ACHTZEHNTER TÄTIGKEITSBERICHT

DES

LANDESBEAUFTRAGTEN FÜR DEN DATENSCHUTZ IN BADEN-WÜRTTEMBERG

LT-Drs. 12/2242

Zur Situation

Die Großwetterlage

Datenschutz ist derzeit kein Thema, das die Gemüter sonderlich bewegt und Schlagzeilen macht. So verständlich dies angesichts der Vielzahl aktueller drängender Probleme wie Arbeitslosigkeit, Leere der öffentlichen Kassen und Kriminalitätsbekämpfung ist, der realen Situation wird dieses Phänomen nur schwerlich gerecht. Denn die Gefahren, die dem von unserer Verfassung garantierten Recht der Menschen, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen, drohen, sind in der heutigen Zeit nicht etwa geringer geworden. Im Gegenteil: Die globalisierte Informationsgesellschaft, die zu einem guten Teil schon Realität ist, birgt Möglichkeiten der Beeinflussung und Ausforschung in sich, die nach Ansicht mancher Experten alle bisherigen Vorstellungen in den Schatten stellen. Viele sehen dabei den Datenschutz schon als klaren Verlierer. Auch wenn man diese Kassandrarufe für übertrieben hält, man muß sich mit dieser Problematik auseinandersetzen und nach Wegen suchen, wie die ständig ansteigenden, weltweiten Informationsströme kanalisiert und beherrschbar gemacht werden können. Zumindest im Bereich der Medien- und Teledienste hat der Gesetzgeber diese Herausforderung angenommen und sich bemüht, Möglichkeiten zur Stärkung des Datenschutzes zu finden. Das Telekommunikationsgesetz, das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag der Länder sehen Regelungen vor, die alles in allem zumindest auf dem Papier datenschutzgerechte Lösungen versprechen. Erwähnenswert ist dabei insbesondere, daß in diesem Bereich künftig der Grundsatz der Datensparsamkeit und die Forderung nach Bereitstellung anonymer Nutzungsformen Beachtung beanspruchen. Freilich, was im Gesetzblatt steht, ist noch lange nicht Realität. Das gilt gerade für diesen Bereich, in dem sich nicht nur die Technik, sondern mit ihr auch ihr Anwendungsbereich ständig fortentwickeln. Da zudem die Interessen derjenigen, die sich dieser neuen Medien, sei es als Betreiber, als Anbieter oder als Nutzer, bedienen wollen, keineswegs kongruent sind und auch nicht unbedingt mit den Intentionen des Gesetzgebers übereinstimmen, wird es sehr auf eine effektive Kontrolle ankommen. Ob das zu schaffen sein wird, ist aber die Frage. Schon jetzt haben sich, hervorgerufen durch die Gemengelage gesetzlicher Regelungen, immense Abgrenzungsprobleme gezeigt, die viele Juristen ins Brot setzen können. Das überaus differenzierte Kontrollsystem im Bereich des Datenschutzes mit dem von Land zu Land unterschiedlichen Nebeneinander von öffentlicher und privater Datenschutzkontrolle sowie von Bundes- und Landeszuständigkeiten tut ein übriges dazu, selbst Experten die Feststellung schwer zu machen, welche Kontrollinstanz wann für was zuständig ist.

Nicht umsonst gibt es bereits eine Arbeitsgruppe von Datenschutzkontrollinstanzen, die sich die Koordinierung zur Aufgabe gestellt hat. Doch schon jetzt ist fraglich, ob dieses Ziel erreicht werden kann: Eine Reihe von Aufsichtsbehörden für den nichtöffentlichen Bereich will sich, aus welchen Gründen auch immer, nicht daran beteiligen.

Kann man das, was im Multimedia-Bereich geregelt wurde, gleichwohl noch insgesamt positiv bewerten, erlauben andere Aktivitäten des Gesetzgebers diese Beurteilung leider nicht. So gerät die nach EU-Recht bis Oktober 1998 zwingend vorgeschriebene Umsetzung der EG-Datenschutzrichtlinie vom 24. Okt. 1995 in nationales Recht allmählich zum Trauerspiel. Obwohl wirklich genügend Zeit dafür gewesen wäre, haben es die beteiligten Bundesministerien noch nicht fertig gebracht, einen gemeinsamen Regierungsentwurf vorzulegen. Betrachtet man freilich das, was unter der Bezeichnung "Referentenentwurf" im Internet oder in anderen Medien zu lesen war, dann kann man sich schon fragen, ob es wirklich ein großes Unglück wäre, wenn sich die Anpassung noch weiter verzögert. Denn anstatt, wie auch von den Datenschutzbeauftragten des Bundes und der Länder gefordert, diesen Anlaß dazu zu benutzen, das deutsche Datenschutzrecht umfassend zu modernisieren, peilt man in Bonn bisher offensichtlich eine Minimallösung an und will nur das ändern, was unbedingt geändert werden muß. Aber selbst damit tut man sich noch schwer und denkt zudem viel zu wenig daran, daß das neue Bundesdatenschutzgesetz nicht nur von Juristen, sondern auch von normalen Bürgern gelesen und verstanden werden sollte. Bleiben wir gleichwohl Optimisten und hoffen, daß sich doch noch alles zum Guten wendet!

Bei einem Gesetzesvorhaben, das schon viele Jahre lang für lebhafte Auseinandersetzungen gesorgt hat, bei dem man jetzt aber den Eindruck haben muß, daß der Worte genug gewechselt sind und die Entscheidung jedenfalls im Grundsatz gefallen ist, hat sich diese Hoffnung nicht erfüllt: Ich meine die Zulassung des Großen Lauschangriffs. Als Datenschutzbeauftragter bedaure ich dies, weil der Staat damit Eingriffe in einen Bereich zuläßt, in dem der einzelne bisher noch weitgehend für sich bleiben und sich zurückziehen konnte, und dies, obwohl fraglich bleibt, ob damit ein nennenswerter Beitrag zur Bekämpfung der organisierten Kriminalität erzielt werden kann. Es geht dabei eben nicht nur um das Abhören von Gangsterwohnungen, wie das in der politischen Auseinandersetzung immer wieder auch von höchster Stelle behauptet wird, sondern um das Eindringen in Wohnungen sowohl von Verdächtigen, für die bis zum Urteil die Unschuldsvermutung zu gelten hat, als auch von völlig Unverdächtigen, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß sich dort ein Verdächtiger aufhält. Angesichts der politischen Konstellation in Bundestag und Bundesrat bleibt leider wohl nur noch zu hoffen, daß wenigstens in folgenden Punkten eine Nachbesserung vorgenommen wird:

- Der Straftatenkatalog, der den Großen Lauschangriff rechtfertigen soll, sollte auf besonders schwere Straftaten, die die Rechtsordnung nachhaltig gefährden, beschränkt werden. Der Entwurf zur Änderung der Strafprozeßordnung enthält Tatbestände, die dieser Qualifizierung nicht gerecht werden.
- Der Schutz der Berufsgeheimnisse, also des Beichtgeheimnisses, der ärztlichen Schweigepflicht, der Geheimhaltungspflicht der Anwälte u.ä. sollte gewahrt bleiben. Bisher fehlt dazu jede Regelung.
- Die Ergebnisse des Abhörens sollten tatsächlich nur in Strafverfahren verwendet werden dürfen, bei denen es um sog. Katalogstraftaten geht. Der Gesetzentwurf zur Änderung der Strafprozeßordnung läßt dem entgegen auch eine Verwendung als Ermittlungsansatz für alle anderen Straftaten zu.

Mit Sorgen müssen aber auch die Aktivitäten gesehen werden, die darauf abzielen, den Sozialdatenschutz auszuhöhlen. Nahezu unerschöpflich scheint der Einfallsreichtum von dazu Berufenen wie Unberufenen zu sein, wenn es darum geht, Maßnahmen vorzuschlagen, die eine mißbräuchliche Inanspruchnahme von Sozialleistungen, insbesondere aber von Sozialhilfeleistungen unmöglich machen sollen. Datenabgleiche selbst mit der Polizei, Sozialdetektive und anlaßunabhängige Einholung von Auskünften bei Dritten, all das und anderes mehr soll Sozialleistungsmißbrauch weitestgehend verhindern. So verständlich es ist, daß insbesondere die Kommunen unter der Last der ständig steigenden Sozialausgaben stöhnen und nach Wegen suchen, zweifellos vorhandene Mißbrauchsfälle zu verhindern, man sollte dabei nicht das Kind mit dem Bade ausschütten. Es gilt, den Grundsatz der Verhältnismäßigkeit nicht aus dem Auge zu verlieren und das auf ihm aufbauende sorgfältig austarierte Ermittlungsinstrumentarium des Sozialgesetzbuchs nicht zu zerstören.

Der Datenschutz im Lande

Auch im Berichtsjahr zeigte sich, daß bei den Behörden im Lande mit dem Datenschutz noch lange nicht alles im Lot ist. Meine Amtsvorgängerin, die frühere Landesbeauftragte für den Datenschutz Frau Dr. Ruth Leuze, hat in ihrem letzten Tätigkeitsbericht (LT-Drs. 11/6900, S. 108) das Fehlen einer Datenschutzkultur bei unseren Behörden moniert. Sie hatte damit recht und diese Klage ist auch heute noch berechtigt. Es muß nachdenklich stimmen, daß sich bei unseren 26 Kontroll- und Informationsbesuchen immer wieder die gleichen, in unseren Tätigkeitsberichten wiederholt beschriebenen Mängel zeigten. Noch viel zu oft stoßen wir bei der Bearbeitung von Bürgereingaben auf schlichtes Unverständnis, wenn wir Behörden auf die datenschutzrechtlichen Implikationen eines Falles hinweisen, für mich ein Zeichen dafür, daß

man sich bisher über Aufgabe, Ziele und Regelungsmechanismen des Datenschutzes keine oder aber nur sehr wenige Gedanken gemacht hat. Viele Mitarbeiter der öffentlichen Verwaltung sehen Datenschutz als ein Rechtsgebiet für Spezialisten an, mit dem sie nichts zu tun haben wollen, und begreifen nicht, daß Datenschutz integraler Bestandteil des jeweiligen Aufgabengebiets ist. Wer sich mit dem Ausländerwesen zu beschäftigen hat, erledigt seine Aufgabe eben nur dann korrekt, wenn er dabei die Regelungen über den Umgang mit den Ausländerdaten berücksichtigt, also Datenschutzrecht praktiziert. Ebenso gehört zum Sozialhilferecht nun auch einmal der Sozialdatenschutz. Beides läßt sich nicht isoliert voneinander sehen. Noch bedenklicher wird es, wenn man glaubt, die Anforderungen des Datenschutzes völlig vernachlässigen und Fragen der unabhängigen Datenschutzkontrolle mit Nichtachtung strafen zu können. Auch das gibt es. So blieb mir beispielsweise nichts anderes übrig, als gegenüber den Bürgermeisterämtern Villingen-Schwenningen und Philippsburg, aber leider auch gegenüber dem Innenministerium Beanstandungen auszusprechen, nachdem sie mein Amt wiederholt erfolglos zur Beantwortung von Fragen aufgefordert hatte. Daß auch sonst bei weitem nicht alles in Ordnung ist, kann man im übrigen auch diesem Tätigkeitsbericht entnehmen.

Es hieße allerdings, die Realität zu verfälschen, wollte man nur alles grau in grau sehen. Wir sind im Rahmen unserer Kontroll- und Beratungstätigkeit sehr wohl auch auf datenschutzbewußte Mitarbeiter und Mitarbeiterinnen in den Verwaltungen und sonstigen öffentlichen Stellen gestoßen, die sich zum Teil sehr große Mühe gaben, den datenschutzrechtlichen Anforderungen gerecht zu werden. Insbesondere im Bereich des technischen und organisatorischen Datenschutzes bestand große Bereitschaft, unseren Vorschlägen und Empfehlungen Rechnung zu tragen. Allerdings stießen wir dort auch häufig auf Mängel, die es eigentlich schon längst nicht mehr geben dürfte. Bei Kontrollbesuchen wurden wir durchweg freundlich aufgenommen und unsere Fragen soweit möglich beantwortet.

Alles in allem: Im Berichtsjahr erlebten wir nicht nur kaum mehr nachvollziehbare Verstöße und Mängel sowie Verständnislosigkeit gegenüber dem Datenschutz, sondern durchaus auch angenehme Überraschungen bei öffentlichen Stellen, denen attestiert werden konnte, daß Datenschutz für sie kein Fremdwort ist.

Zu warnen ist freilich, aus diesem Resümee voreilige Schlüsse zu ziehen. Dafür sind unsere Erfahrungen nicht repräsentativ genug, denn mit 14 Mitarbeiterinnen und Mitarbeitern, die im vergangenen Jahr in meinem Amt engagiert tätig waren, sind nun einmal nur punktuelle, oft von Zufällen abhängige Kontrollen möglich. Die Landkarte von Baden-Württemberg weist

deshalb noch viele weiße Flächen auf, wo noch nie eine Datenschutzkontrolle stattgefunden hat. Und darüber läßt sich dann auch nicht urteilen.

1. Teil: Technik

1. Datenschutz durch Technik

Ist derjenige, der die Segnungen der modernen Informations- und Kommunikationstechnik nutzen will, wirklich auch dazu verdammt, bei seinen Aktivitäten überall Spuren zu hinterlassen und damit am Ende zum gläsernen Menschen zu werden? Fast scheint es so. Wer nach alter Väter Sitte Briefe im verschlossenen Umschlag verschickt, Bücher und Zeitschriften mit Bargeld kauft und darin blättert, kann dies alles tun, ohne daß penibel aufgezeichnet wird, was er im einzelnen gemacht hat. Ganz anders liegen die Dinge bei der Nutzung der neuen Techniken. Wer elektronische Post verschickt, mit diversen Chipkarten bargeldlos bezahlt oder in Mobilfunknetzen telefoniert, muß in Kauf nehmen, daß sein Vorgehen so aufgezeichnet wird, daß detailliert nachvollzogen werden kann, mit wem er kommuniziert, was er gekauft oder wo er sich mit seinem Handy aufgehalten hat. Freilich: Wie viele und welche Datenspuren er hinterläßt, ist nicht naturgegeben und unabänderlich, sondern hängt sehr von der Ausgestaltung der eingesetzten Technik ab.

1.1 Datensparsamkeit tut not

In Zeiten, in denen die Nutzung weltweiter Datennetze oder von allerlei Arten von Chipkartensystemen für viele zur Selbstverständlichkeit geworden ist, reicht es zur Sicherung des Grundrechts auf Datenschutz nicht mehr aus, die bei der Nutzung der neuen Technik angefallenen personenbezogenen Daten möglichst vor Mißbrauch zu schützen. Allein schon angesichts der weltweiten Verflechtung von Datennetzen ist dies ein Ding der Unmöglichkeit. Statt dessen sollten die Systeme von vornherein so gestaltet werden, daß möglichst gar keine oder jedenfalls so wenig wie möglich personenbezogene Daten anfallen. Beschränkung auf das notwendige Minimum und damit Datensparsamkeit heißt also das Gebot der Stunde. Zwei Vorgehensweisen kommt dabei besondere Bedeutung zu:

- Die strengste Form der Datensparsamkeit ist die Datenvermeidung, die sicherstellt, daß bei der Nutzung der Technik überhaupt keine personenbezogenen Daten anfallen. Musterbeispiel dafür ist die herkömmliche Telefonkarte, die dem Inhaber ermöglicht, beim Bezahlen eines Telefongesprächs anonym zu bleiben. Eine solche anonyme Nutzung ist immer dann anzustreben, wenn es nicht notwendig ist, zu wissen, wer die Technik in Anspruch genommen hat.
- Eine weitere Möglichkeit, Datensparsamkeit zu praktizieren, besteht darin, die Angaben, die den Nutzer identifizieren können, durch ein sog. Pseudonym, das für sich allein keine Rückschlüsse auf den Nutzer erlaubt, zu erset-

zen. Der Vorteil ist der: Die Reidentifizierung ist nur dem möglich, der weiß, zu welcher Person welches Pseudonym gehört oder darüber informiert ist, auf welche Weise das Pseudonym gebildet wird. Für alle anderen bleibt der Nutzer anonym. Die Pseudonymisierung kommt immer dann in Frage, wenn es nur in Ausnahmefällen notwendig ist, seine Identität festzustellen.

1.2 Datenschutzfreundliche Technik - beileibe keine Utopie

Bereits heute bestehen Möglichkeiten, Technik datensparsam zu gestalten. Kryptographische Verfahren und Guthabenkarten zum Bezahlen spielen dabei häufig eine wichtige Rolle:

1.2.1 Elektronisches Bezahlen ohne Datenspuren

Bargeldlose elektronische Zahlungsformen gewinnen gegenüber dem Bargeld immer größere Bedeutung.

- In vielen Fällen bezahlt der Kunde mit einer Karte, sei es eine EC- oder eine Kreditkarte. Beim Bezahlen mit einer solchen Karte wird im Gegensatz zur Barzahlung häufig registriert, wer wann welchen Betrag an wen bezahlt hat. Doch es geht auch anders: Man kann zum Bezahlen auch Chipkarten mit einem Wertguthaben (Prepaid-Cards) einsetzen. Das auf einer solchen Karte gespeicherte Guthaben wird dabei bei jedem Kauf um den entsprechenden Kaufpreis reduziert. Der Verkäufer erfährt bei Verwendung einer solchen Chipkarte weder den Namen noch die Bankverbindung des Kunden und keinem Geldinstitut wird mitgeteilt, wann der Kunde welchen Betrag an wen ausgegeben hat. Voraussetzung für einen anonymen Einsatz dieser Karte ist, daß die mit einer Karte getätigten Käufe und Aufbuchungen nicht an zentraler Stelle, etwa unter einer Kartennummer, registriert werden und damit eine Reidentifizierung des Karteninhabers möglich ist.
- Um in elektronischen Kommunikationsnetzen wie dem Internet angebotene Dienstleistungen innerhalb des gleichen Netzes elektronisch bezahlen zu können, wurden inzwischen verschiedene Varianten für elektronisches Geld entwickelt. Bezahlt wird dabei durch Übertragung einer oder mehrerer elektronischer Dateien, die wie ein Geldschein oder eine Münze jeweils einen bestimmten Geldbetrag darstellen. Die Vertrauenswürdigkeit eines derartigen Zahlungsverfahrens setzt unter anderem voraus, daß sich durch bloßes Kopieren von Gelddateien das Guthaben nicht vervielfachen läßt. Außerdem müssen die Gelddateien gegen Verfälschung geschützt sein. Mittels kryptographischer Verfahren ist es möglich, elektronisches Geld zur

Verfügung zu stellen, das die genannten Anforderungen erfüllt und mit dem zugleich anonym bezahlt werden kann.

1.2.2 Datenvermeidung in der Telekommunikation

Wer heutzutage telefoniert, ein Fax verschickt oder Daten etwa über eine ISDN-Verbindung überträgt, über den speichern Telekommunikationsunternehmen in der Regel vielerlei personenbezogene Daten. Hierzu gehören Grundinformationen über Kunden wie Name, Vorname, Anschrift oder Bankverbindung, die sog. Bestandsdaten, ebenso wie die Daten, die zum Aufbau und zum Aufrechterhalten der gewünschten Verbindung erforderlich sind, die sog. Verbindungsdaten. Ausgewählte Verbindungsdaten wie Datum, Beginn und Dauer einer jeden Verbindung sowie die gewählte Rufnummer werden auch gespeichert, um damit die Abrechnung zu erstellen.

Durch konsequenten Einsatz datensparsamer Technologien läßt sich jedoch der Umfang personenbezogener Bestands-, Verbindungs- oder Abrechnungsdaten erheblich reduzieren oder sogar gänzlich vermeiden:

- Abrechnungsdaten lassen sich beispielsweise vermeiden, wenn die genutzten Telekommunikationsdienstleistungen, wie bereits unter 1.2.1 erwähnt, mit Prepaid-Cards bezahlt werden. Folgendes ist hierzu erforderlich:
  - Es müssen Telefon-, Telefax- und andere Telekommunikationsendgeräte für private oder geschäftliche Anschlüsse auf den Markt kommen, die mit Hilfe eines Chipkartenlesers Werteinheiten von Chipkarten abbuchen können. Die Abbuchung kann von Gebührenimpulsen gesteuert werden, die das Telekommunikationsnetz an das Endgerät sendet.
  - Um Chipkarten verwenden zu können, deren Guthaben sich wieder aufladen läßt, muß eine Infrastruktur mit Aufladestellen aufgebaut werden. Denkbar ist, daß die Karten durch Einzahlung von Bargeld oder Belastung des Girokontos an entsprechenden Automaten aufgeladen werden können. In Frage kommt aber auch ein Aufladen der Chipkarten durch Übertragen elektronischer Geldeinheiten. Bei entsprechender Gestaltung der Telekommunikationsendgeräte könnte dann jeder Telefonkunde seine Chipkarte zu Hause am eigenen PC oder Telefonapparat aufladen.

  - Wenn der Telekommunikationstarif so gestaltet wird, daß kein Grundpreis zu zahlen ist, kann ganz auf die Speicherung von Kundendaten für Abrechnungszwecke verzichtet werden.
- Auch das bereits erwähnte anonyme elektronische Geld läßt sich zum Bezahlen von Telekommunikationsdienstleistungen verwenden, beispielsweise indem das Entgelt für jeden neu angebrochenen Zeittakt sofort elektronisch übermittelt wird. Im Vergleich zum Einsatz einer Chipkarte muß man sich bei diesem Zahlungsverfahren nicht mehr um das rechtzeitige Wiederaufladen seiner Chipkarte kümmern.

1.2.3 Unbeobachtete Kommunikation

Datenschutzfreundliche Techniken lassen sich darüber hinaus auch einsetzen, um zu verhindern, daß ein Dritter durch Überwachung der auf den Kommunikationswegen transportierten Daten erkennen kann, ob ein Teilnehmer gerade mit einem anderen kommuniziert und wer der Kommunikationspartner ist. Ferner machen sie es möglich, mobil zu telefonieren, ohne daß der Netzbetreiber hierbei den Standort des Teilnehmers registriert. Technisch lassen sich Mobilfunknetze auch so gestalten, daß die Handys nicht einmal mehr mit Peilsendern geortet werden können.

1.2.4 Medizinische Forschungsregister

Datensparsamkeit läßt sich nutzbringend auch in solchen Bereichen praktizieren, in denen Computer schon längst Einzug gehalten haben. Medizinische Forschungsregister sind Beispiele dafür. Sie stellen stets brisante Datensammlungen dar, enthalten sie doch sensible Angaben über die gesundheitlichen Verhältnisse vieler Personen. Diese sollten daher nach Möglichkeit anonymisiert oder unter einem Pseudonym gespeichert werden. Durch Einsatz der Verschlüsselungstechnik ist beim Krebsregister Baden-Württemberg eine Pseudonymisierung möglich geworden. Durch eine zweifache Verschlüsselung entsteht aus den Identifizierungsdaten eines Krebskranken das Pseudonym. Der große Vorzug: Die Verschlüsselung bewirkt, daß eine bestimmte Person immer dasselbe Pseudonym erhält; Mehrfachmeldungen zu einer Person lassen sich also im Krebsregister zusammenführen. Die Verschlüsselungsfunktion ist dabei nicht umkehrbar; aus dem Pseudonym lassen sich also die Identifizierungsdaten der betreffenden Person nicht berechnen (vgl. dazu unseren 5. Tätigkeitsbericht 1984, LT-Drs. 9/940, S. 29 bis 39 und 14. Tätigkeitsbericht 1993, LT-Drs. 11/2900, S. 81 bis

83). Von wesentlicher Bedeutung ist dabei folgendes: Die Stelle, die die Pseudonyme berechnet, darf das Register nicht in ihrer Obhut haben, denn ansonsten könnte sie ganz leicht herausfinden, ob eine bestimmte Person im Register gespeichert ist. Sie bräuchte dazu nur aus den Identifizierungsdaten dieser Person das zugehörige Pseudonym zu erzeugen und sodann mit allen im Krebsregister gespeicherten Pseudonymen abgleichen. Aus dem gleichen Grund darf die Stelle, die das Register führt, nicht in der Lage sein, die Pseudonyme zu berechnen.

