten, die bei der abgebenden Stelle aufgrund besonderer Vorschriften zum Schutze des Betroffenen hätten gelöscht, gesperrt oder vernichtet werden müssen, muß nach ihrer Übernahme in ein Archiv die

Nutzung grundsätzlich auf Archivzwecke beschränkt werden. Eine Nutzung zu allgemeinen Verwaltungszwekken kann für alle Behörden, auch und gerade für die abgebende Stelle, grundsätzlich nicht eröffnet sein. Die im Entwurf des Archivgesetzes vorgesehene Änderung des Bayer. Datenschutzgesetzes ist zumindest unglücklich formuliert.

Ein Gesichtspunkt, der weniger im Bayer. Archivgesetz als wohl eher im Bundesarchivgesetz geregelt werden müßte, scheint mir von besonderer Bedeutung zu sein:

Werden personenbezogene Daten aus einem Bereich der öffentlichen Verwaltung einem Archiv abgegeben, für den bisher aufgrund einschlägiger Bestimmungen ein Zeugnisverweigerungsrecht und ein Beschlagnahmeverbot bestand, so verlieren diese Unterlagen bei Übergabe an das Archiv diesen gesetzlichen Schutz. Dies würde die Rechtsstellung des Betroffenen verschlechtern, ohne daß dies dem Zweck der Archivierung entspräche. Das Risiko einer Beschlagnahme von Unterlagen, z. B. aus dem Bereich der Krankenhäuser, oder Sozialämter, sollte nicht übersehen werden. Meines Erachtens sollte deshalb ausdrücklich klargestellt werden, daß durch die Archivierung solcher Daten deren gesetzlicher Schutz nicht verloren geht. Das Problem ließe sich im übrigen auch dadurch lösen, daß derartige Unterlagen erst nach dem Tod des Betroffenen archiviert werden.

13. Straßenverkehr

13.1. Führerschein auf Probe

Der „Führerschein auf Probe" als Teil eines Gesamtprojektes zur Erhöhung der Verkehrssicherheit ist durch die inzwischen in Kraft getretene Änderung des Straßenverkehrsgesetzes eingeführt worden. Obwohl nach der nun Gesetz gewordenen Konzeption eine zentrale Datei aller jungen Fahranfänger entsteht – aus datenschutzrechtlicher Sicht grundsätzlich nicht unproblematisch – habe ich mit Nachdruck die Auffassung vertreten, daß die jetzt gefundene Lösung aus der Sicht des Datenschutzes dennoch keinen durchgreifenden Bedenken begegnet. Die nach dem Verhältnismäßigkeitsgrundsatz notwendige Abwägung zwischen dem durch die zentrale Speicherung vorgenommenen Eingriff in die Rechte der Fahranfänger einerseits und den Interessen der Allgemeinheit nach einer maßgeblichen Erhöhung der Verkehrssicherheit andererseits ist sachgerecht vorgenommen worden. Die zeitweise diskutierten Alternativen zu einer zentralen Speicherung der Führerscheinanfänger hätten meiner Ansicht nach zu größeren datenschutzrechtlichen Problemen geführt.

Ich werde jedoch den Vollzug des „Führerscheins auf Probe" sehr aufmerksam verfolgen und durch stichprobenartige Prüfungen feststellen, ob die im Gesetz vorgesehenen technisch-organisatorischen Sicherungsmaßnahmen eingehalten werden und nicht durch zusätzliche Speicherungen personenbezogener Daten, etwa bei den mit der Nachschulung befaßten Stellen, ungerechtfertigte Risiken für die Fahranfänger entstehen.

13.2. Zentrales Verkehrs-Informationssystem (ZEVIS)

Neben den bei den einzelnen Zulassungsstellen geführten örtlichen Fahrzeugregistern, die Angaben zum zugelassenen Fahrzeug und zum Halter enthalten, wird beim Kraftfahrt-Bundesamt in Flensburg ein Zentrales Fahrzeugregister geführt (siehe bereits im 6. und 7. Tätigkeitsbericht). Dieses Fahrzeugregister enthält das Register der Fahrzeuge mit amtlichen Kennzeichen einschließlich der in den letzten fünf Jahren endgültig aus dem Verkehr gezogenen Fahrzeuge sowie das Register der Fahrzeuge mit Versicherungskennzeichen.

Das Zentrale Fahrzeugregister soll vornehmlich zwei Aufgaben erfüllen: im Rahmen der Zulassung von Fahrzeugen die Sicherung der Verfügungsberechtigung am Fahrzeug sowie die Erteilung von Auskünften zur Identifizierung von Fahrzeugen und von Personen in ihrer Eigenschaft als Halter von Fahrzeugen. Der Bestand des Zentralen Fahrzeugregisters beträgt derzeit etwa 33 Millionen Fahrzeuge. Aus dem Zentralen Fahrzeugregister werden jährlich 16,1 Millionen Auskünfte ohne ZEVIS erteilt und daneben noch 2,5 Millionen Auskünfte über ZEVIS.

Durch das Zentrale Verkehrs- und Informationssystem (ZEVIS) sollen Führung und Nutzung der Datenbestände beim Kraftfahrt-Bundesamt verbessert werden. Außerdem sind mit ZEVIS die technischen Möglichkeiten geschaffen worden, die Polizei online (Direktabruf) an die Datenbestände anzuschließen und Auskünfte im einstelligen Sekundenbereich zu geben. Hierauf wie auf die Notwendigkeit der Schaffung normenklarer gesetzlicher Grundlagen für das zentrale Fahrzeugregister habe ich bereits in früheren Jahren hingewiesen.

Seit längerem liegt ein Entwurf zur Änderung des Straßenverkehrsgesetzes vor (letzter Stand derzeit die Fassung vom 28.1.1986). Zwar hatte ich bereits in meinem letzten Tätigkeitsbericht zu dem damaligen Gesetzentwurf bemerkt, daß er sichtlich von dem Bestreben getragen ist, den vom Bundesverfassungsgericht im Volkszählungsurteil entwickelten Grundsätzen für eine den Persönlichkeitsschutz wahrende verfassungsgemäße Erhebung und Verarbeitung personenbezogener Daten Rechnung zu tragen. Doch sind aus der Sicht des Datenschutzes noch einige Probleme offen geblieben oder haben sich in der letzten Fassung des Gesetzentwurfes verschärft:

Zweckbindung

Bei einer gesetzlichen Regelung für die Einführung eines zentralen Verkehrsinformationssystems sollte mehr als bisher bedacht werden, daß durch die Speicherung von derzeit etwa 33 Millionen Kraftfahrzeugen und ihrer Halter eine im Direktzugriff stehende Datenbank entsteht, die einem zentralen Personenregister für die Bundesrepublik Deutschland sehr nahe kommt. Im Lichte dieser Erkenntnis muß dem Grundsatz der strikten Zweckbindung aller gespeicherten Daten größte Beachtung geschenkt werden. Die Daten aus der Kraftfahrzeug-Zulassung dürfen grundsätzlich nur zu dem Zweck verwendet werden, zu dem sie erhoben worden sind, also insbesondere zur Durchsetzung einer verkehrs- oder zivilrechtlichen Haftung der Fahrzeughalter aus ihrer Teilnahme am Straßenverkehr. Eine Halterfeststellung zu beliebigen Zwecken anderer Stellen kann allenfalls aus einem überwiegenden Allgemeininteresse für genau festgelegte Einzelfälle zugelassen werden. Die diesbezüglichen Regelungen im Entwurf sind teilweise nicht ausreichend präzise und erlauben insbesondere Zweckentfremdungen, die nicht durch ein überwiegendes Allgemeininteresse gerechtfertigt und damit wohl unverhältnismäßig

sind. Hierzu zählt bespielsweise die Zulassung der Zweckentfremdung für die Verfolgung von nichtverkehrsbezogenen Ordnungswidrigkeiten und für die Abwehr von nicht verkehrsbezogenen Gefahren für die öffentliche Sicherheit und Ordnung, ohne daß eine derartige Datenübermittlung auf Fälle von erheblicher Bedeutung beschränkt wäre.

Direktabruf

Auch das von mir mehrfach aufgeworfene Problem der sogenannten „P-Anfrage", mit der Polizeidienststellen im Direktabruf unabhängig vom Zweck der bloßen Identifizierung eines Fahrzeugs oder dessen Halter generell erfahren, ob und ggf. welche verschiedenen Fahrzeuge auf eine bestimmte Person zugelassen sind und unter welcher Wohnanschrift diese Person gemeldet ist, ist meines Erachtens noch nicht unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung und der Beachtung des Grundsatzes der Verhältnismäßigkeit gelöst. Ich hatte hier Vorschläge unterbreitet, die der Polizei den im Einzelfall notwendigen schnellen Zugriff auf Halterdaten ermöglicht hätten, ohne daß zu jeder Tages- und Nachtzeit bundesweit über sämtliche angeschlossenen Datensichtgeräte der Polizei solche Direktabrufe zugelassen werden müßten.

Protokollierung

Die zweifelsohne wohlgemeinte Absicht des Gesetzgebers, die Voraussetzungen zu schaffen, um die Berechtigung der einzelnen Datenabrufe zumindest nachträglich stichprobenartig kontrollieren zu können, hat zu einem wohl ungewollten, gleichwohl nicht zu vernachlässigenden neuen Problem geführt: So sieht der Gesetzentwurf derzeit vor, daß das Kraftfahrt-Bundesamt oder die einzelnen Zulassungsstellen über die Datenabrufe Aufzeichnungen zu fertigen haben. Diese müssen die bei den Abrufen verwendeten Daten, den Tag und die Uhrzeit der Abrufe, die Kennung der abrufenden Dienststelle und die abgerufenen Daten enthalten. Die Aufzeichnungen dürfen nur zur Kontrolle der Zulässigkeit der Abrufe verwertet werden und sind durch geeignete Vorkehrungen gegen zweckentfremdete Nutzung und gegen sonstigen Mißbrauch zu schützen. Gewiß muß die Rechtmäßigkeit der Übermittlung von personenbezogenen Daten für interne und externe Datenschutzkontrollen überprüfbar sein. Der Gesetzentwurf trägt diesem Grundsatz durch die vorgesehenen Protokollierungspflichten auch weitgehend Rechnung. Doch bergen diese Protokollierungspflichten für die übermittelnde Behörde andererseits auch die Gefahr eines Mißbrauchs in sich, weil sie ein neues großes Datenpotential schaffen, das sich teilweise schon von seinem Umfang her einer effektiven Kontrolle entziehen müßte. Auch könnte allein wegen der Existenz dieses neuen riesigen personenbezogenen Datenpotentials das Risiko einer möglicherweise im Einzelfall zweckwidrigen Nutzung entstehen. Ich rege daher an, auf die vorgesehene umfassende zentrale Dokumentierung von Übermittlungsvorgängen durch das Kraftfahrt-Bundesamt zu verzichten und statt dessen die Möglichkeiten stichprobenartiger Kontrollaufzeichnungen vorzusehen. Da ohnedies bereits aus personellen Kapazitätsgründen sowohl bei den Kraftfahrzeug-Zulassungsstellen wie bei den Datenschutzbeauftragten nur stichprobenartige Überprüfungen möglich sind, sollten auch für derartige Kontrollen nicht mehr Datengespeichert werden, als hierfür erforderlich sind. Gleichzeitig wäre vermieden, daß eine neue große personenbezogene Datensammlung entsteht.

Ich hoffe, daß es bis zur dringend erforderlichen Verabschiedung der Änderung des Straßenverkehrsgesetzes gelingen wird, die noch bestehenden datenschutzrechtlichen Bedenken zu berücksichtigen.

13.3. Besuch beim Kraftfahrt-Bundesamt

Die Datenschutzbeauftragten des Bundes und der Länder haben im Berichtszeitraum dem Kraftfahrt-Bundesamt einen Besuch abgestattet, um im Hinblick auf die Novellierung des Straßenverkehrsgesetzes und die datenschutzrechtliche Bewertung der Datenübermittlungen zwischen Landesbehörden und dem Kraftfahrt-Bundesamt ausreichende Informationen zu besitzen. Allein die Tatsache, daß diese Bundesbehörde offen und unbefangen einen Einblick in die verschiedenen Formen ihrer Datenverarbeitung eröffnet hat, ist begrüßenswert. Für die datenschutzrechtliche Bewertung der Datenübermittlungen zwischen Landesbehörden und Kraftfahrt-Bundesamt sind zwei Informationen besonders bedeutsam:

Die beim Kraftfahrt-Bundesamt gespeicherten Daten liegen in ihrem Akualitätsstand ca. 3 Wochen hinter den entsprechenden Datenänderungen bei den Kraftfahrzeug-Zulassungsstellen zurück, wenn diese die Daten konventionell bearbeiten und dementsprechend auch die Änderung konventionell dem Kraftfahrt-Bundesamt mitteilen. Sie liegen eine Woche zurück, wenn die Kraftfahrt-Zulassungsstellen automatisiert sind.

Die sogenannte „P-Anfrage" ist derzeit über ZEVIS programmtechnisch noch nicht verwirklicht. Hierzu sind noch Programmänderungen notwendig. Derzeit steht im Kraftfahrt-Bundesamt für eilige Anfragen über Nacht ein Bereitschaftsdienst zur Verfügung. Dieser Bereitschaftsdienst werde, so wurde mir berichtet, etwa ein- bis zweimal pro Woche für Polizeidienststellen tätig. Hierbei seien auch die Personalienabfragen mit eingeschlossen. Sollte nach derzeitigem technischen Stand eine „P-Anfrage" maschinell durchgeführt werden, müßte der gesamte Datenbestand oder der durch Angabe einer Zulassungsstelle örtlich beschränkte Bestand seriell an dem Namen der gesuchten Person vorbeigeführt werden. Die zur „P-Anfrage" bekannt gewordenen geringen Zahlen wecken Zweifel an der Notwendigkeit einer Direktabrufmöglichkeit für alle zugriffsberechtigten Polizeidienststellen und bestätigen damit meine Bedenken gegen die Einführung einer „P-Anfrage".

13.4. Zugriff auf automatisierte örtliche Fahrzeugregister

Mit der oben erörterten Änderung des Straßenverkehrsgesetzes sollen nicht nur die Rechtsgrundlagen für Einrichtung und Benutzung des Zentralen Verkehrsinformationssystems geschaffen werden, sondern auch die Zugriffe auf die örtlichen Fahrzeugregister neu geregelt werden. Dies ist, was ich schon seit Jahren angemahnt habe, ebenfalls dringend erforderlich.

Auch in Bayern haben einzelne Kraftfahrzeug-Zulassungsstellen ihren Datenbestand automatisiert. Um eine rationelle Datenverarbeitung zu ermöglichen, ist der Polizei in einzelnen Fällen der Direktabruf auf diese automatisierten Register eingeräumt. Dies ist jedoch aufgrund der derzeitigen Rechtslage nicht völlig unproblematisch. § 26 Abs. 5 Straßenverkehrszulassungsordnung gestattet derzeit nur Datenabrufe im Einzelfall. Mit der Eröffnung einer Direktabrufmöglichkeit gelten aber nach Datenschutzrecht sämtliche

Daten als übermittelt. Im Hinblick auf die seit Jahren im Raum stehende Novellierung des Straßenverkehrsgesetzes habe ich davon abgesehen, diese vom Gesetz nicht ausreichend gedeckten Direktabrufmöglichkeiten der Polizei bei örtlichen Fahrzeugregistern zu beanstanden. Hierbei habe ich auch berücksichtigt, daß zumindest für eine Übergangszeit ein rechtlich nicht unproblematischer Zustand dann hinzunehmen ist, wenn ohnehin ein Gesetzgebungsverfahren in Gang gesetzt ist und die Datenübermittlung für den Vollzug einer ordnungsgemäßen Datenverarbeitung unbedingt erforderlich ist. Ich habe mich davon überzeugen lassen, daß die in Frage stehenden Fahrzeug- und Führerscheindaten ihrer Art nach zur Erfüllung der der Polizei gesetzlich übertragenen Aufgaben unbedingt erforderlich sind, eine Vielzahl von Einzelauskünften benötigt wird und diese Einzelanfragen häufig auch dringlich sind. Ich habe allerdings deutlich gemacht, daß der im Wege des Online-Anschlusses zur Verfügung gestellte Datenbestand auf das erforderliche Minimum beschränkt sein muß und ich davon ausgehe, daß in nächster Zukunft durch die Änderung des Straßenverkehrsgesetzes eine ausreichende Rechtsgrundlage zur Verfügung steht.

13.5. Gesundheitsbefragung für Ersatzführerschein

Ein Bürger hatte seinen Führerschein verloren und deshalb bei der Führerscheinstelle des für ihn zuständigen Landratsamtes die Erteilung eines Ersatzführerscheines beantragt. Dieses machte die Erteilung der erbetenen Urkunde von der Beantwortung eines Fragebogens „Über den Gesundheitszustand" abhängig, der 26 Fragen enthielt. Neben Fragen über das Seh- und Hörvermögen, den Zustand von Gliedmaßen und Rumpf sowie zum Nervensystem oder etwa zum Stichwort „innere Organe" wurde gefragt, ob der Antragsteller wegen einer Herzerkrankung oder Kreislaufstörung ständig in ärztlicher Behandlung stehe, ob er an einer behandelten Zuckerkrankheit leide und deswegen Tabletten einnehme oder sich Spritzen verabreiche. Weiter wurde unter „Sonstiges" ganz allgemein nach sonstigen schwerwiegenden Krankheiten oder Gebrechen und nach einem eventuellen Grad der Minderung der Erwerbsfähigkeit gefragt. Schließlich enthielt der Fragebogen auch noch eine ganz allgemeine Frage nach etwa anhängigen gerichtlichen Verfahren.

Gegen eine generelle Verwendung eines solchen Fragebogens über den Gesundheitszustand eines Antragstellers im Verfahren zur Erteilung eines Ersatzführerscheines bestehen aus datenschutzrechtlicher Sicht Bedenken. Eine solche Befragung dürfte unverhältnismäßig sein. Zwar ist das Verfahren bei Verlust eines Führerscheins in der Straßenverkehrszulassungsordnung nicht geregelt. Die Ausstellung von Ersatzführerscheinen ist nur in der Dienstanweisung zur Straßenverkehrszulassungsordnung niedergelegt. Danach ist für einen verlorenen, sonst abhanden gekommenen oder unbrauchbar gewordenen Führerschein auf Antrag ein neuer Führerschein auszufertigen. Hierzu ist lediglich ein Nachweis erforderlich, daß der Antragsteller die Fahrerlaubnis besitzt. Außerdem ist ein Auszug aus dem Verkehrszentralregister einzuholen. Ferner kann die Führerscheinstelle über den Verbleib eines verlorenen Führerschein eine eidesstattliche Versicherung verlangen. Die Abgabe einer erneuten Erklärung über den Gesundheitszustand des Antragstellers wird aber auch in der Dienstanweisung für die Ausstellung von Ersatzführerscheinen nicht verlangt. Die Behörde kann zwar grundsätzlich auch bei der Ausstellung eines Ersatzführerscheines die Eignung des Antragstellers zum Führen von Kraftfahrzeugen prüfen, ist dabei aber grundsätzlich nicht berechtigt, den Antragsteller über der Behörde unbekannte, eignungsmindernde oder -ausschließende Tatsachen mittels eines Gesundheitsfragebogens zu befragen. Eine solche Befragung über körperliche und geistige Mängel wäre allenfalls vor der erstmaligen Erteilung einer Fahrerlaubnis zulässig und verhältnismäßig. Bei Antragstellung auf Erteilung eines Ersatzführerscheins kann eine Befragung über den Gesundheitszustand nur dann zulässig sein, wenn die Behörde im Einzelfall konkreten Anlaß hat, an der gesundheitlichen Eignung des Führerscheininhabers zu zweifeln.

14. Weitere Probleme in der Verwaltung

14.1. Maschinenlesbarer Personalausweis

Im Berichtszeitraum habe ich gegenüber dem Bayer. Staatsministerium des Innern eine Stellungnahme zum Entwurf eines 5. Gesetzes zur Änderung des Gesetzes über Personalausweise abgegeben. Dabei war festzustellen, daß der Gesetzentwurf datenschutzrechtlichen Anforderungen in erfreulichem Maße Rechnung trug, wie etwa durch Einführung eines grundsätzlichen Protokollierungsverbotes, durch Festlegung des Zweck des Personalausweisregisters im Gesetz selbst und Schaffung einer bereichsspezifischen Übermittlungsregelung mit Festlegung des Umfangs der Verwendungsverbote im privaten Bereich. Einem datenschutzrechtlichen Anliegen entsprach es auch, die Entscheidung für die Maschinenlesbarkeit im Gesetz selbst zum Ausdruck zu bringen und den Inhalt der automatischen Lesezone gesetzlich festzulegen, wie dies der Entwurf vorsah. Aus meiner Stellungnahme, die auch Anregungen zu einzelnen Punkten des Gesetzentwurfs enthielt, seien die beiden folgenden Punkte hervorgehoben:

- Im Hinblick auf das durch eine zwangsweise automatisierte Datenerhebung beim Bürger berührte Recht auf informationelle Selbstbestimmung habe ich die Ansicht vertreten, daß der Gesetzgeber, wenn er sich nach Abwägung aller Umstände für die Maschinenlesbarkeit des Ausweises entscheidet, die hierfür maßgeblichen wesentlichen Gründe und die mit der Maschinenlesbarkeit verfolgten Ziele und Zwecke darlegen muß. Die im allgemeinen Teil der Gesetzesbegründung hierzu gegebene knappe Erläuterung, „ein moderner Ausweis sollte auch maschinell lesbar sein, um die gesetzlich vorgesehenen Kontrollen zu erleichtern und Eingabefehler auszuschließen", hielt ich nicht für ausreichend. Sie wird weder der Bedeutung und dem verfassungsrechtlichen Rang dieser Problematik gerecht noch der großen Anteilnahme, die die kontroverse Diskussion in einer breiten Öffentlichkeit gefunden hatte. Schließlich halte ich auch die für den Laien bestehende Undurchschaubarkeit automatisierter Datenverarbeitungsprozesse und eine daraus resultierende Verunsicherung staatstreuer Bürger für einen Faktor, dem der Gesetzgeber nicht zuletzt durch Bemühen um Vertrauen durch Begründung und Aufklärung Rechnung tragen sollte (vergl. auch die entsprechenden Ausführungen des Bundesverfassungerichts in der Entscheidung zum Volkszählungsgesetz 1983).

– Die Einführung eines maschinenlesbaren Ausweises macht flankierende Maßnahmen im Sicherheitsbereich erforderlich: Das bedeutet, daß die Schaffung bereichsspezifischer Regelungen für die Verarbeitung der mit Hilfe des Personalausweises erhobenen Daten bei den Sicherheitsbehörden vorangetrieben werden muß. Erst diese Gesetzentwürfe lassen eine endgültige datenschutzrechtliche Gesamtbewertung der Nutzung des maschinenlesbaren Personalausweises und der Folgen dieser Nutzung zu.

In diesem Zusammenhang verweise ich auch auf Ausführungen zur Reform des Strafprozeßrechts sowie zur Schleppnetzfahndung (in diesem Tätigkeitsbericht unter Nr. 6.2 und 6.8).

14.2. Nutzung von Daten aus Gewerbeanmeldungen durch Industrie- und Handelskammern

Wie schon im 7. Tätigkeitsbericht (unter Nr. 8.12, S. 43) weise ich darauf hin, daß die Weitergabe von Daten von Gewerbetreibenden aus der Gewerbekartei – es handelt sich (im Sinne des Volkszählungsurteils des BVerfG) um „zwangsweise" erhobene Daten – baldmöglichst einer angemessenen gesetzlichen Regelung bedarf. Die bisherige Praxis der Datenübermittlung ohne eine entsprechende gesetzliche Zulassung der Datenübermittlungen – für andere Zwecke – bleibt daher zunächst problematisch.

So habe ich die Arbeitsgemeinschaft der Bayerischen Industrie- und Handelskammern darauf hingewiesen, daß die Weitergabe von Daten, die ursprünglich „zwangsweise" im Wege der Gewerbeanmeldung erhoben worden waren, durch die Industrie- und Handelskammern an Dritte zur Förderung des Wirtschaftsverkehrs so bald als möglich bereichsspezifisch gesetzlich zu regeln ist.

Bei der Anmeldung eines Gewerbes wird auf dem Formular des Gewerbeamtes die Zustimmung des Anmeldenden zu einer Übermittlung der Gewerbeanschrift zu Werbezwekken ausdrücklich abgefragt. Die Betroffenen können sich mithin für oder gegen eine Verwendung ihrer Daten – durch das Gewerbeamt – zu Werbezwecken erklären. Sie werden deshalb davon ausgehen, daß zumindest die Gewerbebehörde Daten nicht übermittelt, wenn die Zustimmung versagt wurde. Nach Auskunft der Landeshauptstadt München stimmen etwa 90 % der Anmelder einer Weitergabe zu Werbezwecken auf dem Anmeldungsformular nicht zu.

Gleichwohl gehen die Arbeitsgemeinschaft der Industrie- und Handelskammern und das Staatsministerium für Wirtschaft und Verkehr bisher davon aus, daß die Kammermitglieder eine entsprechende Zurückhaltung der Industrie- und Handelskammer im Umgang mit Daten, die die Industrie- und Handelskammer von den Gewerbeämtern aus den Gewerbeanmeldungen erhalten hat, nicht erwarten. Es besteht dort vielmehr die Überzeugung, daß die Kammermitglieder mit einer Weitergabe der Angaben „Firma" oder „Name", „Adresse", „Branchenzugehörigkeit" oder „Produktpalette", eventuell „Größenklasse nach Mitarbeiterzahl" zur Förderung des Wirtschaftsverkehrs einverstanden sind. Begründet wird dies damit, daß die Kammern aufgrund ihrer Fachkunde und aufgrund der Kenntnis der Interessen ihrer Mitglieder bei der Datenweitergabe nicht schematisch handeln müßten, sondern differenziert im Interesse der Betroffenen verfahren könnten. Neue Kammermitglieder würden über diese Verfahrensweise in einem Begrüßungsschreiben unterrichtet. Altmitglieder sollen nach der Zusicherung der Arbeitsgemeinschaft zuverlässig und umfassend informiert werden, so daß Erkenntnisse darüber gewonnen werden können, ob durch eine Datenweitergabe schutzwürdige Belange beeinträchtigt würden.

Eine solche Verwendung von Daten der Kammern, die aus den Gewerbeanmeldungen stammen, läßt sich meines Erachtens nur noch vorübergehend auf Erwägungen im Rahmen der Vorschrift des Art. 18 Abs. 1 (2. Alternative) BayDSG stützen – auch wenn eine zuverlässige Information aller Mitglieder der Industrie- und Handelskammer sichergestellt wird.

Die Daten, die im Wege der Gewerbeanmeldung erhoben und der Industrie- und Handelskammer übermittelt werden, sind – wie eingangs erwähnt – rechtlich als „zwangsweise erhobene" personenbezogene Daten anzusehen. Ihre Weitergabe, sowohl von der Gewerbebehörde an die Industrie- und Handelskammer als auch die weitere Verarbeitung dieser Daten durch die Industrie- und Handelskammer, enthält jeweils eine Zweckänderung gegenüber dem „gewerbepolizeilichen" Erhebungszweck derGewerbebehörde. Sollte die erforderliche gesetzliche Regelung nicht in absehbarer Zeit ergehen, müßte für die Zeit nach Ablauf des „Übergangsbonus" (im Sinne der Rechtsprechung des Bundesverfassungsgerichts) wohl doch an eine Einwilligungslösung auch für die Altfälle gedacht werden. Ich habe daher den Industrie- und Handelskammern empfohlen, sich für eine baldige (bundes-)gesetzliche Regelung über den Umgang mit den Daten der Gewerbeanmeldungen einzusetzen.

14.3. Übermittlung personenbezogener Daten an eine politische Partei

Der Kreisverband einer politischen Partei erbat von einem Landratsamt „aus gegebenen Anlaß" eine für dienstliche Zwecke erstellte Liste aller Betriebe, bei denen in erheblichem Umfang mit gefährlichen Abfällen zu rechnen ist.

In der vom Landratsamt erbetenen Stellungnahme habe ich zunächst auf die Beschränkung des Datenschutzes auf natürliche Personen hingewiesen. Soweit allerdings deren Daten (in Dateien) verarbeitet würden, wäre eine Datenübermittlung durch das Landratsamt nach Art. 18 BayDSG – Übermittlung an nichtöffentliche Stellen – zu beurteilen. Voraussetzung für die Zulässigkeit der Übermittlung war damit, daß die Übermittlung zur Erfüllung der Aufgaben des Landratsamt erforderlich gewesen wäre – was nicht der Fall war – oder daß die Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht hätten und durch die erbetene Übermittlung schutzwürdige Belange der betroffenen natürlichen Personen nicht beeinträchtigt worden wären. Meines Erachtens fehlte es in diesem Falle bereits an der Glaubhaftmachung berechtigter Interessen, da der Vortrag „aus gegebenen Anlaß" den Anforderungen nicht entspricht.

Darüber hinaus muß seit dem Erlaß des Volkszählungsurteils des Bundesverfassungsgerichts berücksichtigt werden, daß die Daten vom Landratsamt „zwangsweise" zum Zwecke staatlicher Überwachung der Abfallbeseitigung erhoben worden waren. Die Verpflichtung zur Offenbarung persönlicher Daten stellt nach dem Urteil des Bundesverfassungsgerichts eine Beschränkung des informationellen Selbstbestimmungsrechts dar. Das Gericht hat in seinem Urteil ausgeführt, daß Beschränkungen dieses Rechts nach

Art. 2 Abs. 1 des Grundgesetzes einer (verfassungsmäßigen) gesetzlichen Grundlage bedürfen. Die Verwendung zwangsweise erhobener Daten ist danach auf den gesetzlich bestimmten Zweck begrenzt. Eine unverhältnismäßige Zweckänderung, die mit einer Datenübermittlung möglicherweise verbunden wäre, würde im Hinblick auf das informationelle Selbstbestimmungsrecht eine unzulässige Datenübermittlung darstellen. Im Rahmen der Beurteilung nach Art. 18 Abs. 1, 2. Alternative BayDSG, ob schutzwürdige Belange der Betroffenen durch die gewünschte Datenweitergabe beeinträchtigt werden, sind die vorstehenden Überlegungen zu berücksichtigen.

Nach Art. 18 Abs. 1 BayDSG muß eine Abwägung zwischen den berechtigten Interessen an der Kenntnis der Daten und den durch die Übermittlung beeinträchtigten schutzwürdigen Belangen vorgenommen werden. Je schwerwiegender das berechtigte Interesse ist, um so höherwertig müssen schutzwürdige Belange sein, wenn ihre Beeinträchtigung eine Datenübermittlung verhindern soll. Kann der Datenempfänger dagegen nur geringere berechtigte Interessen an der Kenntnis von Daten geltend machen, genügt bereits die Beeinträchtigung geringer schutzwürdiger Belange.

Für den Betroffenen kann die Offenbarung der erbetenen Daten zu einer erheblichen Beeinträchtigung seiner schutzwürdigen Belange führen. Diese kann bereits darin liegen, daß er weder Kenntnis davon noch Einfluß darauf hat, in welcher Weise die erlangten Daten über seine Person weiter verwendet werden. (Das Bundesverfassungsgericht hat im Volkszählungsurteil u. a. die Notwendigkeit betont, daß der Betroffene wissen muß, „wer was bei welcher Gelegenheit über ihn weiß".) Dies gilt jedenfalls für personenbezogene Daten, die den Behörden zum Vollzug ihrer gesetzlich übertragenen Aufgaben anvertraut wurden.

14.4. „Anonyme" Erhebung von Strukturdaten

Mit der datenschutzgerechten Erhebung von Strukturdaten für eine Studie hatte die Regionalplanungsstelle einer bayerischen Bezirksregierung Probleme: Die Regionalplanungsstelle hielt die Daten für nicht personenbezogen, da sie den Namen weggelassen hatte. Personenbezogene Daten sind jedoch auch solche, die sich auf eine namentlich nicht genannte, jedoch bestimmbare Person beziehen lassen. Im Erhebungsbogen fehlte der nach Art. 16 Abs. 2 BayDSG vorgeschriebene Hinweis auf die Freiwilligkeit der Angaben. Der Hinweis auf der Rückseite des Erhebungsbogens, daß die Erhebung selbstverständlich anonym erfolge, war nicht zutreffend und letztlich irreführend. In mehreren Gesprächen wurde eine datenschutzgerechte Abwicklung erreicht.

14.5. Übertragung der Kassengeschäfte eines Landratsamts auf die Kreissparkasse

Ein Landratsamt unterrichtete mich von der Absicht, seine Bar-Kassen-Geschäfte künftig durch die Kreissparkasse abwickeln zu lassen. Ineinem Vorgespräch erhob ich datenschutzrechtliche Bedenken dagegen, daß das Sparkassenpersonal künftig bei allen Ein- und Auszahlungen sowohl vom Namen des Einzahlers/Empfängers, als auch vom Zahlungsgrund Kenntnis erhalten würde. Ich bat das Bayerische Staatsministerium des Innern, im Rahmen des nach Art. 87 Abs. 1 der Landkreisordnung vorgesehenen Genehmigungsverfahrens einen Weg zu finden, Ein- und Auszahlungen möglichst ohne Bekanntgabe von Namen und Zahlungsgrund abzuwickeln. Dem Betroffenen sollte m. E. ermöglicht werden, entsprechende Einzahlungen unmittelbar bei seiner Hausbank (also nicht bei der Kreissparkasse) zu leisten. Falls eine Bekanntgabe des Zahlungsgrundes gegenüber dem Sparkassenpersonal dadurch im Ergebnis nicht ausgeschlossen werden könne, sollte ein Betroffener, der im Einzelfall darauf bestände, Einzahlungen auch unmittelbar bei der Kreiskasse, also nicht bei der Kreissparkasse, leisten können. Unter Beachtung von § 56 KommHV und Nr. 3 VollzBekBayDSG sollte Vorsorge gegen eventuell problematische Nutzungen personenbezogener Ein- bzw. Auszahlungs-Daten durch die beauftragte Kreissparkasse getroffen werden.

15. Neue Medien

Unter dem Schlagwort „Neue Medien" behandle ich, wie schon in den vergangenen Jahren, die Themen Bildschirmtext (Btx), Medienerprobungs- und -entwicklungsgesetz (MEG) und die Fernwirkdienste. Stärker in das Blickfeld getreten ist die Telekommunikationsordnung (TKO). Die Deutsche Bundespost möchte mit dieser Rechtsverordnung eine Reihe von bisher bestehenden Verordnungen für den Fernmeldeverkehr ablösen und die Grundlage für die Einführung neuer Telekommunikationsdienste schaffen. In diesem Bereich geht die Entwicklung derzeit besonders stürmisch voran. Die neuen Telekommunikationsdienste werden in Verbindung mit der elektronischen Datenverarbeitung die Entwicklung zum „elektronischen Büro" fördern und möglicherweise die technischen Voraussetzungen für eine Zunahme der häuslichen Telearbeit schaffen.

15.1. Bildschirmtext

Zur Lage

Nach wie vor gilt, daß sich die Zahlen der Bildschirmtext-Teilnehmer nicht so entwickelt haben, wie dies die Deutsche Bundespost zunächst erwartet hatte. Inzwischen beträgt die Zahl der Teilnehmer in der Bundesrepublik Deutschland etwa 50.000; die Zahlen für Bayern liegen mir nicht vor. 192 externe Rechner sind am System angeschlossen. Die Angebote von ca. 3.800 Anbietern können abgerufen werden. Aus datenschutzrechtlicher Sicht besonders interessant ist die Zahl der auf über 1 Million angewachsenen Verbindungsaufnahmen im Btx-System.

Die Bundespost hat mit Wirkung zum 1.Juli 1986 eine Reihe von Systemverbesserungen eingeführt, die ich bereits im 7. Tätigkeitsbericht kurz angesprochen hatte.

Die landesrechtlichen Regelungen zu Bildschirmtext sind unverändert geblieben. Die Deutsche Bundespost hat in den Entwurf der Telekommunikationsordnung auch Regelungen zu Bildschirmtext aufgenommen (siehe unten).

Probleme der Umsetzung der Datenschutzregelung im Staatsvertrag durch die Deutsche Bundespost

Im letzten Tätigkeitsbericht hatte ich darauf hingewiesen, daß die Deutsche Bundespost mit den in die Fernmeldeordnung aufgenommenen Regelungen zu Bildschirmtext dem in Art. 9 Bildschirmtextstaatsvertrag erreichten Standard nicht entsprochen hat. Weiter habe ich in diesem Zusammenhang gerügt, daß die einzelnen für Bildschirmtext geltenden datenschutzrechtlichen Bestimmungen in der Fernmeldeordnung verstreut und nur schwer auffindbar sind

und somit nicht den vom Bundesverfassungsgericht erhobenen Geboten der Normenklarheit und Transparenz entsprechen.

Der letzteren Forderung ist die Deutsche Bundespost mit der Vorlage eines Entwurfs zur Telekommunikationsordnung für Bildschirmtext weitgehend nachgekommen. Der Bildschirmtextdienst wird in einem eigenen Unterabschnitt geregelt. Außerdem besteht für Datenschutz im Bildschirmtextdienst neben den allgemeinen Datenschutzvorschriften noch eine eigene bereichsspezifische Bestimmung. Damit hat die Deutsche Bundespost wesentlichen Forderungen entsprochen. Allerdings bleiben auch die in der TKO vorgesehenen Regelungen teilweise noch hinter Art. 9 Bildschirmtext-Staatsvertrag zurück; insoweit verweise ich auf den Punkt „Telekommunikation".

Weitere Datenschutzfragen

Amtliche Teilnehmerverzeichnisse über Bildschirmtext

Die Fernsprechteilnehmer, deren Telefonnummern und Anschriften bislang aus einer Vielzahl von örtlichen Fernsprechbüchern zu entnehmen waren, sollen künftig bundesweit über Bildschirmtext abfragbar sein. Derzeit sind nur einzelne Ortsnetze probeweise in Btx. Wegen einer Reihe von Bürgerfragen zur datenschutzrechtlichen Relevanz sei hierzu kurz folgendes bemerkt:

Die Deutsche Bundespost erstellt als Hilfsmittel für den Fernsprech-, Bildschirmtext- und Datex-Dienst amtliche Teilnehmerverzeichnisse, in die grundsätzlich alle Teilnehmer von Amts wegen mit ihrem Namen und – soweit erforderlich – weiteren Angaben eingetragen werden. Die Deutsche Bundespost ist berechtigt, die genannten Verzeichnisse allen Betroffenen, aber auch Dritten zugänglich zu machen. Diese Befugnis schließt grundsätzlich die Befugnis zur Übermittlung der Verzeichnisse an die Deutsche Postreklame GmbH oder sonstige private Unternehmungen, sowie die Befugnis zur Bereitstellung der Verzeichnisse im Btx-System – entweder als Teil eines eigenen Anbieterprogrammes oder innerhalb des vorgeschalteten Netzträgerbereiches – ein. Die Deutsche Postreklame GmbH kann schließlich den privaten Empfängern ihrer Teilnehmerverzeichnisse das Recht einräumen, die Verzeichnisse ihrerseits im Rahmen von Btx-Programmen kommerziell zu verwerten, soweit diese Verwertung datenschutzrechtlich zulässig ist. Derzeit können über Bildschirmtext Teilnehmer der Ortsnetze Berlin, Hamburg und München abgerufen werden.

Die Frage nach der datenschutzrechtlichen Zulässigkeit eines auf diese Weise entstehenden zentralen Telefonbuches auf Bildschirmtext ist im Hinblick auf eine mögliche Beeinträchtigung schutzwürdiger Belange der gespeicherten Telefonteilnehmer zu beantworten.

So bietet das Telefonkundenverzeichnis über Bildschirmtext die Möglichkeit, weitaus einfacher als bisher einen Fernsprechteilnehmer ausfindig zu machen. So könnte z. B. auch ein Telefonteilnehmer relativ einfach gefunden werden, der umgezogen ist, solange er im Nahbereich des bisherigen Wohnortes verblieben ist. Dies kann im Normalfall durchaus vorteilhaft sein, kann allerdings im Einzelfall auch Nachteile für den Betroffenen bringen. Dies kann insbesondere dann geschehen, wenn beispielsweise ein von einem Inkassobüro gesuchter Schuldner umgezogen ist und nun die Suche auf eine mit dem Schuldner namensgleiche Person fällt, die im Nahbereich des bisherigen Wohnsitzes des gesuchten Schuldners wohnt. Dieser Unbeteiligte kann auf diese Weise zum Ziel von Mahnbescheiden und Vollstrekkungsversuchen werden (vgl. 7. Tätigkeitsbericht „Ich habe nichts zu verbergen"). Das Risiko, daß ein Unbeteiligter verwechselt wird und mit Nachteilen zu rechnen hat steigt, wenn dieses über Bildschirmtext geführte Telefonverzeichnis als eine Art Einwohnermeldesystem benutzt wird.

Datenschutzkontrolle

Nach Art. 1 Abs. 2 Ausführungsgesetz zum Bildschirmtext-Staatsvertrag ist die Überwachung der Einhaltung der Datenschutzvorschriften des Bildschirmtext-Staatsvertrages bei öffentlichen Stellen dem Landesbeauftragten für den Datenschutz zugewiesen. Meine stichprobenartigen Kontrollen im Berichtszeitraum haben zu keiner Beantstandung geführt. Auch aus dem privaten Bereich sind mir von den hierfür zuständigen Regierungen keine wesentlichen Datenschutzprobleme über Bildschirmtext mitgeteilt worden.

15.2. Medienerprobungs- und -entwicklungsgesetz (MEG)

Im Berichtszeitraum standen weniger Datenschutzfragen als verfassungsrechtliche Probleme im Mittelpunkt der Diskussion um das Medienerprobungs- und -entwicklungsgesetz. Aus der Sicht des Datenschutzes geht es zunächst auch nicht darum, neue und weitergehende Datenschutzvorschriften zu fordern, sondern um die Umsetzung der bestehenden Datenschutzvorschriften in der Praxis.

15.2.1. Wissenschaftliche Begleitforschung

Die wissenschaftliche Begleitung der Nutzung und Akzeptanz der neuen Medien ist im Medienerprobungs- und -entwicklungsgesetz ausdrücklich vorgesehen. Im Berichtszeitraum hatte ich deshalb auch wieder Gelegenheit, zu einem Vorhaben der Kommunkationsforschung Stellung zu nehmen. Gegen die hierzu vorgesehene Übermittlung der Adressen von 600 Teilnehmern am Pilotprojekt durch die Münchner Pilotgesellschaft für Kabelkommunikation an das Forschungsinstitut zum Zwecke der Durchführung der Hauptuntersuchung hatte ich keine datenschutzrechtlichen Bedenken. Die Zulässigkeit einer solchen Übermittlung folgt grundsätzlich aus Art. 19 Abs. 1 MEG, wonach personenbezogene Daten der Teilnehmer verarbeitet werden können, soweit diese für Zwecke der wissenschaftlichen Begleitforschung im Rahmen des Gesetzes erforderlich sind. Bei dieser Bewertung war auch zu berücksichtigen, daß die Auswertung einer bevölkerungsrepräsentativen Stichprobe eine differenzierte und verallgemeinerungsfähige Aussage zum Untersuchungsgegenstand nicht zugelassen hätte. Allerdings habe ich darauf hingewiesen, daß die Daten möglichst frühzeitig nach Durchführung der Erhebung zu löschen sind und die Befragung durch das Forschungsinstitut ausschließlich auf freiwilliger Grundlage erfolgt. Das Forschungsinstitut hat zugesagt, die Fragebögen unmittelbar nach ihrem Eingang so zu anonymisieren, daß auch später über die Listennummern keine Rückschlüsse auf die Testpersonen gezogen werden können.

Bei Durchsicht der Fragebogen bin ich freilich auf problematische Fragen gestoßen. Es fanden sich beispielsweise Fragen nach der regelmäßigen Teilnahme der Testpersonen an kirchlichen Veranstaltungen, nach den Mitgliedschaften

in Parteien, Gewerkschaften, Bürgerinitiativen, nach Alter und Namen ihrer Kinder sowie nach Alter und ausgeübtem Beruf der Testpersonen. Auch Fragen nach der Mitgliedschaft in einer Religionsgemeinschaft oder nach etwaigen Behinderungen sind aus der Sicht des Datenschutzes nicht unbedenklich. Die Beantwortung dieser in Verbindung mit anderen Fragen könnte in unglücklich gelagerten Fällen, vor allem in der Zusammenschau, zum Entstehen von Persönlichkeitsprofilen einzelner Betroffener führen, die ein Wiedererkennen auch nach erfolgter Anonymisierung ermöglichen können. Diese Bedenken gelten um so mehr, als der Kreis der in Betracht kommenden Testpersonen als Teilnehmer des Kabelpilotprojekts München verhältnismäßig eng begrenzt ist. Ich habe deshalb angeregt, einige besonders sensible Fragen zu streichen. Bei anderen Problemfragen habe ich es als ausreichend angesehen, wenn die Testpersonen hier jeweils noch einmal deutlich auf die Freiwilligkeit ihrer Antwort hingewiesen werden.

Im Berichtszeitraum ist mir außerdem das Ergebnis der Untersuchung über die „Nutzung und Akzeptanz der in München und umliegenden Landkreisen empfangbaren Hörfunkprogramme", verbunden mit einer Abhandlung des für die Kommunikationsforschung zuständigen Mitglieds der Projektkommission, vorgelegt worden. Bei einer Durchsicht habe ich keine Anhaltspunkte dafür feststellen können, daß etwa die Anonymisierungspflicht der personenbezogenen Daten nicht beachtet worden wäre oder tatsächlich einfache Deanonymisierungsmöglichkeiten bestehen würden.

15.2.2. Datenschutzfragen in der Praxis

15.2.2.1. Private Satelliten-Empfangsanlagen

In Bayern sind derzeit mehr als 50 Satelliten-Empfangsanlagen in Betrieb. Nach Auskunft der Bayer. Landeszentrale für neue Medien liegen Anträge auf Genehmigung von mindestens weiteren 50 derartigen Anlagen bei der Deutschen Bundespost. Die Betreiber solcher Anlagen haben vor Aufnahme des Betriebes bei der Deutschen Bundespost eine **fernmelderechtliche** Genehmigung einzuholen. Daneben bedarf der Betreiber aber zusätzlich einer **rundfunkrechtlichen** Genehmigung bzw. Unbedenklichkeitsbescheinigung, die von der Bayer. Landeszentrale für neue Medien zu erteilen ist. Die Bayer. Landeszentrale für neue Medien hat in letzter Zeit festgestellt, daß private Satelliten-Empfangsanlagen zwar mit fernmelderechtlicher Genehmigung in Betrieb genommen worden sind, sie hiervon jedoch keine Kenntnis hatte und dementsprechend auch keine rundfunkrechtliche Genehmigung/Unbedenklichkeitsbescheinigung erteilen konnte. Damit die Bayer. Landeszentrale für neue Medien die für ihre Aufgaben notwendigen Angaben über die Inbetriebnahme von Satelliten-Empfangsanlagen erhält, hat sie mit der Deutschen Bundespost vereinbart, daß diese im Auftrag der Bayer. Landeszentrale für neue Medien den Betreibern ein Antragsformular auf rundfunkrechtliche Genehmigung aushändigt und außerdem eine Abschrift der fernmelderechtlichen Genehmigung der Bayer. Landeszentrale für neue Medien übermittelt.

Aus der Sicht des Datenschutzes sind bei dieser beabsichtigten Verfahrensweise zwei Abschnitte zu unterscheiden: Zum einen ist die Verteilung der Formblätter durch die Deutsche Bundespost und die anschließende Entgegenahme der ausgefüllten Formblätter durch die Bayer. Landeszentrale für neue Medien eine arbeitsteilige Form der Datenerhebung. Zum anderen stellt die Übersendung der fernmelderechtlichen Genehmigungsurkunde der Deutschen Bundespost an die Bayer. Landeszentrale für neue Medien eine Datenübermittlung dar. Die vorgesehene Datenerhebung mittels Formblattes für die rundfunkrechtliche Genehmigung ist aus datenschutzrechtlicher Sicht zulässig, soweit sie für die Erfüllung von Aufgaben der Bayer. Landeszentrale für neue Medien erforderlich ist:

Nach Art. 35 Abs. 2 Satz 2 MEG hat die Bayer. Landeszentrale für neue Medien die Genehmigung für die Weiterverbreitung von Rundfunkprogrammen zu erteilen, wenn die Rundfunkprogramme nicht ortsüblich empfangbar sind und in Kabelanlagen mit 100 oder mehr angeschlossenen Wohneinheiten verbreitet werden sollen. Die Einspeisung der über Satellit empfangenen Programme in eine Gemeinschaftsanlage wird als Weiterverbreitung im Sinne des Art. 35 MEG gesehen. Die Bayer. Landeszentrale für neue Medien prüft auch in den Fällen, in denen die Weiterverbreitung in Kabelanlagen mit weniger als 100 angeschlossenen Wohneinheiten erfolgt, ob die Einspeisung den gesetzlichen Voraussetzungen (Art. 3 und Art. 4 MEG) entspricht und erteilt ggf. Unbedenklichkeitsbescheinigungen. Kabelanlagen mit weniger als 100 angeschlossenen Wohneinheiten sind zwar von der Genehmigungspflicht, nicht jedoch von deren materiellen Voraussetzungen ausgenommen. Im Hinblick auf diese Aufgaben der Bayer. Landeszentrale für neue Medien habe ich aus datenschutzrechtlicher Sicht gegen die vorgesehene Datenerhebung keine Bedenken. Anders habe ich den Sachverhalt allerdings beurteilt, wenn der Betreiber einer Satellitenempfangsanlage diese ausschließlich für seinen eigenen Empfang benutzen will (sogenannte Individualanlage). In diesem Fall liegt keine Weiterverbreitung von Rundfunkprogrammen vor und damit besteht meines Erachtens für die Bayer. Landeszentrale für neue Medien kein Anlaß für rundfunkrechtliche Entscheidungen.