1.3 Wie kann es weitergehen?

Die Datenschutzbeauftragten des Bundes und der Länder haben in zwei umfangreichen Arbeitspapieren für verschiedenste Anwendungsbereiche wie Online-Dienste, elektronischer Zahlungsverkehr, Gesundheitsbereich oder Telekommunikation aufgezeigt, daß bereits heute etliche Möglichkeiten bestehen oder denkbar sind, Technik datensparsam zu gestalten und einzusetzen. Von dieser Möglichkeit macht die Praxis leider noch viel zu wenig Gebrauch. Vor diesem Hintergrund ist es deshalb zu begrüßen, daß die in diesem Jahr in Kraft getretenen gesetzlichen Regelungen über die Tele- und Mediendienste den Einsatz datensparsamer Techniken vorsehen. Das Teledienstedatenschutzgesetz des Bundes regelt dabei insbesondere solche Dienste, bei denen die Individualkommunikation im Vordergrund steht, wie dies beispielsweise bei elektronischer Post, Telearbeit, Telemedizin, Telebanking, Telespielen, Videokonferenzen oder elektronischen Buchungsdiensten der Fall ist. Der von den Ländern abgeschlossene Mediendienste-Staatsvertrag ist dagegen auf Dienste anzuwenden, die für alle Teilnehmer gleiche und zudem redaktionell bearbeitete Informationen bereithalten. Beispiele hierfür sind Pay-TV, Pay per View, Video on Demand oder auch die meisten World-Wide-Web-Angebote des Internet.

Wesentliche datenschutzrechtliche Eckpunkte sind dabei:

- Gebot der Datensparsamkeit
  Die Gestaltung und Auswahl technischer Einrichtungen zum Betrieb der Tele- und Mediendienste hat sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.
- Weitgehend anonyme Nutzungsmöglichkeiten
  Der Diensteanbieter muß, soweit technisch möglich und zumutbar, den Nutzern ermöglichen, die Dienste anonym oder unter einem Pseudonym zu nutzen und zu bezahlen.
- Umgehende Löschung

Der Diensteanbieter muß personenbezogene Verbindungsdaten spätestens unmittelbar nach Ende der Nutzung eines Dienstes löschen, sofern die Daten nicht für die Abrechnung benötigt werden.

- Datenschutz-Audit

  Zur Verbesserung von Datenschutz und Datensicherheit können Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige Gutachter prüfen und bewerten lassen und das Ergebnis anschließend veröffentlichen.

Doch die Verpflichtung zum Einsatz datensparsamer Technologie im Bereich der Tele- und Mediendienste kann nur ein erster Schritt sein. Um der datensparsamen und deshalb datenschutzfreundlichen Technik zum Durchbruch zu verhelfen, muß diese auch in anderen Bereichen eingesetzt werden. Dies zu forcieren, ist Anliegen der Entschließung der Konferenz der Datenschutzbeauftragten zur Erforderlichkeit datenschutzfreundlicher Technologien (vgl. Anlage 8). Für ein Gelingen ist die Mitwirkung vieler erforderlich: Der Gesetzgeber kann, wie bei den Tele- und Mediendiensten, deren breiten Einsatz fördern, indem er die Verwendung datensparsamer Technik in bestimmten Bereichen gesetzlich vorschreibt. Zugleich sind Dienstleistungsanbieter und Hersteller gefordert, datensparsame Dienste und Produkte zu entwickeln und am Markt anzubieten. Dies liegt auch in deren eigenem Interesse, da Datensparsamkeit dazu beitragen kann, die angestrebte breite Akzeptanz der modernen Informations- und Kommunikationstechniken und damit auch den Absatz zu fördern.

2. Die Kryptokontroverse

Der Vorzug leistungsfähiger Verschlüsselungsverfahren, nämlich es dem Absender einer elektronischen Nachricht zu ermöglichen, seine Daten so sicher zu verschlüsseln, daß nur der rechtmäßige Empfänger sie wieder entschlüsseln kann, stellt den Staat vor eine völlig neuartige Situation. Lange Zeit bereitete es ihm keine besonderen Schwierigkeiten, im Zuge angeordneter Überwachungsmaßnahmen die Kommunikation der zu Überwachenden mitzulesen oder mitzuhören. Herkömmliche Briefpost läßt sich leicht öffnen, eine Telefonleitung läßt sich anzapfen. Mit der Nutzung moderner Informations- und Kommunikationstechniken und der Verfügbarkeit der Verschlüsselungstechnik hat sich dies schlagartig geändert. Wer heutzutage etwa über das Internet eine elektronische Post mit PGP (Pretty Good Privacy), einer im Internet verfügbaren und dort weit verbreiteten Verschlüsselungssoftware, verschlüsselt, kann abhörsicher gegenüber jedermann, auch gegenüber staatlichen Stellen, kommunizieren. Dies hat eine auch hierzulande kontrovers geführte Diskussion über die Kryptographie ausgelöst. Insbesondere Sicherheitsexperten verlangen im Interes-

se einer wirksamen Verbrechensbekämpfung eine gesetzliche Regelung. Es könne nicht angehen, daß Kriminelle Datennetze mißbrauchen, indem sie verschlüsselte Botschaften austauschen, ohne daß der Staat die Möglichkeit hat, ihre Kommunikation aufzudecken.

Seit geraumer Zeit prüft nun die Bundesregierung, ob eine Notwendigkeit besteht, den Einsatz der Verschlüsselung einzuschränken. Dabei kommen prinzipiell folgende Varianten in Betracht:

- Der Staat erteilt nur in Ausnahmefällen die Genehmigung zum Einsatz der Verschlüsselung. Ansonsten ist Verschlüsselung generell verboten.
- Der Staat erlaubt nur den Einsatz schwacher Verschlüsselungsverfahren, die keine ausreichende Sicherheit gegen Entschlüsselung bieten.
- Der Staat läßt bestimmte, sichere Verschlüsselungsverfahren zu, verpflichtet aber gleichzeitig denjenigen, der ein Verschlüsselungsverfahren nutzen will, ein Duplikat seines verwendeten Schlüssels oder Duplikate von Teilschlüsseln bei einer zentralen Stelle oder mehreren Stellen zu hinterlegen. Die staatlichen Überwachungsbehörden erhalten dann, wenn eine Überwachungsmaßnahme angeordnet ist, Zugriff auf den hinterlegten Schlüssel bzw. die hinterlegten Schlüsselteile des zu Überwachenden und können so dessen Kommunikation entschlüsseln.

Klar ist, daß jede Einschränkung oder gar ein Verbot der Verschlüsselung einen Eingriff in das Grundrecht auf Datenschutz darstellt, denn dieses beinhaltet auch das Recht, frei und unbeobachtet kommunizieren zu können. Vor diesem Hintergrund ist ein generelles oder weitgehendes Verbot der Verschlüsselung von vornherein abzulehnen. Denn wie anders als durch Verschlüsselung können im Zeitalter weltweiter, für jedermann zugänglicher Datennetze personenbezogene und sonstige sensible Daten wirksam vor unberechtigter Kenntnisnahme geschützt werden? Da der Staat keinen ausreichenden Schutz garantieren kann, müssen die einzelnen Nutzer die Möglichkeit haben, sich selbst zu schützen.

Nicht akzeptabel wäre auch eine Reglementierung der Verschlüsselung, die den Anwendern lediglich den Einsatz schwacher Verschlüsselungsverfahren erlaubt. Denn jeder, der über das notwendige technische Wissen und entsprechende Computerprogramme verfügt, könnte die Informationen wieder entschlüsseln. Der Einsatz schwacher Verschlüsselungsverfahren böte also nur eine Scheinsicherheit.

Bleibt die dritte Variante, bei der Schlüsselduplikate zu hinterlegen sind. Bietet sie einen Ausweg aus dem Dilemma? Ist damit das Ei des Kolumbus gefunden? Ich meine nein. Denn es ist wohl kaum damit zu rechnen, daß sich kriminelle Profis an die vom Staat aufgestellten Spielregeln halten, die besagen, daß derjenige, der verschlüsselt, dies nur mit ganz bestimmten, vom Staat zugelassenen Verschlüsselungsverfahren tun darf und noch dazu seinen Schlüssel hinterlegen muß. Hinzu kommt: Selbst wenn derjenige, der eine Nachricht verschickt, dem staatlichen Appell folgen und seinen

Schlüssel hinterlegen würde, hätten die Sicherheitsbehörden noch lange keine Gewißheit, daß das, was sie mit Hilfe des hinterlegten Schlüssels lesen können, auch tatsächlich die Information ist, die der Absender dem Empfänger zukommen lassen will. Denn gegen steganographische Verfahren ist kein Kraut gewachsen. Mit ihnen kann man nämlich in völlig harmlosen Informationen, beispielsweise in einem Bild, das man über die Datennetze schickt, andere Informationen so verbergen, daß derjenige, der nur das Bild sieht und nichts von der geheimen Botschaft weiß, gar nicht merkt, daß dahinter noch ganz anderes steckt. So geht es - um bei dem Beispiel zu bleiben - jedem Betrachter des Bildes, ganz gleich, ob es offen über die Datennetze läuft oder ob es verschlüsselt eingespeist worden ist und er es mit Hilfe des Schlüssels wieder sichtbar gemacht hat. Wollte der Staat dann auch noch von vornherein, sozusagen prophylaktisch, zumindest durch stichprobenartige Kontrollen diejenigen schwarzen Schafe herausfinden, die verbotene Verschlüsselungsverfahren verwenden, würde dies den Aufbau einer völlig neuartigen Kontrollstruktur notwendig machen. Diese wäre mit hohen Kosten verbunden und das mit der Reglementierung verfolgte Ziel ließe sich gleichwohl nicht erreichen. Treffen würde eine Reglementierung in erster Linie den braven, gesetzestreuen Bürger, der sein Schlüsselduplikat hinterlegt, nicht dagegen diejenigen, die mit der Reglementierung eigentlich avisiert werden sollen, nämlich kriminelle Profis. Dann gibt es aber auch keinen Grund, das Grundrecht auf Datenschutz einzuschränken, denn solche Eingriffe sind überhaupt nur zulässig, wenn sie zur Erreichung des angestrebten Zwecks geeignet sind. Aus diesem Grund plädiere ich dafür, von jeder Reglementierung der Verschlüsselung abzusehen. Für diese Legislaturperiode scheint die Angelegenheit erst einmal vom Tisch zu sein. Bleibt zu hoffen, daß dies auch in der Zukunft so bleibt.

3. Von öffentlichen Stellen, Bürgern und dem Internet

Bereits in den letzten beiden Tätigkeitsberichten haben wir uns ausführlich mit dem Thema Internet beschäftigt (vgl. dazu 16. Tätigkeitsbericht 1995, LT-Drs. 11/6900, S. 45 bis 53 und 17. Tätigkeitsbericht 1996, LT-Drs. 12/750, S. 10 bis 15). Angesichts des anhaltenden Booms rund um das Netz der Netze tauchen allerdings immer wieder neue Fragen und Probleme mit Datenschutzbezug auf.

3.1 Dienste für den Bürger

Ein Behördengang verläuft nicht immer glatt. Manch einer steht außerhalb der Öffnungszeiten vor verschlossenen Türen, wendet sich mit seinem Anliegen an das falsche Amt, das nicht weiterhelfen kann, oder hat notwendige Unterlagen und Dokumente nicht dabei, so daß ein nochmaliger Besuch notwendig ist. Ein Blick ins Internet könnte hilfreich sein, um solchen Unannehmlichkeiten vorzubeugen. Immer mehr Behörden informieren in ihren Angeboten darüber, wel-

ches Amt für welche Anliegen zuständig ist, wo es zu finden ist, wie die Sprechzeiten sind und welche Unterlagen etwa bei einer Ummeldung, der Zulassung eines Kraftfahrzeugs oder der Aufgebotsbestellung im Falle einer Heirat vorzulegen sind. Mitunter besteht für den Antragsteller gleich noch die Möglichkeit, ein leeres Antragsformular abzurufen, das er ausdrucken und in aller Ruhe zu Hause ausfüllen kann.

Beschränken sich die Angebote der Behörden für Bürger auf nichtpersonenbezogene Informationen und Blanko-Formulare, so ist aus datenschutzrechtlicher Sicht nichts weiter dazu zu sagen. Anders liegen die Dinge, wenn mehr möglich ist, so wie beispielsweise bei den Angeboten der Stadt Mannheim. Wer innerhalb Mannheims umzieht oder sich ein bestimmtes Wunsch-Kfz-Kennzeichen reservieren lassen möchte, kann ein leeres Antragsformular am Bildschirm abrufen, es zu Hause am Bildschirm ausfüllen und per elektronischer Post an das zuständige Amt senden, das es sodann ausdruckt. Zum Unterschreiben muß der Antragsteller jedoch wie eh und je vor Ort erscheinen. Auch bei dieser Art von Kommunikation darf aber die Information der Bürger über ihre Rechte und die mit dem Datentransport im Internet verbundenen Risiken nicht zu kurz kommen.

- Jeder Einwohner, der seinen Zuzug, Wegzug oder Umzug beim Einwohnermeldeamt meldet, muß dazu einen Vordruck verwenden, der amtlich vorgeschrieben ist. Das amtliche Vordruckmuster enthält nicht nur die Fragen, die man beantworten muß, nebst zugehörigen Erläuterungen, sondern auch Hinweise darauf, in welchen Fällen der Einwohner der Weitergabe seiner Daten durch das Einwohnermeldeamt widersprechen kann. Diese Datenschutzhinweise dürfen natürlich nicht untergehen, wenn der Bürger sich via Internet anmeldet; die Stadt muß vielmehr dafür sorgen, daß er sie zur Kenntnis nehmen kann, bevor er seine Daten an das Einwohnermeldeamt per elektronischer Post absendet.
- Unverschlüsselt im Internet übertragene Daten sind nicht vor unberechtigter Kenntnisnahme geschützt; ohne eine digitale Signatur kann der Empfänger nicht erkennen, ob er die Daten unverfälscht erhalten hat. Daher sollte eine Behörde, die den Bürgern anbietet, ihr ihre Daten über das Internet zu übermitteln, zugleich eine Verschlüsselungstechnik einsetzen. Solange eine solche nicht zur Verfügung steht, muß sie die Bürger darüber informieren, daß die Daten unverschlüsselt übertragen werden und welche Risiken damit verbunden sind. Damit der Bürger es selbst in der Hand hat, von einem elektronischen Versand seiner Daten Abstand zu nehmen, muß ihn die Information natürlich erreichen, bevor er seine Daten eingibt und elektronisch versendet.

In beiden Punkten mußte die Stadt Mannheim auf meine Hinweise hin nachbessern.

3.2 Wir über uns

Will eine Behörde bürgernah und auf vielfältige Art erreichbar sein, muß sie sich angemessen präsentieren. Vielen genügt heutzutage der Eintrag im Telefon- oder Telefaxbuch nicht mehr. Im Trend liegt, wer sich auch in lokalen Netzen und im Internet darstellt.

- Besonders Hochschulen halten es nicht nur für sinnvoll, sondern im Interesse des globalen Informationsaustauschs für unabdingbar, in lokale Netze und in das Internet nicht nur ihre Organisation, sondern auch ein komplettes Mitarbeiterverzeichnis einzustellen. So soll dann vom Professor bis zur Schreibkraft deren Name, Institutsanschrift, Raumnummer, Telefonnummer, Telefaxnummer und die E-Mail/Internet-Anschrift für jedermann abrufbar sein. Doch hier ist Vorsicht am Platze. Nur soweit es für die Kontaktaufnahme mit den Mitarbeitern und für das Zurechtfinden in der Behörde nötig ist, darf sie solche Mitarbeiterdaten ohne weiteres öffentlich machen. In welchen Fällen diese Voraussetzungen vorliegen, hängt aber davon ab, wie groß die Behörde ist, welcher Hierarchieebene der Mitarbeiter angehört und wie breit die Informationen gestreut werden sollen. Am Beispiel der Hochschule möchte ich das erläutern:
  Ohne ihr Einverständnis dürfen leitende oder in besonderem Maße eigenverantwortlich tätige Personen interessierten Dritten gegenüber benannt werden, damit eine unmittelbare Kontaktaufnahme mit ihnen möglich ist. In einer Hochschule gehören dazu Professoren und Hochschuldozenten sowie die Verwaltungsspitze, aber auch wissenschaftliche Assistenten, wissenschaftliche Mitarbeiter oder Referenten in der Verwaltung. Allerdings können einzelne dieses Personenkreises ein schutzwürdiges Interesse daran haben, nicht in einem elektronischen Verzeichnis zu erscheinen, auf das Personen von außerhalb der Hochschule Zugriff haben. Das muß die Hochschule respektieren. Sie muß deshalb denjenigen, den sie in das elektronische Verzeichnis aufnehmen will, zuvor darauf hinweisen, daß er solche Interessen geltend machen kann. Dann muß sie im Einzelfall auf die Aufnahme verzichten. Dagegen muß die Hochschule immer die ausdrückliche Einwilligung solcher Mitarbeiter einholen, die nicht unmittelbar nach außen wirkende Aufgaben wahrnehmen, wie z.B. Sekretärinnen und Servicepersonal.
- Viele Städte und Gemeinden sowie Landkreise, die ins Internet drängen, stehen vor der Frage, inwieweit und in welcher Form sie Angaben über die Mitglieder ihres Gemeinderats oder Kreistags öffentlich machen dürfen. Dabei ist zu bedenken, daß diese Personen ohnehin mancherlei Publizität in Kauf

zu nehmen haben: Sie müssen sich öffentlich zur Wahl stellen und die Veröffentlichung der Wahlvorschläge und der Wahlergebnisse mit Namen, Berufen und Anschriften hinnehmen. Die Sitzungen des Gemeinderats sind im Regelfall öffentlich und finden häufig ihren Widerhall in der Presse. Vor allem aber folgt schon aus dem Prinzip der repräsentativen Demokratie und der bürgerschaftlichen Selbstverwaltung in den Kommunen, in der den Ratsmitgliedern die Funktion eines Bindeglieds zwischen Bürgern und Verwaltung zugedacht ist, daß die Allgemeinheit über die gewählten Repräsentanten unterrichtet wird. Deshalb haben wir seit jeher für zulässig gehalten, daß eine Gemeinde oder ein Landkreis Namen, Vornamen, Beruf, Anschrift, Fraktionszugehörigkeit und Mitgliedschaft in Ausschüssen der einzelnen Gemeinderats- bzw. Kreistagsmitglieder auch ohne deren ausdrückliche Einwilligung an interessierte Personen oder Stellen auf Anfrage zur Verfügung stellt und diese Angaben auch schriftlich veröffentlicht. Die Weitergabe der privaten Telefonnummer, die man im Telefonbuch ja auch unterdrücken kann, oder weiterer Daten wie beispielsweise Geburtsdatum oder Familienstand wäre dagegen nur mit Einverständnis des einzelnen Ratsmitglieds zulässig.
Die Verbreitung dieser Daten über das Internet stellt aber eine völlig neue Qualität der Veröffentlichung dar. Sie erreicht weltweit einen ungleich größeren Personenkreis als jede auflagenbegrenzte schriftliche Veröffentlichung. Eine solche globale Verfügbarkeit steht in krassem Gegensatz zu der lokalen Begrenzung des Aufgaben- und Wirkungskreises der Kommunen und ihrer Mandatsträger. Weder ist es Aufgabe der Kommunen, den Internet-Nutzern auf der ganzen Welt frei Haus Informationen über die Mitglieder ihrer Gremien zu liefern, noch kann dem überwiegenden Großteil der Internetbenutzer außerhalb des lokalen Raumes und ohne Beziehung zur Kommune ein berechtigtes Interesse an solchen Informationen zuerkannt werden. Auf der anderen Seite bedeuten die mit der Einstellung im Internet verbundenen vielfältigen Auswertungs- und Verknüpfungsmöglichkeiten ein erhöhtes Risiko, daß schutzwürdige Interessen der Gemeinde- und Kreisräte berührt werden. Angesichts dessen sollte eine Gemeinde Informationen über Gemeinderats- bzw. Kreistagsmitglieder nur dann in das Internet einstellen, wenn das einzelne Mitglied gerade darin, also in die Einstellung in das Internet, eingewilligt hat; eine Einwilligung in eine Veröffentlichung ganz allgemein reicht nicht aus.

3.3 Die Hitparade der Abrufe

Wer eigene Angebote ins Internet einstellt, will in aller Regel wissen, wie groß die Nachfrage danach ist. Um dies herauszufinden, protokollierte eine Stadt zu jedem Abruf Datum und Uhrzeit, welches Angebot abgerufen wurde und die

Netzadresse des abrufenden Computers, die sog. IP-Adresse. Aus diesen Protokolldaten erstellte die Stadt in gewissen Zeitabständen eine Statistik, die Aufschluß darüber gab, wie häufig die einzelnen Angebote nachgefragt wurden und woher die Abrufe kamen. War eine solche Statistik produziert, so löschte die Stadt die zugrundeliegenden Protokolldaten. Bei der Speicherung der Netzadressen der abrufenden Computer berücksichtigte die Stadt folgendes nicht:

Die Netzadresse eines am Internet angeschlossenen Computers besteht aus mehreren Zahlen und sagt auf den ersten Blick nicht viel aus. Weil Menschen mit aussagekräftigen Namen wesentlich besser umgehen können als mit Zahlen, läßt sich jedem Rechner des Internet auch ein Name zuweisen. Das Internet stellt eigens einen Dolmetscher-Dienst, den DNS-Dienst (Domain Name Service) bereit, mit dessen Hilfe sich ein Rechnername in die richtige Netzadresse oder auch eine Netzadresse in den zugehörigen Rechnernamen umsetzen läßt. Aus dem Namen geht hervor, in welchem Land der Rechner installiert ist. Der Rechnername gibt außerdem Aufschluß über denjenigen, der den Rechner betreibt. Dies könnte beispielsweise eine Universität oder ein bestimmtes Universitätsinstitut sein. Schon allein dies läßt einen Rückschluß auf den Kreis derjenigen zu, die mit diesem Rechner arbeiten. Vollends zu einem persönlichen Merkmal wird der Rechnername und damit auch die Netzadresse dann, wenn der Internet-Nutzer immer mit demselben Computer arbeitet, diesen Rechner allein nutzt und die Adresse dieses Computers im Internet verwendet wird. IP-Adressen können daher personenbezogen sein. Wer nun aber Angebote zum Abruf für die gesamte Internet-Gemeinde bereithält, mit anderen Worten also einen Mediendienst anbietet, muß die Datenschutzregelungen des Mediendienste-Staatsvertrags der Länder beachten. Dort heißt es klipp und klar, daß der Diensteanbieter personenbezogene Daten spätestens mit dem Beenden der Verbindung löschen muß, es sei denn, er benötigt die Daten noch für Zwecke der Abrechnung. Ich habe die Stadt daher aufgefordert, keine personenbezogenen Angaben über das Ende einer Verbindung hinaus zu speichern. Eine Antwort steht noch aus.