15.2.2.2. Signallieferungsverträge

Die Deutsche Bundespost hat mit einer Reihe von privaten Kabelanlagenbetreibern sogenannte Signallieferungsverträge in Bayern abgeschlossen. In diesen Fällen wird die private Kabelanlage nicht durch eine private Satelliten-Empfangsanlage, sondern durch eine postalische Satelliten-Empfangsanlage mit den Satelliten-Programmen versorgt. Die Deutsche Bundespost schließt solche Signallieferungsverträge nur für private Kabelanlagen ab einer Größe von 2.000 Wohneinheiten ab. Die aufgestellten Satelliten-Empfangsanlagen dienen ausschließlich der Versorgung dieser Anlage. Nach Auffassung der Bayer. Landeszentrale für neue Medien bedarf es hierzu deren rundfunkrechtlicher Genehmigung, weil in diesen Satelliten-Empfangsanlagen grundsätzlich eine kanalselektive Aufbereitung jedes Satelliten-Programms erfolgt und über 100 Wohneinheiten an der privaten Kabelanlage angeschlossen sind. Zur rundfunkrechtlichen Prüfung und ggf. Erteilung einer rundfunkrechtlichen Genehmigung ist die Landeszentrale an der Anschrift des privaten Netzbetreibers interessiert. In meiner gutachtlichen Stellungnahme an die Landeszentrale für neue Medien zu einer eventuellen Anforderung der entsprechenden Betreiberdaten bei der Deutschen Bundespost habe ich geraten, bei den Betreibern, soweit diese nicht juristische Personen sind, eine Einwilligung für diese Datenübermittlung einzuholen. Ich habe im übrigen aber keine

Zweifel, daß die Bayer. Landeszentrale für neue Medien in diesen Fällen zur Erteilung der gesetzlich verlangten rundfunkrechtlichen Genehmigung die entsprechenden Betreiberdaten von der Deutschen Bundespost benötigt.

Ich begrüße es in diesem Zusammenhang, daß mich die Bayer. Landeszentrale für neue Medien zu diesen Fragen der Datenerhebung und Datenübermittlung um gutachtliche Stellungnahmen bittet und mir somit die Möglichkeit eröffnet, frühzeitig datenschutzrechtliche Überlegungen einzubringen. In einer solchen datenschutzrechtlichen Beratung bayerischer Behörden habe ich immer schon ein wichtiges Aufgabenfeld im Rahmen meiner Tätigkeiten nach Art. 28 BayDSG gesehen. Gerade die rechtzeitige und umfassende Beratung kann eventuelle Verstöße gegen Datenschutzvorschriften verhindern und einen sachgerechten Vollzug fördern. Sofern bayerische Behörden, wie die Bayer. Landeszentrale für neue Medien, die sich bezüglich Fragen der Verarbeitung personenbezogener Daten in Verhandlungen mit Bundesbehörden befinden, mich um Stellungnahmen bitten, sehe ich es als selbstverständlich an, mich zur Abklärung sämtlicher Datenschutzvorgänge auch gutachtlich zu einer von einer bayerischen Behörde gewünschten Datenübermittlung von einer Bundesbehörde zu äußern.

15.2.3. Rahmenübereinkommen zwischen der Deutschen Bundespost und der Bayer. Landeszentrale für neue Medien

Die Bayer. Landeszentrale für neue Medien und die Deutsche Bundespost haben ein sogenanntes Rahmenüberkommen getroffen, das die Einspeisung von Rundfunkprogrammen in die Breitbandkabelnetze und die Gemeinschaftantennenanlagen regelt. In diesem Übereinkommen sind auch Datenübermittlungen von Kabelgesellschaften an die Deutsche Bundespost und von der Deutschen Bundespost an Kabelgesellschaften vorgesehen. Von verschiedenen Seiten bin ich zur datenschutzrechtlichen Prüfung aufgefordert worden.

Soweit die Kabelgesellschaften im Rahmen der Begründung von rundfunkrechtlichen Teilnehmerverhältnissen mit den Teilnehmern gleichzeitig im Auftrag für die Deutsche Bundespost auch fernmelderechtliche Teilnehmerverhältnisse begründen, werden die Kabelgesellschaften im Auftrag der Deutschen Bundespost tätig. Die Weitergabe dieser im Auftrag für die Deutsche Bundespost gewonnenen Vertragsdaten an diese ist datenschutzrechtlich grundsätzlich zulässig.

Bei der Frage nach der datenschutzrechtlichen Zulässigkeit der Übermittlung personenbezogener Daten von der Deutschen Bundespost an die Kabelgesellschaften ist zwischen den Teilnehmern zu unterscheiden, mit denen die Deutsche Bundespost erst nach Inkrafttreten des Rahmenübereinkommens ein fernmelderechtliches Teilnehmerverhältnis begründet und den Teilnehmern, die bereits an das Breitbandkabelnetz (BK-Netz) der Deutschen Bundespost angeschlossen sind:

Soweit sich die Deutsche Bundespost bei neu an das BK-Netz anzuschließenden Teilnehmern nach dem Rahmenübereinkommen bereiterklärt, gleichzeitig mit der Begründung des fernmelderechtlichen Teilnehmerverhältnisses im Namen und Auftrag der Kabelgesellschaften die rundfunkrechtlichen Teilnehmerverträge mit den Teilnehmern zu schließen, ist eine Übermittlung dieser so gewonnenen Daten an die Kabelgesellschaften grundsätzlich zulässig.

Hinsichtlich der bereits an das BK-Netz der Deutschen Bundespost angeschlossenen Teilnehmer ist folgendes zu berücksichtigen: Verzichten Teilnehmer ausdrücklich auf den Empfang des sogenannten Zusatzpaketes, also der Programme, die über die ortüblichen empfangbaren Programme hinaus in das Breitbandkabelnetz eingespeist werden, und lassen einen entsprechenden Filter einbauen, dann ist eine Datenübermittlung an die Kabelgesellschaften unzulässig, weil einbesonderes rundfunkrechtliches Teilnehmerverhältnis mit den Kabelgesellschaften gerade nicht begründet werden soll. Gleiches gilt grundsätzlich hinsichtlich der Teilnehmer, die noch nicht ausdrücklich zu einer Entscheidung über Empfang oder Nichtempfang des Zusatzpaketes aufgefordert worden sind. Keine Bedenken habe ich jedoch gegen eine Datenübermittlung hinsichtlich der Breitbandkabel-Anschlußinhaber, die das Zusatzpaket empfangen können und wollen, jedoch das insoweit notwendige rundfunkrechtliche Teilnehmerverhältnis wegen dessen Gebührenfolge nicht begründen wollen. Eine Rundfunkgebühr nicht zahlen zu wollen, ist kein schutzwürdiger Belang, der eine Datenübermittlung unzulässig machen würde.

15.2.4. Datenschutz bei Kabelgesellschaften

Nach Art. 19 Abs. 2 Satz 1 MEG ist dem Bayer. Landesbeauftragten für den Datenschutz auch die Einhaltung der Datenschutzbestimmungen bei den Kabelgesellschaften und den Betreibern von Kabelanlagen zugewiesen. Mit dieser von mir sehr begrüßten Vorschrift wird sichergestellt, daß unabhängig davon, ob im Rahmen des Medienerprobungs- und -entwicklungsgesetzes öffentliche oder private Stellen tätig sind, die Datenschutzkontrolle grundsätzlich in einer Hand liegt.

Bislang habe ich bei Kabelgesellschaften noch keine Prüfung durchgeführt, weil diese sich derzeit erst konstituieren. Ich habe mich um so mehr gefreut, daß sich zwischenzeitlich eine Kabelgesellschaft mit der Bitte um datenschutzrechtliche Stellungnahme an mich gewandt hat. Ich sehe darin ein Anzeichen, daß die Kabelgesellschaften an der Beachtung der datenschutzrechtlichen Bestimmungen des Medienerprobungs- und -entwicklungsgesetzes interessiert sind. Solche Anfragen geben mir im übrigen auch Anhaltspunkte über die im Vollzug dieses Gesetzes anfallenden datenschutzrechtlichen Fragestellungen. Deren Kenntnis ist eine der Voraussetzungen dafür, daß ich meinen Aufgaben als Überwachungsbehörde nachkommen kann. Zu der konkret gestellten Frage, ob die Kabelgesellschaften die Namen ihrer Programmanbieter an Dritte weitergeben dürfen, habe ich darauf hingewiesen, daß derartige Datenübermittlungen grundsätzlich nur mit Einwilligung der Programmanbieter oder zumindest nach Rücksprache mit diesen zulässig sein können.

Ich beabsichtige, im Laufe des nächsten Jahres bei einzelnen Kabelgesellschaften erste datenschutzrechtliche Überprüfungen vorzunehmen.

15.3. Telekommunikationsordnung (TKO)

Mit der Telekommunikationsordnung will die Deutsche Bundespost den rechtlichen Rahmen für die Fortentwicklung der bisherigen Fernmeldedienste schaffen. Um die Bedeutung der Telekommunikationsordnung einschätzen zu können, will ich im folgenden ganz kurz über die derzeitigen Pläne zur Fortentwicklung der Telekommunikationsdienste berichten:

Die Bundesrepublik Deutschland verfügt im internationalen Vergleich bereits heute über ein leistungsfähiges Nachrichtensystem. Dessen Infrastruktur besteht aus einem Fernsprechnetz mit Diensten wie Telefon, Telefax und Bildschirmtext sowie einem Fernschreib- und Datennetz mit den Diensten Telex, Teletex sowie Datex. Daneben bestehen Breitbandverteilnetze für die Fernsehübertragung beispielsweise in Städten oder Abschattungsgebieten und für die einzelnen Kabelpilotprojekte.

Für die nähere Zukunft plant die Deutsche Bundespost

- den Übergang von der Analog- zur Digitaltechnik beim Fernsprechnetz und
- das Zusammenführen der Einzelnetze zu einem einzigen integrierten Netz.

Beginnend ab Ende 1986 in einzelnen Pilotprojekten und ab 1988 im allgemeinen Angebot will die Deutsche Bundespost ISDN (Integrated Services Digital Network) einführen, das alle heute vorhandenen schmalbandigen Dienste der Sprach-, Text- und Datenkommunikation in einem digitalen Fernmeldenetz zusammenfaßt. ISDN wird auf dem heutigen Fernsprechnetz eingeführt. Dessen Übertragungskapazität soll dann 64 000 Bit/s betragen. Durch die Digitalisierung wird mit ISDN nicht nur eine Vereinfachung und Verbesserung der Informationsübertragung erreicht; ISDN soll daneben dem Teilnehmer erlauben, die Vielfalt von herkömmlichen und neuen Diensten über einen einzigen Teilnehmeranschluß zu benützen. Damit sind über ISDN die Dienste Fernsprechen, Datenübermittlung, Teletex, Telefax, Bildschirmtext, Bilddienste und Fernwirken zugänglich.

Aufbauend auf diesem schmalbandigen ISDN soll spätestens ab Ende der 80iger Jahre als weiterer Schritt das sogenannte „Breitband-ISDN" folgen. Neben den bereits genannten Vorteilen des Zugangs zu allen Diensten über einen einzigen Teilnehmeranschluß und die Vergabe einer einzigen Rufnummer für alle Dienste tritt beim Breitband-ISDN eine wesentliche Erhöhung der Übertragungskapzität hinzu. Diese soll bis zu 140 Millionen Bit/s erreichen. Damit können künftig mit ein- und demselben Endgerät über einen einzigen Anschluß gleichzeitig Schmal- und Breitbandkanäle benutzt werden.

Nach der derzeitigen Planung sollen in einem dritten Schritt auch die Rundfunkverteildienste einbezogen werden. Ziel ist also das „Integrierte Breitbandfernmeldenetz". Mit diesem auf der Verwendung von Glasfasern beruhenden Netz sollen künftig alle Massen- und Individualkommunikationsvorgänge abgewickelt werden. Wegen der unglaublichen Fülle der bei der Teilnahme an dieser Massen- und Individual-Kommunikation über eine einzige Anschlußstelle zwangsläufig anfallenden personenbezogenen Daten stellt diese Entwicklung eine Herausforderung für den Datenschutz dar.

Notwendigkeit einer gesetzlichen Regelung

Der Bundespostminister wird die Telekommunikationsordnung (TKO) in der Rechtsform einer Rechtsverordnung aufgrund § 14 des Postverwaltungsgesetzes erlassen. Gegen diesen beabsichtigten Erlaß der TKO als bloße Rechtsverordnung sind Bedenken anzumelden. In Anbetracht der Bedeutung, die der mit der TKO zu treffenden Entscheidung über die Struktur künftiger Telekommunikationsdienste zukommt, und der im einzelnen auf der Grundlage der TKO möglichen künftigen Diensteinführungsentscheidungen sind verfasssungsrechtlich Zweifel angebracht, ob die Verordnungsermächtigung aus § 14 Postverwaltungsgesetz für die Regelung solcher wesentliche Bereiche des öffentlichen Lebens bestimmender Sachverhalte noch als ausreichend anzusehen ist. Meines Erachtens muß der Gesetzgeber selbst derart wesentliche Entscheidungen treffen (vgl. BVerfGE 47, 46/79). Im übrigen ergeben sich auch Zweifel an der genannten Verordnungsermächtigung aus dem Wortlaut von § 14 Postverwaltungsgesetz selbst, der der Post eine Verordnungsermächtigung für das „Post- und Fernmeldewesen" zuweist. Ob hierunter auch die beabsichtigte weitgehende Entwicklung und Einführung völlig neuer Telekommunikationsdienste sowie die Verbindung von Datenübermittlung, Datenverarbeitung und Massenkommunikation zu verstehen ist, ist sehr fraglich.

M. E. ist daher eine neue, der Bedeutung der Entwicklung der Telekommunikationsdienste angemessene gesetzliche Verordnungsermächtigung für die Telekommunikationsordnung in Form eines Bundesgesetzes zu schaffen. Daneben sind auch die Länder aufgerufen, die zur Nutzung neuer Telekommunikationsdienste und die für die Einbeziehung der Rundfunkverteildienste in dieses Netz notwendigen landesgesetzlichen Regelungen zu erlassen. Erste Anhaltspunkte für entsprechende Datenschutzregelungen in den Landesgesetzen könnten der Bildschirmtext-Staatsvertrag und die entsprechenden Ausführungsgesetze der Länder sein.

Datenschutz und Telekommunikationsordnung

Aus der Sicht des Datenschutzes kommt dem Gebot der Normenklarheit wesentliche Bedeutung zu. Deshalb habe ich im Zusammenhang mit Bildschirmtext die Unübersichtlichkeit der Fernmeldeverordnung kritisiert. Die TKO soll die Benutzungsverordnungen zum Fernmeldewesen ablösen, nämlich die Fernmeldeordnung mit ihren zwischenzeitlich 29 Änderungsverordnungen, die Verordnung für den Fernschreib- und den Datex-Dienst, die Verordnung über das öffentliche Direktrufnetz und die Telegrammordnung. Mit dieser Zusammenfassung und der deutlichen Gliederungsstruktur der TKO wird die Transparenz des Fernmelderechts wesentlich verbessert.

Die TKO enthält außerdem einen eigenen Abschnitt zum Datenschutz, bei dessen Formulierung die Deutsche Bundespost in der letzten nun vorliegenden Fassung eine Reihe von Datenschutzforderungen berücksichtigt hat. Damit wird die Telekommunikationsordnung aus der Sicht des Datenschutzes eine wesentliche Verbesserung gegenüber dem bisherigen Stand des Fernmelderechts erreichen.

Trotz dieses aus der Sicht des Datenschutzes bereits sehr begrüßenswerten Entwicklungsstandes der Datenschutzregelungen in der TKO zeigt eine Prüfung unter Berücksichtigung der vom Bundesverfassungsgericht zum Volkszählungsgesetz entwickelten Vorgaben und anhand vergleichbarer, von den Ländern geschaffener Datenschutzregelungen (z.B. Art. 9 Bildschirmtext-Staatsvertrag, Art. 19, 31, 32, 33 MEG), daß die TKO die Datenschutzbelange noch nicht in allen Punkten ausreichend berücksichtigt. Schlagwortartig lassen sich einige dieser Problempunkte wie folgt darstellen:

- Das Gebot der Normenklarheit verlangt eine präzisere Umschreibung der öffentlichen Telekommunikationsdienste und eine klarere Definition der für die einzelnen Telekommunikationsdienste erforderlichen personenbezogenen Daten. Hierzu zählt auch eine übersichtlichere Definition der datenschutzrelevanten Grundbegriffe der Telekommunikationsdienste.
- Das Recht auf informationelle Selbstbestimmung setzt voraus, daß der Bürger im Wissen um Inhalt und Auswirkung der einzelnen Dienste seine Entscheidungen über die Teilnahme an diesen Diensten trifft. So sollte beispielsweise die vom Teilnehmer beantragbare „andere Art der Verarbeitung" von Verbindungsdaten, aus der Rückschlüsse über Zeit und Partner seiner Kommunikation möglich sind, genauer umschrieben werden. Unter diesem Gesichtspunkt ist auch der „Zwangseintrag" für die Teilnehmerverzeichnisse im Telefondienst zu überdenken.
- Der Grundsatz der Zweckbindung erfordert wohl eine Nutzungsbeschränkung der bei der Nutzung der einzelnen Kommunikationsdienste angefallenen personenbezogenen Daten. Deren Verwendung nicht nur für die Zwecke der tatsächlich jeweils in Anspruch genommenen Dienste, sondern allgemein zu „Telekommunikationszwecken" geht zu weit. Weiter erfordert dies einen Ausschluß der Verbindungsdaten von jeglicher Übermittlung.
- Um das Risiko bei der Nutzung neuer Telekommunikationsdienste für den Bürger so gering wie möglich zu halten, sind bereits in der Telekommunikationsordnung weitergehende technisch-organisatorische Maßnahmen vorzusehen; hierzu kann beispielsweise das Angebot eines Dienstes zur Verschlüsselung von Nachrichten gehören. Soweit durch technisch-organisatorische Maßnahmen nicht sämtliche Risiken beseitigt werden können, sollte die Bundespost zur entsprechenden Aufklärung verpflichtet werden.
- Schließlich sind die Datenschutzregelungen für Gebührendaten, den Umgang mit den Inhalten der Einzelkommunikationen, zur Vergleichszählung und zum Feststellen ankommender Wählverbindungen („Fangschaltung") noch nicht ausreichend.
- Auch der Datenschutz bei Bildschirmtext bleibt hinter der vergleichbaren Regelung im Bildschirmtext-Staatsvertrag zurück. Nach Art. 9 Abs. 3 Satz 1 Bildschirmtext-Staatsvertrag soll der exakte Zeitpunkt des Abrufes von Angeboten nicht festgehalten werden, damit nicht Rückschlüsse auf das zeitbezogene Benutzerverhalten eines Teilnehmers möglich werden. Hingegen sieht die entsprechende Bestimmung in der TKO vor, daß bei den Vergütungsdaten auch „der Zeitpunkt der Beendigung der Verbindung zu den Endeinrichtungen des Informationsanbieters" erhoben wird.

  Auch die entsprechende Datensicherungsvorschrift der TKO enthält nicht die Forderung nach Löschung der Verbindungsdaten unmittelbar nach dem Ende der Verbindung (vergl. Art. 9 Abs. 3 Ziff. 1 Bildschirmtext-Staatsvertrag), da die Deutsche Bundespost offensichtlich Verbindungsdaten nicht in jedem Fall löschen will. Weiter fehlen auch für Bildschirmtext klare Verbote der Benutzung von Verbindungsdaten durch Dritte sowie der Übermittlung von Daten, die im Zusammenhang mit der Übermittlung von Mitteilungs- und Antwortseiten anfallen.

Trotz der Fülle der noch offenen Datenschutzanliegen darf ich abschließend noch einmal feststellen, daß aus meiner Sicht bereits der jetzige Stand der TKO eine wesentliche Verbesserung des Datenschutzes darstellt.

15.4. Fernwirkdienste

Die Deutsche Bundespost bereitet die Einführung des Fernwirksystems „TEMEX" vor. TEMEX wird, wie ich bereits in früheren Tätigkeitsberichten erklärt habe, im wesentlichen über das herkömmliche Fernsprechnetz abgewickelt. Als Anwendungsgebiete sind das Fernwirken, Fernmessen, Fernanzeigen, Fernschalten und Ferneinstellen vorgesehen. Vor der endgültigen Entscheidung über die Einführung des TEMEX-Verfahrens hat die Deutsche Bundespost System- und Betriebsversuche vorgeschaltet. In München hat die Bundespost inzwischen mit einem Systemversuch begonnen. Dessen Zweck ist es, die Art der Dienstleistung dieses Fernwirksystems zur Debatte zu stellen und zu prüfen, ob ein derartiger Einsatz sinnvoll ist und inwieweit ein Bedarf hierfür besteht. Dies geschieht unter Anwendung einer vereinfachten Technik, die nur Fernanzeigen und Fernschalten erlaubt. Beim Systemversuch in München sind derzeit noch keine öffentlichen Anbieter vertreten. Bei meinen Gesprächen mit einem privaten Anbieter von Fernwirkleistungen habe ich bisher keine neuen datenschutzrechtlichen Probleme erkennen können.

Die Deutsche Bundespost hat inzwischen in ihrer 29. Änderung der Fernmeldeordnung auch den TEMEX-Dienst geregelt und dabei auch den Datenschutz angesprochen. So werden die Anbieter verpflichtet, in eigener datenschutzrechtlicher Verantwortung ihre Kunden insbesondere über die Voraussetzungen, den Umfang und den Zeitpunkt der Informationsübermittlung zu unterrichten. Weiter ist der zulässige Umfang der von der Deutschen Bundespost zu speichernden Daten im Rahmen des Fernwirkdienstes festgelegt. Zwar enthält diese Datenschutzregelung die dem Grundgedanken des Rechts auf informationelle Selbstbestimmung entsprechende Unterrichtung des betroffenen Kunden, doch fehlt eine Art. 33 Abs. 1 Satz 2 MEG vergleichbare Regelung, daß einem Betroffenen keine besonderen Nachteile entstehen dürfen, wenn er am Fernwirkdienst nicht teilnimmt. Auch hätte ich es begrüßt, wenn die ausdrückliche Verpflichtung des Anbieters in die Fernmeldeordnung aufgenommen worden wäre, vom Teilnehmer die schriftliche Einwilligung zur Speicherung und Weiterverarbeitung seiner personenbezogenen Daten zu erholen.

16. Technischer und organisatorischer Bereich

Die fortschreitende Entwicklung der Informationsverarbeitungstechnik ist dafür verantwortlich, daß sich meine Mitarbeiter ständig neuen Problemen gegenübergestellt sehen. Gerade auf dem Gebiet der Datenkommunikation ist eine ständige Beobachtung neuer Entwicklungen dringend geboten. Meine Mitarbeiter pflegen deshalb den Dialog zu den Herstellern, denn nur derjenige, dem die neuen Techniken geläufig sind, wird die Risiken, die mit der Einführung neuer Techniken verbunden sind, erkennen und Lösungen zur Risikominderung vorschlagen können. Zu erwähnen ist in diesem Zusammenhang auch die aktive Mitarbeit meiner Mitarbeiter in einschlägigen Gremien und Benutzervereinigungen.

Weitere Schwerpunkte bildeten Personal Computer, Bürokommunikation, Lokale Netzwerke und nach wie vor die Revisionsfähigkeit maschineller Datenverarbeitung. Nicht zuletzt galt es sich mit den Computerviren zu beschäftigen, die, wenn auch in meinem Bereich kein derartiger Fall festzustellen war, die Datenverarbeitungsszene gehörig verunsicherten. Neben diesen Grundsatzfragen und der Einarbeitung in neue Datenverarbeitungstechniken bestimmen Beratung und Kontrolle die Tätigkeit im technischen und organisatorischen Bereich.

16.1. Technische und organisatorische Grundsatzfragen

16.1.1. Protokollierung und Auswertung von DV-Aktivitäten

In den vergangenen Jahren habe ich mich erneut eingehend mit der Frage des Nachweises der ordnungsgemäßen Datenverarbeitung im Rahmen der Protokollierungsmöglichkeiten verschiedener DV-Systeme auseinandergesetzt. Diese Grundsätze wurden bereits in früheren Tätigkeitsberichten (7. Tätigkeitsbericht, Nr. 18.1.1, 6. Tätigkeitsbericht, Nr. 5.1.1) beschrieben. Die Analyse der Protokollierungskomponenten – insbesondere unter Beachtung der Zugriffssicherungsmechanismen ergab, daß manche Systeme den aus der Sicht des Datenschutzes zu stellenden Anforderungen nicht entsprachen. Die Mängel bei der Protokollierung wurden den jeweiligen Herstellern vorgetragen. In einigen Fällen konnte Einvernehmen über Verbesserungsmöglichkeiten erzielt werden.