3.4 Internet und persönliche Datenspuren

Die Grundsätze der Datenvermeidung oder zumindest der Datensparsamkeit sind im Internet derzeit weitgehend Fiktion. Datenspuren können dabei nicht nur im Netz, sondern auch auf dem PC des Nutzers entstehen:

- Der Abruf eines Angebots im World Wide Web (WWW) kann dazu führen, daß der angefragte WWW-Server Informationen, ein sog. Cookie, auf der Festplatte des abfragenden PC ablegt, beispielsweise in einer Datei namens "cookies.txt" (cookie, engl.: Keks, Plätzchen). In einem Cookie kann der

Betreiber des WWW-Servers Informationen über das Nutzungsverhalten des Abrufers speichern lassen, so wie er eben will. So ist es beispielsweise ohne weiteres möglich, festzuhalten, wie lange und in welcher Reihenfolge sich der Abrufende die einzelnen Angebote angeschaut hat. Was die Cookies für Diensteanbieter so verlockend macht, ist: Wählt ein Internet-Nutzer ein Angebot, das er zu einem früheren Zeitpunkt schon einmal besuchte, erneut an, so werden die Cookies, die dieser Diensteanbieter anlegte, an ihn übermittelt. Der Diensteanbieter weiß damit auf einen Schlag, was der Nutzer bislang gemacht, für was er sich interessiert und was er gekauft hat. Tauschen mehrere Anbieter ihre Cookies untereinander aus, können noch detailliertere Nutzungsprofile die Folge sein. Im Zuge der zunehmenden Kommerzialisierung des Internet und dem Wunsch der Diensteanbieter, ihre Kunden gezielt bewerben zu können, nimmt die Verwendung des Cookie-Mechanismus sprunghaft zu. Inzwischen soll knapp die Hälfte der kommerziellen Internet-Anbieter Cookies anlegen.

- Jede Angebotsseite, die ein Nutzer im WWW abruft, wird auch als Kopie auf der Festplatte seines PC abgespeichert, im sog. Cache-Bereich des Browsers. Der Vorteil ist der: Will der Nutzer auf eine Angebotsseite zugreifen, die bereits auf der Festplatte hinterlegt ist, muß er sie nicht erneut aus dem Internet anfordern, sondern läßt sie sich von der Festplatte laden. Dies spart Übertragungszeit und nicht zuletzt Übertragungskosten. Die Kehrseite dieser Medaille ist freilich, daß alle diejenigen, die diesen PC nutzen können, sich die auf der Festplatte gespeicherten Seiten anschauen und damit feststellen können, auf welche Angebote die anderen Surfer zugriffen.

Den durch diese Datenspuren hervorgerufenen Gefährdungen gilt es entgegenzuwirken. Folgendes kommt dazu in Betracht:

- Neuere Versionen der Browser lassen sich so einstellen, daß vor dem Speichern eines Cookies eine Warnmeldung erfolgt. Der Nutzer kann die Speicherung dann erlauben oder ablehnen. Die neueste Version eines Browsers bietet sogar schon die Möglichkeit, das Ablegen von Cookies generell zu unterbinden. Ältere Browser-Versionen leisten das alles noch nicht. Um das Speichern von Cookies auf der Festplatte zu verhindern, muß der Nutzer einen Schreibschutz setzen, so daß nur noch lesender Zugriff möglich ist. Will der Nutzer vermeiden, daß der Diensteanbieter erfährt, was er die vorigen Male gemacht und für was er sich interessiert hat, muß er die Cookies regelmäßig löschen.
- Wer verhindern will, daß andere die auf der Festplatte des PC gespeicherten, bereits abgerufenen Seiten lesen, muß den PC wirksam gegen solche Zugriffe schützen. Es gibt jedoch auch Fälle, in denen mehrere Personen be-

rechtigt sind, mit einem PC zu arbeiten. Dem einzelnen Nutzer, der vermeiden will, daß die anderen Berechtigten herausfinden, was er gemacht hat, bleibt dann nichts anderes übrig, als die auf der Festplatte gespeicherten Seiten zu löschen, sobald er seine Arbeit im Internet beendet. Schließlich ist es auch möglich, den Browser so einzustellen, daß abgerufene Seiten nicht auf der Festplatte gespeichert werden. Längere Übertragungszeiten und höhere Übertragungskosten sind dann jedoch in Kauf zu nehmen.

3.5 Hinweise zum gesicherten Anschluß von Netzen

In jüngster Zeit war mein Amt im Zuge seiner Kontroll- und Beratungstätigkeit mit einer Reihe spezieller Fragen zu dieser Thematik konfrontiert:

- Eine Stadt speicherte die Angebote, die sie zum Abruf im WWW bereithält, auf ihrem Firewall-Rechner. Diese Vorgehensweise widersprach dem Grundsatz, daß ein Firewall-Rechner nur für die Aufgaben eingesetzt werden sollte, die er unbedingt erbringen muß, also für eine wirksame Abschottung des internen Computernetzwerks vom Internet und eine Protokollierung wichtiger Ereignisse. Wenn der Firewall-Rechner mehr leisten muß, müssen zusätzliche Programme installiert und betrieben werden. Dies allein erschwert schon die Kontrolle, ob auf diesem für die Sicherheit so entscheidenden Rechner alles einwandfrei und wie vorgesehen abläuft. Hinzu kommt, daß - abgesehen von ganz einfachen Programmen - kein Computerprogramm völlig fehlerlos arbeitet. Zusätzliche Programme auf dem Firewall-Rechner erhöhen daher das Risiko, daß aufgrund von Programmfehlern etwas schiefläuft, was dazu führen könnte, daß mehr Daten zwischen internem Computernetz und Internet fließen können als vorgesehen. Ich habe der Stadt daher empfohlen, ihre Angebote auf einem separaten Rechner abzulegen. Dieser Rechner läßt sich auf geschickte Weise so zwischen Firewall-Rechner und Internet anordnen, daß Zugriffe von außen gar nicht mehr an die Firewall gelangen müssen. Eine Antwort auf meine Empfehlung steht noch aus.
- In zwei Fällen schotteten Stellen ihr internes Computernetzwerk vom Internet durch eine Firewall ab. Die Abschottungsfunktionen bündelten die Stellen jeweils auf einem einzigen Rechner. In beiden Fällen empfahl ich, wenigstens noch eine weitere Schutzbarriere vorzusehen, beispielsweise die Filtermöglichkeiten von Routern zu nutzen. Solange der für die Abschottung eingerichtete Rechner korrekt eingerichtet ist und alles einwandfrei und wie vorgesehen abläuft, gibt es zwar keinen Grund, dies zu tun. Zu bedenken ist aber, daß Hardware und Software nie völlig fehlerfrei arbeiten. Eine zusätzliche Barriere kann daher die Sicherheit erhöhen. Schließlich wird ein Angreifer aus dem Internet, dem ein solcher Fehler bekannt wird und der ihn ausnut-

zen möchte, noch durch eine weitere Barriere davon abgehalten, in das interne Netz einzudringen. Die Schutzwirkung stellt sich insbesondere dann ein, wenn sich die Barrieren technisch voneinander unterscheiden, so daß es unwahrscheinlich ist, daß beide gleichartige Fehler aufweisen. In einem Fall will die Stelle entsprechend meiner Empfehlung verfahren; im anderen Fall steht eine Antwort noch aus.

4. Outsourcing

Not macht erfinderisch. Daran muß man unwillkürlich denken, wenn man die vielfältigen Bemühungen verfolgt, mit denen die Verwaltung versucht, Kosten einzusparen. Eine Möglichkeit, den Haushalt zu entlasten, wird darin gesehen, Computer, Netzwerke und EDV-Verfahren nicht selbst zu betreiben, sondern damit private Unternehmen zu beauftragen, auf neudeutsch: Outsourcing zu betreiben. Das soll auch in der Landesverwaltung praktiziert werden. Unter anderem wird dabei daran gedacht, daß die Landesbehörden ihre Bürokommunikationssysteme durch andere betreiben lassen. Dazu plant das Innenministerium einen Rahmenvertrag abzuschließen. Der mir zur Stellungnahme zugeleitete Vertragsentwurf gab mir Anlaß, darauf hinzuweisen, was dabei zur Wahrung des Datenschutzes beachtet werden muß:

- Bei einem derartigen Outsourcing müssen die Regelungen der Datenschutzgesetze über die Datenverarbeitung im Auftrag beachtet werden. Deshalb muß sich eine Behörde, die sich zum Outsourcing entschließt, vor Vertragsschluß von den Bewerbern darlegen lassen, welche technischen und organisatorischen Maßnahmen sie zum Schutz der zu verarbeitenden personenbezogenen Daten ergreifen wollen.
- Da sich bei einer Beauftragung eines privaten Unternehmens Interessenkonflikte ergeben können, wenn die zu verarbeitenden Daten auch für die Aufgaben des Unternehmens oder für die Mitarbeiter von Nutzen sind, sollten sensible Daten wie Patienten-, Sozial-, Steuer- und Personaldaten oder Daten von Sicherheitsbehörden jedenfalls dann durch Verschlüsselung geschützt werden, wenn die Mitarbeiter des Outsourcing-Unternehmens sie zur Erfüllung ihrer Aufgaben weder lesen noch gar bearbeiten müssen.
- Will der Auftragnehmer Unteraufträge an Dritte vergeben, ist zwischen ihm und dem Auftraggeber einvernehmlich festzulegen, was dabei beachtet werden muß. In jedem Fall muß der Auftraggeber vorab über eine derartige Beteiligung Dritter informiert sein.
- Sofern der Auftragnehmer die von ihm betreuten und beim Auftraggeber aufgestellten Computer per Ferndiagnose auf ihre Funktionsfähigkeit überprüfen und optional auch im Wege der Fernwartung betreuen können soll, ist festzulegen, ob und unter welchen Voraussetzungen er dabei auf personenbezogene Daten

zugreifen darf, und sicherzustellen, daß keine unberechtigten Zugriffe stattfinden können.

- Es sollte darauf geachtet werden, daß die auftraggebende Behörde auch noch nach dem Outsourcing über ausreichenden Sachverstand verfügt, daß sie in der Lage ist, die vom Auftragnehmer getroffenen technischen und organisatorischen Datenschutzmaßnahmen zu beurteilen und bei Bedarf zusätzliche Maßnahmen zu verlangen.
- Falls der Auftragnehmer in bestehende Wartungs- oder Pflegeverträge eintreten soll, ist jeweils zu prüfen, ob diese auch für diesen Fall ausreichende Datenschutzregelungen enthalten.
- Es sollte vereinbart werden, daß der Auftragnehmer die auftraggebende Behörde darüber informiert, wann ein Austausch der Festplatte eines Computers vorgesehen ist, damit sie die Möglichkeit hat, darauf gespeicherte personenbezogene Daten vorher zu löschen.
- Die Mitarbeiter des Auftragnehmers sollten nicht nur auf das Datengeheimnis, sondern auch nach dem Verpflichtungsgesetz verpflichtet werden, damit sie im Falle eines Fehlverhaltens in der gleichen Weise wie Mitarbeiter der auftraggebenden Behörde dafür verantwortlich gemacht werden können. Zudem sollte ein Auftragnehmer möglichst nur fest angestellte Beschäftigte einsetzen können.
- Damit das bisherige Datenschutzniveau möglichst nicht absinkt, ist vertraglich sicherzustellen, daß mein Amt auch vor Ort beim Auftragnehmer anlaßunabhängige Datenschutzkontrollen durchführen kann und dabei entsprechend § 25 LDSG vom Auftragnehmer unterstützt wird.

Erfreulicherweise hat das Innenministerium diesen Hinweisen und Empfehlungen in seinem überarbeiteten Vertragsentwurf weitgehend Rechnung getragen.

5. Das Client-Server-Verfahren LISSA

Vorbei sind die Zeiten, in denen die EDV des Landes von Großrechnern, "dummen" Terminals und unvernetzten Computern bestimmt wurde. Inzwischen sind lokale PC-Netze einzelner Behörden ebenso selbstverständlich wie deren landesweite Vernetzung über das Landesverwaltungsnetz (LVN). Damit sind auch die Voraussetzungen für den Einsatz von Client-Server-Verfahren geschaffen. In der Regel werden dabei die Daten auf PC erfaßt und mitunter räumlich weit entfernt auf einem leistungsstarken Server vorgehalten. Die Sachbearbeitung erfolgt dann wiederum auf PC. Die Kultusverwaltung setzt mit LISSA ein solches Verfahren ein, um die Staatlichen Schulämter bei ihrer Planung des Lehrereinsatzes an den Schulen zu unterstützen. Für uns Grund genug, bei allen derzeit am Betrieb des Verfahrens beteiligten Stellen nachzuprüfen, ob und welche Probleme und Mängel sich dabei zeigen. Besucht haben wir deshalb

- ein Staatliches Schulamt, das mit Hilfe dieses Verfahrens Daten von ca. 3 000 Grund-, Haupt-, Real- und Sonderschullehrern speichert und bearbeitet,
- das Oberschulamt Stuttgart, das den in sein lokales Netz integrierten LISSA-Datenbankrechner betreibt,
- die Zentrale EDV-Stelle der Kultusverwaltung, die das Kultusdatennetz, ein Teilnetz des LVN, betreibt, über das unter anderem die LISSA-Lehrerdaten zwischen Staatlichem Schulamt und Oberschulamt hin- und herfließen, und
- das Zentrum für Kommunikationstechnik und Datenverarbeitung, das das LVN mit seinen mehr als 60 Netzknoten im ganzen Land betreibt, welches Behörden aller Ressorts miteinander und mit anderen Netzen wie dem Internet verbindet.

Die einzelnen Prüfungen ergaben folgende Mängel, die die Sicherheit der in LISSA gespeicherten personenbezogenen Lehrerdaten beeinträchtigten:

5.1 Zentrum für Kommunikationstechnik und Datenverarbeitung (ZKD)

Der Betrieb des Landesverwaltungsnetzes war nicht frei von Mängeln:

- Obwohl das Datenschutz- und Sicherheitskonzept für das LVN verlangt, daß das ZKD alle zum Kultusdatennetz wie auch die zu anderen Teilnetzen gehörenden LVN-Anschlüsse jeweils in einer sog. Geschlossenen Benutzergruppe zusammenfaßt und dadurch gegenüber anderen Teilnetzen abschottet, hatte es zum Zeitpunkt unserer Kontrolle noch keine solche Geschlossene Benutzergruppe eingerichtet.
- Das vom ZKD zur Administration der Netzknoten eingesetzte Programm bot nur einen unzureichenden Paßwortschutz, denn es garantierte weder eine Paßwortmindestlänge noch deren automatischen Verfall. Mehrmalige Anmeldefehlversuche hatten weder eine Anmeldesperre noch eine Protokollierung dieser Versuche zur Folge.
  Zudem hatten einige Mitarbeiter des ZKD Administrationsberechtigungen, die es ihnen erlaubten, alle Einstellungen der Knoten zu lesen und sogar zu ändern, obwohl das für ihre dienstlichen Aufgaben gar nicht erforderlich war. Auch wurden Änderungen der Systemkonfiguration nicht protokolliert.

5.2 Zentrale EDV-Stelle der Kultusverwaltung (ZEDV)

Datenschutzmängel traten auch bei der Überprüfung des Kultusdatennetzes zutage:

- Die ZEDV hatte die von den Netzknotencomputern, den sog. Routern, angebotenen Möglichkeiten zur Beschränkung des Datenflusses nicht ausreichend genutzt: Zum Teil hätten Kommunikationspartner erreicht werden können, mit denen dienstlich kein Datenaustausch erforderlich war. Außerdem nutzte die ZEDV nicht die Möglichkeit, technisch sicherzustellen, daß nur

bestimmte, durch Datenabsender, -empfänger und gewünschte Anwendung beschriebene Datenpakete im Netz transportiert werden können.
- Zwei Paßwörter, die es gestatten, sicherheitsrelevante Router-Einstellungen zu lesen, waren im Klartext gespeichert. Sie waren damit nicht ausreichend gegen eine Kenntnisnahme durch Dritte geschützt.
- Obwohl erst die Dokumentation erfolgloser Anmeldeversuche den Netzbetreiber auf mögliche Eindringversuche hinweisen kann, fehlte eine solche Protokollierung bei Zugriffen auf Router des Kultusdatennetzes, und zwar selbst bei versuchten Systemverwalter-Zugriffen.

Damit aber nicht genug:
- Es gab keine Terminalbeschränkung bei der Systemverwalter-Anmeldung an den Routern.
- Die schriftlichen Vereinbarungen mit dem Unternehmen, das den LISSA-Datenbankcomputer und andere Server im Wege der Fernwartung betreute, waren unzureichend. Zudem fehlten Regelungen darüber, wie intern mit der Fernwartung umzugehen ist.
- Es existierte kein schriftliches Datenschutz- und Datensicherheitskonzept für den Betrieb des Kultusdatennetzes.

5.3 Oberschulamt

Auch beim Oberschulamt Stuttgart, das den Datenbankcomputer betreibt, zeigten sich Mängel:
- Fünf für den Rechnerbetrieb verantwortliche EDV-Mitarbeiter konnten über eine Telefonverbindung und mit Hilfe eines Modems von zu Hause eine Online-Verbindung zum Netz des Oberschulamts und über dieses auch zum Kultusdatennetz aufbauen. Dabei war nicht ausreichend sichergestellt, daß nicht auch Dritte diese Möglichkeit ausnutzen und auf im Computer des Kultusdatennetzes gespeicherte Daten zugreifen konnten.
- An ca. 140 vernetzten PC des Oberschulamts, die mit dem LISSA-Server und den Systemverwalter-Arbeitsplätzen in einem Netz zusammengefaßt waren, konnte jeder Nutzer alle Betriebssystemfunktionen nutzen. Er hätte daher auch ein sog. Sniffer-Programm installieren und mit dessen Hilfe von LISSA-Daten, Systemverwalter-Aktivitäten oder anderen im Netz transportierten Informationen erfahren können, die nicht für ihn bestimmt waren.
- Tagessicherungsbänder, auf denen die am jeweiligen Tag vorgenommenen Dateneingaben gespeichert waren, bewahrte die ZEDV, obwohl dienstlich nicht notwendig, drei Monate auf.

Darüber hinaus war zu monieren:

- Das Systemverwalter-Paßwort für den LISSA-Datenbankcomputer war sieben und damit zu vielen Personen bekannt.
- Es gab keine Terminalbeschränkung für die Systemverwalter des LISSA-Datenbankcomputers und anderer Server.

5.4 Staatliches Schulamt

Die Datensicherheit war beim PC-Netz des Staatlichen Schulamts unter anderem deshalb nicht ausreichend gewährleistet, weil

- Arbeitsplatz-PC unzureichend gesichert waren und einen unbeschränkten Zugriff auf Betriebssysteme und Diskettenlaufwerke gestatteten und außerdem
- keine wirksame Bildschirmsperre eingerichtet war, die den Bildschirm nach längerer Zeit ohne Eingaben abdunkelte und sperrte.

In ihren Stellungnahmen zu den Mängeln im Bereich des Staatlichen Schulamts, der ZEDV und des ZKD sagten das Kultusministerium und das Innenministerium in den meisten Fällen zu, die Mängel zu beheben. Teilweise ist dies bereits geschehen. Was die beim Oberschulamt festgestellten Mängel angeht, so steht die Antwort des Kultusministeriums noch aus.

Neben zahlreichen einzelnen Mängeln machte die Überprüfung des Verfahrens LISSA auch deutlich, daß das neuartige, für Client-Server-Verfahren charakteristische Zusammenspiel verschiedener Computer und Netze auch eine Herausforderung für die Gewährleistung des Datenschutzes darstellt, denn hierzu sind Maßnahmen auf verschiedenen Ebenen erforderlich. Ist es in vielen Fällen - wie es die bisherigen Kontrollerfahrungen mehr als deutlich erkennen lassen - schon schwierig genug, abgestimmte Sicherheitsmaßnahmen für eine einzelne Stelle zu realisieren, so erfordert ein solches, von mehreren Stellen arbeitsteilig betriebenes Client-Server-Verfahren einen noch höheren Aufwand, denn die Maßnahmen sind hierbei von unterschiedlichen Stellen zu ergreifen, müssen aber trotzdem in ihrer Wirkung aufeinander abgestimmt sein.

6. Sonstige Probleme

Wer personenbezogene Daten mit Hilfe von Computern verarbeitet, muß technische und organisatorische Maßnahmen treffen, um eine datenschutzgerechte Verarbeitung sicherzustellen. Die Erfahrungen aus der Kontroll- und Beratungstätigkeit meines Amts zeigen leider, daß es die Behörden und sonstigen öffentlichen Stellen des Landes häufig am Notwendigen fehlen lassen. Auch in diesem Jahr mußten wir wieder etliche Mängel feststellen; manche davon entwickeln sich geradezu zu Dauerbrennern.

6.1 Unzureichende Sicherung der Arbeitsplatz-PC

Die datenverarbeitenden Stellen legen oft zu wenig Augenmerk auf die Sicherung ihrer Arbeitsplatz-PC:

- Eine Stadtverwaltung speicherte auf einem Arbeitsplatz-PC in der Stadtbibliothek personenbezogene Daten, die im Rahmen des Ausleihbetriebs anfallen. Da die Stadtverwaltung für diesen PC keinen Paßwortschutz einrichtete, konnte jeder, der Zugang zu diesem PC hatte oder ihn sich verschaffte - also auch jemand, der dazu gar nicht berechtigt war -, mit diesem Rechner arbeiten. Dazu mußte er ihn lediglich einschalten. Ein leichtes war es, sodann auf alle dort gespeicherten personenbezogenen Daten zuzugreifen. Das gleiche Problem stellte sich auch in einem städtischen Krankenhaus, das für keinen seiner vernetzten Arbeitsplatz-PC einen Paßwortschutz eingerichtet hatte. Dies ist ein Mangel, da stets sicherzustellen ist, daß nur Berechtigte auf personenbezogene Daten zugreifen können.
- Eine andere Stadtverwaltung sah ebenfalls für keinen ihrer vernetzten Arbeitsplatz-PC einen Paßwortschutz vor. Zudem war jeder dieser Rechner mit einem funktionsfähigen Diskettenlaufwerk ausgestattet, unabhängig davon, ob das Laufwerk an dem jeweiligen Arbeitsplatz benötigt wurde oder nicht. Somit konnte jeder, der einen solchen PC einschaltete, auch gleich eigene Programme installieren. Verfügbare Diskettenlaufwerke bergen zudem das Risiko, daß unberechtigt Daten kopiert oder Viren eingeschleppt werden. Ich habe deshalb die Stadt aufgefordert, einen Paßwortschutz für die Arbeitsplatz-PC einzurichten und nicht benötigte Diskettenlaufwerke für die Nutzung zu sperren.

6.2 Paßwortmängel

Ausführungen zu einem wirksamen Paßwortschutz sind inzwischen Legion und müßten eigentlich allen für Sicherheitsfragen Verantwortlichen bekannt sein. Mein Amt hat sich dazu bereits wiederholt in seinen Tätigkeitsberichten ausführlich geäußert und dargelegt, wie Paßwörter zu gestalten und zu verwenden sind (vgl. dazu den 10. Tätigkeitsbericht 1989, LT-Drs. 10/2730, S. 140 bis 142 und 14. Tätigkeitsbericht 1993, LT-Drs. 11/2900, S. 112 bis 115). Um so unverständlicher ist es, daß wir auch im vergangenen Jahr wieder Paßwortmängel feststellen mußten, die zum Teil so gravierend waren, daß ich sie beanstandete:

- In einem Standesamt verwendeten die dort Beschäftigten bei der Anmeldung am Computernetzwerk jeweils ihren Vornamen und bei der Anmeldung an der Fachanwendung jeweils ihren Nachnamen als Paßwort. Solch triviale Paßwörter bieten aber keinen wirksamen Schutz, da sie leicht zu erraten sind.

- Häufig akzeptieren die eingesetzten EDV-Systeme und EDV-Verfahren Paßwörter, die nur aus einem einzigen Zeichen bestehen können. Je kürzer ein Paßwort ist, desto leichter läßt es sich aber durch Ausprobieren herausfinden.
- In mehreren Fällen war das Paßwort nicht nur dem jeweiligen Benutzer bekannt, sondern auch noch dem Administrator.
- Wiederholt stellten wir fest, daß der Benutzer sein Paßwort nicht selbst ändern konnte.
- In einer Stadtbibliothek kamen Gruppenkennungen zum Einsatz. Arbeiten mehrere Personen mit einem EDV-Verfahren, so ist jedoch notwendig, daß jeder Benutzer eine eigene Kennung und ein eigenes Paßwort verwendet. Nur so lassen sich die einzelnen Nutzungsberechtigten im EDV-System unterscheiden.