In einem Fall jedoch blieb meinen Bemühungen bislang der Erfolg versagt. Es handelt sich dabei um ein DV-System, das hauptsächlich in Behörden mittlerer Größe zum Einsatz kommt. Eine zentrale Stelle ist für die Entwicklung der Anwenderverfahren und gleichzeitig für die Anwenderunterstützung bei der Implementierung des Systems zuständig.

Kritikpunkte bei der Aufzeichnung von Ablaufdaten im vorgenannten Fall sind dabei das Fehlen folgender Leistungsmerkmale:

- Kennzeichnung des Umfangs der Protokollierung (Benennung der aktiven Protokollsätze im ersten Satz der Protokolldatei),
- Verweis auf die Vorgänger-Log-Datei zur Sicherstellung einer lückenlosen Aufzeichnung,
- Protokollierung des Beendigungsgrundes von Programmen,
- Informationen zur Bearbeitungsart von Dateien (z.B. Lesen, Schreiben, Ändern),
- Nachweise für Unterbrechungen aller Art, die vom Maschinenbediener veranlaßt wurden, beispielsweise die Unterbrechung eines Druckvorganges,
- Informationen über die Benutzung von bestimmten Dienstprogrammen, die vom Systemverwalter aktiviert werden, und
- revisionsfähige, d. h. maschinell erzeugte, Nachweise für die Verwaltungstätigkeiten bei der Definition und der Modifikation von Benutzerprofilen und der Systemsicherungen.

Nachdem der Hersteller des DV-Systems derzeit keine Anstalten macht, eigene Auswerteprogramme für die Protokollebene anzubieten, die eine gezielte Selektierung, Sortierung und Verknüpfung von wahlfreien Aufzeichnungskriterien, wie

- Zeitrahmen,
- Benutzer,
- Ressourcen (Terminals, Programme, Dateien),
- Sicherheitsverletzungen oder sonstige Dateninformationen,

ermöglichen, ist der Anwender, sofern er nicht eigene Lösungen realisiert, was bei den meisten datenverarbeitenden Stellen personell ausgeschlossen ist, auf die auf dem Softwaremarkt angebotenen Produkte angewiesen.

In diesem speziellen Fall ist mir ein Programm bekanntgeworden, das in dieser Beziehung Abhilfe schaffen kann. Dem Hersteller dieser Software habe ich einen Forderungskatalog für wünschenswerte, zusätzliche Funktionen übermittelt. Das Softwarehaus hat diese Anregung überprüft und eine Berücksichtigung bei neuen Release-Ständen wurde mir zugesagt.

Generell wäre wünschenswert, wenn die Hersteller von DV-Systemen zur Unterstützung der Revision der Datenverarbeitung folgende Leitsätze beachten würden:

- Reduzierung des Umfangs von Protokollaufzeichnungen auf bestimmte signifikante Tätigkeiten oder Anwendungen, die der Anwender bestimmen kann, insbesondere beim Einsatz dedizierter Systeme;
- Sanktionen nach fehlerhaften Anmelde- oder Zugriffsversuchen, z. B. durch Sperren des Terminals, von dem der mißbräuchliche Zugriffsversuch aus gestartet wurde, für jede weitere Benutzung;
- Realisierung einer Routine, die zeitabhängig oder programmgesteuert die Datenendgeräte und die Leitungen zu- und abschalten kann;
- Verbesserung des Zeitverhaltens bei der Aufzeichnung von Ablaufdaten.

16.1.2. Sicherungsmaßnahmen bei Installation eines dezentralen DV-Systems

Vermehrt wenden sich Landratsämter, Gemeinden und Krankenhäuser an mich und lassen sich über die notwendigen Datensicherungsmaßnahmen bei der Installation einer eigenen dezentralen DV-Anlage beraten. Diese DV-Anlagen besitzen heute die Leistungsfähigkeit früherer Großrechner. Bei den Sicherungsmaßnahmen kann man sich allerdings nicht nach den für einen Großrechner adäquaten Maßnahmen richten, da die Datenverarbeitung weitgehend anders organisiert ist, so daß viele Eigenschaften, die ein Rechenzentrum charakterisieren, fehlen.

Für dezentrale DV-Systeme sind nach meinen Erfahrungen die folgenden Datensicherungsmaßnahmen anzustreben, wobei davon ausgegangen wird, daß Rechner und rechnernahe Peripherie in einem Raum untergebracht sind und der Rechner im wesentlichen im bedienerlosen 24-Stunden-Betrieb läuft:

Zugangskontrolle

- Der Zugang zum Rechnerraum ist – soweit kein Ausweisleser installiert wurde – ausschließlich mit einem Schlüssel außerhalb des sonstigen Schließsystems möglich, wobei darauf zu achten ist, daß nur an solche Personen Schlüssel oder Ausweise auszuhändigen sind, die ihren Aufgaben nach Zugang zum Rechnerraum haben müssen.

- Die Drücker an der Außenseite der Zugangstüren zum Rechnerraum sind grundsätzlich durch Türknaufe zu ersetzen.
- Personen ohne Zugangsberechtigung müssen sich in geeigneter Weise bemerkbar machen können. Um diesen Personenkreis einwandfrei identifizieren zu können, könnte es sich empfehlen, am Zugang eine Kamera anzubringen.
- Überwachung der Türöffnungszeiten
- Bei der Verarbeitung von sensiblen personenbezogenen Daten ist zu erwägen, ob für die Zugangskontrolle ein Zugangsleser mit Protokollierung der Zu- und Abgänge unter Berücksichtigung der Paarigkeitskontrolle einzusetzen ist.

Raumsicherung

- Der Raum, in dem das DV-System installiert ist, ist mit einem Bewegungsmelder und durch Türschließkontaktmelder an den Zugangstüren zu sichern, wenn die Anlage rund um die Uhr in Betrieb ist und Festplattenmodule installiert sind. Die Entsicherung und Scharfschaltung außerhalb der Dienstzeit läuft über ein Blockschloß.
- Die Fenster sind durchwurfhemmend (E30) auszugestalten.
- Ein ausgelöster Alarm läuft bei einer zentralen Stelle auf. Wird er dort nicht quittiert, muß er automatisch an weitere Adressaten durchgeschaltet werden.

Brandschutz

- Zumindest für den Rechnerraum ist ein eigener Brandabschnitt (Klasse F 90) einzurichten.
- Installation von Brandmeldern
- Entfernung unnötiger Brandlasten aus dem Bereich unmittelbar neben dem Rechner
- Feuerfeste Abschottung der Kabelschächte
- Adäquate Ausgestaltung der Türen, Fenster oder sonstiger Durchlässe bezüglich der brandhemmenden Wirkung

Sonstiges

- Absicherung der Luftansaugstutzen für die Klimaanlage des Rechners
- Anschaffung eines Datensicherungsschrankes (zumindest S 60D) für die Sicherungsdatenträger
- Auslagerung einer Sicherungskopie in ein anderes Gebäude
- Vermeidung aller Hinweise, daß für Außenstehende der geschützte Bereich als solcher erkennbar wird.

16.1.3. Sicherheit in Datenfernverarbeitungsnetzen

Der Datentransfer zwischen zentralem Rechner und Endbenutzern außerhalb der Grundstücksgrenzen wird in der Datenfernverarbeitung häufig auf festgeschalteten Leitungen abgewickelt. Die Deutsche Bundespost bietet bei der Verteiltechnik auf festgeschalteten Leitungen zur Zeit zwei Alternativen an, die Schnittstellenvervielfachung und die Kanalteilung. Bei der Verwendung des Synchronknotens SK 12 als Schnittstellenvervielfacher kann es zu Datensicherungsproblemen kommen, wenn an einem Knoten Endbenutzer angeschlossen sind, die unterschiedlichen speichernden Stellen angehören.

Die Verteiltechniken sollen im folgenden näher erläutert werden:

Verteiltechniken

Als Verteiltechniken bietet die Deutsche Bundespost, wie oben bereits erwähnt, für festgeschaltete Leitungen die Schnittstellenvervielfachung und die Kanalteilung an. Beide Techniken unterscheiden sich grundlegend.

Ein Schnittstellenvervielfacher ermöglicht zusammen mit Übertragungseinheiten und Datenanschlußgeräten den Mehrpunktbetrieb und gestattet von einer Zentrale die Verzweigung auf mehrere Teilnehmer. Mit einer Kaskadenschaltung läßt sich die Zahl der angeschlossenen Endbenutzer weiter erhöhen. Der Einsatz des Schnittstellenvervielfachers wird wegen der hohen Übertragungsgeschwindigkeit (meist 9600 bit/sec.) und vor allem aus Kostengründen gewählt, da für den Anwender die Leitungskosten bis zum Schnittstellenvervielfacher nur einmal anfallen. Ein Beispiel für einen Schnittstellenvervielfacher ist der Synchronknoten SK 12. Werden Daten von der Zentrale in Richtung Endbenutzer übertragen, vervielfacht der SK 12 die Daten und sendet diese an alle angeschlossenen Datenendgeräte. Der SK 12 verfügt über keine Intelligenz, die eine Selektierung bereits im Knoten vornehmen könnte. Über die in der Nachricht mitgeführten Adresse erkennen die Datenendgeräte, ob die gesendete Nachricht für sie bestimmt ist oder nicht.

Bei der Kanalteilung einer fest geschalteten Leitung erfolgt eine Aufteilung des Übertragungsfrequenzspektrums in Kanäle bestimmter Bandbreite, meist 2400 bit/sec. Bei dieser gegenüber dem SK 12 kostenintensiveren Lösung erhält das Datenendgerät nur die auch für dieses Gerät bestimmte Nachricht. Wegen der Kanalteilung ist die Übertragungsgeschwindigkeit geringer als bei Verwendung des Synchronknotens. Neuerdings bietet die Deutsche Bundespost die Kanalteilung auch für eine 64 kbit-HfD-Leitung an, so daß die systembedingten Einbußen bei der Übertragungsgeschwindigkeit nicht mehr so ins Gewicht fallen.

Mißbrauchsmöglichkeiten

Der Einsatz des Synchronknotens SK 12 als Schnittstellenvervielfacher begünstigt die mißbräuchliche Verwertung der übertragenen Nachrichten. Zwar ist es nicht möglich, an einer angeschlossenen Datensichtstation durch Manipulation der Adresse dieses Gerätes den Halbdialog eines anderen Gerätes zu empfangen und auf dem Bildschirm sichtbar zu machen, weil das Terminalsteuerprogramm das manipulierte Gerät bereits bei der Anmeldung abweist, wenn ein Gerät der betreffenden Adresse bereits aktiv ist. Für den Fall, daß es nicht aktiv ist, können keine Dialogdaten empfangen werden. Problematisch wird es allerdings dann, wenn man an die Leitung unmittelbar vor dem Endgerät einen sogenannten Leitungsmonitor anschließt. Der Leitungsmonitor empfängt sämtliche Nachrichten, die über den SK 12 allen angeschlossenen Endgeräten angeboten werden, im Falle der Kanalteilung jedoch nur die Informationsmenge für ein bestimmtes Datenendgerät.

Sicherungsmaßnahmen

Bei der Verwendung des Schnittstellenvervielfachers SK 12 ist darauf zu achten, daß die an den SK 12 angeschlossenen Datenendgeräte ausschließlich in einem bestimmten, geschlossenen Anwenderkreis eingesetzt werden. Die

Generierung der Geräteadresse sollte, sofern möglich, an zentraler Stelle softwaremäßig erfolgen. Die Manipulation der Geräteadressen erfordert dann grundsätzlich eine Neugenerierung an der zentralen Stelle. Will man ganz sicher gehen und ausschließen, daß alle Datenendgeräte die Nachrichten einer Zentrale empfangen können, so muß man die Kanalteilung, separate Leitungen oder einen intelligenten Netzknoten verwenden, der an den Endbenutzer nur die für ihn bestimmten Nachrichten übermittelt. Die Kosten für intelligente Netzknoten sind allerdings höher.

16.1.4. Vireninfizierte Systeme

Großes Aufsehen haben die Versuche des amerikanischen Computerexperten Fred Cohen mit sogenannten Computerviren erregt. Anhand von Beispielen zeigt er, wie schnell sich Computerviren ausbreiten, gesunde Systeme infizieren und letztendlich ganze Computersysteme verseuchen und unbrauchbar machen können.

Ein Virus ist ein Programmbaustein, der den ordnungsgemäßen Ablauf eines Programmes verhindert. Dieser Baustein kopiert sich selbst an eine bestimmte Stelle eines gesunden, noch nicht verseuchten Programmes. Beim Aufruf eines infizierten Programmes werden entweder eine endlose Programmschleife oder Befehle durchlaufen, die Datenbestände und Programme (Objekte) mit einer sinnlosen Zeichenfolge überschreiben und damit zerstören, oder sich selbst in ein gesundes Programm an eine bestimmten Stelle hineinkopieren. Experten sind der Ansicht, daß es nicht ganz einfach ist, einen entsprechenden Ausbreitungsmechanismus für das Programmvirus zu schreiben.

Es erhebt sich die Frage, wie man sich gegen Programmviren schützen kann. Eines sei jedoch vorweggenommen: Gegen einen virenimplantierenden Systemverwalter gibt es keinen wirksamen Schutz.

Programmviren zeichnen sich im wesentlichen durch zwei Eigenschaften aus, durch ihre Transitivität und ihre Unsichtbarkeit.

Programmviren können grundsätzlich dann die Grenzen eines Benutzers A zu einem anderen Benutzer B überschreiten, wenn der Benutzer B seine Objekte durch das Attribut „share-yes" anderen Benutzern zugänglich gemacht hat und darüber hinaus anderen Benutzern einen schreibenden Zugriff auf seine Objekte erlaubt. Greift unter dieser Voraussetzung ein Benutzer A mit einem infizierten Programm auf ein Objekt eines anderen Benutzers B zu, so kann man davon ausgehen, daß binnen kurzer Zeit auch die Objekte, das sind die Programme und die Dateien des Benutzers B, verseucht sind. Besonders schlimm ist es, wenn Systemprogramme verseucht sind, da sich die Systemprogramme im privilegierten Status befinden und der privilegierte Benutzer, also der Systemadministrator, sich über alle Sicherungs-Maßnahmen hinwegsetzen kann.

Unsichtbar sind Programmviren deshalb, weil man es verseuchten Programmen nicht ansieht, daß oder ob sie verseucht sind. Die heutigen Betriebssysteme können nämlich nicht entscheiden, ob ein Programm manipuliert oder modifiziert wurde. Schließlich gibt es Programmviren, die erst dann aktiv werden, wenn die Spuren zum Inplanteur bereits getilgt sind. Sie werden nämlich erst nach einer bestimmten, vom Inplanteur festgelegten Zeit aktiv.

Ein Benutzer kann sich heute gegen einen anderen Benutzer, außer gegen das Betriebssystem und den Systemverwalter, dadurch schützen, daß er auf seine Objekte ein Schreibpaßwort legt und sie nicht als „sharable" definiert. Die Einschränkung der Mehrfachbenutzbarkeit führt allerdings häufig zu Systemeinbußen. Systemprogramme sind grundsätzlich mit einem WRITE-Paßwort zu schützen. Außerdem kann man besonders wichtige Programme dadurch sichern, daß man sie unmittelbar nach dem Übersetzen und Binden auf einen Sicherungsdatenträger bringt. Es gibt bereits Software, die Programme und Daten bis auf Bitebene miteinander vergleichen kann. Vor der Ausführung eines so geschützten Programmes wird der Vergleich mit der gespeicherten Version durchgeführt. Treten Differenzen auf, ist das ein Indiz für eine Manipulation der auf der Anlage gespeicherten Daten und Programme.

Programmviren hätten schließlich dann keine Möglichkeit mehr Unheil anzustiften, wenn es dem Betriebssystem gelänge, manipulierte Programme als solche zu erkennen. Mit Hilfe kryptographischer Verfahren ließe sich das realisieren. Man denkt hier in erster Linie an die Verwendung asymetrischer Algorithmen, wie sie im RSA-Verfahren (ein public-key-System nach Rivest-Shamir-Adleman) enthalten sind. Durch seine digitale Unterschrift teilt der rechtmäßige Eigner eines Objektes dem System seine Authentität mit. Nach einer Manipulation eines Objektes paßt die digitale Unterschrift nicht mehr zu dem gespeicherten Code und das Betriebssystem würde diesen Code nicht mehr zur Ausführung zulassen, so daß ein verseuchtes Programm keine Chance mehr hätte, ein gesundes Programm zu infizieren. Bei der heutigen Rechnergeneration würde die Einführung solcher Sicherungsfunktionen allerdings noch zu erheblichen Performance-Verlusten führen.

16.1.5. Bürokommunikation

Die Bürokommunikation ist kein Schlagwort mehr. Zwar sind wir noch ein gutes Stück von den Zielvorstellungen der Planer entfernt, treffen jedoch vereinzelt bereits auf Insellösungen, wie die Textverarbeitung, die automatisierte Registraturverwaltung oder die Telefongesprächsdatenerfassung, die später in das Bürokommunikationssystem einfließen sollen.

Um auf Risiken rechtzeitig reagieren und Sicherungsmöglichkeiten vorschlagen zu können, haben sich die Datenschutzbeauftragten frühzeitig mit diesen neuen Techniken beschäftigt. Bereits im 7. Tätigkeitsbericht war die Textziffer 18.1.3 auf Seite 71 dieser Problematik gewidmet. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder hat sich im Berichtszeitraum u.a. auch der Bürokommunikation angenommen. Das in einer Unterarbeitsgruppe entstandene Papier über „Risiken und Chancen der Bürokommunikation in der öffentlichen Verwaltung", in der auch ein Mitarbeiter meiner Geschäftsstelle beteiligt war, wird diesem Bericht als **Anlage 4** beigefügt.

16.2. Prüfungs- und Beratungstätigkeit

16.2.1. Kontrolle der technischen und organisatorischen Maßnahmen

Im Berichtszeitraum wurden wiederum die Datensicherungsmaßnahmen bei einer Reihe von datenverarbeitenden Stellen überprüft. Im einzelnen handelte es sich dabei um

eine Industrie- und Handelskammer, drei kommunale Rechenzentren, die Verwaltung von drei kreisfreien Städten, zwei Stadtverwaltungen, eine Gemeindeverwaltung, zwei Landratsämter und drei Krankenhäuser. Obwohl sich keine groben Verstöße gegen das Datenschutzgesetz gezeigt haben, ergaben die Prüfungen, daß eine Reihe von Mängeln bei der Datensicherung, insbesondere bezüglich der Zugangskontrolle, der Revisionsfähigkeit der Datenverarbeitung, der Aufbewahrung bzw. der Entsorgung von personenbezogenen Unterlagen vorhanden waren.

Darüber hinaus wurden die im Krankenversicherungsdialogsystem KVDS und beim Betrieb des Systems getroffenen technischen und organisatorischen Datensicherungsmaßnahmen überprüft. Das Krankenversicherungsdialogsystem wurde von der Allgemeinen Ortskrankenkasse Lindau in Zusammenarbeit mit der Fa. Nixdorf entwickelt. Die Überprüfung ergab, daß sich die Entwickler große Mühe gegeben haben, den Erfordernissen des Datenschutzes in technischer Hinsicht gerecht zu werden. Überprüft wurden folgende Komponenten:

- Anmelde- und Abmeldeprozeduren
- Schutzklassen
- Benutzerprofile
- Speicherkontrolle
- Datensicherung und Wiederanlauf
- Abwehr unzulässiger Zugriffsversuche
- Verfahrensbezogene Protokollierung
- Dokumentation
  - Anwendungshandbuch
  - Bedienungsanleitung
  - Verfahrensdokumentation
  - Programmierrichtlinien
  - Programmverwaltung
  - Änderungsdienst
  - Freigabe
- Unterlagen für die Revision
  - Maschinenprotokoll
  - Einrichten von Benutzerprofilen
  - Netzkonfiguration/Steuerung
  - Bibliotheksverwaltung
  - Terminüberwachung für Batchanwendungen.

Größere Mängel bei den Datensicherungsmaßnahmen konnten nicht festgestellt werden, wenngleich zu bestimmten Problemkreisen, insbesondere für den laufenden Betrieb, noch einige Verbesserungsvorschläge und Anregungen gegeben worden sind.

Neben diesen Prüfungen nahm die Zahl der Beratungsgespräche im Zuge von Neu- und Umbaumaßnahmen bei verschiedenen Behörden weiter zu und überstieg die Anzahl der Prüfungen bereits beträchtlich.

Schließlich kommt es auch immer häufiger zu Nachprüfungen, wenn bei der Realisierung der Maßnahmen aufgrund meiner Prüfungsbemerkungen die speichernde Stelle verschiedene Lösungsmöglichkeiten anbietet und Unterstützung bei der Entscheidungsfindung wünscht.

Beispielhaft seien einige Anregungen, die ich für den Ablauf der maschinellen Datenverarbeitung gebe, genannt:

- Die Revisionsfähigkeit von Online-Anwendungen ist durch geeignete Maßnahmen sicherzustellen. Dabei handelt es sich insbesondere um die Dokumentation des Verfahrens, die Benutzungsregeln und die Benutzerprofile.
- Programmänderungen sind grundsätzlich unter nachweislicher Einbindung der Fachabteilung zu regeln. Programmänderungen müssen schriftliche Aufträge zugrundeliegen.
- Die bei Online-Anwendungen eingerichteten Benutzerprofile sind mit Datum- und Zeitangaben zu versehen, so daß nachweisbar wird, wer wann mit welchen Zugriffsberechtigungen ausgestattet war. Diese Unterlagen sind ein wesentlicher Bestandteil für die Revision und sollten über einen Zeitraum von mindestens 3 Jahren zurückverfolgbar sein.
- Werden Echtdaten zu Testzwecken verwendet, so ist jeweils die Zustimmung der betroffenen Fachabteilung einzuholen. Die Zustimmungserklärung muß schriftlich erfolgen und ist für Dokumentationszwecke aufzubewahren.
- Die Abwicklung und der Ablauf von Batchanwendungen sind zu protokollieren. Ist die Anzahl der Batchanwendungen groß, ist eine Terminplanung durchzuführen.
- Um falschen Paßworteingaben innerhalb von Online-Anwendungen nachgehen zu können, sind diese mit Datum, Uhrzeit und verursachendem Terminal in einem Verarbeitungsprotokoll aufzuzeichnen.
- Persönliche Kennworte sind öfters zu verändern.

Auch in der manuellen Datenverarbeitung und innerhalb des allgemeinen Dienstbetriebes treten Mängel auf, die zu Datenpannen führen können. Die Kontrollen ergaben, daß in den nachfolgenden Bereichen immer wieder Mängel zu erkennen waren:

- Karteien und sonstige Unterlagen mit personenbezogenen Daten werden nicht ausreichend sicher unter Verschluß gehalten. Vorhandene verschließbare Behältnisse werden nicht abgeschlossen. Defekte Schließvorrichtungen werden nicht instand gesetzt.
- Zu bearbeitende Vorgänge mit personenbezogenen Daten bleiben nach Dienstende auf den Schreibtischen.
- Für die ordnungsgemäße Entsorgung von Unterlagen und Altpapier mit personenbezogenen Daten ist keine besondere Sorge getragen. Eine Kenntnisnahme durch Unbefugte müßte weitestgehend ausgeschlossen werden. Falls solche Unterlagen bis zu ihrer endgültigen Vernichtung zwischengelagert werden müssen, sollten hierfür entsprechende Sicherungsmaßnahmen getroffen werden.
- Bei Behörden und Parteiverkehr wird oft keine Möglichkeit zu einer diskreten Sachbehandlung angeboten.
- Die sichere Entsorgung von Carbonbändern ist nicht gewährleistet. Hierauf ist besonders großer Wert zu legen, da bedingt durch deren einmalige Verwendung auf ihnen geschriebene Texte reproduzierbar sind.

16.2.2. Nachkontrolle

Bereits im 5. Tätigkeitsbericht wurde unter der Textziffer 5.2.1 auf Seite 55 darüber berichtet, wie zeitaufwendig sich die Überwachung des Vollzugs der Prüfungsbemerkungen

nach Kontrollbesuchen gestaltet. Nach Art. 30 Abs. 1 BayDSG müssen Verletzungen von Vorschriften über den Datenschutz beanstandet und ihre Behebung in angemessener Frist gefordert werden. Obwohl bei der Schlußbesprechung nach Prüfungsbesuchen in der Regel bei allen Beteiligten Einigkeit über die erforderlichen technischen und organisatorischen Maßnahmen besteht, zieht sich deren Realisierung manchmal über Jahre hinweg, so daß die Nachkontrolle verhältnismäßig viel Arbeitskraft bindet. Meine Mitarbeiter sind stets darauf bedacht, bei der Wahl von wirksamen und geeigneten Mitteln zur Sicherstellung der technischen und organisatorischen Maßnahmen zum Datenschutz Anregungen zu geben. Wie wichtig eine Nachkontrolle ist, zeigte sich bei einem Kontrollbesuch in einem Rechenzentrum, das sowohl für den öffentlichen als auch für den nichtöffentlichen Bereich arbeitet. Wegen der Auftragsdatenverarbeitung wurde das Rechenzentrum von der Aufsichtsbehörde nach § 40 BDSG überprüft. Im Prüfungsbericht der Aufsichtsbehörde wurden einige technische Mängel angesprochen und deren Behebung in angemessener Frist gefordert. Obwohl der Kontrollbesuch meiner Mitarbeiter in diesem Rechenzentrum erst einige Jahre später erfolgte, hatte man keinerlei Anstrengungen zur Behebung der von der Aufsichtsbehörde festgestellten Mängel unternommen.

Werden zur Behebung der Mängel größere bauliche Maßnahmen erforderlich, für die zunächst keine Haushaltsmittel vorhanden sind, müssen ohnedies längere Fristen zur Mängelbehebung in Kauf genommen werden. Bei einem Rechenzentrum, dessen Umbau sich schon über Jahre hinzieht, mußte ich feststellen, daß bei den Mitteln für Datensicherungsmaßnahmen besonders gespart wird, obwohl die Haushaltsansätze für Datenverarbeitung ein Vielfaches dessen betragen, was für eine ordnungsgemäße Datensicherung notwendig erscheint. Insgesamt bestätigt sich die von einigen Experten vor etwa sieben Jahren gemachte Aussage, daß die Aufwendungen für die Datensicherung als Folge des Datenschutzrechts ca. 3 % dessen ausmachen, was für die gesamte Datenverarbeitung ausgegeben wird.

16.3. Einzelprobleme

16.3.1. Personal Computer

Wegen der vielseitigen Verwendbarkeit wird die Notwendigkeit, den Personal Computer auch in der Verwaltung einzusetzen, immer größer. Die Zahl der im Einsatz befindlichen Geräte hält sich zwar heute noch in Grenzen, in den kommenden Jahren ist jedoch damit zu rechnen, daß diese Geräte immer häufiger auf Schreibtischen von Sachbearbeitern stehen werden. Um so dringlicher erscheint es, daß man sich bereits frühzeitig Gedanken über Risiken und Sicherungsmaßnahmen macht, die mit dem Einsatz der Personal Computer verbunden sind. In der Anlage 3 wurde versucht, in Abhängigkeit von der Betriebsart Sicherungsmaßnahmen beim Einsatz von Personal Computern stichpunktmäßig zusammenzustellen.

Allgemein sollte gelten, daß die Verarbeitung geschützter personenbezogener Daten nur auf solchen Geräten erfolgt, die bestimmte Mindestanforderungen an Datensicherungsmaßnahmen erfüllen. Auf die Beschaffung von Geräten ohne diese Sicherungskomponenten ist zu verzichten.

16.3.2. Versand und Transport von sensiblen personenbezogenen Daten

Aus gegebenem Anlaß muß ich darauf aufmerksam machen, daß beim Versand und Transport von sensiblen Unterlagen mit personenbezogenen Daten auch innerhalb der Verwaltung die Vorschriften nachArt. 15 BayDSG, § 6 BDSG und § 35 SGB I zu beachten sind. Bei einer Übermittlung oder beim Transport dürfen diese personenbezogenen Daten nur den mit der Sachbearbeitung betrauten Personen offenbart werden.

In einem mir zur Kenntnis gelangten Fall wurden an eine Stelle Unterlagen aus dem Bereich der Sozialverwaltung durch Bedienstete einer anderen speichernden Stelle in offener Sammelpost zugeleitet. Die vom Absender gewählte offene Versandart durch Sammelpost stellt keine vertrauliche Behandlung der sensiblen personenbezogenen Informationen sicher. Ich habe deshalb gefordert, daß die Unterlagen mit schutzwürdigen personenbezogenen Daten, insbesondere in den Bereichen Sozial- und Personalwesen, so kuvertiert werden, daß eine Kenntnisnahme des Inhalts durch unbefugte Dritte verhindert wird, wobei der Transport in Kuverts durchaus auch durch Sammelpost erfolgen kann. Briefumschläge mit Adhäsionsverschluß erscheinen mir dabei nicht geeignet.

Auch beim internen Postaustausch einer speichernden Stelle, bei der ein Sachgebiet bereits als eine speichernde Stelle im Sinne des Bayer. Datenschutzgesetzes gelten kann, ist darauf zu achten, daß sensible personenbezogene Daten nur den mit der Sachbearbeitung beauftragten Personen zugänglich sind.

16.3.3. Vernichtung von Datenträgern

Die sichere Vernichtung von Datenträgern mit personenbezogenen Informationen beschäftigt meine Dienststelle nach wie vor. Immer wieder werden Fälle bekannt, in denen Personendaten, die der Geheimhaltung unterliegen, durch unsachgemäße Behandlung bei der Entsorgung in fremde Hände geraten.

Im Herbst 1985 trat die neue DIN-Norm 32757, Teil I über die Vernichtung von Informationsträgern in Kraft. Bei der Informationsträgervernichtung wird dort zwischen 5 Sicherheitsstufen unterschieden. Schon die Sicherheitsstufe 3 fordert für die Vernichtung von Informationsträgern, daß die Reproduktion der dort wiedergegebenen Informationen nur unter erheblichem Aufwand möglich ist. Bei der Vernichtung von Papier werden dafür Partikel bis zur Größe von 240 mm² oder Streifen bis zu einer Breite von 2 mm gefordert. Diese Forderungen werden heute schon von verschiedenen modernen und leistungsfähigen Aktenvernichtern erfüllt.

Probleme treten häufig auch dort auf, wo große Mengen Papier, etwa nach Aussonderungsaktionen, zu entsorgen sind, da die meisten Aktenvernichtungsanlagen diesem Anfall mengenmäßig nicht gewachsen sind. In solchen Fällen ist auch das Transportrisiko nicht zu unterschätzen, wenn das Entsorgungsgut an einer anderen Stelle, also außer Haus, vernichtet werden soll. Für die Vernichtung von großen Mengen unter der Beaufsichtigung der speichernden Stelle gibt es zwei Möglichkeiten:

- Spezialgroßvernichtungsanlagen haben ein Leistungsvermögen von mehreren Tonnen Papier pro Tag. Bei derartigen Anlagen handelt es sich aber um Sonderanfertigungen, deren Anschaffungspreis bei etwa 200 000.– bis 250 000.– DM liegt.
- Außerdem gibt es mobile Schredderanlagen, die bei der Vernichtung ebenfalls die Sicherheitsstufe 3 erreichen.

16.3.4. Wahrung des Persönlichkeitsschutzes im Parteiverkehr

Immer wieder erreichen mich Zuschriften von Bürgern, die darauf hinweisen, daß der Persönlichkeitsschutz bei der Abwicklung des Parteiverkehrs, insbesondere im Sozialamtsbereich, nicht gewährleistet ist.

Auf meine Anfrage bei einer dieser Stellen wurde mir mitgeteilt, daß die räumliche beengte Situation im Sozialamtsbereich bekannt sei. Nicht zuletzt habe die ständige Zunahme an Sozialfällen zu dieser Situation beigetragen. Um den betroffenen Bürgern eine möglichst gute, umfassende und den Anforderungen des Gesetzes entsprechende Hilfe angedeihen zu lassen, habe man das Personal im Sozialamt verstärkt, was letztlich zur Folge hatte, daß wegen der beschränkten Raumverhältnisse die Dienstzimmer teilweise mit 2 oder 3 Sachbeabeitern besetzt werden mußten. Man weise aber die Bediensteten stets darauf hin, Fragen so zu stellen, daß das Sozialgeheimnis gewahrt werde, wenn sich mehrere Antragsteller im Dienstzimmer aufhalten. Darüber hinaus bestehe die Möglichkeit, in besonders gelagerten Fällen einen Gesprächstermin außerhalb der Parteiverkehrszeit zu vereinbaren, oder das Gespräch als Einzelgespräch im Zimmer des Gruppenleiters, der über ein Einzelzimmer verfügt, weiterzuführen. Die mißliche Raumsituation werde sich erst dann ändern, wenn andere Räumlichkeiten zur Verfügung stehen.

Solche räumlichen Verhältnisse müssen aus der Sicht des Persönlichkeitsschutzes Sorge bereiten. Gleichwohl können technische und organisatorische Maßnahmen zur Verbesserung des Datenschutzes nicht völlig losgelöst von den finanziellen Konsequenzen betrachtet werden. Im Anwendungsbereich des § 6 BDSG bzw. Art. 15 BayDSG sind vielmehr entsprechende Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck besteht. Unter Berücksichtigung der gegebenen Verhältnisse scheinen die betroffenen Stellen in den meisten Fällen die ihnen gebotenen und wirtschaftlich vertretbaren Möglichkeiten auszuschöpfen, damit der Persönlichkeitsschutz, insbesondere auch das Sozialgeheimnis gewahrt werden können. Die Sozialbehörde könnte daher trotz der Raumverhältnisse nicht beanstandet werden. Im Zuge von Um- oder Neubaumaßnahmen muß jedoch Abhilfe geschaffen werden.

Viele Beratungsgespräche befaßten sich deshalb auch mit Umbaumaßnahmen, die die Wahrung des Persönlichkeitsschutzes zum Ziele hatten. Auf die Ausführungen im 7. Tätigkeitsbericht unter der Textziffer 18.3.1 auf Seite 72 wird Bezug genommen.

16.3.5. Sicherungsmaßnahmen zur Abschottung von Statistik und Verwaltungsvollzug

Als Folge des Volkszählungsurteils des Bayerischen Verfassungsgerichts müssen Überlegungen angestellt werden, wie ein kommunalstatistische Amt von der Vollzugsverwaltung abgeschottet werden kann. Hierzu wurden eine Reihe technischer und organisatorischer Sicherungsmaßnahmen vorgeschlagen.

Oberster Grundsatz der Sicherungsmaßnahmen ist die personelle, räumliche und organisatorische Abschottung von Statistik und Verwaltungsvollzug.

Eine organisatorische Abschottung ist dann gegeben, wenn das Statistische Amt eine eigenständige Stelle ohne Aufgaben im Verwaltungsvollzug ist.

Im einzelnen halte ich folgende Maßnahmen für geeignet:

Maßnahmen bei der manuellen Bearbeitung

- Aufbewahrung von Fragebögen in eigenen Räumen.
- Bearbeitung der Fragebögen von eigenen Bediensteten (Zeit- und Aushilfskräfte gelten als eigenes Personal, auf eine Auftragsvergabe an Dritte ist zu verzichten).
- Nach der Erfassung und Auswertung sind die Fragebögen in einem Vernichtungsgerät (Reißwolf) sicher zu vernichten.

Maßnahmen bei automatisierter Bearbeitung

Maßnahmen in personeller Hinsicht:

- Festlegung der Verfügungs- und Zugriffsberechtigten.
- Online-Auswertungen sind nur von Bediensteten des Statistischen Amtes vorzunehmen.
- Das statistische Amt sollte anstreben, die DV-technische Verwaltung und alle Auswertungen der eigenen Daten durch eigenes Personal durchführen zu können.
- Erledigen städtische Organisatoren im Auftrag des Statistischen Amtes maschinelle Auswertungen der Bestände des statistischen Amtes, sind über solche Fälle Log-Aufzeichnungen zu führen.
- Auf eine Datenverarbeitung im Auftrag an private Dritte ist zu verzichten.

Maßnahmen in DV-technischer Hinsicht:

- Grundsätzlich ist bei Statistikdaten die Speicherung auf der eigenen DV-Anlage, die ausreichende technische Sicherungsmaßnahmen bietet, anzustreben.
- Sicherung der Datenbestände durch Paßworte gegen den Zugriff Unbefugter.
- Es ist zu überprüfen, ob die Datenbestände ständig im direkten Zugriff gehalten werden müssen.
- Vermeidung des Aufbaus einer technischen Infrastruktur, die eine spätere physische Verlagerung von Statistik- und Verwaltungsvollzugsdaten auf zwei getrennte Anlagen erschweren würde.
- Die Verknüpfung von Statistikdaten mit Vollzugsdateien ist unzulässig („autarke" Bestände für Vollzug und Statistik). Etwaige Datenübermittlungen vom Vollzug zur Statistik sind im Einzelfall auf ihre Rechtmäßigkeit hin zu überprüfen.

Maßnahmen bei der Speicherung, Verarbeitung und Auswertung:

- Eine Verknüpfung von Individualdaten mit Daten aus anderen Dateien, auch solchen, die beim statistischen Amt gespeichert werden, ist dahingehend zu überprüfen, ob zusätzliche Merkmale einer anderen Qualität entstehen können. Die Schaffung neuer personenbezogener Informationen kann problematisch sein. Keinesfalls darf ein Personenprofil, auch nicht ein „Teil-Abbild" der Personen, entstehen.
- Die statistischen Erhebungsdaten sind möglichst bald zu anonymisieren.

- Die Veröffentlichung von Individualdaten ist unzulässig.
- Zur Gewinnung von Erfahrungen sollten alle Auswertungen der Datenbestände zunächst so protokolliert werden, daß eine Datenschutzkontrolle im Nachhinein ermöglicht wird.

16.3.6. Wartung von Festspeichereinheiten

Als Speichermedien bei modernen DV-Anlagen werden in zunehmendem Maße Festplatten benützt. Im Berichtszeitraum wurde ich des öfteren mit der Frage konfrontiert, welche Sicherungsmaßnahmen bei der Reparatur und Wartung dieser Datenspeicher angemessen sind. Gerade Anwender von dezentralen Systemen verfügen häufig nicht über genügend große Systemkenntnisse, Risiken beurteilen und geeignete Sicherheitsvorkehrungen treffen zu können.

Die lokale Wartung und die Fernwartung von DV-Systemen wurden in den letzten Tätigkeitsberichten wiederholt behandelt. Durch geeignete Maßnahmen läßt sich weitgehend ausschließen, daß im Rahmen der Wartung ein unkontrollierter Zugriff auf Anwenderdaten erfolgt. Bei Kleinsystemen, etwa Einzel- oder Mehrplatzsystemen, kann es aber durchaus vorkommen, daß bei der Fehlerbehebung auf Anwenderdaten zugegriffen werden muß. In solchen Fällen ist die Einhaltung des Datengeheimnisses schriftlich zu vereinbaren.

Trotz des hohen Qualitätsstandes der Festplattenspeicher treten ganz vereinzelt immer wieder Fehlerfälle, (z. B. Head-Crash) auf, die eine besondere Behandlung dieser Speichereinheiten erforderlich machen. Die Reparatur der Festplatten ist in vielen Fällen nur beim Hersteller möglich, wozu die Plattenspeicher aus den Geräten ausgebaut werden müssen. Der Hersteller hat sich dann schriftlich zu verpflichten, die auf dem Plattenspeicher vorhandenen Kundendaten physikalisch zu löschen und zu erklären, daß eine Weitergabe dieser Daten an Dritte ausgeschlossen ist. In vielen Fällen genügt eine derartige Versicherung, wobei der Anwender auf die Ausstellung einer eigenen Löschbestätigung nicht verzichten soll. Der Transport der Datenträger erfolgt in der Regel auf dem Postweg in verschließbaren Spezialbehältern. Sofern der Anwender auf einem Sondertransport, etwa durch einen Kurier, besteht, ist dies zwar möglich, die Mehrkosten sind jedoch in der Regel vom Anwender zu tragen. Alle vom Hersteller reparierten Plateneinheiten werden vor der Neuauslieferung an den Kunden gelöscht. Wesentlich an diesem Verfahren ist allerdings, daß die Löschung meist erst nach der Reparatur erfolgen kann. Besteht der Anwender auf der sofortigen Löschung des Datenträgers, also vor der Reparatur, ist das nur durch Anlegen eines starken äußeren Magnetfelds möglich. Enthält ein Plattenspeicher besonders sensible Daten, ist zu prüfen, ob dieser vor der Reparatur beim Anwender physikalisch gelöscht werden kann. Aber auch in einem solchen Fall empfiehlt es sich, sich vom Hersteller eine Löschbestätigung aushändigen zu lassen. Mit Wechselplatten ist in analoger Weise zu verfahren.

16.3.7. System- und Betriebsversuche von TEMEX

Vor der Entscheidung über eine endgültige Einführung von TEMEX will die Deutsche Bundespost die Akzeptanz dieses Dienstes in System- und Betriebsversuchen testen. Das soll zwar nur unter Anwendung der vereinfachten Technik (Kategorie 1) geschehen, die lediglich Fernanzeigen und Fernschalten erlaubt und nur die Übertragung zweiwertiger Informationen zuläßt. Die Betriebsversuche, die auch Aufschluß über die Tauglichkeit der Technik liefern sollen, sollten Ende 1985 anlaufen. Sie haben sich aber um einige Monate verzögert. Als Anbieter kommen in erster Linie Bewachungsunternehmen in Frage. Die Nachfrage bei den Betriebsversuchen in München ist geringer als ursprünglich angenommen.

An einen Temex-Netzabschluß sind insgesamt 16 Temex-Endeinrichtungen (Kriterien) z. B. Alarmschleifen, anschließbar. Für die Einrichtung eines Anschlusses ist an die Deutsche Bundespost derzeit eine einmalige Gebühr von DM 65.– zu entrichten. Pro Kriterium sind an die Post monatlich DM 3.– zu zahlen. Die monatlichen Aufschaltgebühren an ein Bewachungsunternehmen betragen etwa DM 45.-. An ein Kriterium können über eine Alarmschleife mehrere Sensoren angeschlossen werden, z. B. Glasbruch- und Bewegungsmelder in einem Einfamilienhaus. Die Mißbrauchsmöglichkeiten erhöhen sich durch den Einsatz dieser Technik nicht. Die Zentrale, an derein Alarm aufläuft, ist besonders gesichert, so daß ein Einbruch, um an die Alarmunterlagen zu gelangen, ausgeschlossen werden kann.

Etwas populärer und verbreiteter sind die Altennotrufe, angeboten von privaten Hilfsorganisationen, die allerdings außerhalb von TEMEX ablaufen und nicht in meinen Zuständigkeitsbereich fallen.

17. Datenschutzregister

Im Berichtszeitraum erreichten meine Geschäftsstelle täglich neue Meldungen zum Datenschutzregister. Zum Zeitpunkt der Veröffentlichung des ersten Nachtrags zur Übersicht über das Datenschutzregister beim Landesbeauftragten für den Datenschutz am 18. November 1985 hatten insgesamt 4 342 speichernden Stellen 15 285 Dateien zum Datenschutzregister gemeldet. Gegenüber dem Vorjahr ergibt das bei den Dateien eine Zunahme von 7 % und bei den speichernden Stellen eine Zunahme von 5 %. Die hohe Zahl der Einzeldateien ist in erster Linie auf die große Redundanz bestimmter Dateien, etwa das automatisierte Einwohnerwesen, das etwa 90 % aller bayerischen Gemeinden melden, die Lohn- und Gehaltsabrechnung oder die Schülerdateien, zurückzuführen.

Auch die Zahl der Verfahrensänderungen, die sich letztlich in Änderungsmeldungen niederschlagen, nimmt zu und bindet eine Arbeitskraft in zunehmendem Maße. Viele stapelverarbeitungsorientierte Verfahren werden auf Dialoganwendungen umgestellt. Darüber hinaus nimmt die Anzahl der Kleinsysteme, wie Textsysteme, ständig zu. Zwar zählen Dateien von Textbausteinen und Briefen nicht zu den meldepflichtigen Dateien, jedoch sind auf diesen Systemen meist Adreßdateien gespeichert, die in der Regel den Dateibegriff erfüllen. Dafür sind Meldungen zum Datenschutzregister erforderlich. Schließlich ist festzustellen, daß eine Reihe von Gemeinden eigene DV-Systeme anschaffen, so daß auch hier Änderungsmeldungen zum Datenschutzregister notwendig werden.

Besonders große Resonanz erzeugte eine Pressenotiz über die Veröffentlichung des ersten Nachtrags zur Übersicht über das Datenschutzregister im Bayer. Staatsanzeiger Nr. 50/1985 vom 13.12.1986. Wandte sich bis zu diesem Zeitpunkt durchschnittlich ein Bürger in der Woche mit der

Bitte an mich, ihm bei der Wahrnehmung seines Auskunftsrechts über gespeicherte Daten Hilfestellung zu leisten, so stieg die Zahl derer, die wissen wollten, welche Daten über sie gespeichert werden, nach der Veröffentlichung der Pressenotiz sprunghaft an. Innerhalb eines Monats hatte ich ca. 300 Bürgeranfragen dieser Art zu beantworten.

Zur Zeit hat sich das Interesse wieder etwas gelegt, es ist jedoch anzunehmen, daß die Zahl derer, die Auskunft über gespeicherte Daten oder Hinweise über den Auskunftsanspruch erhalten wollen, jederzeit, insbesondere vor und nach der Volkszählung 1987, wieder zunehmen wird.

18. Datenschutz beim Bayerischen Rundfunk

Die Einhaltung des Datenschutzes beim Bayerischen Rundfunk wird nach Art. 21 Abs. 3 BayDSG vom dortigen Datenschutzbeauftragten überwacht, der den Organen der Anstalt jährlich einen Bericht über seine Tätigkeit zu erstatten hat. Den gesetzlichen Bestimmungen entsprechend hat der Datenschutzbeauftragte des Bayerischen Rundfunks mir auch in diesem Jahr seinen Bericht für die Zeit vom 1.1.1985 bis 31.12.1985 übermittelt. Dem Bericht lassen sich folgende Schwerpunkte entnehmen:

Im Rahmen eines einführenden Überblicks über die Entwicklung des Datenschutzrechts geht der Bericht kurz auf den Stand der Beratungen zur Novellierung des Bundesdatenschutzgesetzes ein. Weiterhin setzt ersich im Anschluß an entsprechende Erörterungen aus dem Jahr 1983 mit Überlegungen auseinander, auf dem Verordnungswege eine Rechtsgrundlage für Kontrollmitteilungen der Rundfunkanstalten an die Finanzbehörden über Honorarzahlungen zu schaffen. Hiergegen werden erhebliche Bedenken auch datenschutzrechtlicher Art geltend gemacht. ARD und ZDF haben aus diesem Grunde bei den Ländern bereits Vorbehalte gegen eine entsprechende Regelung angemeldet.

Bei der Überwachung der Datenverarbeitung beim Bayer. Rundfunk standen im letzten Jahr der Personalbereich, die EDV-Abteilung und der Programmbereich im Mittelpunkt. In der Personalabteilung wurde, wie im Vorbericht bereits angekündigt, eine neue Form der Gehaltsabrechnung eingeführt. Datenschutzprobleme haben sich hierbei nicht ergeben. Die Telefondatenerfassung im Bayerischen Rundfunk wurde entsprechend einer bereits im letzten Tätigkeitsbericht dargestellten Forderung des Datenschutzbeauftragten weitgehend anonymisiert. Die bisher in diesem Bereich aufgetretenen Probleme sind auch infolge neuerer obergerichtlicher Entscheidungen zu diesem Komplex fürs erste geklärt. Weiter befaßt sich der Bericht hier mit einer Erweiterung des Personaldatensystems (Abrechnung ausgegebener Essensmarken) und mit der Installierung eines PC im Sozialreferat zur Durchführung von Berechnungen für die Altersversorgung.

In der EDV-Abteilung wurde ein neues System zur Verbesserung der Zugriffskontrolle eingeführt. Dieses von der Abteilung selbst erarbeitete System stellt sicher, daß künftig der einzelne Benutzer nur die für ihn zugelassenen Programme und Anwendungen aufrufen kann. Ferner wurde der Postversand von Datenbändern überprüft, wobei insbesondere der Transportkontrolle Aufmerksamkeit geschenkt wurde. Im Programmbereich lag ein Schwerpunkt der Tätigkeit des Datenschutzbeauftragten für den Bayerischen Rundfunk und seiner Kollegen aus den anderen Rundfunkanstalten bei der Beurteilung der Zulässigkeit einer von ARD und ZDF als Gemeinschaftseinrichtung geplanten Pressedatenbank. Die Konzeption sieht hier eine zentrale Auswertung eines einvernehmlich festzulegenden Spektrums überregionaler Zeitungen des In- und Auslandes, von Wochenzeitungen, Zeitschriften und Magazinen sowie sonstiger Publikationen (ausgenommen regionale Tagespresse) in mehreren Schritten vor. Vorgesehen ist ferner die Errichtung einer Personendatenbank. Die Speicherung der Dokumente soll in der Form erfolgen, daß diese am Sitz der Pressedatenbank auf Mikrofilm vervielfältigt werden und den beteiligten Rundfunkanstalten zur dezentralen Dokumentenverwaltung überlassen werden. Offen ist hier noch, ob auf eine solche Gemeinschaftseinrichtung das sog. Medienprivileg (Einschränkung von datenschutzrechtlichen Ansprüchen Betroffener) Anwendung finden kann und wie die Einhaltung datenschutzrechtlicher Bestimmungen sichergestellt werden soll. Die Entscheidung über eine Realisierung des Projekts, insbesondere über eine Beteiligung des Bayerischen Rundfunks, ist noch nicht getroffen. Ansonsten hatte sich der Datenschutzbeauftragte im Programmbereich mit einem Pilotprojekt des Wirtschaftsfunks zu befassen, mit dem erstmals erprobt werden sollte, den Redaktionen in Verbindung mit dem Schreibbüro Textbe- und -verarbeitungsfunktionen zur Verfügung zu stellen. Ein weiteres Projekt betraf die Abteilung Unterhaltung-Wort. Hier ging es um ein Retrieval-Programm zur Nutzung des umfangreichen internen Unterhaltungs-Repertoires.