6.3 Fehlende Terminalbeschränkungen

Ein gut eingerichteter Paßwortschutz bietet zweifellos einen Schutz vor unberechtigten Zugriffen auf personenbezogene Daten. Dennoch sollte man sich nicht allein auf ihn verlassen, denn es läßt sich nie ganz ausschließen, daß ein Paßwort doch einmal einem Unberechtigten bekannt wird. Mehr Sicherheit kann erreicht werden, wenn sich ein EDV-Verfahren nicht von jedem beliebigen PC aus starten läßt, sondern nur von den Arbeitsplätzen aus, an denen mit dem Verfahren gearbeitet wird. Eine solche Terminalbeschränkung ist auch für die Anmeldung unter einer Benutzerkennung vorzusehen, die mit Administrationsrechten verknüpft ist. Mit besonders weitreichenden Zugriffsrechten gehen nämlich auch erhöhte Mißbrauchsgefahren einher. Diesen gilt es entgegenzuwirken. Leider trugen dem eine ganze Reihe von kontrollierten Stellen nicht Rechnung.

6.4 Zu viele Administratoren

Je umfangreicher die Zugriffsrechte sind, die einer Person eingeräumt werden, desto höher sind auch die damit verbundenen Mißbrauchsgefahren. Deswegen ist der Kreis derjenigen, denen die besonders weitreichenden Zugriffsrechte eines Administrators eingeräumt werden und die folglich weitgehend unkontrolliert und unkontrollierbar auf gespeicherte personenbezogene Daten zugreifen können, so klein wie möglich zu halten. Dies wird nicht immer beherzigt. In einer Stadtbibliothek konnten 23 Personen mit dem dortigen EDV-Verfahren arbeiten. Zehn davon und damit viel zu viele waren Systemverwalter. Inzwischen hat die Stadt die Zahl der Systemverwalter deutlich herabgesetzt. In einem anderen Fall stattete ein städtisches Krankenhaus vier seiner Mitarbeiter mit Administratorrechten aus. Auch hier halte ich eine Reduzierung für geboten.

6.5 Mängel bei der Benutzerverwaltung

Jeder Mitarbeiter darf nur die Zugriffsrechte auf die personenbezogenen Daten erhalten, die er für die Erfüllung seiner dienstlichen Aufgaben benötigt. Dies ist ein Grundanliegen des Datenschutzes, für dessen technische Umsetzung der Benutzerverwalter zuständig ist. Er richtet neue Benutzerkennungen ein, aktualisiert Zugriffsberechtigungen bereits eingerichteter Benutzer und löscht eine Kennung dann, wenn der betreffende Mitarbeiter ausscheidet. Damit der Benutzerverwalter seinen Aufgaben auch gerecht werden kann, braucht er die richtige Unterstützung. Damit haperte es an zwei Stellen:

- Ein städtisches Krankenhaus traf keinerlei Vorkehrungen, um sicherzustellen, daß der Benutzerverwalter vom Ausscheiden eines Mitarbeiters erfährt. Somit bestand die Gefahr, daß das Krankenhaus Zugriffsberechtigungen bereits ausgeschiedener Mitarbeiter im Computersystem nicht löschte.
- Das Patientenverwaltungssystem eines anderen Krankenhauses bot keine Möglichkeit, eine Übersichtsliste mit allen eingerichteten Benutzern und den ihnen eingeräumten Zugriffsrechten zu erstellen. Bei der Vielzahl von etwa 200 Benutzern, die der Benutzerverwalter betreuen mußte, ist aber unverzichtbar, daß er sich rasch und mühelos einen Überblick verschaffen kann, welche Personen mit welchen Zugriffsrechten auf gespeicherte Patientendaten zugreifen können.

6.6 Gefahren durch einen Download

Häufig sind EDV-Verfahren, die für den Betrieb in einem Netzwerk konzipiert sind, so angelegt, daß die personenbezogenen Daten auf einem zentralen Rechner, dem sog. Server, gespeichert werden. Mitunter besteht dabei die Möglichkeit, sämtliche oder nur einen Teil der gespeicherten personenbezogenen Daten auf die Festplatte eines Arbeitsplatz-PC zu kopieren, also einen sog. Download durchzuführen. Dadurch entstehen aber zusätzliche datenschutzrechtliche Risiken. So muß beispielsweise dann, wenn Daten zu löschen sind, darauf geachtet werden, daß die Löschung nicht nur auf dem Server, sondern auch auf der Festplatte erfolgt. Daher darf die Download-Möglichkeit nur denjenigen Mitarbeitern offenstehen, die diese Funktion für die Erfüllung ihrer dienstlichen Aufgaben benötigen. In einem städtischen Krankenhaus war dies nicht der Fall. Dort konnte jeder Mitarbeiter, der mit dem Patientenverwaltungssystem arbeiten durfte, einen Download veranlassen.

6.7 Schutz vor Eindringversuchen

Mehrmalige fehlerhafte Anmeldeversuche mit derselben Benutzerkennung können ein Indiz dafür sein, daß jemand Benutzerkennungen und Paßwörter ausprobiert, um sich Zugang zu gespeicherten personenbezogenen Daten zu ver-

schaffen, auf die er gar nicht zugreifen darf. Deswegen gilt es, solchen Fällen nachzugehen. Bei einer Kontrolle stellten wir fest, daß die Benutzerkennung nach mehr als 7 Fehlversuchen und nur für die Dauer von 15 Minuten gesperrt wird. In einer solch kurzen Zeit ist es aber kaum möglich nachzuprüfen, ob ein Mitarbeiter lediglich Schwierigkeiten mit der Anmeldung hatte oder ob etwa ein Unberechtigter versuchte, sich unter einer falschen Identität anzumelden. Zudem war die Anzahl von 7 möglichen Fehlversuchen ohne Folgen recht großzügig bemessen. Ich habe deshalb verlangt, daß die Benutzerkennung zeitlich unbefristet gesperrt und die Anzahl möglicher Fehlversuche ohne Folgen auf 3 reduziert wird.

6.8 Fernwartung

Heutzutage ist es üblich geworden, bei auftretenden Fehlern oder Störungen im EDV-Betrieb fremde Hilfe, etwa durch die Herstellerfirma, in Anspruch zu nehmen. Vielfach vorbei sind dabei die Zeiten, in denen die Spezialisten vor Ort tätig wurden. Aus Kostengründen setzen viele auf die Fernwartung, bei der die datenverarbeitende Stelle einer externen Stelle via Datenleitung Zugriff auf ihr EDV-System und darauf gespeicherte Daten erlaubt. Zusätzliche Risiken für den Datenschutz sind die Folge. Um diese Risiken soweit wie möglich zu begrenzen, ist eine Fernwartung nur zulässig, wenn die datenverarbeitende Stelle das Fernwartungsunternehmen schriftlich beauftragt und in dem Vertrag klipp und klar regelt, was bei der Fernwartung alles zu beachten ist, damit der Datenschutz gewahrt bleibt. Zwischen dieser Anforderung und der Wirklichkeit klaffen häufig jedoch Welten. Vielfach schließen die datenverarbeitenden Stellen mit dem Fernwartungsunternehmen zwar einen Vertrag ab, der jedoch lediglich einen ganz allgemeinen und lapidaren Hinweis auf die Einhaltung der Datenschutzbestimmungen enthält. Dies reicht aber nicht aus. Vielmehr ist im abzuschließenden Fernwartungsvertrag konkret zu regeln, was die datenverarbeitende Stelle und das Fernwartungsunternehmen im einzelnen zu beachten haben. Insbesondere ist folgendes festzulegen:

- Die datenverarbeitende Stelle muß präzise beschreiben, welche Arbeiten für welche EDV-Systeme das Fernwartungsunternehmen durchzuführen hat.
- Die Fernwartungsarbeiten sind möglichst so zu gestalten, daß das Fernwartungsunternehmen keine Möglichkeit hat, auf gespeicherte personenbezogene Daten zuzugreifen. Sollte in Ausnahmefällen doch einmal ein solcher Zugriff notwendig sein, so unterliegen diese Daten einer Zweckbindung, d.h. das Fernwartungsunternehmen darf diese Daten ausschließlich für Wartungszwecke nutzen. Eine Weitergabe der durch den Zugriff auf die Daten erworbenen Kenntnisse an Dritte ist dem Fernwartungsunternehmen zu untersagen.

- Festzulegen ist, ob und, wenn ja, unter welchen Voraussetzungen Unterauftragsverhältnisse zulässig sind.
- In dem Vertrag sind schließlich auch die erforderlichen technischen und organisatorischen Maßnahmen festzulegen.
- Das Fernwartungspersonal ist auf das Datengeheimnis nach § 5 des Bundesdatenschutzgesetzes zu verpflichten.

6.9 Vernichtung von Unterlagen

Mühe bereitet mitunter auch die datenschutzgerechte Vernichtung von Unterlagen:

- Zwei Krankenhäuser ließen ihre Unterlagen zwar durch Spezialfirmen vernichten. Es existierten jedoch keinerlei schriftliche Vorgaben dafür, wie die Vernichtung zu erfolgen hat.
- Ein Sozialversicherungsträger vernichtete seine Unterlagen mit einem eigenen Aktenvernichter. Diese Maschine produzierte jedoch Papierteilchen, die bei weitem nicht den Anforderungen entsprachen, die die für die Vernichtung von Datenträgern einschlägige DIN-Norm 32757-1 für die Vernichtung von Unterlagen mit personenbezogenen Daten verlangt. Anstelle der für solche Fälle mindestens einzuhaltenden Sicherheitsstufe 3 entsprach die Vernichtung nur der Sicherheitsstufe 1.

6.10 Schriftliche Regelungen zum Datenschutz und zur Datensicherheit: Das Verfahrensverzeichnis

Wer personenbezogene Daten per EDV verarbeitet, ohne zugleich schriftlich zu dokumentieren, was er eigentlich tut, verliert nur allzu schnell den Überblick darüber, welche Daten er mit welchen EDV-Verfahren verarbeitet, wer auf die Daten zugreifen darf, wann er welche Daten wieder löschen muß und welche technischen und organisatorischen Maßnahmen er getroffen hat, um den mit der Datenverarbeitung einhergehenden Datenschutzrisiken entgegenzuwirken. Aus gutem Grund verlangt deshalb das Landesdatenschutzgesetz, diese und noch einige weitere Angaben in einem Verfahrensverzeichnis schriftlich festzuhalten. Nicht zuletzt erleichtert ein gut geführtes Verfahrensverzeichnis auch datenschutzrechtliche Überprüfungen, etwa durch einen internen Datenschutzbeauftragten vor Ort oder durch mein Amt. Die datenverarbeitenden Stellen tun sich bedauerlicherweise mit diesem Verzeichnis sehr schwer. Kaum eine Stelle konnte uns ein Verfahrensverzeichnis vorlegen, das diesen Namen auch verdient. Manche Stellen führen überhaupt kein solches Verzeichnis. Andere führen zwar ein Verzeichnis, das jedoch unvollständig ist. Wieder andere machen in ihrem Verfahrensverzeichnis nur wenig aussagekräftige Angaben. So war in einem Verfahrensverzeichnis für ein Bibliotheksverfahren zu lesen, damit wür-

den Daten "natürlicher Personen" verarbeitet. Gemeint waren natürlich die Personen, die am Ausleihverkehr der Bibliothek teilnehmen. Wegen der Bedeutung, die ein gut geführtes Verfahrensverzeichnis hat, habe ich Mängel in der Regel beanstandet und beabsichtige, dies auch in Zukunft zu tun.

2. Teil: Justiz und Öffentliche Sicherheit

1. Abschnitt: Die Justiz

1. Datenschutz - zu teuer?

   Spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 ist klar, daß gerade auch im Justizbereich, wo in großem Umfang sehr sensible Daten der Bürger verarbeitet werden, der Gesetzgeber gefordert ist. Das eine oder andere Gesetzesvorhaben hat inzwischen Bundestag und Bundesrat passiert; beispielsweise dieses Jahr das Justizmitteilungsgesetz. Andere, die teilweise bereits vor Jahren auf den Weg gebracht worden sind, haben die Ziellinie noch nicht erreicht. Leider erschöpfen sich die Aktivitäten des Gesetzgebers meist darin, die seit langem im Justizbereich praktizierte Datenverarbeitung in Gesetzesform zu gießen, anstatt sie auf den Prüfstand zu stellen und nur im wirklich unerläßlich notwendigen Umfang zuzulassen. Vorschläge meines Amtes und meiner Kollegen im Bund und in den Ländern hierzu verhallen oft genug. Mitunter werden in Gesetzentwürfen der Bundesregierung noch vorhandene datenschutzfreundliche Regelungen im Laufe des Gesetzgebungsverfahrens im Bundesrat gestrichen oder ins Gegenteil verkehrt. Dabei zeigt sich deutlich, daß in den Ländern der Datenschutz mehr und mehr nur als Kostenfaktor gesehen wird und dadurch den - zugegebenermaßen - angespannten Landeshaushalten immer öfter zum Opfer fällt. Damit wird man aber dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht.

   - Geradezu ein Musterbeispiel hierfür ist das vom Bundestag mit Zustimmung des Bundesrats beschlossene Justizmitteilungsgesetz (BGBl. I 1997, S. 1430), das am 1. Juni 1998 in Kraft tritt. In diesem Gesetz ist beispielsweise nichts mehr darüber zu lesen, daß Beschuldigte eines Strafverfahrens wenigstens in bestimmten Fällen - wie dies im Entwurf 1995 noch stand - darüber informiert werden müssen, wenn Gericht oder Staatsanwaltschaft eine Mitteilung über das Verfahren oder dessen Inhalt, z.B. an den Arbeitgeber oder Dienstherrn, vorgenommen haben. Dies wäre aber allein schon deshalb geboten gewesen, weil ein Betroffener dem Gesetz selbst nicht eindeutig entnehmen kann, mit welchen Mitteilungen er rechnen muß. Kein Wort ist im Justizmitteilungsgesetz auch darüber zu lesen, wer letztlich im Einzelfall die Mitteilung anzuordnen hat. Dabei wäre es wegen der nur allgemein und teilweise wenig präzise gefaßten gesetzlichen Mitteilungsermächtigungen und der damit einhergehenden, mitunter recht diffizilen Abwägungen wichtig gewesen, im Justizmitteilungsgesetz selbst festzulegen, in welchen Fällen dem Richter oder dem Staatsanwalt die Entscheidung über eine Mitteilung vorzubehalten ist. Das war jedoch dem Bundesrat zuviel des Aufwands und damit, kurz ge-

sagt, zu teuer. Dabei wäre auch ein anderer Weg zur Reduzierung des Verwaltungsaufwands gangbar gewesen: Anstatt an den datenschutzrechtlichen Standards zu sparen, hätte man durchaus Mitteilungsermächtigungen streichen können. Statt dessen hat das Justizmitteilungsgesetz diese Möglichkeiten gegenüber dem Status quo erweitert. So können beispielsweise nach dem neu geschaffenen § 49a Abs. 1 Satz 2 des Ordnungswidrigkeitengesetzes nun auch in Bußgeldsachen Daten an den Dienstherrn, die aufsichtführende Stelle oder den Arbeitgeber mitgeteilt werden.
Bis zum Inkrafttreten des Justizmitteilungsgesetzes am 1. Juni 1998 müssen jetzt die Verwaltungsvorschriften für die Mitteilungen in Straf- und Zivilsachen erarbeitet werden. Darin sollen dann die Fallgestaltungen konkret geregelt werden, in denen eine Mitteilung zu erfolgen und wer sie anzuordnen hat. Vielleicht lassen sich auf diesem Weg noch Verbesserungen für den Datenschutz erreichen. Das hängt nicht zuletzt davon ab, ob das Justizministerium des Landes sich in den maßgeblichen Gremien dafür einsetzen wird.

- Unter keinem allzu guten Stern steht auch das Strafverfahrensänderungsgesetz 1996. Mit dem von der Bundesregierung Ende 1996 vorgelegten Gesetzentwurf wird der weiß wievielte Anlauf unternommen, die Verarbeitung personenbezogener Daten im Strafverfahren in der Strafprozeßordnung zu regeln. Anfang des Jahres nahm mein Amt dem Justizministerium gegenüber dazu dezidiert Stellung, machte Vorschläge für datenschutzrechtliche Verbesserungen und bat es, sich bei der Beratung in den Gremien des Bundesrates dafür einzusetzen. Nach den ersten Beratungen des Gesetzentwurfs im Bundesrat mußten meine Kollegen und ich feststellen, daß unsere Bedenken und Empfehlungen nahezu ungehört geblieben waren. Damit nicht genug, der Bundesrat plädierte in seiner Stellungnahme auch noch für die Streichung einiger durchaus datenschutzfreundlicher Regelungen. Dabei tat sich das hiesige Justizministerium in den Beratungsgremien nicht gerade als Verfechter des Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung hervor. Im Gegenteil: Es setzte sich in den Beratungen im Verein mit anderen Bundesländern dafür ein, daß
  - der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung gestrichen werden soll,
  - das Auskunfts- und Akteneinsichtsrecht für öffentliche Stellen erheblich erweitert werden soll,
  - das Verbot gestrichen werden soll, bei Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens über die Grunddaten hinausgehende weitere Angaben in Dateien zu speichern,
  - Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien ersatzlos gestrichen werden sollen,

- Kontrollverfahren für automatisierte Abrufverfahren aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten entfallen sollen.

Dem Innenministerium war anderes ein Dorn im Auge. Es stieß bei den Beratungen im Bundesrat mit anderen Bundesländern ins gleiche Horn und setzte sich für die Streichung

- des Richtervorbehalts bei der Anordnung einer längerfristigen Observation und
- der Verwendungsbeschränkungen von Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht erhoben worden sind,

ein. Diese Entwicklung veranlaßte meine Kollegen und mich, in einer Entschließung (vgl. Anhang 5) die Bundesregierung und den Deutschen Bundestag aufzufordern, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen.

- Andere Gesetzesvorhaben, zu denen wir Stellung genommen haben, stecken dagegen noch in den Kinderschuhen:

  - Referentenentwurf eines Vierten Gesetzes zur Änderung des Bundeszentralregistergesetzes
    Wenn es nach ihm geht, darf - was zu begrüßen ist - die Tatsache, daß ein Strafverfahren oder Ermittlungsverfahren wegen Schuldunfähigkeit eingestellt worden ist, im Bundeszentralregister nur eingetragen werden, wenn ein Sachverständiger die Schuldunfähigkeit festgestellt hat und der Betroffene über die Eintragung unterrichtet ist. Wie notwendig eine solche Unterrichtung ist, weil eine Eintragung für den einzelnen erhebliche Konsequenzen haben kann, haben wir bereits im 16. Tätigkeitsbericht (LT-Drs. 11/6900, S. 41 f.) betont. Reduziert werden muß allerdings der im Entwurf zu großzügig vorgesehene Online-Zugriff auf das Bundeszentralregister; er sollte wegen den damit verbundenen Gefahren nur den Staatsanwaltschaften und Strafgerichten ermöglicht werden.

  - Vorläufige Referentenentwürfe eines Gesetzes über den Vollzug der Untersuchungshaft und eines Gesetzes zur Änderung des Strafvollzugsgesetzes
    Die dazu bisher bekanntgewordenen Entwürfe bestechen nicht gerade durch Klarheit, vor allem weil die Bestimmungen über die Datenverarbeitung generalklauselartig ausgefallen sind. Insbesondere fehlen konkrete Regelungen über die Führung und den Aufbau der Personalakten der Gefangenen. Wichtig wäre insbesondere, daß Gesundheitsakten und Akten, in denen gegebenenfalls angehaltene Schriftstücke und Mitschriften von Besucher- und Telefongesprächsüberwachungen aufgenommen werden, von den allgemeinen Personalakten getrennt geführt werden.

2. Unterbliebene Beteiligung mit Folgen

Bei der Lektüre der Stellungnahme des Justizministeriums zum Antrag der Fraktionen der CDU und der FDP/DVP zum Opferschutz und Täter-Opfer-Ausgleich (LT-Drs. 12/1359) stieß ich darauf, daß das Justizministerium die Verwaltungsvorschrift zum Landesgesetz für die Sozialarbeiter der Justiz (VV-JSG) geändert hatte. Die Änderung trat am 1. Juli 1997 in Kraft. An den Vorarbeiten zur Änderung der VV-JSG hatte das Justizministerium mein Amt nicht beteiligt, obwohl in den Vorschriftenrichtlinien der Landesregierung klipp und klar steht, daß es uns frühzeitig Gelegenheit geben muß, zu Entwürfen, die Auswirkungen auf die Verarbeitung personenbezogener Daten durch Behörden oder sonstige öffentliche Stellen haben, Stellung zu nehmen. Dabei wäre eine Beteiligung meines Amtes bei der Überarbeitung der Verwaltungsvorschriften dringend geboten gewesen. Denn aus der Sicht des Datenschutzes sind die in Kraft gesetzten Verwaltungsvorschriften in mancherlei Hinsicht verbesserungsbedürftig. Dies gilt insbesondere für die Regelung über die Akteneinsicht in Nr. 10 Abs. 2 VV-JSG. Denn danach soll die Einsichtnahme in die Bewährungshilfeakten durch andere Stellen und damit auch eine Übermittlung personenbezogener Daten bereits dann möglich sein, wenn keine gesetzlichen Bestimmungen, Verwaltungsvorschriften oder dienstliche Interessen entgegenstehen. Dieser Regelung liegt ein völlig antiquiertes Datenschutzverständnis zugrunde, sie ist deshalb nicht akzeptabel. Denn spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dez. 1983 steht fest, daß eine Übermittlung personenbezogener Daten wegen des damit einhergehenden Eingriffs in das Recht auf informationelle Selbstbestimmung nur aufgrund einer verfassungskonformen gesetzlichen Erlaubnisvorschrift erfolgen kann und nicht bereits dann - wie es aber in Nr. 10 Abs. 2 VV-JSG heißt - zulässig ist, wenn keine gesetzlichen Bestimmungen, Verwaltungsvorschriften oder dienstliche Interessen entgegenstehen. Darauf und auf andere Schwachstellen der Verwaltungsvorschrift wies ich Anfang Juli den Herrn Justizminister hin und bat ihn insbesondere, dafür zu sorgen, daß sein Haus mein Amt künftig bei Vorschriften, die für den Datenschutz von Bedeutung sind, frühzeitig beteiligt. Dieses ließ mich daraufhin wissen, daß es meine Kritik an der Regelung über die Akteneinsicht in Nr. 10 Abs. 2 VV-JSG teilt und die Dienststellen über die tatsächliche Rechtslage in puncto Akteneinsicht unterrichtet hat. Mein Amt habe es bei der Überarbeitung der VV-JSG nicht gehört, weil Vorschriften über die Verarbeitung personenbezogener Daten lediglich aus der alten Verwaltungsvorschrift wortgleich abgeschrieben worden seien. Das machte die Sache nicht besser, sondern war ja gerade die Crux. Weil die Reparatur der Regelung über die Akteneinsicht in den Verwaltungsvorschriften keinen Niederschlag gefunden hat und auch sonst manches verbesserungsbedürftig ist, habe ich das Justizministerium gebeten, die erneute Überarbeitung der VV-JSG alsbald in die Wege zu leiten.

3. Endlich datenschutzgerechter Erlaß für die Blutalkoholuntersuchung

Im Sommer 1994 hatte unser Amt unter die Lupe genommen, wie Polizei und Untersuchungsstellen im Rahmen von Blutalkoholbestimmungen mit den Daten erwischter alkoholisierter Autofahrer umgehen. Das Fazit war, daß Polizei und Untersuchungsstellen erheblich gegen den Datenschutz verstießen, weil sie sich an die "Gemeinsame Verwaltungsvorschrift von Innen-, Justiz-, Wissenschafts-, Sozial- und Umweltministerium zur Feststellung von Alkohol im Blut bei Straftaten und Ordnungswidrigkeiten" vom 2. Dez. 1988 (GABl. 1989, S. 34) hielten. Denn darin hatten die Ministerien Polizei und Untersuchungsstellen Weisungen erteilt, deren Befolgung geradewegs zu Verletzungen des Grundrechts auf Datenschutz vieler Bürger im Lande führte (vgl. 15. Tätigkeitsbericht, LT-Drs. 11/5000, S. 10 ff.). Deshalb war klar, daß die Gemeinsame Verwaltungsvorschrift einer ebenso raschen wie gründlichen Reparatur bedurfte. Das sah die Landesregierung in ihrer Stellungnahme zu unserem 15. Tätigkeitsbericht genauso (LT-Drs. 11/5653, S. 23). Dennoch kam die Sache unter der Federführung des Justizministeriums nicht recht vom Fleck. Nach einem glatten Fehlstart waren die Ministerien ein dreiviertel Jahr später praktisch noch keinen Schritt weiter. Das bedeutete im Ergebnis, daß nach wie vor unzulässige Datenübermittlungen zuhauf an Untersuchungsstellen und Rechtsmedizinische Institute erfolgten - gerade so, als ob die in Art. 20 GG festgelegte Bindung der Verwaltung an Recht und Gesetz hier nicht gelte und als ob in § 33 LDSG nicht stünde, daß unzulässige Datenübermittlungen den Tatbestand einer Ordnungswidrigkeit erfüllen. Auf unsere nachdrückliche Aufforderung, die bisherige Praxis unverzüglich einzustellen, zog das Innenministerium im Oktober 1995 die Notbremse und gab den Polizeidienststellen neue, ganz erheblich abgespeckte Formulare für die Aufträge von Blutalkoholuntersuchungen an die Hand. Damit war freilich das andere Problem, wie die Rechtsmedizinischen Institute für ihre Forschungsarbeiten in datenschutzgerechter Weise die Blutentnahmeprotokolle bekommen können, nicht vom Tisch. Erst nach mehr als insgesamt zwei Jahren schafften es die Ministerien endlich, die Materie datenschutzgerecht zu regeln. Der "Gemeinsame Erlaß des Innenministeriums, des Ministeriums für Wissenschaft, Forschung und Kunst, des Justizministeriums, des Ministeriums Ländlicher Raum, des Sozialministeriums und des Ministeriums für Umwelt und Verkehr über die Feststellung von Alkohol, Medikamenten, Drogeneinfluß bei Straftaten und Ordnungswidrigkeiten; Sicherstellung und Beschlagnahme von Fahrausweisen" (Die Justiz 1997, S. 110) trat am 15. März 1997 in Kraft. Jetzt gibt die Polizei den Untersuchungsstellen nicht mehr wie früher das komplette Blutentnahmeprotokoll weiter. Sie erfahren nur noch die Angaben, die sie für die Bestimmung des Blutalkoholgehalts und für die eindeutige Zuordnung der Blutprobe zu demjenigen brauchen, von dem sie stammt. Die Rechtsmedizinischen Institute erhal-

ten für ihre Forschungsarbeit die kompletten Blutentnahmeprotokolle nur noch in anonymisierter Form.

4. Aus dem Justizalltag

Wie in den vergangenen Jahren wandten sich auch heuer viele Bürger an mein Amt, weil sie nicht damit zufrieden waren, wie Justizbehörden mit ihren Datenschutzrechten umgingen. Manche hatten Recht. Die Ursachen lagen unterschiedlich. Sogar ein glatter Fall von Datenmißbrauch einer Oberamtsanwältin war darunter.

4.1 Die Auskunft: Eine schwere Geburt

Das Auskunftsrecht ist seit jeher das vornehmste Datenschutzrecht eines jeden Bürgers. Wie schwer sich Staatsanwaltschaften noch heute damit tun, erlebten wir 1997. Ein Mann hatte bei zwei Staatsanwaltschaften um Auskunft nachgesucht, was über ihn jeweils in der Zentralen Namenskartei gespeichert ist. Die beiden Staatsanwaltschaften teilten ihm kurz und knapp mit, daß ihm eine Auskunft über die in der Zentralen Namenskartei zu seiner Person gespeicherten Daten nicht erteilt werden könne, weil es sich dabei nicht um eine Datei im Sinne des Landesdatenschutzgesetzes, sondern um eine rein interne Hilfe zum Auffinden von Aktenvorgängen handele. Der Mann staunte nicht schlecht und wandte sich an uns.

Mit ihrer Ansicht lagen die beiden Staatsanwaltschaften gründlich daneben. Wie in vielen anderen Fällen hätte ein Blick in das Gesetz, hier in das Landesdatenschutzgesetz, geholfen. In dessen § 17 steht klipp und klar, daß dem Betroffenen auf Antrag unentgeltlich Auskunft über die zu seiner Person gespeicherten Daten zu erteilen ist. Statt dessen hielten sich die beiden Staatsanwaltschaften an den Buchstaben der Allgemeinen Verfügung des Justizministeriums zu den Zentralen Namenskarteien fest, in der tatsächlich steht, daß die Zentralen Namenskarteien ein internes Hilfsmittel zum Auffinden der Akten sind und daher Auskunftsersuchen aus ihnen nicht beantwortet werden dürfen. Um zu verstehen, was mit diesem, in der Tat mehr als mißverständlichen Passus in der Allgemeinen Verfügung wirklich gemeint ist, muß man folgendes wissen:

Seit langem führen die Staatsanwaltschaften im Land Zentrale Namenskarteien. Darin erfassen sie alle Personen, gegen die bei ihnen ein Ermittlungsverfahren läuft oder lief. Als unser Amt schon 1980 feststellte, daß die Staatsanwaltschaften in ihren Zentralen Namenskarteien viel zu viele Personen viel zu lange speichern - manchmal sogar noch nach rechtskräftigem Freispruch wegen erwiesener Unschuld - und deshalb deren Bereinigung forderte, pflichtete uns das Justizministerium zwar im Grundsatz bei. Anstatt jedoch das Problem an der

Wurzel zu packen, verfiel es auf eine Scheinlösung. Es erklärte 1982 die Zentralen Namenskarteien zu sog. internen Karteien, um den Reglementierungen des alten Landesdatenschutzgesetzes zu entgehen und insbesondere dessen Vorschriften über das Speichern, Übermitteln und Löschen sowie über die Auskunftserteilung an Bürger, die wissen wollten, was in den Zentralen Namenskarteien über sie steht, nicht anwenden zu müssen. Dies konnte das Justizministerium wegen der Regelung des § 2 Abs. 2 des alten Landesdatenschutzgesetzes nur erreichen, indem es den Staatsanwaltschaften jegliche Datenübermittlungen aus den Zentralen Namenskarteien - also auch die Beantwortung von Anfragen anderer Behörden aus diesen Karteien - untersagte. Dies tat es dann mit seiner Allgemeinen Verfügung vom 13. Sept. 1982 (Die Justiz, S. 360). Daß das Justizministerium in diesem Zusammenhang bei den Anfragen anderer Behörden von Auskunftsersuchen sprach und dies bei der Überarbeitung der Allgemeinen Verfügung so stehen ließ, war und ist in zweierlei Hinsicht irreführend: Zum einen steht der Begriff der Auskunft in der datenschutzrechtlichen Terminologie für das Recht des Betroffenen, zu erfahren, welche Daten über ihn gespeichert sind. Zum anderen kennt das seit 1. Dez. 1991 geltende neue Landesdatenschutzgesetz keine Extrawürste mehr für sog. interne Karteien. Seither ist klar, daß jeder Bürger nach § 17 LDSG Anspruch hat zu erfahren, was die Staatsanwaltschaften über ihn in ihren Zentralen Namenskarteien speichern.

Auf die Gefahr einer solche Fehlinterpretation des in der Allgemeinen Verfügung verwendeten Begriffs "Auskunftsersuchen", wie sie den beiden Staatsanwaltschaften unterlaufen ist, haben wir das Justizministerium bereits 1994 im Zuge der Überarbeitung der Allgemeinen Verfügung hingewiesen. Unseren Vorschlag, der für Klarheit gesorgt hätte, hat das Justizministerium nicht aufgegriffen. Wie notwendig dies gewesen wäre, zeigt das Beispiel der beiden Staatsanwaltschaften. Deshalb habe ich das Justizministerium im März dieses Jahres erneut gebeten, diesen Punkt für die Neufassung der Allgemeinen Verfügung zu den Zentralen Namenskarteien vorzumerken und in geeigneter Weise sicherzustellen, daß die Staatsanwaltschaften bei Auskunftsanträgen über Datenspeicherungen in ihren Zentralen Namenskarteien so verfahren, wie es § 17 LDSG gebietet. Was das Justizministerium dazu unternommen hat, hat es mir bisher nicht mitgeteilt.

4.2 Zur Besichtigung freigegeben?

"Wie ein Äffle in der Wilhelma" fühlte sich ein Strafgefangener der Außenstelle einer Justizvollzugsanstalt, wie er mir schrieb. Er verbüßte dort eine dreimonatige Freiheitsstrafe und sah sich den Blicken einer Schulklasse und anderer Be-

sucher ausgesetzt, die ohne Vorankündigung durch die Anstalt und den Arbeitsbetrieb geführt worden waren. Da der Gefangene nach seiner Entlassung wieder seiner alten Tätigkeit nachgehen und auf Wochenmärkten in der Gegend Geflügel und Eier verkaufen wollte, befürchtete er, dann dort von Besuchern der Außenstelle erkannt zu werden. Um so verständlicher war sein Wunsch, die Tatsache seines Gefängnisaufenthalts möglichst geheimzuhalten. Ein solches Anliegen von Strafgefangenen halte ich für berechtigt, da das Bekanntwerden einer Inhaftierung zu einer sozialen Abstempelung auch über die Dauer der Haft hinaus und zu erheblichen Belastungen für die Familien der Gefangenen führen kann. Deshalb bat ich die Justizvollzugsanstalt, Besucherführungen vorher anzukündigen und den Gefangenen die Möglichkeit zu geben, sich zurückzuziehen. Sie zeigte uns jedoch die kalte Schulter. Wer seine Anonymität wahren wolle, dürfe eben nicht in den offenen Vollzug in der Außenstelle einwilligen, ließ uns die Justizvollzugsanstalt wissen. Dabei hatte sie jedoch folgendes nicht bedacht: Daß mit der Unterbringung eines Gefangenen im offenen Vollzug Kontakte mit anstaltsfremden Personen einhergehen können, liegt in der Natur der Sache. Das weiß jeder Gefangene, der in den offenen Vollzug einwilligt. Zu den mit dem offenen Vollzug zwangsläufig verbundenen Kontakten gehören aber Besucherführungen gerade nicht. Vielmehr stellt sich das Problem, wie dabei der Persönlichkeitsschutz der Gefangenen gewährleistet werden kann, im offenen wie im geschlossenen Vollzug gleichermaßen. Deshalb ist klar, daß ein Gefangener mit seiner Einwilligung in den offenen Vollzug nicht gleichzeitig auch darin einwilligt, den Blicken von Besuchern und damit der Gefahr eines Wiedererkanntwerdens ausgesetzt zu sein. So sah es auch das Justizministerium, als wir es auf die Haltung der Justizvollzugsanstalt ansprachen. Per Erlaß empfahl es der Justizvollzugsanstalt, sich der in vielen anderen Justizvollzugsanstalten gepflegten Praxis anzuschließen und den Gefangenen die Führung von Besuchern kurz vorher anzukündigen und ihnen die Möglichkeit zu geben, sich der Blicke der Besucher auf geeignete Weise zu entziehen. Dies sollte wirklich in allen Justizvollzugsanstalten Standard sein.

4.3 Briefumschlag für die Postzustellung

Manchmal geraten auch so profane Dinge wie Briefumschläge ins Visier unseres Amtes. So geschehen, als wir der Klage einer verärgerten Bürgerin nachgingen, ihr würde ein Amtsgericht immer wieder Schreiben, in denen es unter anderem um die Unterbringung ihres Sohnes in einer geschlossenen Anstalt ging, durch die Post in unverschlossenen oder unzureichend verschlossenen Briefumschlägen zustellen lassen. Rasch stellte sich bei unseren Recherchen heraus, daß die vom Gericht verwendeten blauen Briefumschläge der Stein des Anstoßes waren. Sie waren an der linken Seite nur unzureichend verklebt und

entsprachen deshalb nicht den Anforderungen der Zivilprozeßordnung. Diese verlangt nämlich für eine wirksame Zustellung, daß das amtliche Schriftstück in einem verschlossenen Umschlag zugestellt wird. Außerdem soll der Postzustellungsbriefumschlag, wie jeder Briefumschlag, das darin verschlossene Schriftstück vor der Einsichtnahme Dritter schützen. Man denke nur daran, daß das amtliche Schreiben mit den darin enthaltenen sensiblen Informationen nicht direkt dem Empfänger, sondern ersatzweise anderen Personen übergeben wird. Auf diesen Mangel der für die Postzustellung eingesetzten Briefumschläge haben wir das Justizministerium hingewiesen. Nachdem es mit der Herstellerfirma Rücksprache gehalten hatte, ließ es uns wissen, daß die Briefumschläge ab der nächsten Neuauflage auch auf der linken Seite vollständig verklebt werden.

4.4 Die Gefangenenpost

Auch ein Strafgefangener hat grundsätzlich das Recht, unbeschränkt Schreiben abzusenden und zu empfangen. Zwar darf in dieses Recht aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt eingegriffen werden. Der Schriftverkehr mit Verteidigern, mit den Volksvertretungen des Bundes und der Länder sowie deren Mitgliedern, mit der Europäischen Kommission für Menschenrechte sowie mit den Datenschutzbeauftragten des Bundes und der Länder ist jedoch für die Vollzugsanstalten tabu; sie müssen solche Briefe den Gefangenen ungeöffnet aushändigen. So steht es in den einschlägigen Vorschriften. Damit hat die Justizvollzugsanstalt Bruchsal offenbar enorme Probleme. Sie hatte innerhalb von drei Monaten an ein und denselben Strafgefangenen adressierte Briefe eines Abgeordneten des Bundestages, des Petitionsausschusses des Deutschen Bundestages und des Landtags von Baden-Württemberg sowie mehrere Briefe des Bundesbeauftragten für den Datenschutz geöffnet. Als wir sie darauf hinwiesen, berief sie sich auf die täglich anfallende große Menge an Post, die durch die Poststelle zu bearbeiten sei, und auf den vertretungsweisen Einsatz von weniger erfahrenen Bediensteten in der Poststelle. Damit solche Briefe künftig nicht mehr geöffnet werden, nahm die Justizvollzugsanstalt - wie sie uns wissen ließ - den Vorfall zum Anlaß, die zuständigen Beamten erneut auf ihre besondere Sorgfaltspflicht beim Umgang mit Gefangenenpost hinzuweisen. Das scheint jedoch nicht viel geholfen zu haben: Denn kurz danach hat sich wiederum ein Gefangener der Justizvollzugsanstalt Bruchsal bei mir darüber beklagt, daß ein an ihn gerichteter Brief eines Bundestagsabgeordneten von der Justizvollzugsanstalt geöffnet worden war. Bei allem Verständnis für die Arbeit der Poststelle muß es doch möglich sein, bei der sowieso notwendigen Vorsortierung der eingehenden Post die von der Überwachung ausgenommenen Briefe auszusortieren und den Gefangenen ungeöffnet auszuhändigen. Dies gebietet auch der Respekt vor den Abgeordneten der Par-

lamente und den anderen genannten Stellen, deren Post an Strafgefangene ungeöffnet bleiben muß.

4.5 Mühsame Wahrheitsfindung

Mit einem bösen Erwachen begann für eine Frau der Tag der Deutschen Einheit im letzten Jahr - am Morgen des Feiertags war ihr Auto weg. Doch nicht ein Dieb, sondern ihr Ehemann, von dem sie sich getrennt hatte, hatte das Vehikel an sich genommen. Das kam so: Eine Nachbarin störte es, daß das Auto der Frau mit Kennzeichen aus dem Süden des Landes vor ihrem Haus geparkt war. Sie klemmte deshalb einen Zettel unter die Scheibenwischer, auf dem der Hinweis "Dies ist kein Dauerparkplatz!" stand. Weil das Parken dort aber nicht verboten war, ließ die Frau ihr Auto stehen. Dann habe sich ihr, wie die Nachbarin die Geschichte später darstellte, "berufsbedingt der Verdacht aufgedrängt, daß mit dem Auto etwas nicht stimmen könnte". Sie habe deshalb das zuständige Polizeirevier gebeten, sich der Sache anzunehmen. Innerhalb einer Woche habe sie von dort aber nichts gehört. Nun schritt sie selbst zur Tat und wurde "amtlich". Sie nutzte ihre Stellung als Oberamtsanwältin bei der Staatsanwaltschaft und ersuchte per Telefax das Bürgermeisteramt der Kreisstadt, ihr den Halter des fraglichen Fahrzeugs zu nennen. Weil das örtliche Fahrzeugregister aber nicht von der Stadt, sondern vom Landratsamt geführt wird, gab sie das Ersuchen an diese Stelle weiter. Von dort bekam die Oberamtsanwältin den Ehemann der Petentin als Halter genannt. Sie rief ihn an und gab ihm den Standort des Autos bekannt, worauf dieser das Auto abholte. Von meinem Amt mit diesem Sachverhalt konfrontiert, beschränkte sich die Staatsanwaltschaft darauf, die Oberamtsanwältin anzuhören und schenkte ihrer Behauptung Glauben, sie habe die Halteranfrage aus rein dienstlicher Motivation gestellt. Unsere parallel geführten Recherchen förderten allerdings ganz anderes zutage, denn zum Glück hatte das Landratsamt entgegen der sonst üblichen Gepflogenheit das Auskunftsersuchen aufgehoben. Dem war nämlich als Grund für die Anfrage ein von ihr willkürlich ausgewähltes Ermittlungsverfahren zu entnehmen. Dabei nannte sie auch noch die zwei dort Beschuldigten namentlich. Zudem stellte sich heraus, daß sie das Ersuchen schon zwei Wochen früher als von ihr behauptet gestellt hatte. Als dann noch die Polizei mitteilte, sie wisse nichts von einem Kontakt mit der Oberamtsanwältin in dieser Sache, überraschte das nicht. Auf Vorhalt unseres Ermittlungsergebnisses räumte die Staatsanwaltschaft - ein Jahr war inzwischen vergangen - den privaten Charakter der Halteranfrage und damit den Datenschutzverstoß ein. Diesen beanstandete ich ebenso wie die Weitergabe der Namen der Beschuldigten an die Stadt. Das Justizministerium sah die Sache genauso, hielt aber die förmliche Beanstandung nicht für angemessen, weil die Staatsanwaltschaft die Verstöße nicht habe

vermeiden können und für sie nichts zu veranlassen gewesen sei. Hier irrt das Justizministerium, denn offenbar ist bei der betroffenen Staatsanwaltschaft nicht ausreichend sichergestellt, daß ihre Mitarbeiter dem strafprozessualen Grundsatz der Aktenwahrheit und Aktenvollständigkeit Rechnung tragen und ihre Ermittlungshandlungen und deren Ergebnis aktenkundig machen. Anders ist nicht zu erklären, daß die Staatsanwaltschaft aufgrund unserer Anfrage nicht nach der Halterauskunft des Landratsamts sowie dem zugrundeliegenden Ersuchen forschte und sich die betreffenden Akten vorlegen ließ. Wäre das Ersuchen und die Auskunft in der von der Oberamtsanwältin angegebenen Ermittlungsakte enthalten gewesen, wäre der private Charakter des Auskunftsersuchens offenkundig gewesen. Wären dagegen das Ersuchen und die Auskunft dort nicht dokumentiert gewesen, hätte es auf der Hand gelegen, an der Richtigkeit der Einlassungen der Oberamtsanwältin zu zweifeln.

2. Abschnitt: Polizei

Lange stand die Polizei hierzulande vor einem Dilemma: Ging es darum, ob und wie sie Informationen in ihren eigenen Systemen, beispielsweise in ihrer PAD, verarbeiten darf, konnte sie seit 1992 im damals geänderten Polizeigesetz des Landes nachschauen, seit August 1997 auch noch in einer dazu ergangenen umfangreichen Verwaltungsvorschrift des Innenministeriums. Anders sah es dagegen bei den von den Polizeien des Bundes und der Länder gemeinsam geführten Informationssystemen, beispielsweise dem bundesweiten Kriminalaktennachweis (KAN), aus. Dabei half ihr ein Blick in das einschlägige Bundeskriminalamtsgesetz (BKAG) bis vor kurzem nichts. Denn erst das neue Bundeskriminalamtsgesetz, das am 1. Aug. 1997 in Kraft getreten ist, enthält dazu konkrete Aussagen. Dabei gibt es Licht und Schatten. Erfreulich ist insbesondere, daß

- Zeugen, mögliche Opfer, Hinweisgeber und sonstige Auskunftspersonen grundsätzlich nur mit ihrer Einwilligung registriert werden dürfen,
- die Übermittlung von Informationen verboten ist, wenn überwiegende schutzwürdige Interessen der Betroffenen oder gesetzliche Verwendungsregelungen entgegenstehen und
- die im Polizeigesetz und der Durchführungsverordnung zum Polizeigesetz geregelten Löschungsfristen für Datenspeicherungen unserer Polizei in INPOL maßgebend sind.

Zu den neuralgischen Punkten des neuen Bundeskriminalamtsgesetzes zählt dagegen insbesondere:

- Es verwendet den recht konturenlosen Begriff der Straftaten von erheblicher Bedeutung. Die Folge davon ist, daß nicht eindeutig vorhersehbar ist, wann die an diesen Begriff anknüpfenden Datenverarbeitungsbefugnisse eröffnet sind, wann also bei-

spielsweise Informationen über Kontakt- und Begleitpersonen gespeichert werden dürfen.
- Das Bundeskriminalamt darf als Zentralstelle an ausländische und zwischenstaatliche Stellen Daten übermitteln und mit diesen sogar einen automatisierten Datenverbund eingehen, ohne die jeweils verantwortlichen Länderpolizeien, von denen die Daten stammen, fragen zu müssen.
- Beim Einsatz von sog. Personenschutzsendern angefallene Zufallserkenntnisse dürfen als Ermittlungsansatz für die Verfolgung jedweder Straftat genutzt werden.