Wie schon im Vorjahr nimmt der Themenbereich Gebühreneinzug (Datenschutz bei der GEZ) wiederum einen breiten Raum im Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten ein. Das bereits im Bericht für 1984 angesprochene Problem der Aktualisierung von Lastschriftzahleradressen scheint sich einer für alle Beteiligten annehmbaren Lösung zu nähern. Künftig soll auf der Anmeldung des Rundfunkteilnehmers in die Abbuchungsermächtigung ein Zusatz aufgenommen werden, der die ausdrückliche Ermächtigung der GEZ enthält, sich von dem jeweiligen Kreditinstitut Adressenänderungen mitteilen zu lassen. Die ebenfalls schon im Vorbericht behandelten Direktwerbemaßnahmen der GEZ zur Förderung der Bereitschaft, betriebene Rundfunkgeräte auch anzumelden, konnten in der bisherigen Form nicht fortgeführt werden. Der externe Adressenlieferant sah sich nicht in der Lage, einen Liefervertrag mit den Rundfunkanstalten abzuschließen. Die Rundfunkanstalten haben deshalb ein anderes Konzept entwickelt und versucht, Adressen von Jugendlichen zu erhalten, die im Bestand der gemeldeten Rundfunkteilnehmer nicht ausreichend vertreten sind. Zielgruppe einer für 1986 vorgesehenen Werbeaktion sollen dann vornehmlich diejenigen Jugendlichen sein, die ein eigenes Einkommen besitzen, aber noch bei ihren Eltern leben. Dieser Personenkreis ist entgegen einer weit verbreiteten Ansicht in der Bevölkerung verpflichtet, Rundfunkgebühren zu entrichten. Der Arbeitskreis der Datenschutzbeauftragten der Rundfunkanstalten hat das vorgesehene Konzept eingehend diskutiert und das geplante Anschreiben an die Jugendlichen überprüft. Er vertritt die Auffassung, daß es vor allem Angelegenheit des Lieferanten der benötigten Adressen ist, jeweils in eigener Verantwortung zu prüfen, ob eine Datenübermittlung an die Rundfunkanstalten zulässig ist. Der Arbeitskreis befaßte sich im letzten Jahr ferner mit Problemen bei der Bearbeitung von Anträgen auf Befreiung von der Rundfunkgebührenpflicht. Der Antragsteller wird künftig deutlich darauf

hingewiesen werden, daß zur Entscheidung über den Antrag auch Sozialdaten (z.B. Höhe des Wohngeldes) herangezogen werden müssen. Ein geplantes automatisiertes Verfahren zur Unterstützung der Antragsbearbeitung wird von der GEZ auch aus datenschutzrechtlichen Gründen nicht weiter verfolgt werden. Weitere Einzelfragen betrafen den Einsatz von Bildschirmtext (Btx) durch die GEZ, die Einführung tragbarer Datensichtgeräte für Beauftragte, die Realisierung eines Konzepts für eine zeitgemäße Datenkommunikation zwischen GEZ und Rundfunkanstalten sowie Probleme bei der Altpapierentsorgung.

Zusammenfassend stellt der Datenschutzbeauftragte des Bayerischen Rundfunks fest, daß sowohl die Mitarbeiter des Hauses als auch die Rundfunkteilnehmer mittlerweile ein unproblematisches Verhältnis zum Datenschutz gewonnen haben. Die von den Medien begleitete öffentliche Diskussion zu datenschutzrechtlichen Fragen werde aber auch in Zukunft dazu beitragen, daß neue Techniken, denen sich die Rundfunkanstalten grundsätzlich schon aus Konkurrenzgründen nicht verschließen können, jedenfalls nicht unkritisch angenommen und verwendet werden.

19. Weiterentwicklung des Datenschutzrechts

Novellierung des Bundesdatenschutzgesetzes (BDSG)

Hatte über den Gesetzentwurf der SPD-Fraktion im Deutschen Bundestag zur Änderung des Bundesdatenschutzgesetzes (Drucksache 10/1180) bereits am 24. Juni 1985 eine öffentliche Anhörung im Innenausschuß des Bundestages stattgefunden (siehe dazu im 7. Tätigkeitsbericht S. 80ff), fand eine weitere Anhörung über diesen Entwurf und insbesondere den neu eingebrachten Entwurf der Koalitionsfraktionen zur Änderung des Bundesdatenschutzgesetzes, des Verwaltungsverfahrensgesetzes, des Bundesverfassungsschutzgesetzes und des Straßenverkehrsgesetzes – Drucksache 10/4737 – am 21. April 1986 statt. Dazu ist zu bemerken:

Die Vorlage von Gesetzentwürfen zur Änderung des Bundesdatenschutzgesetzes – wie auch für die sogenannten „Sicherheitsgesetze" – ist grundsätzlich zu begrüßen.

Der derzeit vorliegende Entwurf ist jedoch meines Erachtens verfassungsrechtlich nicht völlig bedenkenfrei, soweit dessen Geltung auf Dateien beschränkt ist, die Datenerhebung nicht im Bundesdatenschutzgesetz geregelt wird und der vorgesehene Umfang der Kontrolle durch den Bundesbeauftragten für den Datenschutz deutlich begrenzt ist.

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Volkszählungsgesetz 1983 aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein Grundrecht auf „informationelle Selbstbestimmung" abgeleitet (E 65, 1 ff). Dieses Recht gewährleistet die Befugnis des einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbart und in welcher Weise seine persönlichlichen Daten verwendet werden. Informationelle Selbstbestimmung bedeutet, daß der Bürger wissen können muß, wer was wann und bei welcher Gelegenheit über ihn weiß. Unter den Bedingungen der modernen Datenverarbeitung gibt es kein „belangloses" Datum mehr. Für die Frage, wie weit Informationen „sensibel" sind, ist nicht allein entscheidend, ob die Informationen intime Vorgänge betreffen. Wesentlich ist vielmehr die Frage des Verwendungszusammenhangs. Entscheidend sind somit Nutzbarkeit und Verwendungsmöglichkeiten der Daten, unabhängig von der Art ihrer Organisation. Die Verarbeitung sensibler personenbezogener Daten berührt das Grundrecht auf informationelle Selbstbestimmung und bedarf daher einer Rechtsgrundlage. Neben den bisher im Bundesdatenschutzgesetz geregelten Phasen der Datenverarbeitung hat das Bundesverfassungsgericht ausdrücklich auch die Erhebung als schutzbedürftig erkannt. Das Verlangen des Staates zur Abgabe personenbezogener Daten ist ein Eingriff.

Allerdings ist das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet. Der einzelne muß Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Derartige Beschränkungen dieses Grundrechts bedürfen aber einer ausdrücklichen gesetzlichen und verfassungsmäßigen Grundlage. Der Gesetzgeber hat hierbei den Grundsatz der Verhältnismäßigkeit und das Gebot der Normenklarheit zu beachten. Das Bundesverfassungsgericht hat den Gesetzgeber aufgefordert, mehr als früher auch „organisatorische und verfahrensrechtliche Vorkehrungen" zu treffen. In diesem Zusammenhang hat das Bundesverfassungsgericht ausdrücklich klargestellt, daß zugleich „eine effektive Kontrolle durch die Datenschutzbeauftragten notwendig" sei. Dieser Forderung liegt auch der Gedanke zugrunde, daß wegen der Komplexität moderner Datenverarbeitung und teilweise auch wegen besonderer Sicherheitsinteressen der Bürger selbst nicht immer wissen kann, wer was wann über ihn weiß. Hier sollen die Kontrollmöglichkeiten der unabhängigen Datenschutzbeauftragten einen Ausgleich schaffen. Dieser Gesichtspunkt war auch entscheidend im Beschluß des Bundesverfassungsgerichts zur Post- und Telefonkontrolle nach § 3 des Gesetzes zu Art. 10 GG. Das Bundesverfassungsgericht führt insoweit aus, daß die Befugnis, den von einer strategischen Überwachungsmaßnahme Betroffenen nicht in Kenntnis zu setzen, verfassungsrechtlich nur hingenommen werden kann, weil die Kontrolle der Maßnahmen durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane (Kontrollkommission und Datenschutzbeauftragte) sichergestellt sei (BVerfGE 67, 157/185).

Diesen vom Bundesverfassungsgericht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleiteten Grundsätzen wurde der Entwurf zur Novellierung des Bundesdatenschutzgesetzes m. E. nicht ausreichend gerecht. Wegen des Ablaufs der Legislaturperiode wird der Gesetzentwurf nicht abschließend behandelt. Daher erübrigen sich derzeit nähere Ausführungen. Auf die Protokolle über die o. a. Anhörungen und meine dort vorgetragenen Stellungnahmen verweise ich.

Die Datenschutzbeauftragten des Bundes und der Länder haben zur Novellierung des Bundesdatenschutzgesetzes eine Stellungnahme abgegeben, die als Anhang 2 diesem Bericht beigefügt ist.

20. Der Beirat

Einrichtung und Aufgaben des gemäß Art. 29 BayDSG beim Landesbeauftragten für den Datenschutz gebildeten Beirats sind in früheren Tätigkeitsberichten beschrieben

worden (siehe insbesondere im 5. Tätigkeitsbericht, Textziff. 2.1, S. 7). Auf die wertvolle und tatkräftige Unterstützung meiner Tätigkeit durch den Beirat habe ich in der Vergangenheit immer wieder hingewiesen und wiederhole dies für den Berichtszeitraum ausdrücklich.

Die dem Landtag angehörenden Mitglieder werden jeweils für die Wahldauer des Landtags bestellt, die übrigen Mitglieder jeweils für 4 Jahre. Nach der Landtagswahl im Herbst 1986 werden die Mitglieder des Beirats neu zu bestellen sein.

Im Berichtszeitraum war Vorsitzender des Beirats der Abgeordnete Hermann Regensburger, stellvertretender Vorsitzender der Abgeordnete Klaus Warnecke. Mitglieder des Beirats und ihre Stellvertreter waren:

Die Landtagsabgeordneten:

Hermann Regensburger	Dr. Paul Wilhelm
Franz Josef Brosch	Manfred Humbs
Wolfgang Dandorfer	Johann Böhm
Franz Gruber	Konrad Kobler
Klaus Warnecke	Rolf Langenberger
Alfred Münch	Heinz Mehrlich

Die Senatoren:

Wolfgang Burnhauser	Otto Neukum

Für die Staatsregierung:

Dr. Friedrich Giehl Ministerialdirigent im Bayer. Staatsministerium des Innern	Dr. Werner Böhme Ministerialrat im Bayer. Staatsministerium der Finanzen

Für die Kommunalen Spitzenverbände:

Dr. Georg Wilhelm Geschäftsleitender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Klaus Eichhorn Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern

Für die Sozialversicherungträger:

Franz-Martin Fehn Erster Direktor der Landesversicherungsanstalt für Oberfranken und Mittelfranken	Herbert Schmaus Verwaltungsdirektor beim Landesverband der Ortskrankenkassen in Bayern

Für den Verband der Freien Berufe in Bayern e.V.:

Dr. med. H. Braun Präsident des Verbandes Freier Berufe in Bayern e.V.	Winfried Wachter Präsidiumsmitglied des Verbandes Freier Berufe in Bayern e.V.

1985 und bis Mitte 1986 tagte der Beirat sechsmal, nämlich am 5. März, 22. Oktober und 3. Dezember 1985, sowie am 11. März, 13. Mai und 15. Juli 1986. Er befaßte sich in seinen Sitzungen insbesondere mit den folgenden Themen:

- Erlaß der Bayerischen Meldedaten-Übermittlungsverordnung,
- Volkszählung, einschließlich freiwilliger Probeerhebung,
- Mikrozensus,
- Bayerisches Archivgesetz,
- Mitteilungen in Strafsachen (MiStra),
- Übermittlung von Pflegschaftsdaten durch die Wahlbehörde an die Führerscheinbehörde,
- Datenabfrage der Polizei bei der Allgemeinen Ortskrankenkasse im Zusammenhang mit Verkehrsordnungswidrigkeiten,
- Berichte des Datenschutzbeauftragten über durchgeführte Datenschutzprüfungen,
- Berichte des Datenschutzbeauftragten über Beanstandungen öffentlicher Stellen,
- Kontrollkompetenz des Bayerischen Landesbeauftragten für den Datenschutz,
- Vorberatung des 7. Tätigkeitsberichts gemäß Art. 26 Abs. 6 BayDSG,
- Beratung der Ausführungen über die Sicherheitsbehörden im 7. Tätigkeitsbericht,
- Bericht über die Grundsätze der Novellierung des Bundesdatenschutzgesetzes,
- Bericht über Stand der Gesetzgebung und Stellungnahme der Datenschutzbeauftragten zu den Sicherheitsgesetzen,
- Bericht zum Stand der Erörterungen zum Krebsregister,
- Gesetz über den Gesundheitsdienst (Geheimhaltungsregelungen),
- Änderungsgesetz zum Bayer. Krankenhausgesetz (Datenschutzbestimmungen),
- Bürokommunikation,
- Bericht über den Ablauf technisch-organisatorischer Datenschutzprüfungen,
- Information durch das Bayer. Staatsministerium des Innern über Prüfungserfahrungen im nichtöffentlichen Bereich,
- Verfassungsschutz – Stand der Dienstanweisungen,
- Vergabe von Datenerfassungsarbeiten an private Erfassungsunternehmen,
- Bericht zur Telekommunikationsordnung,
- Verschlüsselungsverfahren für Meldungen an Krankheitsregister,
- Polizeiliche Datenverarbeitung.

Zur Tätigkeit des Beirats siehe im übrigen in den Tätigkeitsberichten I unter 1.4, II unter 1.3, III unter 1.2.1, IV unter 1.5, V unter 2.1, VI 1.1 und VII unter 23.

21. Behandlung des 7. Tätigkeitsberichts im Parlament

Der 7. Tätigkeitsbericht wurde am 29.1.1986 im Ausschuß für Verfassungs-, Rechts- und Kommunalfragen des Bayerischen Landtags und am 19. März 1986 im Rechts- und Verfassungsausschuß des Bayerischen Senats beraten.

1. Bei der Beratung im Bayer. Landtag wies der Berichterstatter, Abgeordneter Hermann Regensburger, auf die Aktualität der Beratung des 7. Tätigkeitsberichts angesichts der in Bonn zu beratenden Sicherheitsgesetze und der Notwendigkeit der Umsetzung des Volkszählungsurteils des Bundesverfassungsgerichts vom 15.12.1983 hin. Wegen der zahlreichen Datenschutzfragen, die nach diesem Urteil zu klären waren, hatte der Bayer. Landtag mit Beschlußvom 5.3.1985 (Drucksache 6265) auf Antrag von MdL Regensburger die Staatsregierung ersucht, zu prüfen und umgehend zu berichten,

welche Konsequenzen sich aus dem Urteil des Bundesverfassungsgerichts für die bayerische Gesetzgebung und Verwaltungspraxis ergeben. Wie MdL Regensburger ausführte, mache der mittlerweile vorliegende Bericht des Staatsministeriums des Innern deutlich, daß Neuregelungen nicht zuletzt aus Gründen der Rechtseinheitlichkeit im Bundesgebiet nicht sofort möglich seien, sondern komplizierte Abstimmungen mit dem Bund und den übrigen Bundesländern erfordern.

Die Schlagzeilen in der Presse, die der 7. Tätigkeitsbericht ausgelöst hätte, würden diesem nicht gerecht, da sich die Berichterstattung vorwiegend auf spektakuläre Fälle wie z. B. die Speicherung der Daten eines Vierjährigen und eines Vierundachtzigjährigen im Polizeicomputer beschränkten. Unerwähnt bliebe dagegen die Feststellung des Datenschutzbeauftragten, wonach besonders bei der Polizei eine deutliche Verbesserung des Datenschutzbewußtseins und der Datenverarbeitungspraxis festzustellen sei. Besonders erfreulich sei die Feststellung des Berichts, daß Polizei und Verfassungsschutz die früheren Beanstandungen durch konkrete Maßnahmen ausgeräumt hätten. MdL Regensburger wies allerdings darauf hin, daß noch viel Aufklärungsarbeit bei den Mitarbeitern der Behörden notwendig sei, grundsätzlich würden nämlich eher mehr als zuwenig Daten gesammelt und aufbewahrt. Angesichts des naturgemäß hohen sensiblen Polizeidatenbestandes müsse besonders die interne Schulung der damit befaßten Mitarbeiter intensiviert werden – möglicherweise durch Bestellungen interner Datenschutzbeauftragter nicht nur beiden Polizeidirektionen, sondern bei jeder Polizeidienststelle, um das Datenschutzbewußtsein zu schärfen und Abweichungen von den Vorschriften frühzeitig aufzudecken.

Im Gegensatz zu dem Sprecher der SPD, MdL Warnekke, der sich für eine stärkere Artikulierung des Datenschutzbeauftragten in der Öffentlichkeit ausgesprochen hatte, hielt MdL Regensburger den etwas lautloseren Weg des Bayer. Datenschutzbeauftragten für sachdienlicher. Der Bayer. Beauftragte habe keinerlei Schwierigkeiten im Umgang mit bayerischen Behörden; alle Türen und Schränke stünden ihm offen.

Der 7. Tätigkeitsbericht enthalte eine interessante Sammlung zu den vielfältigen aktuellen Datenschutzproblemen und ergebe zusammen mit den vorhergehenden Tätigkeitsberichten ein einmaliges Nachschlagewerk zu nahezu allen relevanten Datenschutzfragen. MdL Regensburger dankte dem Datenschutzbeauftragten und seinen Mitarbeitern ausdrücklich für ihre Arbeit.

Mitberichterstatter MdL Warnecke erneuerte in seinen Ausführungen zunächst seine Sorge, der Tätigkeitsbericht sei teilweise etwas verharmlosend und schonend. Es würden immer mehr Daten gespeichert. Die Entwicklung des Datenschutzes halte dabei nicht mit der Entwicklung der Speichertechnik stand. Die Verkleinerung der DV-Anlagen und die immer dichter werdende Vernetzung erschwere den Datenschutz.

MdL Warnecke stellte in Bonn eine Trendwende in Sachen Datenschutz fest. Auch die arglosesten Bürger könnten den Datenschutz nicht mehr nur als politische Randerscheinung betrachten, da auch sie zunehmend Interesse an seinem Funktionieren haben müßten. Es sei deshalb schlimm, wenn von der Polizei Daten eines Vierjährigen, der einen Diebstahl begangen haben soll oder eines Fünfjährigen, der einen Ladendiebstahl begangen haben soll, gespeichert würden. Es sei zu fragen ob solche Datenspeicherungen die Folge vorhandener großer Speicherkapazitäten seien, weil diese zu einer großzügigen Einspeicherung verleiten könnten. Bei der Polizei sei dies auch deshalb problematisch, da die Richtlinien zur Führung der Kriminalaktennachweise z. B. schon seit längerer Zeit bestünden, so daß die Zeit der Gewöhnung hieran abgeschlossen sein müßte.

In der Öffentlichkeit werde der Datenschutz im Bereich des Sozialwesens häufig unterschätzt, die größten Datenspeicherer schlechthin seien nicht die Sicherheits-, sondern die Sozialbehörden, Rentenversicherungsverwaltung, Krankenversicherungsverwaltung, Arbeitsverwaltung. Es sei darum wiederum verständlich, daß die Sicherheitsbehörden auf diese gespeicherten Daten schnell zugreifen wollten. Die Regelung im 10. Buch des SGB hierzu sei unzulänglich.

Im Bereich der Statistik wies MdL Warnecke auf die Diskrepanz zwischen eingehenden rechtlichen Regelungen über die dortige Datenverarbeitung und den möglicherweise zu sorglosen Umgang mit Computerausdrucken (im Müllcontainer) hin. Die Vernichtung unmittelbar vor Ort sei der beste und sicherste Weg. Dies müßte gegenüber eventuellen finanziellen Bedenken auch vom Parlament unterstützt werden.

Bei der Erörterung übereinen „Bayerischen Weg" im Bereich des Datenschutzes sei zu beachten, daß die Datenschutzbelange bundesweit gleichermaßen gelten. Dem Bayerischen Datenschutzbeauftragten stünden die Türen und Schränke der Behörden zugegebenermaßen weiter offen, als Amtskollegen in anderen Bundesländern. Die Basis hierfür dürfte jedoch nicht Wohlverhalten, sondern könnte nur die Kontrollrechte des Beauftragten sein. Im übrigen genüge auch nicht, daß in der Öffentlichkeit nur anläßlich des Tätigkeitsberichts einmal jährlich über den Datenschutz gesprochen werde. Die bestehenden Zielkonflikte zwischen Datenschutz und anderen fachlichen Interessen müßten vielmehr häufiger auch öffentlich ausgetragen werden. Der Datenschutzbeauftragte solle konfliktfreudiger handeln.

MdL Langenberger erläuterte die Berichterstattung über Datenschutzverstöße von Sicherheitsbehörden in den Medien mit dem Hinweis, daß diese Behörden mit besonders sensiblen Material umgehen und Pannen gerade in diesem Bereich schlimmere Auswirkungen für den Bürger haben können als in anderen Bereichen. Eine eingehendere Schulung des Personals sei deshalb gerade in diesem Behördenbereich notwendig.

MdL Moser hob die Notwendigkeit, zwischen der Datenschutzkontrolle bei öffentlichen und privaten Stellen zu koordinieren, hervor und stellte die Frage, wie gewährleistet sei, daß der Datenschutz im privaten Bereich landesweit einheitlich vollzogen werde und wie festgestellt werden könne, ob im privaten Bereich Bedarf an weiteren Datenschutzregelungen bestünde. Der Datenschutz-Tätigkeitsbericht wäre noch viel informativer, wenn er neben dem öffentlichen auch den privatwirtschaftlichen Bereich umfasse.

MdL Warnecke hielt einen zweijährigen Datenschutztätigkeitsbericht-Turnus für nur überlegenswert, wenn der Datenschutzbeauftragte konkrete Einzelfälle außerhalb des turnusmäßigen Tätigkeitsberichts veröffentlichen würde.

Der Landesbeauftragte für den Datenschutz wies in diesem Zusammenhang auf die Möglichkeit des Landtags und des Senats gem. Art. 28 Abs. 5 BayDSG hin, dem Landesbeauftragten besondere Prüfungsaufträge zu geben.

MdL Regensburger hielt die Schulung der Sachbearbeiter im Bereich der Sicherheitsbehörden möglicherweise noch für verbesserungsbedürftig und schlug vor, bei jeder Polizeiinspektion einen internen Datenschutzfachmann zu bestellen, der vor Ort und am Datenspeichergerät immer wieder nachprüfe, ob dem Datenschutz entsprochen werde. Schulungsmaterial biete hierfür der Tätigkeitsbericht. Er nahm gleichzeitig die Mitarbeiter von Sicherheitsbehörden gegen den in der Presse (nicht im Tätigkeitsbericht) geäußerten Verdacht der Sammelwut in Schutz und wies auf das Verständnis der Allgemeinheit für den Einsatz moderener Computertechnik für die Verbrechensbekämpfung hin. Dieser fordere zwangsläufig größere Datensammlungen, wobei der Verhältnismäßigkeitsgrundsatz aber stets beachtet werden müsse.

MdL Warnecke hob in diesem Zusammenhang zwei spezifische Merkmale der Sicherheitsbehörden hervor: Sie besäßen besondere Macht und Exekutivbefugnisse gegenüber den Bürgern – z. B. Festnahmerecht und Anklagebefugnis – und treten ihnen in hoheitlicher Form gegenüber. Außerdem unterlägen sie nicht im Verhältnis zum Bürger der sonst für die staatliche Verwaltung geltenden Auskunftpflicht.

2. Im Bayerischen Senat erläuterte ich den 7. Tätigkeitsbericht am 19. März dieses Jahres in der 11. Sitzung des Rechts- und Verfassungsausschusses. Im Anschluß an die Vorstellung des Berichts wurden aktuelle Fragen der Einführung des maschinenlesbaren Personalausweises diskutiert. Des weiteren befaßten sich die Mitglieder des Senats mit der Frage, ob an der bisherigen jährlichen Berichtspflicht des Datenschutzbeauftragten gegenüber dem Parlament und der Staatsregierung festgehalten werden, sowie, ob die Führung des Datenschutzregisters und der Übersicht in der bisherigen Weise beibehalten werden solle. Das Spannungsverhältnis, Schutz der Persönlichkeit einerseits, Datenwünsche der Forschung, insbesondere der Hochschulforschung, andererseits, stellten neben den Fragen der datenschutzrechtlichen Probleme im kommunalen Bereich weitere Schwerpunkte der Diskussion dar. Der Ausschußvorsitzende, Senator Dr. Herrmann, erklärte abschließend, daß zwischen dem Landesbeauftragten für den Datenschutz und dem Ausschuß in allen wichtigen Fragen ein gutes Einvernehmen bestünde.