Die angesprochene Verwaltungsvorschrift des Innenministeriums zum Polizeigesetz gibt den Polizeibeamten für ihre tägliche Arbeit Hinweise, was sie beim Erheben, Speichern, Nutzen und Übermitteln von Informationen beachten müssen. Deshalb schalteten wir uns intensiv in die Vorbereitung dieser Verwaltungsvorschrift ein. Viele unserer Vorschläge fanden Gehör. Einige Punkte haben wir uns anders vorgestellt:

- Muß ein Behördenmitarbeiter beurteilen, ob eine Behörde eine Polizeibehörde im Sinne des Polizeigesetzes ist, verlangt die Verwaltungsvorschrift von ihm schier Unmögliches: Er muß sich nämlich darüber klar werden, ob die Behörde "nach Landesrecht und herkömmlichem Verständnis in nicht ganz unerheblichem Umfang Aufgaben der Gefahrenabwehr wahrnimmt". Das ist keine ganz unwichtige Frage. Von ihrer Beantwortung hängt nämlich ab, ob die Behörde die Datenverarbeitungsregelungen des Polizeigesetzes oder des Landesdatenschutzgesetzes, die ja durchaus unterschiedlich sind, zu beachten hat. Unser Vorschlag war, daß eine Behörde nur dann Polizeibehörde sein soll, wenn ein Gesetz sie ausdrücklich als solche bezeichnet oder ihr Aufgaben und Befugnisse nach dem Polizeigesetz eingeräumt sind. Damit wäre eine klare Abgrenzung möglich gewesen.
- Die Frage, ob es beim Einsatz Verdeckter Ermittler sog. unvermeidbar betroffene Dritte geben kann und, wenn ja, wer dies sein soll, stellte sich schlaglichtartig im Zusammenhang mit dem Einsatz zweier Verdeckter Ermittler des Landeskriminalamts 1992 in Tübingen. Die beiden Verdeckten Ermittler verkehrten unter anderem in einem Arbeitskreis der evangelischen Studentengemeinde und hatten über eine Reihe von völlig unverdächtigen Teilnehmern dem Landeskriminalamt regelmäßig berichtet (vgl. 14. Tätigkeitsbericht, LT-Drs. 11/2900, S. 36). Uns kam es deshalb darauf an, solchem künftig via Verwaltungsvorschrift vorzubauen. Ob dies mit dem Hinweis in der Verwaltungsvorschrift bewerkstelligt werden kann, daß unvermeidbar betroffene Dritte auch Personen sind, mit denen ein Verdeckter Ermittler im Rahmen der sozial üblichen Kontakte in Verbindung getreten ist, ist zumindest fraglich. Denn was unter üblichen sozialen Kontakten zu verstehen ist, erläutert die Verwaltungsvorschrift nicht.
- Hat die Polizei Informationen erhoben, die einem Berufs- oder besonderen Amtsgeheimnis - z.B. dem Arztgeheimnis - unterliegen, darf sie diese zu einem anderen Zweck nur verwenden, wenn die zur Verschwiegenheit verpflichtete Stelle - in unse-

rem Beispiel also der Arzt - eingewilligt hat. So steht es auch in der Verwaltungsvorschrift. Um in der polizeilichen Praxis den unzutreffenden Eindruck zu vermeiden, der Arzt könnte nach eigenem Gusto einwilligen oder nicht, wäre uns ein Hinweis darauf wichtig gewesen, daß der Arzt dies nur tun darf, wenn ihm eine gesetzliche Vorschrift die Durchbrechung seiner ärztlichen Schweigepflicht erlaubt oder wenn der Patient, um dessen Daten es geht, eingewilligt hat.

Klare gesetzliche Regelungen und erläuternde Hinweise in Verwaltungsvorschriften sind freilich eine Sache, die Praxis der polizeilichen Datenverarbeitung ist mitunter eine andere. Dies zeigte sich auch 1997.

1. Strukturelle Fehler bei der Speicherung von Rauschgiftdelikten

Wer unerlaubt Haschisch, Marihuana, Kokain, Heroin oder sonstige Betäubungsmittel anbaut, herstellt, veräußert, abgibt, erwirbt oder damit handelt, macht sich strafbar; so steht es im Betäubungsmittelgesetz (BtMG). Wen dabei die Polizei ertappt, gegen den leitet sie strafrechtliche Ermittlungen ein. Außerdem muß er damit rechnen, daß er sich in der Personenauskunftsdatei (PAD), das ist das landesweit automatisiert geführte Informationssystem der baden-württembergischen Polizei, und in der Falldatei Rauschgift (FDR), der auf dem Rechner des Bundeskriminalamts laufenden, bundesweiten Datei über mutmaßlich oder tatsächlich begangene Rauschgiftdelikte, wiederfindet. Dazu muß man wissen: Ermittelt die Polizei wegen einer Rauschgiftstraftat, muß sie - wie bei jeder anderen Straftat auch - den üblichen Formularsatz für die Datenerfassung ausfüllen. Darin trägt sie unter anderem ein, wie der Beschuldigte heißt, wann er geboren ist, wo er wohnt und faßt in wenigen Sätzen zusammen, welches Rauschgiftdelikt ihm zur Last gelegt wird. Einen Durchschlag davon schickt sie der Datenstation ihrer Polizeidirektion für die Registrierung des Beschuldigten in der PAD, einen weiteren Durchschlag erhält das Landeskriminalamt für die FDR-Erfassung, das diese Aufgabe zentral erledigt.

Vor kurzem nahmen wir dieses Zusammenspiel bei der FDR- und PAD-Erfassung von mutmaßlich oder tatsächlich begangenen Rauschgiftdelikten im Landeskriminalamt und bei den Polizeidirektionen Esslingen und Ulm unter die Lupe. Zuvor hatten wir anhand einer systematischen Auswertung der FDR, die Bundes- und Landeskriminalamt auf meine Bitte durchgeführt hatten, festgestellt, daß das Landeskriminalamt Ende Juni 1997 insgesamt 51 000 Personen in der FDR erfaßt hatte; 33 000 Personen davon waren jeweils wegen eines einzigen mutmaßlich oder tatsächlich begangenen Rauschgiftdelikts registriert. Auf diese Einmalspeicherungen in der FDR konzentrierten wir uns bei unseren Kontrollbesuchen, bei denen wir uns eine Stichprobe von insgesamt 350 Fällen näher ansahen. Das Ergebnis sieht so aus:

1.1 Rechtzeitige Löschung in der FDR nicht gewährleistet

Keine Frage: Ohne das Sammeln und Speichern von Daten ist polizeiliche Arbeit nicht denkbar. Genauso klar ist aber auch, daß sich die Polizei wieder von ihren Informationen trennen muß, wenn die dafür maßgebende Speicherfrist abgelaufen ist oder wenn sie schon vorher im Einzelfall feststellt, daß sie die Informationen für die vorbeugende Bekämpfung von Straftaten nicht mehr braucht. Ist dies so, muß die Polizei die in ihrem Computer gespeicherten Daten löschen und die der Datenspeicherung zugrundeliegenden Akten und Unterlagen vernichten. So verlangen es die §§ 38, 46 des Polizeigesetzes (PolG). Hat sie ein und denselben Fall in zwei verschiedenen Computern gespeichert, muß sie natürlich dafür sorgen, daß der Fall unverzüglich hier wie dort gelöscht wird.

1.1.1 Die Realität in der FDR

Wir staunten nicht schlecht, als wir bei unseren Kontrollbesuchen sahen, wie dieser Gleichschritt bei der Datenlöschung in der FDR außer Tritt geraten war. In sage und schreibe der Hälfte der Fälle der Stichprobe hatten die Polizeidirektionen Esslingen und Ulm schon lange vor dem Kontrollbesuch selbst festgestellt, daß die weitere Speicherung der mutmaßlich oder tatsächlich begangenen Rauschgiftdelikte für die Arbeit der Polizei nicht mehr notwendig war und daraus die gebotenen Konsequenzen gezogen: Löschung der Rauschgiftdelikte in der PAD und die Vernichtung der einschlägigen Akten und Unterlagen. Auch das Landeskriminalamt hatte seine Durchschläge des Datenerfassungsformulars längst durch den Reißwolf geschoben. Trotzdem sind die Rauschgiftdelikte aber nach wie vor in der FDR gespeichert - nur weil die Polizeidienststellen, als sie zur Datenlöschung schritten, aus den Augen verloren hatten, daß die Fälle einst auch in die FDR eingespeichert worden waren, unterblieb deren Löschung dort. So kam es, daß eine Vielzahl von Personen länger in der FDR gespeichert ist als erlaubt. Beispielsweise ist

- über einen Ulmer Studenten in der FDR immer noch gespeichert, daß er im September 1990 auf dem Gelände der Universität Ulm einmal Haschisch geraucht haben soll;
- über einen 29 Jahre alten Straßenwart in der FDR immer noch registriert, daß er im Sommer 1990 in Ulm einmal eine Haschischzigarette erworben haben soll;
- über einen 37 Jahre alten Feinmechaniker in der FDR immer noch gespeichert, daß er im Sommer 1992 in Esslingen einmal Haschisch erworben haben soll;

- über einen amerikanischen Soldaten in der FDR immer noch festgehalten, daß er vor mehr als 10 Jahren einmal Haschisch besessen haben soll;
- über eine 35 Jahre alte Hotelfachfrau in der FDR immer noch registriert, daß sie im Oktober 1988 einmal Betäubungsmittel (Heroin) erworben haben soll.

Wer meint, solches sei belanglos, irrt. Wer nämlich mit einem Hinweis auf Rauschgift in der FDR, die alle Polizeibeamten rund um die Uhr in Sekundenschnelle abfragen können, gespeichert ist, läuft Gefahr, beispielsweise bei polizeilichen Kontrollen als jemand angesehen zu werden, der nach wie vor mit Rauschgift zu tun hat. Wie belastend dies sein kann, erfuhr beispielsweise ein 40jähriger Mann. Er war im Frühjahr 1997 in eine Polizeikontrolle geraten. Nachdem die Polizeibeamten eine Computerabfrage gestartet und dabei erfahren hatten, daß der Mann wegen eines Verstoßes gegen das Betäubungsmittelgesetz registriert war, unterzogen sie ihn einer Leibesvisitation. Weil er sich zu Unrecht registriert sah, wandte der Mann sich an mein Amt. Wie es 1991 zur Einspeicherung des Rauschgifthinweises gekommen war und was genau damals dahinter stand, ließ sich nicht mehr klären. Versichern konnte ich ihm jedoch, daß die Polizei auf unsere Initiative hin den Rauschgifthinweis im Computer gelöscht hatte; anderes war über ihn nicht gespeichert.

Wenngleich es freilich nicht jedem so ergehen muß, der über Gebühr lange in der FDR erfaßt ist, ist dennoch unerläßlich, daß die Polizei für eine rechtzeitige Löschung in der FDR sorgt und niemanden länger als von Rechts wegen erlaubt wegen eines mutmaßlich oder tatsächlich begangenen Rauschgiftdelikts in der FDR speichert. Gerade das Gegenteil geschah aber nur zu oft.

1.1.2 Die Ursachen

Wie es kommen konnte, daß die Datenlöschung in der FDR so aus dem Ruder lief, ließ sich nicht mehr hieb- und stichfest klären. Sämtliche Akten und Unterlagen über diese FDR-Speicherungen hatte die Polizei - zu Recht - ja schon längst vernichtet. Die FDR-Computerausdrucke gaben nicht auf alle Fragen Anwort; dafür sind sie auch nicht geschaffen. Immerhin ließ sich mit ihrer Hilfe noch manches rekonstruieren. Danach spricht alles dafür, daß das Malheur mit den unterbliebenen Löschungen in der FDR mehrere Ursachen hat:

- Das Innenministerium senkte 1991 die PAD-Regelspeicherfrist für Erwachsene von zehn auf fünf Jahre, nachdem unser Amt in seinem 11. Tätigkeitsbericht die unverhältnismäßig lange PAD-Speicherfristenspirale kritisiert und der Landtag daraufhin eine Änderung der PAD-Programme verlangt hatte (vgl. LT-Drs. 10/4510, S. 40 f.; LT-Drs. 10/6358). Die gewiß mit nicht wenig Aufwand verbundene Umstellung der PAD-Speicherfristen meisterte die Polizei in den Jahren 1993 und 1994. Dabei löschte sie zigtausende PAD-Speicherungen, darunter viele mutmaßlich oder tatsächlich begangene Rauschgiftdelikte. Offenbar hatte sie sich damals ganz auf die PAD konzentriert und übersehen, daß sie die Fälle Zug um Zug auch in der FDR hätte löschen müssen.
- Die Polizeidienststellen sind nach den einschlägigen Vorschriften verpflichtet, das Landeskriminalamt zu unterrichten, wenn sie aufgrund einer Einzelfallentscheidung schon vor Ablauf der Regelspeicherfrist ein Rauschgiftdelikt in der PAD löschen. Das ist auch gut so. Denn jetzt weiß das Landeskriminalamt, daß es den Fall auch in der FDR löschen muß. Solche Hinweise an das Landeskriminalamt sind jedoch nicht Usus bei den vielen Regellöschungen, bei denen die Polizeidienststellen im Halbjahresturnus die Fälle mit abgelaufener Speicherfrist in der PAD löschen. Handelt es sich dabei um ein Rauschgiftdelikt, kann die Löschung in der FDR auf der Strecke bleiben, weil das Landeskriminalamt nicht erfährt, daß es die FDR-Löschtaste drücken muß.
- Das Landeskriminalamt wies uns auf ein weiteres Manko hin. Es hatte sich im Zuge unserer Kontrollbesuche die Listen, die es regelmäßig vom Bundeskriminalamt über FDR-Speicherungen mit alsbald ablaufender Speicherfrist erhält, näher angeschaut und dabei festgestellt, daß diese Listen offenbar nicht vollständig waren. An was das wiederum genau lag, wußte das Landeskriminalamt selbst nicht.

1.1.3 Bewertung

Diese Gestaltung des FDR-Löschverfahrens trägt den §§ 38, 42 PolG i.V. mit § 11 BKAG nicht Rechnung. Danach darf die Polizei Personen, die eines Rauschgiftdelikts verdächtig sind oder ein solches begangen haben, nur so lange in der FDR registrieren, wie dies zur Strafverfolgung und zur vorbeugenden Bekämpfung von Rauschgiftdelikten erforderlich ist. Liegen diese Voraussetzungen nicht mehr vor, muß die Polizei die FDR-Speicherungen umgehend löschen. Gerade dies ist aber in praktisch jedem zweiten Fall der Stichprobe unterblieben, obwohl die

ermittelnden Polizeidienststellen in Kenntnis aller Umstände selbst längst festgestellt hatten, daß jegliche polizeiliche Datenspeicherung über diese mutmaßlich oder tatsächlich begangenen Rauschgiftdelikte für die Aufgabenerfüllung der Polizei nicht mehr erforderlich ist. Daß die FDR-Speicherungen trotzdem nicht gelöscht worden sind, ist auch mit § 48 PolG i.V. mit § 9 LDSG nicht zu vereinbaren, weil die Polizei entgegen diesen Vorschriften nicht alle gebotenen organisatorischen Maßnahmen für einen reibungslosen Ablauf der Datenlöschung in der FDR getroffen hat.

1.1.4 Konsequenzen

Als wir vor kurzem das Landeskriminalamt auf die unterbliebenen Löschungen in der FDR ansprachen, ging es mit uns schnell d'accord, daß das bei den Stichproben in Esslingen und Ulm gefundene Ergebnis repräsentativ für die ca. 33 000 Personen ist, die jeweils wegen eines einzigen mutmaßlich oder tatsächlich begangenen Rauschgiftdelikts in der FDR erfaßt sind. Klar war ihm auch sofort, daß deshalb ein Herumdoktern an Einzelfällen nicht weiterhilft, sondern eine Überprüfung aller 33 000 FDR-Speicherungen geboten ist. Daß es dies umgehend in Angriff nehmen wird, sagte uns das Landeskriminalamt sofort zu. Es versprach uns auch, den Verfahrensablauf bei der Datenlöschung in der FDR so zu verbessern, daß in Zukunft die rechtzeitige Löschung sichergestellt ist und uns sobald als möglich darüber zu informieren, welche Schritte es dazu in die Wege geleitet hat.

1.2 Mit der zehnjährigen Maximalspeicherfrist in der PAD zu schnell bei der Hand

Es ist ein Unterschied, ob jemand eine Haschischzigarette zum Rauchen erwirbt oder ob jemand mit Heroin handelt. Dies muß die Polizei bedenken, wenn sie festlegt, wie lange sie jemanden wegen eines mutmaßlich oder tatsächlich begangenen Rauschgiftdelikts in der PAD registriert. Um der Polizei die Arbeit bei der Festlegung der Speicherfristen zu erleichtern, gibt die Durchführungsverordnung zum Polizeigesetz folgende Marschrichtung vor: Erwachsene und Jugendliche darf die Polizei wegen eines mutmaßlich oder tatsächlich begangenen Rauschgiftdelikts fünf Jahre speichern. Abweichend hiervon darf sie Erwachsene für zehn Jahre registrieren, wenn sie gewerbsmäßig Rauschgift in den Verkehr bringen, Rauschgift an Minderjährige abgeben, als Mitglied einer Bande Rauschgifthandel betreiben oder andere schwere Rauschgiftstraftaten von überregionaler Bedeutung begehen. Sind Unrechtsgehalt und Folgen des Rauschgiftdelikts dagegen als gering einzustufen, darf die Polizei den Beschuldigten allenfalls drei Jahre in der PAD registrieren. Statt bei Rauschgiftdelikten

aus dieser Palette jeweils die angemessene Speicherfrist zu wählen, waren die beiden Polizeidirektionen, vor allem aber die Polizeidirektion Ulm, mit der zehnjährigen PAD-Maximalspeicherfrist zu schnell bei der Hand, wie schon folgende wenige Bespiele zeigen:

- 1 Gramm Haschisch
  Die Polizeidirektion Ulm erfaßte einen 28 Jahre alten Mann wegen Verstoßes gegen das Betäubungsmittelgesetz für zehn Jahre bis 1. Okt. 2002 in der PAD, weil ihn die Polizei im September 1992 bei einem Open-air-Konzert beim Drehen einer Haschischzigarette ertappte und er 1 Gramm Haschisch in der Tasche hatte. Ein solcher Tatvorwurf rechtfertigt die zehnjährige PAD-Maximalspeicherfrist nun wirklich nicht. Vielmehr handelt es sich um einen Fall von geringer Bedeutung. Das belegt nicht nur, daß das Amtsgericht den Mann mit einer am untersten Rand des Strafrahmens liegenden Geldstrafe von 25 Tagessätzen davonkommen ließ; so hatte auch das Landeskriminalamt den Fall eingestuft, als es das Formular für die FDR-Erfassung des Haschischdelikts erhielt. Weil die für solche geringfügigen Verstöße gegen das Betäubungsmittelgesetz angemessene dreijährige PAD-Speicherfrist schon längst abgelaufen ist und weil der junge Mann seit der Haschischzigarette weder ein Rauschgiftdelikt noch eine sonstige Straftat begangen hat, muß die Polizeidirektion Ulm ihn in der PAD umgehend löschen.
- Für 50 DM Haschisch in Stuttgart gekauft
  Die Polizeidirektion Ulm erfaßte einen anderen jungen Mann wegen Verstoßes gegen das Betäubungsmittelgesetz für zehn Jahre bis 1. Febr. 2002 in der PAD, weil er im Dezember 1991 in Stuttgart für 50 DM Haschisch gekauft, und davon zehn Tage später bei einer Kontrolle noch 2,4 Gramm in der Tasche hatte. Auch hier muß die Polizeidirektion Ulm die PAD-Speicherung löschen, weil der Haschischkauf ein Fall von geringer Bedeutung ist, den die Polizei allenfalls drei Jahre - also nur bis Ende 1994 - speichern durfte. Davon, daß es sich bei dem Haschischkauf um eine Bagatelle gehandelt hat, sind auch Amtsgericht Ulm und Landeskriminalamt ausgegangen: Das Amtsgericht hat den jungen Mann mit einer geringen Geldstrafe belegt; das Landeskriminalamt hat den Haschischkauf zu Recht als Fall von geringer Bedeutung eingestuft, als es den Erfassungsbeleg für die Falldatei Rauschgift durchgesehen hat.
- Haschisch als Geschenk
  Die Polizeidirektion Ulm erfaßte einen Soldaten wegen Verstoßes gegen das Betäubungsmittelgesetz für zehn Jahre bis 1. Okt. 2002 in der PAD, weil er seinem Unteroffizier ein Briefchen Haschisch schenken wollte, das er selbst zuvor von einem Freund, der ihm Geld schuldete, bekommen hatte. Auch

dieses Haschischdelikt rechtfertigt die zehnjährige PAD-Maximalspeicherfrist nicht. Angemessen wäre vielmehr die für Fälle von geringer Bedeutung vorgesehene kurze dreijährige PAD-Speicherfrist gewesen; als solchen Fall hat auch das Landeskriminalamt die Geschenkofferte angesehen, als es den Durchschlag für die FDR-Erfassung des Falles gelesen hat.

- Blutprobe mit Folgen
  Die Polizeidirektion Ulm erfaßte einen Autofahrer wegen eines Verstoßes gegen das Betäubungsmittelgesetz mit Cannabis für zehn Jahre bis 1. September 2001 in der PAD, weil die Untersuchung einer im Zuge einer Verkehrskontrolle angeordneten Blutprobe Hinweise auf Haschischkonsum ergeben hatte. Dieser Tatvorwurf hat in der PAD nichts zu suchen. Der Autofahrer hat sich nämlich wegen eines Rauschgiftdelikts gar nicht strafbar gemacht. Bloßen Haschischkonsum stellt das Betäubungsmittelgesetz nicht unter Strafe - und mehr als die Tatsache, daß der Autofahrer kurz zuvor Haschisch konsumiert haben mußte, läßt sich mit dem besten Willen aus der Blutuntersuchung nicht ableiten; anderes haben auch die weiteren polizeilichen Ermittlungen nicht zutage gefördert.
- 1 Briefchen Kokain
  Die Polizeidirektion Esslingen erfaßte einen 23jährigen Ausländer wegen Verstoßes gegen das Betäubungsmittelgesetz mit Kokain für zehn Jahre bis 1. März 2003 in der PAD, weil die Polizei bei einer Kontrolle in seiner Jackentasche 1 Zigarette mit einem Tabak/Kokaingemisch und 1 Faltbriefchen mit Kokain gefunden hatte. Ein solch geringfügiger Tatvorwurf rechtfertigt eine so lange PAD-Speicherung nie und nimmer. Wenigstens hätte die Polizeidirektion Esslingen die PAD-Speicherfrist erheblich reduzieren müssen, als sie die Staatsanwaltschaft im September 1993 wissen ließ, daß sie das Ermittlungsverfahren wegen Geringfügigkeit eingestellt hat. Denn jetzt hatte die Polizeidirektion Esslingen schwarz auf weiß, daß es sich bei dem Kokain des Ausländers nun wirklich nicht um ein schweres Rauschgiftdelikt gehandelt hat.

Diese Beispiele und noch eine ganze Reihe weiterer Fälle mit zu langen PAD-Speicherfristen habe ich vor kurzem gegenüber dem Innenministerium beanstandet. Weil sie zeigen, daß die Polizei bei mutmaßlich oder tatsächlich begangenen Rauschgiftdelikten einen Hang zu unangemessen langen PAD-Speicherfristen hat, ist es nicht damit getan, daß die beiden Polizeidirektionen in den Beispielsfällen die PAD-Speicherfristen entsprechend unseren Hinweisen verkürzen. Notwendig ist vor allem, sicherzustellen, daß die Polizei künftig bei Rauschgiftdelikten nur noch dann zur zehnjährigen PAD-Maximalspeicherfrist greift, wenn dies tatsächlich gerechtfertigt ist.

2. Von Staatsschutzdezernaten und Staatsschutzdateien und -karteien

Jede Polizeidirektion und jedes Polizeipräsidium hat ein Staatsschutzdezernat. Sie befassen sich vor allem mit Staatsschutzdelikten und mit anderen Straftaten mit politischem oder fremdenfeindlichem Hintergrund. Um ihre Akten wiederfinden zu können, registrieren manche Staatsschutzdezernate diese anhand der Personalien der Person, um die es in der Akte geht, in ihrer Staatsschutzkartei, andere Staatsschutzdezernate benutzen dazu einen PC. Die beiden Varianten sahen wir uns vor Ort bei zwei Polizeidirektionen an. Um es gleich vorweg zu sagen: Die PC-Variante zeigt, daß der Einsatz moderner IuK-Technik nicht nur Gefahren für das Grundrecht auf Datenschutz mit sich bringt, sondern diesem auch nutzen kann, wenn man ihre meist sowieso vorhandenen Programmroutinen auch für diesen Zweck einsetzt. Darauf hat sich das Staatsschutzdezernat mit der PC-Variante besonnen. Es kann mit Hilfe des elektronischen Gehirns seines PC die Speicherfristen überwachen. Will das Staatsschutzdezernat der anderen Polizeidirektion dies tun, muß es Karteikarte für Karteikarte seiner Staatsschutzkartei in die Hand nehmen; Fehler sind hier geradezu vorprogrammiert. Von ihnen und anderen Schwachstellen, auf die wir bei unseren Kontrollbesuchen stießen, jetzt der Reihe nach:

2.1 Datenspeicherungen aus zweiter Hand

Führen Polizeidienststellen anderer Bundesländer strafrechtliche Ermittlungsverfahren und wohnt einer der Beschuldigten in Baden-Württemberg, ersuchen sie die hiesige Wohnortpolizeidienststelle oft um Unterstützung, sei es, daß sie beispielsweise den Beschuldigten vernehmen oder sei es, daß sie an der Durchsuchung seiner Wohnung mitwirken soll. Die Polizeidienststellen kommen den Ersuchen nach. Geht es um bestimmte schwere Straftatvorwürfe, tun sie noch ein weiteres: Sie erfassen den Beschuldigten in den polizeilichen Informationssystemen. Beispielsweise registrierte ein Staatsschutzdezernat, welches das Landeskriminalamt eines anderen Bundeslandes bei der Durchsuchung der Wohnung eines tamilischen Asylbewerbers unterstützt hatte, den Asylbewerber 1991 für zehn Jahre wegen des Verdachts der Schutzgelderpressung in seiner Staatsschutzdatei und in der PAD, obwohl es nur wußte, daß der Asylbewerber als Provinzsekretär einer tamilischen Organisation von Landsleuten Geld zur Finanzierung des tamilischen Befreiungskrieges in der Heimat erpreßt haben soll.

Aufgrund so knapper Informationen durfte das Staatsschutzdezernat den Asylbewerber wegen eines solch gravierenden Tatvorwurfs nicht so lange in seiner Staatsschutzdatei und in der PAD registrieren. Denn ehernes Gebot jeder polizeilichen Datenspeicherung ist: In den Akten und Unterlagen muß belegt sein, worauf der Tatvorwurf fußt und auf welche tatsächlichen Umstände die Polizei

ihre Annahme stützt, der Betroffene werde künftig wieder in den Verdacht einer Straftat geraten. Erhellendes dazu stand aber in den Akten des Staatsschutzdezernats nicht. Es wußte nicht einmal, ob sich nach der Durchsuchung der Tatverdacht einer Schutzgelderpressung überhaupt noch aufrechterhalten ließ und wie das Ermittlungsverfahren ausgegangen war. Da aber die Beurteilung der Rechtmäßigkeit der Datenspeicherung häufig vom Ausgang des Verfahrens abhängt, durfte das Staatsschutzdezernat - wie aber geschehen - nicht bloß auf eine Nachricht des ermittelnden Landeskriminalamts warten; es hätte sich vielmehr selbst darum kümmern müssen, daß es rechtzeitig davon erfährt. Kurzum: Weil das Staatsschutzdezernat durch die Datenspeicherungen in das Grundrecht auf Datenschutz eingreift, ist es auch für deren Rechtmäßigkeit verantwortlich und muß die Fakten belegen können, auf die es sich dabei stützt. Dies ist die Kehrseite der Medaille, wenn hiesige Polizeidienststellen in strafrechtlichen Ermittlungen auf Ersuchen einer Polizeidienststelle eines anderen Bundeslandes tätig werden und meinen, sie müßten den Tatverdächtigen in ihren Informationssystemen erfassen. Als wir das Staatsschutzdezernat darauf aufmerksam machten, erkundigte es sich bei dem ermittelnden Landeskriminalamt und erfuhr, daß die Staatsanwaltschaft das Ermittlungsverfahren bereits 1996 mangels hinreichenden Tatverdachts eingestellt hatte. Will es den Asylbewerber trotzdem weiterhin registrieren, muß es dartun, weshalb dies notwendig sein soll. Kann es dies nicht, muß es die Daten des Asylbewerbers löschen. Diese Konsequenz hat das Staatsschutzdezernat in anderen Fällen aus dem Verfahrensausgang, den es auch hier erst im Zuge unserer Kontrollen bei den ermittelnden Polizeidienststellen erfragt hat, bereits gezogen.

2.2 Das lange Leben von Zeitakten

Bei den Staatsschutzdezernaten gehen täglich, meist per Fernschreiben über das eigene Kommunikationsnetz, Hinweise, Erkenntnisanfragen oder Bitten anderer Polizeidienststellen oder Behörden um Mithilfe bei der Erledigung ihrer Aufgaben ein. Diese Fernschreiben und ihre Antworten und Berichte über das Veranlaßte legen die Staatsschutzdezernate als sog. Zeitakten in ihrer Registratur ab und registrieren sie unter dem Namen der Person, um die es bei dem Hinweis oder in der Anfrage ging, in ihrer Staatsschutzkartei/-datei. Solche Zeitakten dürfen die Staatsschutzdezernate nach § 37 PolG nur so lange aufbewahren, wie dies zur Erfüllung ihrer Aufgaben erforderlich ist. Um den Polizeibeamten eine Richtschnur an die Hand zu geben, was dies im Klartext heißt, hat das Innenministerium in den KpS-Richtlinien von 1981 bestimmt, daß Zeitakten wegen ihrer mangelnden Relevanz grundsätzlich nach einem Jahr auszusondern sind. Daran hielten sich die beiden Staatsschutzdezernate nicht immer.

Bloß weil sie sich von ihren Zeitakten nicht rechtzeitig trennen konnten, war 1997 beispielsweise

- ein Mann, der zwei alte Panzer besaß und aufgrund eines Hinweises einer anderen Polizeidienststelle in den Blick des Staatsschutzdezernats geraten war, immer noch in dessen Staatsschutzdatei erfaßt, obwohl er bereits 1993 der Polizei anhand der Bescheinigung des Bundesamts für gewerbliche Wirtschaft belegt hatte, daß die Panzer ordnungsgemäß demilitarisiert waren und daher nicht unter das Kriegswaffenkontrollgesetz fielen;
- ein 77 Jahre alter Mann immer noch in der Staatsschutzkartei registriert, weil ihn das Staatsschutzdezernat 1993 auf Ersuchen einer Staatsanwaltschaft als Zeuge zu nationalsozialistischen Gewaltverbrechen vernommen hatte.

Diese und andere Zeitakten haben die Staatsschutzdezernate inzwischen in den Reißwolf geschoben und ihre Staatsschutzdatei/-kartei entsprechend bereinigt.

2.3 Eine folgenschwere Verquickung

Wer mit Karteien arbeitet, weiß, wie mühsam das mitunter ist. Das entbindet ihn jedoch nicht, dafür zu sorgen, daß Personen darin nicht über Gebühr lange registriert werden. Mit der Frage konfrontiert, wie es dies bei Personen, die wegen mutmaßlich oder tatsächlich begangener Straftaten erfaßt sind, in seiner Staatsschutzkartei bewerkstelligen kann, verfiel das Staatsschutzdezernat auf folgende Idee: Es sah jeweils in der PAD nach und vermerkte den für die mutmaßlich oder tatsächlich begangene Straftat eingespeicherten PAD-Löschtermin auf der entsprechenden Karteikarte seiner Staatsschutzkartei. Diese Methode hatte freilich einen Geburtsfehler. Setzte nämlich jetzt eine Polizeidienststelle den PAD-Löschtermin herunter oder löschte sie die mutmaßlich oder tatsächlich begangene Straftat in der PAD gleich ganz, bekam das Staatsschutzdezernat davon nichts mit; die fällige Korrektur in seiner Staatsschutzkartei unterblieb. Dazu nur zwei Beispiele:

- Das Staatsschutzdezernat erfaßte 1988 einen Mann für zehn Jahre wegen eines Vergehens eines Hausfriedensbruchs in seiner Staatsschutzkartei und vermerkte als Löschtermin auf der Karteikarte den 22. Juni 1998, weil die ermittelnde Polizeidienststelle den Mann genauso in der PAD registriert und dem Staatsschutzdezernat ein Doppel der Ermittlungsakte zugeleitet hatte. Danach hatte es der Mann einst mit der Polizei zu tun bekommen, weil er der Aufforderung des Bürgermeisters, vor der Tür des Einwohnermeldeamts zu warten bis er an der Reihe war, nicht nachgekommen war und statt dessen die für einen Wahlvorschlag der NPD gesammelten Unterstützerunterschriften sofort bestätigt haben wollte. Die ermittelnde Polizeidienststelle besann

sich dann doch noch darauf, daß solche Bagatellen allenfalls für drei Jahre in der PAD erfaßt werden dürfen und löschte den Hausfriedensbruch. In der Staatsschutzkartei stand er jedoch nach wie vor.

- Das Staatsschutzdezernat erfaßte 1994 eine Tierschützerin für drei Jahre wegen Beleidigung und Volksverhetzung in der Staatsschutzkartei und vermerkte als Löschtermin den 29. Okt. 1997, weil die ermittelnde Polizeidienststelle die Frau so in der PAD registriert und dem Staatsschutzdezernat ein Doppel der Ermittlungsakte geschickt hatte. Gegen die Tierschützerin hatte die Polizei ermittelt, weil ihr Name unter einem harschen, an die israelitische Gemeinde Berlin gerichteten Protestbrief gegen das Schächten von Tieren stand. Weil sich im Zuge der Ermittlungen rasch herausgestellt hatte, daß ihre Unterschrift gefälscht worden war, löschte die ermittelnde Polizeidienststelle die Tatvorwürfe in der PAD; in der Staatsschutzkartei standen sie jedoch nach wie vor.

Auf unsere Hinweise hat das Staatsschutzdezernat beide Fälle gelöscht, die Koppelung der Datenspeicherungen in seiner Staatsschutzkartei an den PAD-Löschtermin aufgegeben und seine Staatsschutzkartei einer Totalrevision unterzogen.

2.4 Das mitteilsame Staatsschutzdezernat

Ist jemand zu Unrecht in der Staatsschutzkartei registriert, ist dies kein Pappenstiel. Denn er muß nicht nur damit rechnen, daß solche Informationen bei jedem, der in die Staatsschutzkartei schaut, ein schiefes Licht auf ihn werfen, sondern läuft auch noch Gefahr, daß diese Informationen an andere Stellen weitergegeben werden. So ging es beispielsweise einer Frau, die in Hessen auf dem Gelände einer Abschiebehaftanstalt gegen die Abschiebung von abgelehnten Asylbewerbern demonstriert hatte. Auf die Anfrage der dortigen Polizeidienststelle nach Erkenntnissen über die Frau schaute das Staatsschutzdezernat in seiner Staatsschutzkartei nach und teilte der Polizeidienststelle unter anderem mit, daß die Frau - wie sich aus den zwar durchgestrichenen, aber immer noch deutlich lesbaren Eintragungen auf der Karteikarte ergab - während der Pershing II-Stationierung mehrmals an einer Sitzblockade teilgenommen hatte. Seine Antwort streute das Staatsschutzdezernat auch noch an das hiesige und das Hessische Landeskriminalamt.

Keine Frage: Diese Mitteilungen waren nicht in Ordnung. Die Hinweise auf die Teilnahme der Frau an solchen Sitzblockaden hätte das Staatsschutzdezernat in seiner Staatsschutzkartei nämlich längst ordentlich schwärzen müssen. Denn spätestens seit dem Beschluß des Bundesverfassungsgerichts vom 10. Jan.

1995 (1 BvR 718/89) steht fest, daß die Teilnahme an solchen Sitzdemonstrationen nicht als Nötigung strafbar ist. Gespeicherte Daten über Verhaltensweisen, die nach geltendem Recht nicht strafbar sind, muß die Polizei aber löschen und darf sie nicht statt dessen auch noch an andere Stellen weitergeben. Dies hat das Staatsschutzdezernat nach unserem Hinweis auf diese Rechtslage eingesehen.

3. Aus dem Polizeialltag

Auch 1997 wandten sich viele Bürger an mein Amt, weil sie befürchteten, daß die Polizei Daten über sie verarbeitet. Oft lagen sie damit richtig. Exemplarisch seien hierzu zwei Fälle angeführt:

3.1 Noch einmal: Die Polizeidirektion Ulm und ihre Neigung zu unangemessen langen Speicherfristen bei Rauschgiftdelikten

Wer oben gelesen hat, wie die Polizeidirektion Ulm bei mutmaßlichen oder tatsächlichen Verstößen gegen das Betäubungsmittelgesetz mit Kanonen auf Spatzen schießt, wird sich über die PAD-Erfassung des jungen Mannes nicht wundern, von der jetzt die Rede ist: Ihn registrierte die Polizeidirektion Ulm 1996 für sage und schreibe fünf Jahre in der PAD wegen des Tatvorwurfs eines Verstoßes gegen das Betäubungsmittelgesetz mit Cannabis. Das kam so: Der junge Mann war einer Polizeistreife aufgefallen, weil er mitten in der Nacht mit eingeschaltetem Standlicht auf einem Waldweg geparkt hatte. Mit im Auto saßen zwei seiner Freunde. Die Polizeibeamten kontrollierten alle drei und durchsuchten sie und das Auto. Dabei fanden sie zwischen Sitzfläche und Rückenlehne des Fahrersitzes 0,4 g Haschisch und auf der Mittelkonsole eine kleine Filmdose mit Antragungen von Haschisch/Marihuana. Die Durchsuchung des jungen Mannes und seiner beiden Freunde und seines Zimmers im Haus der Eltern verlief den Polizeiprotokollen zufolge negativ. Der junge Mann gab bei seiner polizeilichen Vernehmung an, daß er das Haschisch für 10 DM zum Eigenkonsum gekauft hatte.

Dieser nun wirklich geringfügige Verstoß gegen das Betäubungsmittelgesetz vermag - selbst wenn man berücksichtigt, daß der junge Mann nach dem Ergebnis der Untersuchung einer Urinprobe, die er freiwillig bei der Polizei abgegeben hatte, Haschisch oder Marihuana geraucht haben mußte - eine fünfjährige PAD-Speicherfrist nicht zu rechtfertigen. Die Polizeidirektion Ulm hätte vielmehr allenfalls eine verkürzte dreijährige Speicherfrist vergeben dürfen. Denn Fälle von geringer Bedeutung darf die Polizei nach § 5 Abs. 3 der Durchführungsverordnung des Innenministeriums zum Polizeigesetz nur so lange in der PAD erfassen. Gerade um einen solchen Fall von geringer Bedeutung handelte

es sich bei den 0,4 g Haschisch, weil der Unrechtsgehalt des Verstoßes gegen das Betäubungsmittelgesetz gering war und der Verstoß keine nennenswerten Folgen nach sich zog. Da die Polizeidirektion Ulm trotz unserer Hinweise hartnäckig an der fünfjährigen Speicherfrist festhielt, mußte ich die überlange Speicherung gegenüber dem Innenministerium beanstanden. Zwar ging dieses mit uns einig, daß es - was die Polizeidirektion Ulm zunächst in Bausch und Bogen verneint hatte - auch bei Verstößen gegen das Betäubungsmittelgesetz Fälle von geringer Bedeutung gibt, es meinte aber, der Haschischverstoß des jungen Mannes sei kein solcher Fall. Das Innenministerium verwies auf die angeblich "ungewöhnliche Antreffsituation (in einem Pkw nach Mitternacht auf einem Feldweg mit zwei Begleitern) und den Auffindeort des Betäubungsmittels (zwischen Sitzfläche und Rückenlehne des Fahrersitzes)". Die Filmdose bezeichnete es als Tarnbehälter für den Transport von Betäubungsmitteln, in dem ja mehr als die sichergestellte Menge Platz finde. Am Ende war der junge Mann sogar jemand, der im Umgang mit Betäubungsmitteln nicht unerfahren ist. Dabei verlor das Innenministerium freilich aus den Augen, daß es - wie man den Fall auch dreht und wendet - um 0,4 g Haschisch zum Eigenkonsum ging. Wie zum Beleg dafür, daß es sich dabei um einen Fall von geringer Bedeutung handelt, stellte die Staatsanwaltschaft Ulm das Ermittlungsverfahren gegen den jungen Mann mangels öffentlichen Interesses an der Strafverfolgung ein und vermerkte zur Begründung, daß die Schuld des jungen Mannes als gering anzusehen ist, da es lediglich um Besitz von sog. weichen Drogen zum Eigenverbrauch in geringer Menge ging und er bisher strafrechtlich wegen eines Betäubungsmitteldelikts nicht in Erscheinung getreten war. Vielleicht revidieren Innenministerium und Polizeidirektion Ulm doch noch ihre Meinung, wenn sie sich die Sicht der Staatsanwaltschaft noch einmal in Erinnerung rufen.

3.2 Ein merkwürdiges Zusammenspiel

Vor geraumer Zeit schrieb uns eine Mitarbeiterin einer Behörde, sie vermute, ihre Umsetzung auf einen anderen Arbeitsplatz sei daran gescheitert, daß polizeiliche und andere Informationen über sie im Umlauf seien. Als wir ihren Brief lasen, in dem sie im einzelnen dargelegt hatte, worauf sie ihre Annahme stützte, ahnten wir nicht, wie schwierig es werden wird, Licht in die Sache zu bringen. Erst nach einem langen Schriftwechsel mit der Behörde, einer Polizeidirektion, einer Landespolizeidirektion, dem Landeskriminalamt, dem Landesamt für Verfassungsschutz und einem Kontrollbesuch bei diesem sowie der Einsichtnahme in die Akten der Behörde lichteten sich die Nebel.

Die Mitarbeiterin sollte im Zuge einer Änderung der Organisation der Behörde auf einen anderen Arbeitsplatz umgesetzt werden. Dagegen erhob ein an dieser

Entscheidung beteiligter Mitarbeiter der Behörde Bedenken und schrieb an die Personalstelle, er wisse aufgrund interner Kenntnisse, daß die Frau früher einmal einer linksextremistischen bzw. autonomen Szene angehört habe. Zugleich schlug er vor, man solle die Frau einer Sicherheitsüberprüfung unterziehen. Woher der Behördenmitarbeiter seine Informationen hatte, gab er nicht an. Als wir die Polizeidirektion fragten, teilte sie uns kurz und knapp mit, eine Datenübermittlung an die Behörde sei nicht erfolgt. Weil wir aus anderem Zusammenhang wußten, daß Polizeidirektion und Landeskriminalamt solche Informationen über die Frau jedenfalls zu dem Zeitpunkt, als es um ihre Umsetzung ging, gespeichert hatten, hakten wir nach. Die Polizeidirektion befragte den Polizeibeamten ihres Staatsschutzdezernats, auf den die Frau getippt hatte. Jetzt hieß es, der Polizeibeamte habe nach seiner Erinnerung keinerlei Informationen über die Frau an deren Vorgesetzten gegeben, er erinnere sich aber, daß er einmal wegen eines befürchteten Sicherheitsrisikos angesprochen worden sei, damals jedoch auf den Dienstweg verwiesen habe. Klarer stand es in der Sicherheitsakte der Frau bei ihrer Behörde. Deren Geheimschutzbeauftragter hatte inzwischen nolens volens eine Sicherheitsüberprüfung eingeleitet und die Frau gebeten, die üblichen Formulare hierfür auszufüllen. In ihrer Sicherheitsakte hatte der Geheimschutzbeauftragte dann vermerkt, er wisse inzwischen, daß der Behördenmitarbeiter sein Wissen über die Frau aus seinem rein persönlichen Kontakt zu dem Polizeibeamten des Staatsschutzdezernats der Polizeidirektion hat.

Damit war klar, wie die polizeilichen Informationen gelaufen waren. Denn an dem Vermerk des Geheimschutzbeauftragten gab es nichts zu kritteln und nichts zu deuteln. Zudem hatte eine andere Stelle der Behörde unabhängig davon festgestellt, daß der Behördenmitarbeiter seine Informationen über die Frau außerdienstlich erhalten hatte. Bei Licht besehen stand dem die Einlassung des Polizeibeamten gar nicht entgegen, da er darin nur die Unterrichtung des Vorgesetzten der Frau - was der Behördenmitarbeiter nicht war und worauf wir unsere Frage gar nicht begrenzt hatten - verneint hatte. Selbstverständlich war die Weitergabe der polizeilichen Informationen an den Mitarbeiter der Behörde unzulässig. Denn polizeiliche Informationen sind nicht dafür da, daß sie von Polizeibeamten im privaten Bereich zu Markte getragen werden.

Natürlich hätte der Geheimschutzbeauftragte die Frau keiner Sicherheitsüberprüfung unterziehen dürfen. Denn die Sicherheitsüberprüfung dient nicht dazu, dem Leumund der Frau auf den Grund zu gehen. Sicherheitsüberprüft werden darf vielmehr nur, wer Zugang zu oder Umgang mit Verschlußsachen der Geheimhaltungsgrade VS-Vertraulich, Geheim oder Streng geheim hat oder erhal-

ten soll. Solche Verschlußsachen hätte aber die Frau, wie uns die Behörde bestätigt hat, an ihrer neuen Arbeitsstelle nie und nimmer zu Gesicht bekommen.

Was war das Fazit für die Frau? Die Informationen über sie waren in der Welt, das ließ sich nicht mehr ungeschehen machen. Erreichen konnten wir für sie, daß das Landeskriminalamt ihre Daten gelöscht hat. Ihre Behörde forderte ich auf, die bei der unzulässigen Sicherheitsüberprüfung angefallene Akte der Frau durch den Reißwolf zu schieben und künftig Mitarbeiter nicht unnötig mit einer Sicherheitsüberprüfung zu durchleuchten.

3. Abschnitt: Verfassungsschutz

Ganz gleich, ob wir im Landesamt für Verfassungsschutz datenschutzrechtlichen Fragen bei einer Kontrolle vor Ort oder im schriftlichen Verfahren nachgehen, unsere Arbeit gestaltet sich in diesem Bereich oft schwieriger als anderswo. Das liegt nicht etwa daran, daß uns das Landesamt für Verfassungsschutz Steine in den Weg legen würde - das Gegenteil ist dort inzwischen zu konstatieren. Die Ursachen sind vielmehr vor allem darin zu suchen, daß kaum ein Rechtsgebiet so von unbestimmten Rechtsbegriffen und Generalklauseln geprägt ist, wie dasjenige über die Informationsverarbeitung des Verfassungsschutzes. Damit waren wir auch 1997 konfrontiert.

1. Prüfung beim Landesamt für Verfassungsschutz

   An zweieinhalb Tagen führte einer meiner Mitarbeiter im Juli dieses Jahres eine Prüfung beim Landesamt für Verfassungsschutz durch. Bei der Kontrolle ging es uns nicht so sehr darum, "Verstöße" gegen datenschutzrechtliche Vorschriften festzustellen. Vielmehr wollten wir uns in erster Linie über Umfang und Art der Datenverarbeitung bei sog. linksextremistischen Verdachtsfällen informieren. Das sind in der Terminologie des Verfassungsschutzes Personen, deren Aktivitäten einem linksextremistischen Beobachtungsfeld noch nicht eindeutig zugeordnet werden können oder deren linksextremistische Hintergründe noch nicht abschließend geklärt sind.
   Ausgangspunkt der Überprüfung waren zwölf Ordner über solche Verdachtsfälle, die wir nach dem Zufallsprinzip gezogen hatten. Anhand dieser Unterlagen gingen wir zwei Fragen nach; zum einen: Warum registriert das Landesamt jemanden als linksextremistischen Verdachtsfall in seinen Akten? Zum anderen: Warum erfaßt es jemanden so auch noch im NADIS und wie geht es dabei vor? NADIS ist das gemeinsame Informationssystem des Bundesamts und der Landesämter für Verfassungsschutz. Es dient - kurz gesagt - der gegenseitigen Unterrichtung der Verfassungsschutzämter. Zu diesem Zweck werden neben den Personalien und anderen Informationen über Personen im wesentlichen Fundstellennachweise - also Hinweise darauf registriert, bei welchem Verfassungsschutzamt es aus welchem Anlaß Ak-

ten/Unterlagen über jemanden gibt. Seit 1990 hat das Landesamt - wie es mich wissen ließ - seinen NADIS-Bestand immer wieder eingehenden Überprüfungen unterzogen und die Zahl der registrierten Personen enorm reduziert, ein Vorgehen, das ich nur begrüßen kann. Dennoch taten sich bei unserer Kontrolle Fragen auf.