22. Btx-Angebot des Bayer. Landesbeauftragten für den Datenschutz

Der Bayer. Landesbeauftragte für den Datenschutz ist seit Mai dieses Jahres mit Informationen zum Datenschutz im Bildschirmtextsystem vertreten. Er ist unterder Teilnehmernummer 089/2283873 oder im Rahmen des gemeinsamen Programmangebots der Bayer. Staatsregierung zu erreichen. Der Bürger wird damit über Btx unterrichtet, wer ihn in Datenschutzfragen berät, welche Rechte ihm nach den Datenschutzgesetzen zukommen, welche Vorschriften über den Datenschutz, einschließlich der wesentlichen bereichsspezifischen Regelungen bestehen und wie weit die Datenschutzkontrolle reicht. Außerdem hat der Bürger die Möglichkeit, sich **direkt** an den Landesbeauftragten für den Datenschutz mit einer Mitteilung zu wenden. Es ist sichergestellt, daß die Vertraulichkeit dieser Mitteilung gewahrt ist und ausschließlich der Landesbeauftragte für den Datenschutzsie lesen kann. Schließlich kann der Bürger über Bildschirmtext Informationsmaterial zum Datenschutz anfordern. Das Angebot umfaßt insgesamt 29 Seiten und ist selbstverständlich nicht vergütungspflichtig.

23. Arbeitsbedingungen der Geschäftsstelle

Leider kann ich bezüglich der Arbeitsbedingungen der Geschäftsstelle für das Berichtsjahr nur wiederholen, was im 7. Tätigkeitsbericht ausgeführt wurde:

Die Personalkapazität der Geschäftsstelle reicht zur Bewältigung der anfallenden Arbeiten nach wievor bei weitem nicht aus. Die in meinem 6. Tätigkeitsbericht hierzu gemachten näheren Darlegungen treffen noch immer zu. Sie enden mit der Hoffnung auf Unterstützung von Landtag und Staatsregierung bei der Zurverfügungstellung 3 weiterer Planstellen. Diese Hoffnung hat sich bisher nur teilweise erfüllt. Der Haushaltsplan 1985/86 sieht zwar 3 zusätzliche Abordnungsstellen vor, ihre Beschaffung bereitet jedoch Schwierigkeiten: Bei Abordnungsstellen darf das abgebende Ressort die entsprechenden Stellen während der Abordnungszeit des Beamten nicht besetzen, sie gehen ihm für diese Zeit praktisch verloren. Wie erwartet, haben sich deshalb fast unüberbrückbare Hindernisse ergeben, im Wege von Abordnungsstellen zusätzliches Personal für die Geschäftsstelle zu erhalten. Lediglich das Bayerische Staatsministerium der Finanzen ordnete im Frühjahr dieses Jahres einen Beamten zu meiner Geschäftsstelle ab. Nach Beendigung der Abordnung wird sich die Frage nach der Besetzungsmöglichkeit dieser Abordnungsstelle erneut stellen. Die anderen beiden Abordnungsstellen konnten nicht besetzt werden.

Für den Haushalt 1987/88 habe ich daher erneut um die Zurverfügungstellung „echter" Planstellen anstelle von Abordnungsstellen gebeten.

24. Konferenz der Datenschutzbeauftragten

Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz haben 1985, sowie bis Mitte 1986 in sieben Tagungen gemeinsam interessierende Fragen erörtert. Beispielhaft seien genannt die Befassung mit der Vorbereitung der Volkszählung, mit Mikrozensus und Personalausweisgesetz, mit Btx und TEMEX sowie mit Anforderungen an Datenschutzregelungen im Polizeirecht. Breiten Raum nahmen die Erörterungen zur Novellierung der Sicherheitsgesetze ein. Die Entschließung zu den „Sicherheits- und Datenschutzgesetzen" ist in der Anlage dieses Tätigkeitsberichts abgedruckt. Weiter befaßte sich die Konferenz mit Datenschutzfragen des

Ausländerzentralregisters sowie des Führerscheins auf Probe, mit Datenschutz im Krankenhaus und der Telekommunikationsordnung. Zur Novellierung des Bundesdatenschutzgesetzes nahmen die Datenschutzbeauftragten ebenfalls Stellung (abgedruckt in der Anlage zu diesem Tätigkeitsbericht).

Anhang Nr. 1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Januar 1986 zu den „Sicherheits- und Datenschutzgesetzen"

Die Datenschutzbeauftragten erinnern an ihre Entschließungen zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts, zur Einführung eines maschinenlesbaren Personalausweises und zur Datenverarbeitung bei Polizei und Verfassungsschutz. Sie stellen fest, daß die angekündigten „Sicherheits- und Datenschutzgesetze" den von Ihnen erhobenen Forderungen nur unzureichend Rechnung tragen und den Vorgaben des Bundesverfassungsgerichts nur teilweise entsprechen. Die geplanten Regelungen haben erhebliche Konsequenzen für die Datenverarbeitung in den Ländern und präjudizieren die Landesgesetzgeber in vielerlei Hinsicht.

Die Datenschutzbeauftragten sehen sich zu folgender ersten Bewertung veranlaßt:

1. Zum Bundesdatenschutzgesetz (siehe gesonderte Anlage)
2. Zum Personalausweisgesetz und Paßgesetz
   - Die Einführung des maschinenlesbaren Ausweises verändert entscheidend die Bedingungen, unter denen Informationen über die Bürger im Sicherheitsbereich erhoben und verarbeitet werden. Mit seiner Hilfe soll die Polizei vorhandene Dateien automatisiert abrufen und abgleichen sowie neue Datensammlungen anlegen können. Der behauptete Sicherheitsgewinn ist bis heute nicht dargetan.
   - Darüber hinaus fehlt es an bereichsspezifischen Gesetzen, die den Umgang der Sicherheitsbehörden mit dem Ausweis regeln, wie sie auch der Deutsche Bundestag in seiner Entschließung vom 17.1.1980 gefordert hat. Die jetzt diskutierten Begleitgesetze einschließlich der Ergänzung der Strafprozeßordnung genügen den Anforderungen nicht. Dies gilt umso mehr, als auch unverdächtige Bürger betroffen sind.
   - Die Gefahren wachsen, wenn die gleichzeitig beabsichtigte automatisierte Nutzung des Verkehrszentralregisters in der vorgesehenen Form verwirklicht und der Datenverbund der Sicherheitsbehörden untereinander weiter ausgebaut wird.
3. Zum Bundesverfassungsschutzgesetz

   Auch für den Verfassungsschutz gilt, daß seine Aufgaben im Gesetz klar in einer für den Bürger nachvollziehbaren Weise zu beschreiben sind. Gerade weil seine Tätigkeit weitgehend im Geheimen stattfindet, müssen die Bürger die Gewißheit haben, daß der Verfassungsschutz an eindeutige, eng umrissene und abschließend geregelte Aufgaben und Befugnisse gebunden ist. Der vorliegende Entwurf verfehlt dieses Ziel. Weitere Mängel kommen hinzu:
   - Dem Bürger kann nach wie vor jegliche Auskunft verweigert werden.
   - Es fehlen gesetzliche Fristen für die Löschung gespeicherter Daten.
   - Dem Verfassungsschutz darf nicht das Recht zugestanden werden, in jedes amtliche Datenregister Einblick zu nehmen und jede Art von Daten anzufordern. Im Gesetzentwurf sind davon nicht einmal Gesundheits- und Steuerdaten ausgenommen.
   - Während sich das nachrichtendienstliche Informationssystem (NADIS) bisher nur auf die Speicherung von Aktennachweisen beschränkte, sollen nach dem Gesetzentwurf auch Textzusätze über den Bürger automatisiert den Nachrichtendiensten bundesweit zur Verfügung stehen. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen.
4. Zur Zusammenarbeit von Nachrichtendiensten und Polizei
   - Die rechtsstaatlichen Grenzen der Zusammenarbeit von Nachrichtendiensten und Polizei werden durch das Trennungsgebot bestimmt. Das Trennungsgebot erschöpft sich nicht in einer bloßen organisatorischen Trennung zwischen Nachrichtendiensten und Polizei. Gerade wegen der automatisierten Datenverarbeitung kommt es mindestens ebenso auf eine strikte Trennung der Informationsbestände an. Das Trennungsgebot darf nicht durch einen umfassenden Inforamtionsaustausch unterlaufen werden.
   - Im übrigen darf eine Zusammenarbeit zwischen Polizei, MAD, Verfassungsschutz und BND erst erfolgen, wenn für die einzelnen Dienste eindeutige auch den Datenschutz sichernde Rechtsgrundlagen geschaffen sind.

Anhang Nr. 2

Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zur Änderung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten beurteilen den Entwurf zur Novellierung des Bundesdatenschutzgesetzes (Drucks. 10/4737) nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts, den Notwendigkeiten, die sich aus der technischen Entwicklung der Informationsverarbeitung ergeben, und den Forderungen, die sie bereits in früheren Entschließungen formuliert haben. Sie messen ihn auch an der Erklärung der Bundesregierung, den Datenschutz im Interesse der Bürger zu verbessern und die Datenverarbeitung transparenter zu gestalten.

Die Datenschutzbeauftragten stellen fest, daß der Entwurf zwar Verbesserungen enthält (I), insgesamt die Erwartungen jedoch nicht erfüllt (II). Sie bemängeln insbesondere die Beschränkungen des Gesetzes auf Dateien, die Ausklammerung der Datenerhebung, die unzureichenden Kontrollbefugnisse des Datenschutzbeauftragten und die unbefriedigenden Regelungen für den nicht-öffentlichen Bereich.

I.

1. Die Klarstellung, daß Datenschutz weder Schutz von Daten noch ausschließlich Schutz vor Mißbrauch, sondern Schutz des Bürgers vor Verletzungen seines Persönlichkeitsrechts ist, wird begrüßt.

2. Einige der vorgesehenen Änderungen entsprechen Forderungen, die die Datenschutzbeauftragten immer wieder erhoben haben. Das gilt – unbeschadet noch notwendiger Verbesserungen in Einzelheiten – für
   - die Einführung eines verschuldensunabhängigen Schadensersatzanspruchs, auch für Nichtvermögensschäden,
   - die Aufnahme einer Regelung der Datenverarbeitung für wissenschaftliche Zwecke,
   - die Abschaffung der Entgeltpflicht für die Auskunft über die eigenen Daten und die Ausdehnung der Auskunft auf Herkunft und Empfänger der Daten,
   - die Pflicht zur Löschung von Daten, die für den Speicherungszweck nicht mehr erforderlich sind,
   - die gesetzliche Anerkennung der Zweckbindung personenbezogener Daten,
   - die Klarstellung, daß Geheimhaltungsvorschriften der Kontrolle durch den Bundesbeauftragten nicht entgegengehalten werden können,
   - die Verstärkung der Befugnisse der Aufsichtsbehörden für den nicht-öffentlichen Bereich und der Stellung des betrieblichen Datenschutzbeauftragten.

II.

Einzuwenden ist gegen den Entwurf vor allem:

1. Ein gravierender Mangel ist bereits die Beschränkung auf die Datenverarbeitung in Dateien, die schon in der neuen Gesetzesbezeichnung zum Ausdruck kommt und den gesamten Entwurf prägt (§ 1 Abs. 1). Das Recht auf informationelle Selbstbestimmung umfaßt jeden Umgang mit personenbezogenen Daten. Die dem Volkszählungsurteil folgende Einbeziehung der Datennutzung bleibt weitgehend wirkungslos, weil nur die Nutzung unmittelbar aus Dateien gewonnener Daten geregelt wird. Die zunehmende Verknüpfung von Akten-, Text- und Datenverarbeitung wurde ebensowenig berücksichtigt wie z. B. neue Formen der Bildverarbeitung, etwa durch Videoaufzeichnungen. Im übrigen ist auch der neue Dateibegriff zu eng.

2. Neue Vorschriften im Verwaltungsverfahrensgesetz des Bundes über den Schutz personenbezogener Daten bei ihrer Verarbeitung außerhalb von Dateien gleichen die Nachteile des auf Dateien beschränkten Anwendungsbereichs des BDSG nicht aus, zumal nach § 19 Abs. 1 ihre Einhaltung nur begrenzt kontrollierbar ist. Außerdem gilt das Verwaltungsverfahrensgesetz im Gegensatz zum BDSG nicht umfassend, sondern von seinem Anwendungsbereich sind große und wichtige Verwaltungsbereiche und -tätigkeiten, wie Finanzverwaltung, Post, Strafverfolgung, Verfolgung von Ordnungswidrigkeiten und weite Bereiche der Sozialverwaltung ausgenommen, ebenso die privatrechtliche Betätigung der öffentlichen Hand. Auch im nicht-öffentlichen Bereich bleibt die Datenverarbeitung außerhalb von Dateien ungeregelt.

3. Der BDSG-Entwurf enthält keine ausdrückliche Regelung der Datenerhebung, obwohl gerade die Erhebung den Bürger unmittelbar belastet. Kein ausreichender Ersatz ist die Erhebungsvorschrift im Verwaltungsverfahrensgesetz. In ihr fehlt zudemdie Verpflichtung der erhebenden Stelle, den Erhebungszweck ausdrücklich festzulegen, an den die gesamte weitere Verarbeitung und Nutzung grundsätzlich gebunden ist. Er müßte dem Betroffenen auch mitgeteilt werden, um ihm Kenntnis darüber zu verschaffen, wer was wann und bei welcher Gelegenheit über ihn weiß.

4. Die weitgehende Ausklammerung „interner Dateien" ist nicht hinnehmbar (§ 1 Abs. 3). Es ist verfassungsrechtlich bedenklich, die interne Datenverarbeitung von jeglicher Kontrolle durch die Betroffenen, die Datenschutzbeauftragten und die Aufsichtsbehörden freizustellen.

5. Da das Gesetz jede Datenverarbeitung zuläßt, wenn die Einwilligung des Betroffenen vorliegt, muß der Gesetzgeber durch besondere Regelungen den Betroffenen davor schützen, daß er durch soziale, wirtschaftliche und psychische Zwänge (etwa als Mieter, Patient oder Arbeitsuchender) in seiner Entscheidungsfreiheit unangemessen eingeschränkt wird.

6. Die Regelung für die Datenverarbeitung zu Zwecken der wissenschaftlichen Forschung (§ 3 a) weist noch eine Reihe von Mängeln auf. Der Vorrang der Berufs- und besonderen Amtsgeheimnisse muß klargestellt werden. Auch muß – nach dem Vorbild des Sozialgesetzbuchs – ein Forschungsgeheimnis aufgenommen werden, das den Betroffenen vor jeder zweckfremden Nutzung der für ein Forschungsvorhaben zur Verfügung gestellten Daten schützt.

7. Der zunehmende Ausbau von Datenverarbeitungsnetzen und der vermehrte Einsatz von Kleincomputern (PC) erfordern weitere gesetzliche Maßnahmen zur Gewährleistung der Transparenz und der Kontrollierbarkeit dieser Datenverarbeitungsformen. Die unveränderte Übernahme von § 6 und dessen Anlage vernachlässigt den Einfluß neuer Technologien auf die automatisierte Datenverarbeitung.

8. Die Regelung für automatisierte Abrufverfahren (Online) (§ 6a) weist Mängel auf. Die inhaltlichen Anforderungen an die Zulassung solcher Verfahren sind weiter zu präzisieren. Die Risiken, die in der möglichen Selbstbedienung des Datenempfängers liegen, müssen zumindest durch wirksame Kontrollmechanismen gemindert werden. In der öffentlichen Verwaltung ist die Einführung von Online-Verfahren jedenfalls in besonders sensiblen Bereichen unter den Vorbehalt einer Rechtsvorschrift zu stellen.

9. Die Datenspeicherung sollte grundsätzlich nur für den bei der Erhebung festgelegten Zweck zugelassen werden, der dem Betroffenen bekanntzugeben ist (§ 9). Der Katalog erlaubter Zweckänderungen ist zu weit; soweit zweckfremde Datenspeicherungen und -nutzungen zugelassen werden, müßten sie den Betroffenen mitgeteilt oder in anderer Weise transparent gemacht werden. Das gilt auch für Datenübermittlungen, sofern damit eine Zweckänderung verbunden ist.

10. Das Recht des Bürgers auf Auskunft über seine Daten (§ 13) muß Herkunft und Empfänger umfassen, auch wenn diese Informationen nicht in Dateien gespeichert sind. Das Auskunftsrecht darf im übrigen nicht dadurch geschmälert werden, daß Nachrichtendienste ohne Verpflichtung zur Interessenabwägung im Einzelfall und ohne Begründung die Auskunft verweigern dürfen.

11. Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz (BfD) wird – gemessen auch an der gegenwärtigen Kontrollpraxis – insgesamt dadurch verschlechtert,
    - daß eine Kontrolle der Einhaltung „anderer Vorschriften" über den Datenschutz bei einer Datenverarbeitung außerhalb von Dateien nur noch dann möglich ist, wenn durch eine Beschwerde oder auf andere Weise Anhaltspunkte für eine Rechtsverletzung vorliegen,
    - daß in solchen Fällen systematische Kontrollen des BfD – z. B. im Sozialleistungsbereich – entgegen der bisherigen Praxis ausgeschlossen sind, weil die Kontrolle auf den Einzelfall beschränkt wird,
    - daß die Formulierung in § 19 Abs. 1 Satz 1, wonach die Kontrolle der Behörden „unbeschadet ihrer fachlichen Beurteilung und Verantwortlichkeit" stattfindet, von den kontrollierten Stellen so verstanden werden könnte, als ob eine Datenverarbeitung künftig nicht mehr inhaltlich, z. B. nicht mehr auf ihre Erforderlichkeit, überprüft werden kann,
    - daß die Datenerhebung selbst dann nicht mehr kontrollierbar ist, wenn sie zur Dateispeicherung führt, weil sie nicht mehr im BDSG geregelt wird und auch nicht als Datenverarbeitung oder Nutzung im Sinne des § 19 Abs. 1 Nr. 1 und 2 gilt,
    - daß nach § 19 Abs. 5 Satz 3 Nr. 1 personenbezogene Daten durch besonderes Gesetz von der Kontrolle ausgenommen werden können, obwohl es nach dem Volkszählungsurteil keine kontrollfreien Räume geben darf,
    - daß nach § 19 Abs. 5 Satz 3 Nr. 2 personenbezogene Daten, die bei Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses nach dem G 10 anfallen, der Datenschutzkontrolle grundsätzlich entzogen sind, obwohl das Bundesverfassungsgericht im Beschluß vom 20. Juni 1984 die Kontrolle durch Datenschutzbeauftragte zur Voraussetzung für die Zulässigkeit solcher Maßnahmen erklärt hat.

    Schließlich ist festzustellen:
    - § 19 Abs. 5 Satz 3 Nr. 3 muß gestrichen werden, da es für die Datenschutzbeauftragten selbstverständlich ist, das informationelle Selbstbestimmungsrecht bei der Kontrolle zu wahren und die geplante Regelung dazu führen kann, die Datenschutzkontrolle nachhaltig zu erschweren.
    - Die Klarstellung, daß (bundesrechtliche) Berufs- oder Amtsgeheimnisse der Datenschutzkontrolle nicht entgegengehalten werden können, muß auch die Kontrolle durch die Landesbeauftragten für den Datenschutz einbeziehen.
    - Es fehlt eine zum Teil in früheren Gesetzentwürfen vorgesehene Verpflichtung der Behörden, den BfD über Planungen wichtiger Automationsvorhaben zu unterrichten und bei datenschutzrelevanten Gesetzgebungsvorhaben zu beteiligen.

12. Die Datenschutzvorschriften für den nicht-öffentlichen Bereich orientieren sich nicht am Grundsatz der Zweckbindung und räumen verfassungsrechtlich bedenkliche Verarbeitungsprivilegien ein. So kann die Personengruppe, über die listenmäßig bestimmte Daten übermittelt werden dürfen, beliebig festgelegt werden (§ 24 Abs. 1 Nr. 3). Für Zwecke der Markt- und Meinungsforschung und der Werbung können auch Vertragsdaten, beispielsweise aus einem Arbeitsverhältnis, ohne Einwilligung des Betroffenen und ohne Rücksicht auf seine schutzwürdigen Belange listenmäßig übermittelt werden.

13. Die Auskunft an den Betroffenen über seine Daten muß auch im nicht-öffentlichen Bereich den Speicherungszweck umfassen (§ 26). Gleiches gilt für die Benachrichtigung über die erstmalige Speicherung von Daten. Über Herkunft und Empfänger ist auch dann Auskunft zu erteilen, wenn diese Angaben nicht in Dateien gespeichert sind.

14. Der Empfänger übermittelter Daten muß strenger an den Übermittlungszweck gebunden werden. Zweckfremde Nutzungen dürfen nicht schon dann zulässig sein, wenn der Nutzer keinen Grund zur Annahme sieht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 24 Abs. 3).

15. Die Datenschutzbeauftragten halten eine Ergänzung des BDSG um Sonderregelungen für den Adreßhandel für erforderlich.

16. Im übrigen erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen nicht nur für den öffentlichen, sondern auch für den nicht-öffentlichen Bereich. Hierzu zählen insbesondere Regelungen für die Verarbeitung von Arbeitnehmerdaten sowie für den Kredit- und Versicherungsbereich.

Anhang Nr. 3

Datensicherungsmaßnahmen beim Einsatz von Personal Computern

Bevor auf die Sicherungsmaßnahmen von Personal Computern näher eingegangen wird, empfiehlt es sich die Einsatzart dieser Geräte zu betrachten und die damit verbundenen Risiken aufzuzählen. Personal Computer gehören wegen ihrer vielfältigen Verwendungsmöglichkeiten an den Arbeitsplatz des Sachbearbeiters, deshalb ist es nicht einfach, sie gegen unberechtigten Zugang zu sichern.

In den Betriebssystemen dieser kleinen DV-Anlagen existiert nur in Ausnahmefällen ein Zugriffskontrollsystem, ein Protokollierungsfeature fehlt nahezu überall; der Benutzer des Personal Computers ist meist Bediener, Systemprogrammierer, Dateiverwalter, Programmierer (Auftragnehmer) und Auftraggeber in einer Person.

1. Betriebsarten des Personal Computers

1.1 Single-User-Betrieb, ausschließliche Nutzung durch ein und dieselbe Person

1.2 Multi-User-Betrieb,
mehrere Benutzer benützen ein und denselben Personal Computer

a) nacheinander (Einzelplatzsystem) oder

b) gleichzeitig (Mehrplatzsystem).

1.3 Der Personal Computer kann als Ein- oder Mehrplatzsystem mit anderen Geräten über Leitungen vernetzt werden:

- in einem inhouse-Netz,
- durch einen Anschluß an den Großrechner (Emulation von Terminalfunktionen) oder
- durch Anschluß an beliebiges System über Akustikkoppler, Fernsprechapparat und Fernsprechnetz.

2. Besondere Risiken beim Einsatz von Personal Computern

Manche Eigenschaften der Personal Computer bieten zwar Vorteile, die bei intensiver Betrachtungsweise aber auch Risiken beinhalten, wie

- die Miniaturisierung der Bauteile, inbesondere der peripheren Speichermedien erleichtert das mißbräuchliche Kopieren von Datenbeständen,
- die Vernetzung mit Rechnern ein gezieltes Abhören der Leitungen gestattet und
- Möglichkeiten die Hardware z. B. durch Adapterkarten zu verändern.

Die Vielfachverwendbarkeit und die leichte Handhabung dieser Geräte erzeugt unter Umständen zusätzliche technische und organisatorische Risiken, wobei es durchaus systembedingte Unterschiede gibt:

- Fehlen von Eingabe- und Zugriffsberechtigungsprüfungen
- Unzureichende maschinelle Protokollierungseinrichtungen
- Bedienung der Personal Computer durch wenig geschultes Personal
- Arbeiten mit selbstentwickelten Programmen, die keiner Kontrolle unterzogen und mangelhaft ausgetestet wurden.
- Arbeiten mit wenig erprobter Software (Fehlen von Prüf- und Abstimmungsroutinen, von aussagefähigen Fehlerlisten)
- Mangelhafte Dokumentation der Programme und Verfahren
- Wiederauffinden logisch gelöschter Daten
- Zweckentfremdung

Probleme können auch bei der Wartung der Hardware auftreten. Unter Umständen müssen Geräte incl. der Daten zur Reparatur an die Wartungsfirma oder an den Hersteller gesandt werden.

Schließlich gibt es auch beim ordnungsgemäßen Betrieb eine Reihe technischer Probleme, die Risiken beinhalten können, wie

- die Aussendung einer kompromittierenden Abstrahlung von Bildschirmen, Druckern und Leitungen,
- die Empfindlichkeit gegenüber Stromausfällen und
- Fehlende Systemeigenschaften bezüglich
  - Benutzerberechtigungsprüfung
  - Zugriffsberechtigungsprüfung
  - Protokollierung der Systembenutzungen.

3. Mißbrauchsmöglichkeiten von Personal Computern

3.1 Single-User-Betrieb

Mißbrauchsmöglichkeiten durch Benutzer:

- Gerät kann zweckentfremdet eingesetzt werden (Diebstahl von Rechenzeit)
- Unzulässige Verarbeitung und Datenspeicherung
- Entfernung vom Arbeitsplatz (Mitnahme in die eigene Wohnung)
- Daten- und Programmanipulation
- Daten- und Programmdiebstahl
- Selbstzerstörung der Programme nach unbefugtem Kopieren
- Veränderungen der Hardware

Mißbrauchsmöglichkeiten durch Dritte:

- Unzulässige Nutzung des Gerätes
- Unzulässiger Datenzugriff
- Daten- und Programmanipulation
- Zerstörung der Programme
- Zerstörung des Gerätes und der Datenträger
- Diebstahl der Programme und Daten
- Diebstahl oder zeitweises Entwenden des Gerätes und der Datenträger

3.2 Mehrplatzsystem unvernetzt (Multi-User-Betrieb)

Hier gelten im wesentlichen dieselben Mißbrauchsmöglichkeiten, wie sie unter 3.1 aufgeführt wurden. Als zusätzliche Mißbrauchsmöglichkeit durch den Benutzer kommt der Zugriff auf Daten anderer Benutzer hinzu.

3.3 Netzbetrieb

Mißbrauchsmöglichkeiten durch Benutzer:

- Daten- und Programmanipulation
- Unzulässige Verarbeitung und Datenspeicherung
- Daten- und Programmdiebstahl
- Selbstzerstörung der Programme nach unbefugtem Kopieren
- Diebstahl von Rechnerkapazität
- Anschluß an nicht zugelassene Rechner
- Datenübertragung an nicht zugelassene Rechner
- Unberechtigte Zugriffsversuche in anderen Systemen
- Zweckentfremdete Nutzung von aus dem Host übertragenen Daten (Filetransfer)
- Unzulässige Anwendung bestimmter Verfahren (Btx, Teletex etc.)
- Versand falscher Nachrichten

Mißbrauchmöglichkeiten durch Dritte:

- Unzulässige Nutzung des Gerätes
- Unzulässiger Datenzugriff
- Daten- und Programmanipulation
- Bewußte Zerstörung der Programme und Daten
- Zerstörung des Gerätes und der Datenträger
- Diebstahl der Programme und Daten

- Diebstahl des Gerätes und der Datenträger
- Abhören und Löschen von Nachrichten
- Abhören der Kommunikation in einem lokalen Netzwerk (local area network)

4. Sicherungsmaßnahmen

Bei der Beschaffung ist darauf zu achten, daß in Abhängigkeit von der späteren Verwendung gewisse Mindestanforderungen für Datensicherungsmaßnahmen gegeben sind.

4.1 Single-User-Betrieb

Gegen die Mißbrauchsmöglichkeiten des Benutzers gibt es folgende technische, vor allem aber organisatorische Datensicherungsmaßnahmen:

- Kopierschutz für Daten und Programme
- Belehrung und Schulung der Benutzer
- Erlaß einer Dienstanweisung für den Einsatz und Betrieb des Personal Computers
- Vorgabe der zu verwendenden Programme
- Verbot selbst Programme zu erstellen
- Verhinderung des Anschlusses von Datenfernverarbeitungs-Hardware (Akustikkoppler)
- Unangemeldete und in unregelmäßigen Zeitabschnitten durchgeführte Kontrollen, mit dem Ziel die Verarbeitung und den Inhalt der Datenträger zu überprüfen.
- Dokumentationsrichtlinien
- Standardvorgaben bei der Software (Menuetechnik, Bedienerführung)
- Ausgabe von Kontrollsummen bei der Verarbeitung und Kontrolle des Fehlerprotokolls.

Gegen Dritte:

- Aufbewahrung des Personal Computers in einem verschließbaren Sicherheitscontainer
- Absicherung des Raumes gegen Zutritt Unbefugter
- Aufbewahrung der Datenträger in einem besonderen Sicherungsschrank
- Abschließen der Tastatur
- Kopierschutz für Daten und Programme
- Verschlüsselung von Daten und Programmen
- Absperren der Diskettenlaufwerke
- Verbot, die Geräte an allgemein zugänglichen Stellen aufzustellen.

4.2 Multi-User-Betrieb

Gegen Benutzer (soweit die Funktionen vom System unterstützt werden):

- Verwendung von Paßworten
- Verschlüsselung von Daten und Programmen
- Kopierschutz für Daten und Programme
- Ein Systemverantwortlicher verwaltet die Paßworte und sichert den unberechtigten Zugriff auf die Paßwort-Datei durch ein „Master-Paßwort" ab.
- Jeder Benutzer benutzt seine eigenen Datenträger und ist für deren sichere Aufbewahrung zuständig.

Ansonsten sind die bei 4.1 aufgezählten Maßnahmen zu beachten.

Gegen Dritte:

- Aufbewahrung des Personal Computers in einem verschließbaren Sicherheitscontainer
- Absicherung des Raumes/Gebäudes gegen Zutritt Unbefugter
- Aufbewahrung der Datenträger in Sicherungsschränken, die in anderen Räumen stehen.
- Abschließen der Tastatur
- Kopierschutz von Daten und Programmen
- Verschlüsselung von Daten und Programmen
- Maschinelle Protokollierung aller unzulässigen Zugriffsversuche
- Auswertung des Zugriffskontroll-Loggings
- Physikalische Löschung nicht mehr benötigter Dateien.

4.3 Netzbetrieb

Gegen Benutzer:

- Jeder Benutzer erhält sein eigenes Paßwort.
- Bestimmung eines Systemverantwortlichen, der die Paßworte sicher verwaltet und den unberechtigten Zugriff auf die Paßwortdatei durch ein „Masterpaßwort" absichert.
- Jeder Benutzer benutzt seine eigenen Datenträger und ist für deren sichere Aufbewahrung zuständig.
- Protokollierung der Benutzung des Großrechners im Betriebssystem des Großrechners
- Identifikations- und Authentifikations-Prozeduren am Großrechner
- Definition des Rechneranschlusses, Protokollierung der Rufnummer des Rechners bei Wählverbindung
- System- und Programmänderungen bleiben ausschließlich privilegierten Benutzern vorbehalten.
- Einführung von Normen für Kommunikation und Benutzung (Menuetechnik, transaktionsorienterte Verarbeitung)
- Festlegung und Normierung der Benutzung der Postdienste
- Kontrolle der Anschlußzeiten an andere Systeme (z. B. Btx)
- Allgemein verwendbare Programme sind dezentral nur im Objektcode vorzuhalten, damit keine Veränderungen vorgenommen werden können; die Programmpflege erfolgt zentral.
- Einschränkung des Funktionsumfanges
- Keine Zulassung beweglicher Datenträger

Auch hier sind die unter 4.1 beschriebenen Maßnahmen zu beachten.

Gegen Dritte:

- Aufbewahrung des Personal Computers in einem verschließbaren Sicherheitscontainer
- Absicherung des Raumes/Gebäudes gegen Zutritt Unbefugter

- Sicherung der Paßworte
- Aufbewahrung der Datenträger in anderen Räumen und sicheren Schränken
- Einsatz von intelligenten Chip-Karten zur Zugangssicherung
- Abschließen der Tastatur
- Automatische Abmeldeprozedur bei längerem Inaktivsein
- Sperren der Wählleitungen
- Absichern der Anwendungen (z. B. Btx) durch Paßworte
- Verschlüsselung von Daten und Programmen
- Maschinelle Protokollierung aller unzulässigen Zugriffsversuche
- Auswertung des Loggings bezogen auf den Zugriff bestimmter Verfahren und Dateien.

Anhang Nr. 4

Arbeitskreis: „Technische und organisatorische Datenschutzfragen"

Risiken und Chancen der Bürokommunikationssysteme in der öffentlichen Verwaltung
Stand: 2.4.1986

1. Definition und Leistungsspektrum eines Bürokommunikationssystems

   Bürokommunikationssysteme (BKS) sind lokale Kommunikationsnetze, an die eine Vielzahl unterschiedlicher Terminals – z. B. Bildschirme, Fernkopierer, Telefonapparate – online angeschlossen sind. Es handelt sich also um Local Area Networks (LAN), wie etwa HICOM der Siemens AG, die auf Großrechnern im Teilhaberbetrieb laufende Basis-Software DISOSS der IBM, aber nicht über öffentliche Leitungen betriebene Systeme für Heimarbeiter. Die Übertragungskapazität kann schmalbandig (z. B. DISOSS mit 9600 bit/s; HICOM mit 144 kbit/s) oder breitbandig (Glasfaser-ISDN mit 2 Mbit/s) sein.

   Technisch besonders weit entwickelte BKS verfügen über Multifunktionsterminals, mit denen die Bürobediensteten
   - auf Großrechnern laufende interne und externe Informationssysteme nutzen,
   - Telefongespräche führen,
   - Btx-Angebote abrufen,
   - Dateien und Register einrichten, bearbeiten, versenden und empfangen sowie
   - Grafiken und Texte erstellen, ausdrucken, empfangen, versenden und archivieren können.

   Ein wichtiger Bestandteil der BKS sind Geräte, die ohne aufwendige manuelle Dateneingabe Schriftstücke jeder Art automatisiert lesen. Der Markt bietet dafür Scanner und Vielschriftenleser. Scanner lesen ein Schriftstück als Bild. Geschriebener Text kann nur als Ganzes nur beschränkt weiterverarbeitet werden, insbesondere ist das automatisierte Suchen einzelner Worte nicht möglich, es sei denn, Suchkriterien werden gesondert erfaßt. Vielschriftenleser erkennen demgegenüber jedes Zeichen und setzen es einzeln in einen Code um, den ein Programm beliebig weiterverarbeiten kann. Suchen nach Worten und Wortbestandteilen ist dann ebenso problemlos möglich, wie das Einfügen neuen Textes mit anschließendem Umformatieren. An solche BKS sind außerdem Teletex-Einrichtungen und große Datenspeicher für das elektronische Archiv angeschlossen. Das Breitbandnetz eines BKS hat zudem Schnittstellen zu den Postnetzen (Fernschreiben, Datex-L/P, HfD).

   Beispiel für Bürokommunikationssysteme:
   - HICOM der Siemens AG auf ISDN-Basis
   - System M32 der Triumph Adler AG
   - DISOSS (Distributed Office Support System) der IBM mit DIA (Document Interchange Architecture)/DCA (Document Content Architecture)/SNADS (SNA Distribution Services)
   - Das Token-Ring-Konzept der IBM zur Vernetzung insbesondere von PCs
   - das SNA-kompatible KINET von Mannesmann-Kienzle
   - LANs von Ericsson, Wang, XMIT GmbH Düsseldorf, Telenorma, Olivetti, NCR und anderen.

2. Arbeitsweise eines Bürokommunikationssystems

   Derzeit gibt es in der Verwaltung unterschiedliche Zuständigkeiten für Telefon, Schreibdienst, Büroorganisation und Datenverarbeitung. Die Folge davon sind Medienbrüche: Will man etwa den Text einer Fernkopie in die Textverarbeitung des Schreibdienstes oder in die Datenverarbeitung aufnehmen, dann ist der gesamte Text neu zu erfassen, weil die Geräte nicht kompatibel sind. Bei den künftigen Bürokommunikationssystemen soll dieser Zwischenschritt entfallen:

   Eingehende Post wird mit einem Vielschriftenleser oder Scanner in das BKS eingelesen, sofern sie nicht schon unmittelbar maschinenlesbar übertragen wird. Danach ordnet man das eingelesene mit Datum/Uhrzeit, einer eindeutigen Dokumentennummer und evtl. der Kennung des Verantwortlichen der Poststelle versehene Dokument einem im BKS geführten Vorgang bzw. einer im elektronischen Archiv geführten Akte zu. Ist kein Vorgang und keine Akte vorhanden, kreiert das BKS einen neuen Vorgang bzw. eine neue Akte. Anschließend sendet es den Vorgang in den elektronischen Postkorb des zuständigen Bearbeiters. Dieser kann die Bearbeitung delegieren und sie zusammen mit beliebig vielen Kollegen durchführen. Dazu können die einzelnen Sachbearbeiter Hilfsmittel, z.B. Juris, Fachinformationsbanken, Btx-Datenbanken, usw. heranziehen, evtl. Umfragen unter Kollegen durchführen, lokal im Multifunktionsterminal geführte Handakten, Adreßregister oder sonstige Dateien auswerten und Telefonate führen. Alle dabei anfallenden Dokumente (formatfreie und formatgebundene Texte, Sprachinformation, Bilder, Grafik) gehören standardmäßig zum Vorgang. Am Ende der Bearbeitung steht ein Produkt, z.B. ein von einem oder mehreren Sachbearbeitern erstelltes Schreiben, das weiteren Mitarbeitern zugeleitet, an Externe versandt oder anderweitig (z.B. für die Wiedervorlage) verfügt wird.

Eine Reihe von Sicherheitsfunktionen ist dafür notwendig: Vorgänge dürfen nicht endlos lange unbearbeitet herumliegen oder hin- und hergeschoben werden. Eine Zeitüberwachung muß dies sicherstellen. Aus Gründen der Eingabekontrolle und zur Umsetzung der heute im manuellen Bereich üblichen Arbeitsweise bei Verfügungen, Mitzeichnungen, Schlußzeichnungen usw., ist festzuhalten, wer wann welche Dokumente oder Dokumententeile erstellte, änderte, löschte und wer für was verantwortlich ist. Zur Kontrolle des wirtschaftlichen Verhaltens der Behördenbediensteten könnte analog zur heutigen Gesprächsdatenerfassung festgehalten werden, wer wann in welchem Umfang zur Bearbeitung welchen Vorgangs welche kostenpflichtigen Dienste (Btx-Datenbank, Telefon, Fernkopierer, Teletex usw.) in Anspruch nahm.

Das Archiv des BKS enthält als Datenobjekte Akten, das sind Dokumente, die aus Sprach-, Text-, Bild- und Grafikteilen bestehen. Der Zugriff auf das Archiv ist üblicherweise möglich über

- Aktennummer
- Dokumentennummer
- Formatnummer (entsprechend der heutigen Formularnummer) von Dokumenten
- Attributen von Dokumenten (z.B. enthält Sprache, enthält Bild, usw.)
- Bearbeiterkennungen
- Eigennamen von Personen und Organisationen
- Datum des ersten Auftretens
- Wiedervorlagedatum
- bestimmte Stichworte und/oder Synonyme
- beliebige Worte und Wortteile.

3. Chancen und Risiken

3.1 Chancen

BKS können technisch so gestaltet werden, daß sie die Datensicherung im Vergleich zu den herkömmlichen Büros in einigen Punkten verbessern. Allerdings ist dies keine zwangsläufige Folge des Einsatzes von BKS, sondern im jeweiligen Einzelfall zu überprüfen.

3.1.1 Klare Definition der Verantwortlichkeit

Wenn BKS so gestaltet werden, daß jedes erstellte und bestimmten Akten zugeordnete Dokument (also alles außer Notizdokumenten) automatisiert unlöschbar und mit einer Sachbearbeiterkennung versehen wird, kann jederzeit leicht festgestellt werden, wer für welche Verarbeitungsvorgänge bei welchen Personendaten verantwortlich ist.

3.1.2 Keine fehlenden Akten oder Dokumente

Wenn das BKS die Bearbeitung der Vorgänge überwacht und alle bei der Bearbeitung von Vorgängen entstehenden Dokumente standardmäßig unlöschbar dem Vorgang zuordnet, können keine Informationen und Dokumente mehr verloren gehen. Unabhängig vom Bearbeitungsgang sind die Akten dann immer vollständig und zentral verfügbar.

3.1.3 Richtige Daten

Weil der Sachbearbeiter bei BKS die Daten selbst eingibt, entfallen Fehlermöglichkeiten, die heute durch die Verteilung der Datenerfassung auf mehrere Personen entstehen. Allerdings gibt es keine technischen Möglichkeiten, Sachbearbeiter zu sorgfältiger Dateneingabe zu zwingen.

3.1.4 Automatisierte Aussonderung

Das Löschen (Vernichten) von Akten ist einfach zu überwachen und durchzuführen, falls keine optischen Speichermedien verwendet werden. (Die heute auf dem Markt befindlichen optischen Speichermedien erlauben kein Löschen.) Die derzeitigen Schwachstellen bei der Vernichtung von Unterlagen entfallen.

3.1.5 Schnelles Auffinden von Vorgängen

Der schnelle Zugriff auf Akten und Dokumente im elektronischen Archiv verkürzt im Vergleich zum manuellen Verfahren die Suchzeiten erheblich. Neue Zugriffsmöglichkeiten kommen dazu. Insbesondere kann man auch Sprachinformationen und Grafiken suchen.

3.1.6 Verkürzung der Laufzeiten

Die herkömmlichen Botendienste entfallen. Akten und Dokumente transportiert das BKS in Sekunden zum zuständigen Empfänger. Die Zeit für das Erstellen von Kopien reduziert sich auf Sekunden: Kosten fallen praktisch keine an.

3.2 Risiken

Die bekannten Risiken der integrierten Datenverarbeitung treten auch hier auf. Neue Risiken entstehen durch die Vielfalt und Menge der zusätzlich automatisiert gespeicherten Informationen. Risiken entstehen auch, weil eine große Zahl bislang manuell bearbeiteter Daten in automatisierten Dateien gespeichert werden und im direkten Zugriff stehen und weil bei der Bearbeitung selbst weitere Daten anfallen. Deshalb fallen die bei manueller Bearbeitung zwangsläufig vorhandenen Nutzungsbeschränkungen weg. Für die Nutzung personenbezogener Daten durch die Behörde selbst bestehen im Datenschutzrecht kaum Regelungen, abgesehen von den Vorschriften über technische und organisatorische Maßnahmen (vgl. 3.2.2).

3.2.1 Auswertung des Archivs

Alles, was in Akten und Dokumenten steht, ist mit Ausnahme der von Scannern gelesenen Schriftstücke jederzeit nach beliebigen Kriterien inhaltlich auswertbar. Bislang getrennt zu einer Person verwaltete Vorgänge und Informationen können einfach zusammengeführt werden. Unabhängig davon, welche Abschottungsmechanismen in ein BKS integriert werden, sind diese umfassenden Auswertungs- und Verknüpfungsmöglichkeiten zumindest für zentrale Stellen der jeweiligen Behörden, etwa den Betreiber (Systemverwalter) des BKS, immer gegeben.

3.2.2 Kontrolle der Bediensteten

Die herkömmlich im Rahmen der Mitzeichnung bzw. Schlußzeichnung usw. anfallenden Informationen über die Bearbeitung eines Vorgangs können mit dem BKS

nicht nur wie bisher zur Feststellung, wer für was verantwortlich zeichnete, verwendet werden. Der Arbeits- und Leistungsprozeß der Bediensteten kann nämlich anhand dieser Informationen mit dem BKS einfach, schnell und oft festgestellt werden. Die Leistungsbeurteilung kann dann anhand einer Vielzahl gemessener Werte „objektiviert" werden. (Vgl. W. Fischer, E. Mundhenke, Informationstechnik im öffentlichen Bereich, Nomos, 1985, S. 49.). Das hat Vor- und Nachteile. Nachteile können für den Bediensteten etwa entstehen, weil eine lückenlose Speicherung des Arbeitsverhaltens eines Arbeitnehmers die freie Entfaltung seiner Persönlichkeit, auf die er auch am Arbeitsplatz Anspruch hat, behindern kann. Dieser Konflikt muß im Dienst- bzw. Arbeitsrecht etwa durch Mitbestimmungsregelungen gelöst werden.

Viele Informationen über die Leistung der Bediensteten beinhalten auch die bei der Abrechnung z. B. der Telefongespräche, der Btx-Abrufe, der Juris-Abrufe usw. anfallenden Daten und eine Reihe der Betriebsdaten (beispielsweise ist die Logon-Zeit in etwa die tägliche Arbeitszeit).

3.2.3 Unkontrollierbarkeit

Je mehr die Bediensteten Gelegenheit haben, eigene Register, Dateien, Aktensammlungen (z.B. elektronische Handakten) in beliebiger Größe und Format anzulegen, um so unkontrollierbarer wird die Arbeit einer mit einem BKS ausgestatteten Behörde. Schwierig und im Extremfall unmöglich wird es etwa, festzustellen, welche Personendaten überhaupt gespeichert sind, wer sie wie zu welchem Zweck verarbeitet und wer unbefugt von ihnen Kenntnis erhielt. Für die Behördenleitung wird es im Vergleich zu heute noch schwieriger zu verhindern, daß Mitarbeiter anstatt der richtigen offiziellen Akten unrichtige (weil unvollständige oder nicht aktualisierte) Handakten bei der Bearbeitung eines Vorgangs verwenden. Besondere Beachtung verdienen auch die enorm gesteigerten Möglichkeiten, neue – gefälschte – Dokumente zusammenzustellen, indem etwa die zu einem Dokument A gesprochene Mitteilung an ein Dokument B angebunden wird. Außerdem erhöht sich, etwa bei der Verarbeitung von Verschlußsachen, das Risiko, daß sehr einfach sehr große Datenmengen absichtlich unbefugt an Dritte weitergegeben werden können. Die Weitergabe kann dabei entweder durch Kopieren der Informationen auf Datenträger oder durch Versenden elektronischer Post erfolgen.

3.2.4 Abschottung

Derzeit ist kein System bekannt, in dem eine flexible abgestufte und individuell vergebbare Berechtigung realisiert ist. Diese Berechtigung muß sich u a. auf die Möglichkeiten, das Archiv zu durchsuchen, interne und externe Informationssysteme zu nutzen, Dateien anzulegen, zu empfangen, zu versenden, zu sichern und zu bearbeiten, Registraturverfügungen zu erlassen, Löschungen durchzuführen, Leistungsverhalten zu messen, beziehen.

3.2.5 Protokollierung

Derzeit ist nicht klar, wie bei einem BKS welche Datenverarbeitungsvorgänge (anonym oder personenbezogen) protokolliert werden könnten, um auch in großem zeitlichen Abstand wirksame Datenschutzkontrollen durchzuführen. Von besonderer Wichtigkeit sind Eingabe-, Transport- und Übermittlungskontrollen.

4. Technische Manipulationsmöglichkeiten

4.1 Unbefugtes Abhören

4.1.1 Abhören durch elektrische Induktion

Fast unabhängig von der Architektur des BKS ist ein Abhören aller im Ring oder Bus übertragenen Daten durch elektrische Induktion bei Kabelnetzen möglich, wenngleich dies je nach Anwendung extrem schwierig sein kann. Durch die Verwendung von Lichtwellenleitern läßt sich diese Gefahr weitestgehend beseitigen.

4.1.2 Abhören durch Zwischenschalten einer nicht berechtigten Datenstation

Diese Methode kann jemand anwenden, wenn er etwa alle an eine bestimmte Datenstation gehende Informationen bequem mitverfolgen will. Sie ist bei Bus-Systemen (etwa bei Ethernet und HICOM) erfolgreich, falls ein Busanschluß und ein kompatibles Gerät verfügbar sowie eine gültige Adresse bekannt ist. Bei Token-Protokollen im Ring-Netz kann diese Schwachstelle durch eine entsprechende Gestaltung des Protokolls beseitigt werden (vgl. F.H. Kauffels, Schwachstellen der Informationssicherheit in lokalen Netzen, Informatik-Fachbericht Nr. 113, Springer 1985, S. 61).

4.2 Unbefugtes Eingeben falscher Informationen

Die unter Nr. 4.1.2 beschriebene Methode erlaubt, aktiv (also auch schreibend) unbefugt am Datenverkehr des BKS teilzunehmen. Dieses Risiko läßt sich durch ein entsprechend gestaltetes Token-Protokoll vermeiden. Auch die Verwendung von HDLC/SDLC-Protokollen macht es sehr schwer, Nachrichten unbefugt in ein BKS einzuschleusen.

4.3 Unbefugtes Eindringen in Teilhabersysteme, die an BKS angeschlossen sind.

BKS erlauben i. d. R. mit den angeschlossenen Multifunktionsterminals die Verbindung zu zentralen Teilhabersystemen (z. B. automatisches Melderegister, INPOL) aufzubauen. Technisch geschieht dies etwa bei HICOM so, daß das Teilhabersystem ständig mit einer bestimmten Komponente des BKS, einem sog. Server, verbunden ist. Jedes Multifunktionsterminal kann diesen Server ansprechen und eine Verbindung zum Teilhabersystem anfordern. Damit keine unbefugten Zugriffe möglich sind, müssen das BKS und das Teilhabersystem aufeinander abgestimmte Zugriffskontrollen haben. Die Sicherheit hängt wesentlich von der Zugriffskontrolle des Zentralen Systems und seinen EDV-Verfahren ab. Diese können unterlaufen werden, wenn man den File-Transfer der im zentralen System gesicherten Dateien gestattet.