1.1 Feststellungen und Schlußfolgerungen

In einer ersten Zwischenbilanz, die ich vor kurzem dem Landesamt für Verfassungsschutz und dem Innenministerium vorgelegt habe, stellte ich folgendes fest:

1.1.1 Präzisere Begründung der NADIS-Erfassung notwendig

Das Landesamt für Verfassungsschutz darf nach § 7 LVSG Informationen über Personen in seinen Akten festhalten und Hinweise darauf im NADIS speichern, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß sie Bestrebungen gegen die freiheitlich demokratische Grundordnung verfolgen. Als Bestrebungen gegen die freiheitlich demokratische Grundordnung gelten solche politisch bestimmten, ziel- und zweckgerichteten Verhaltensweisen in oder für einen Personenzusammenschluß, der darauf gerichtet ist, einen der in § 4 LVSG genannten Verfassungsgrundsätze außer Kraft zu setzen oder zu beseitigen. Wer solche Ziele verfolgt, muß dies aktiv sowie ziel- und zweckgerichtet tun, es muß ihm also auch darauf ankommen, diesen Erfolg herbeizuführen. Deshalb reicht es nicht aus, wenn jemand nur mit einer Organisation oder Person, die solche Ziele verfolgt, übereinstimmt oder sympathisiert. Notwendig ist vielmehr, daß die Person Aktivitäten an den Tag legt, die auf die Beeinträchtigung der freiheitlich demokratischen Grundordnung abzielen. Diese müssen in den Akten und Unterlagen des Landesamts für Verfassungsschutz anhand von tatsächlichen Anhaltspunkten dokumentiert sein. Gerade das war jedoch in den eingesehenen Akten mitunter das Problem. Dazu nur ein Beispiel:

Das Landesamt für Verfassungsschutz hat 1991 neun Personen, die zusammen mit weiteren 50 Personen an einer öffentlichen Veranstaltung zum Golf-Krieg teilgenommen hatten, im NADIS registriert. Zur Begründung der NADIS-Erfassungen hatte es lediglich vermerkt: "Mögliche extremistische Beeinflussung" der Gruppierung, die die Veranstaltung organisiert hatte, durch die neun. Worin es die Beeinflussung sah, ist in der Begründung nicht angeführt. Deshalb lasen wir den langen Bericht über die Veranstaltung. Darin steht, daß sich sieben der neun Personen bei der Veranstaltung weder zu Wort gemeldet noch sich

sonst aktiv daran beteiligt hatten. Von den beiden anderen Personen heißt es, daß eine von ihnen als Versammlungsleiter fungiert und einen Info-Stand zum Thema Golf-Krieg aufgebaut und die andere Person einen Büchertisch der örtlichen Volksfrontgruppe betreut hatte. Daß an dem Info-Stand und an dem Büchertisch Informationsmaterial mit extremistischem Inhalt zu dem Thema der Veranstaltung feilgeboten worden war, erwähnt der Bericht nicht, er spricht auch nicht davon, daß der Versammlungsleiter in seinem Vortrag über die Militärhilfe der Bundesrepublik Deutschland für die Türkei oder durch seine Versammlungsleitung oder sonstwie versucht hatte, die Veranstaltung oder die veranstaltende Gruppierung extremistisch zu beeinflussen. Zu den an die Vorträge anschließenden Diskussionen heißt es im Bericht ausdrücklich, daß sie keine nachrichtendienstlich relevanten Erkenntnisse brachten.

Auf unseren Hinweis auf die nicht aussagekräftige Begründung der NADIS-Erfassungen ließ uns das Landesamt für Verfassungsschutz inzwischen wissen, daß sich aus dem Bericht selbst in der Tat keine eindeutig linksextremistischen Bezüge ergeben; vier andere Gesichtspunkte sprächen jedoch für das Vorliegen solcher Bestrebungen. Ob sie tatsächlich stichhaltig sind, muß hier offenbleiben. Unser Kernproblem war nicht diese Frage, sondern zunächst einmal die mangelnde Transparenz und Nachvollziehbarkeit der Entscheidung, die neun Veranstaltungsteilnehmer im NADIS zu erfassen. Hierfür wäre es viel besser gewesen, wenn das Landesamt die vier Gründe, die es jetzt benannt hat, beispielsweise stichwortartig in seiner Akte vermerkt und sich nicht bloß auf den Hinweis "Mögliche linksextremistische Beeinflussung" beschränkt hätte. Denn solche Schlagworte lassen nicht erkennen, auf welche tatsächlichen Anhaltspunkte sich eine NADIS-Erfassung wegen eines linksextremistischen Verdachtsfalles stützt. Das sieht offenbar auch das Landesamt so, denn es gab mir zu verstehen, daß es sich schon seit Jahren mit der Frage der Begründung einer Speicherung im NADIS beschäftigt und Anfang des Jahres Regelungen für die Verbesserung der Nachvollziehbarkeit der Speicherungen getroffen hat.

1.1.2 Zu vieles in den Akten registriert

Ohne Informationen ist die Arbeit des Verfassungsschutzes nicht denkbar. Deshalb dürfen andere Behörden das Landesamt informieren, wenn sie tatsächliche Anhaltspunkte für gewalttätige Bestrebungen gegen die freiheitlich demokratische Grundordnung haben. Polizei und Staatsanwaltschaften dürfen den Verfassungsschutz darüber hinaus

auch über rein extremistische Bestrebungen ohne Gewaltkomponente unterrichten. Erhält das Landesamt für Verfassungsschutz solche Informationen, muß es unverzüglich prüfen, ob die übermittelten Informationen zur Erfüllung seiner Aufgaben wirklich erforderlich sind. Ergibt seine Prüfung, daß dem nicht so ist, muß es die Unterlagen vernichten. Aufbewahren darf es solche Mitteilungen nur, wenn die Trennung von anderen Informationen, die es zur Erfüllung seiner Aufgaben unbedingt braucht, nicht oder nur mit unvertretbarem Aufwand möglich ist; ist dies so, muß das Landesamt für Verfassungsschutz die mitgeteilten Informationen, die es zur Erfüllung seiner Aufgaben nicht braucht, sperren. So steht es seit 1992 im Landesverfassungsschutzgesetz; so war es aber auch zuvor. Denn seit jeher gilt: Eine Behörde darf nur solche Informationen speichern, die zur Erfüllung ihrer Aufgaben unerläßlich sind. Diesen Anforderungen trug und trägt das Landesamt für Verfassungsschutz nicht immer Rechnung, wie folgende Fälle exemplarisch zeigen:

- Zwei junge Naturschützer sind in den Akten des Landesamts für Verfassungsschutz als linksextremistische Verdachtsfälle registriert, weil das Landesamt folgendes Fernschreiben des Landeskriminalamts, anstatt es sofort in den Reißwolf zu schieben, dort abgelegt hat:

  > "Am ... (Datum) findet in ... (Name einer Stadt) ein Demonstrationszug durch die Innenstadt mit anschließender Kundgebung auf dem Marktplatz statt. Veranstalter ist ... (Bezeichnung der Naturschutzgruppe). Die Anmelder der Veranstaltung ... (Name, Geburtsdatum, Adresse) und ... (Name, Geburtsdatum, Adresse) erwarten ca. 30 bis 40 Teilnehmer. Die Veranstaltung erfolgte bereits zweimal in den Vorjahren, es kam zu keinerlei Störungen. Die Polizeidirektion ... beabsichtigt verkehrslenkende und überwachende Maßnahmen."

- Ein Professor ist in den Akten des Landesamts für Verfassungsschutz als linksextremistischer Verdachtsfall registriert, weil das Landesamt ein Fernschreiben des Landeskriminalamts, anstatt es sofort zu vernichten, zu seinen Akten genommen hat - und dies, obwohl in dem Fernschreiben lediglich steht, daß der Professor bei einer Veranstaltung, bei der es der polizeilichen Überprüfung zufolge keinerlei Auffälligkeiten gegeben hat, vor ca. 150 Personen über Gefahren beim Castortransport gesprochen hat.
- Fünf Personen sind in den Akten des Landesamts für Verfassungsschutz über linksextremistische Verdachtsfälle registriert, weil das Landesamt ein Fernschreiben der Stuttgarter Polizei von 1984 über

eine demonstrative Aktion vor dem Landtag, anstatt es sofort zu vernichten, zu seinen Akten genommen hat - und dies, obwohl darin lediglich steht:

> "Anläßlich einer im Landtag stattfindenden Plenarsitzung mit anschließender Umweltschutzdebatte über Manöverschäden führten ... mehrere Mitglieder des Landtags aus der Fraktion ... vor dem Eingang des Landtags eine demonstrative Aktion durch. Es handelte sich um ... (es folgen vier Namen) und Frau ... (Name). Während der Aktion luden sie Abfälle, wie leere Flaschen, Dosen, Einwegpackungen u.a. ab und umgaben den Abfall mit einer S-Drahtrolle. Die Abfälle stammten angeblich aus den zu Ende gegangenen NATO-Manövern. Gegen 9.45 Uhr wurden die Beteiligten durch den Polizeiführer aufgefordert, die Abfälle zu beseitigen, was unverzüglich geschah. ... "

Mancher wird sich, genauso wie wir, gefragt haben, warum die Polizei dieses Fernschreiben überhaupt dem Landesamt für Verfassungsschutz geschickt hat. Doch dieser Frage konnten wir bei unserer Kontrolle nicht auch noch nachgehen. Daß aber das Landesamt für Verfassungsschutz die ihm übermittelten Informationen für seine Tätigkeit der Extremismusbeobachtung nun wirklich nicht gebraucht hat und auch nicht braucht, liegt auf der Hand. Denn irgendwelche Anhaltspunkte für eine extremistische Betätigung oder auch nur für einen dahin gehenden Verdacht gab und gibt es in allen Beispielsfällen nicht. Ich habe deshalb das Landesamt für Verfassungsschutz gebeten, in diesen und anderen Fällen die Fernschreiben der Polizeidienststellen aus den Akten zu nehmen und zu vernichten. Weil es aber damit nicht getan ist, habe ich das Landesamt für Verfassungsschutz darüber hinaus gebeten, bei Mitteilungen anderer Behörden künftig mehr Augenmerk auf seine Prüfpflicht zu legen und im Rahmen des Möglichen seine Akten zu bereinigen und überflüssige Polizeifernschreiben, die den Weg dorthin gefunden haben, auszusortieren. Das Landesamt hat mir inzwischen zugesagt, dies zu tun.

2. Auf den falschen Souffleur gehört

Ein freiberuflicher Dolmetscher schrieb mir 1997, er habe im Zusammenhang mit seiner Übersetzertätigkeit erfahren, daß Verfassungsschutzbehörden Informationen über ihn speichern. Das Landesamt für Verfassungsschutz habe jedoch seinen Auskunftsantrag abgelehnt und ihm dazu mitgeteilt:

> "Gemäß § 13 Abs. 2 Landesverfassungsschutzgesetz (LVSG) unterbleibt eine Auskunftserteilung. Gemäß § 13 Abs. 3 LVSG bedarf die Ablehnung einer Auskunftserteilung keiner Begründung. Es wird jedoch

> darauf hingewiesen, daß Sie sich diesbezüglich an den Landesbeauftragten für den Datenschutz Baden-Württemberg, Marienstraße 12, 70178 Stuttgart, wenden können."

Um diese Hinweise auf Vorschriften des Landesverfassungsschutzgesetzes zu verstehen, muß man wissen: Jedermann hat gegenüber dem Landesamt für Verfassungsschutz einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Dieser Anspruch ist allerdings mit einigen Kautelen verbunden. Denn das Landesamt braucht einem Auskunftsantrag von vornherein nur dann näherzutreten, wenn der Antragsteller hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an der Auskunft darlegt. Damit hat er die begehrte Auskunft allerdings noch lange nicht in Händen. Denn § 13 Abs. 2 LVSG räumt dem Landesamt ein weites Auskunftsverweigerungsrecht ein. Vier Fallgestaltungen unterscheidet diese Regelung. Eine Auskunft unterbleibt danach, soweit

- eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist,
- durch die Auskunftserteilung Quellen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder die Arbeitsweise des Landesamts für Verfassungsschutz zu befürchten ist,
- die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
- die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen.

Beruft sich das Landesamt auf einen der vier Auskunftsverweigerungsgründe, bedarf die Ablehnung eines Auskunftsantrags keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Es muß den Antragsteller aber auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinweisen, daß er sich an den Landesbeauftragten für den Datenschutz wenden kann.

Als wir das Schreiben des Dolmetschers lasen, dachten wir, das Landesamt für Verfassungsschutz könnte uns mit einem Blick in seine Akte die Gründe seiner Auskunftsverweigerung benennen. Diese muß es nämlich aktenkundig machen, so steht es in § 13 Abs. 3 LVSG. Statt dessen schrieb uns das Landesamt dann, der Dolmetscher habe beim Bundesamt für Verfassungsschutz ebenfalls einen Auskunftsantrag gestellt; dieses habe die Auskunft verweigert. Um die Auskunftsverweigerung des Bundesamts nicht zu unterlaufen, habe sich das Landesamt für Verfassungsschutz entgegen seiner ursprünglichen Absicht auch dazu entschlossen, die Auskunft in toto zu verweigern. Auf welche konkreten Umstände des Einzelfalls sich das Bundesamt für seine Auskunftsverweigerung gestützt hat, wisse das Landesamt nicht, es könne hier nur mutmaßen. Da aber die Beurteilung der Frage, ob die Voraussetzungen für einen der vier Auskunftsverweigerungsgründe vorliegen, ohne genaue Kenntnis der

hierfür einschlägigen Umstände schlechterdings nicht möglich ist, sahen wir uns die Akte des Landesamts näher an. Dabei bestätigte sich, daß es für die Ablehnung jeglicher Auskunft keinen ausreichenden Grund gab. Deshalb baten wir das Landesamt, dem Dolmetscher in dem Umfang Auskunft über die zu seiner Person gespeicherten Informationen zu geben, wie es dies ursprünglich beabsichtigt hatte. Dies hat das Landesamt - wie es uns vor kurzem wissen ließ - inzwischen getan.

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

1. Datenschutz im Krankenhaus

Seit eh und je bildet die Frage, wie Krankenhäuser mit Patientendaten umgehen dürfen, einen Schwerpunkt in der Arbeit unseres Amtes. Das war auch im Berichtsjahr so.

1.1 Erfahrungen aus der Kontrollpraxis

Bei Kontrollen in einem Zentrum für Psychiatrie und einem großen städtischen Krankenhaus der Maximalversorgung zeigten sich insbesondere Probleme beim Einsatz der EDV. Beide Krankenhäuser setzen je ein Patientenverwaltungssystem ein, mit dem sie Stammdaten ihrer Patienten, Diagnosen und sonstige für die Abrechnung mit den Krankenkassen benötigte Daten verarbeiten. Das städtische Krankenhaus verwendet dasselbe Patientenverwaltungssystem wie das Universitätsklinikum in Ulm. Mit dem aus datenschutzrechtlicher Sicht keineswegs befriedigenden Zustand dieses Verfahrens mußten wir uns bereits in unserem letztjährigen Tätigkeitsbericht ausführlich beschäftigen (vgl. 17. Tätigkeitsbericht 1996, LT-Drs. 12/750, S. 36 - 43).

1.1.1 Zu viele Angaben erfragt

Beschränkung auf das Notwendige ist eine elementare Grundregel des Datenschutzes. Deshalb dürfen Krankenhäuser von ihren Patienten nur die Angaben erfragen, die sie für deren medizinische Versorgung, für die verwaltungsmäßige Abwicklung des Behandlungsverhältnisses oder für Zwecke der Krankenhausseelsorge benötigen. Bei nahezu jeder Überprüfung der Datenverarbeitung von Krankenhäusern müssen wir leider feststellen, daß sie bei der Patientenaufnahme zu viel erfragen. So auch jetzt wieder die beiden Krankenhäuser bei ihren Fragen nach dem Hauptversicherten eines Patienten, der Religionszugehörigkeit und dem exakten Familienstand (geschieden, verwitwet!), obwohl wir in der Vergangenheit wiederholt (zuletzt im 16. Tätigkeitsbericht, LT-Drs. 11/6900, S. 54) die Rechtslage dargelegt haben. Beide Krankenhäuser wollen wenigstens jetzt daraus die gebotenen Konsequenzen ziehen.

1.1.2 Probleme mit den Eingabemasken

Verbesserungsbedürftig war die Gestaltung der EDV-Eingabemasken für die Patientenaufnahme im städtischen Krankenhaus. Sie enthielten Eingabefelder wie "Pfarrgemeinde" oder "Organspender", die das Krankenhaus bei der Patientenaufnahme nicht erfragen darf, und Freitextfelder, ohne daß das Krankenhaus geregelt hatte, was in ihnen gespeichert werden darf. Inzwischen hat es mitgeteilt, diese Schwachpunkte seien jetzt abgestellt.

1.1.3 Zu weitgehende Zugriffsrechte

Man kann es nicht oft genug wiederholen: Ein wesentliches Grundanliegen des Datenschutzes ist, daß jeder Mitarbeiter nur die Zugriffsrechte auf die im Computer gespeicherten Daten erhält, die er für die Erfüllung seiner dienstlichen Aufgaben tatsächlich benötigt. Dies war im städtischen Krankenhaus nur eingeschränkt gewährleistet:
Für viele, die Angehörige oder Freunde in einem Krankenhaus besuchen wollen, ist es eine große Hilfe, wenn sie sich an der Krankenhauspforte an freundliches Auskunftspersonal wenden können, die ihnen sagen, auf welcher Station der zu Besuchende gerade liegt. Daher ist im Regelfall nichts dagegen einzuwenden, wenn das Auskunftspersonal einige wenige Daten im Computer abrufen kann, um solche Auskünfte geben zu können. In eklatanter Weise schoß dabei aber das städtische Krankenhaus über das Ziel hinaus: Ein Mangel war schon, daß das Auskunftspersonal selbst am Computer einstellen konnte, wie lange nach der Entlassung eines Patienten noch ein Zugriff auf dessen Daten möglich war. Das Krankenhaus hatte diesen Zeitraum auf drei Tage voreingestellt. Dem Auskunftspersonal war es jedoch jederzeit möglich, diesen Zeitraum zu erhöhen mit der Folge, daß es auf Daten von weitaus mehr Patienten zugreifen konnte. Dies war aber noch nicht alles:

- Das Auskunftspersonal konnte, wenn es wollte, auf Daten sämtlicher stationärer und ambulanter Patienten, auch wenn sie bereits verstorben waren, zugreifen. Dabei war die gezielte Suche nach ganz bestimmten Patienten durch Eingabe eines Namens oder Namensbestandteils ein Kinderspiel.
- Gab das Auskunftspersonal einen beliebigen Zeitraum in den Computer ein, so konnte es sich alle Patienten am Bildschirm anzeigen lassen, die in diesem Zeitraum Geburtstag haben.
- Das Auskunftspersonal konnte einen beliebigen Zeitraum in den Computer eingeben und alle Patienten abrufen, die das städtische Krankenhaus in diesem Zeitraum aufgenommen hatte. Dabei wurde gleich noch unterschieden, ob der Patient aus einem anderen Kran-

kenhaus gekommen war oder ob es sich um eine normale Aufnahme, eine Notaufnahme oder einen Unfall gehandelt hatte.
- Schließlich konnte das Auskunftspersonal auch noch abrufen, wann welche Patienten von einer Station in eine vom Auskunftspersonal wählbare andere Station verlegt worden waren.

Auf meine Beanstandung teilte das städtische Krankenhaus inzwischen mit, es habe die Zugriffsrechte des Pfortenpersonals reduziert. Auch könnten diese Beschäftigten das Eingabefeld, wie lange entlassene Patienten noch angezeigt werden, nicht mehr verändern.

Frei von Problemen war aber auch die angetroffene Situation im Zentrum für Psychiatrie nicht. Dort konnten 12 Stationssekretärinnen lesend auf Daten sämtlicher Patienten zugreifen, obwohl ein Zugriff auf Patientendaten jeweils einer oder einiger weniger Stationen ausgereicht hätte. Darüber hinaus konnten die Stationssekretärinnen auch Daten sämtlicher bereits entlassener Patienten lesen, wozu überhaupt keine Notwendigkeit bestand. Schließlich konnten alle Stationssekretärinnen Privatgelder aller Patienten verbuchen, obwohl jede nur das Privatgeld ganz bestimmter Patienten zu verwalten hatte. Diese zu weitgehenden Zugriffsrechte beanstandete ich. Das Krankenhaus untersucht derzeit Möglichkeiten, die Zugriffsrechte auf das Erforderliche zu beschränken. Das EDV-System ermöglicht dies bislang nicht. Die Erörterungen hierüber sind noch nicht abgeschlossen.

1.1.4 Löschprobleme

Wer personenbezogene Daten mit Hilfe der EDV verarbeitet, muß, beginnend mit der Speicherung von Daten, festlegen, wann welche personenbezogenen Daten wieder zu löschen sind. Eine entsprechende Löschkonzeption hatten weder das städtische Krankenhaus noch das Zentrum für Psychiatrie ausgearbeitet. Ich habe daher beide aufgefordert, dies umgehend in Angriff zu nehmen. Beide Krankenhäuser haben dies inzwischen zugesagt.

1.1.5 Die Einführung von Software

Mit der Einführung seines Patientenverwaltungssystems und weiterer EDV-Verfahren beauftragte das städtische Krankenhaus ein privates Unternehmen. Dies ist nicht von vornherein unzulässig. Krankenhäuser können unter den in § 48 des Landeskrankenhausgesetzes (LKHG) genannten Voraussetzungen auch externe Stellen mit der technischen Durchführung der Datenverarbeitung betrauen. Die datenschutzrechtli-

chen Anforderungen berücksichtigte das Krankenhaus aber nicht ausreichend:

- Unzureichend geregelt war die schriftliche Beauftragung des Unternehmens. Der abgeschlossene Vertrag enthielt zwar auch einen Passus über den Datenschutz. Dort hieß es aber nur ganz lapidar, daß die Mitarbeiter des Unternehmens die gesetzlichen Bestimmungen über den Datenschutz beachten müssen und die aus dem Bereich des Krankenhauses erlangten Informationen, soweit sie nicht offenkundig sind, nicht an Dritte weitergeben oder sonst verwerten dürfen. Ein solch allgemeiner Hinweis auf den Datenschutz reicht jedoch nicht aus. Vielmehr ist in dem Vertrag präzise zu regeln, welche Maßnahmen im einzelnen notwendig sind, um den Datenschutz sicherzustellen.
- Es existierten 14 Benutzerkennungen für Mitarbeiter des Unternehmens. Das Krankenhaus stattete alle diese Kennungen mit äußerst weitreichenden Rechten aus, die lesenden und schreibenden Zugriff auf sämtliche im Patientenverwaltungssystem gespeicherten Daten ermöglichten. Die Hälfte der Kennungen war sogar mit Administrationsrechten versehen. Im Zeitpunkt der Kontrolle waren diese Kennungen gesperrt. Zu erfahren war jedoch, daß phasenweise bis zu zehn Mitarbeiter der Firma gleichzeitig vor Ort im Krankenhaus tätig waren. Eine weitere Zugriffsmöglichkeit bestand auch via Datenfernübertragung über das öffentliche Telefonnetz. Bei dieser Vorgehensweise ließ das Krankenhaus außer acht, daß es einer anderen Stelle nur aus zwingenden Gründen eine Zugriffsberechtigung auf Patientendaten einräumen darf.

Diese Mängel mußte ich beanstanden. Das städtische Krankenhaus hat zugesagt, bei ähnlichen Fällen in Zukunft datenschutzrechtlichen Belangen in vollem Umfang Rechnung zu tragen.

1.1.6 Die Abrechnung mit den Kostenträgern

Beschränkung auf das Notwendige muß auch die Devise sein, wenn ein Krankenhaus seine Kosten mit dem jeweiligen Kostenträger abrechnet. Damit nicht zum besten stand es beim Zentrum für Psychiatrie:

- Wenn dieses Krankenkassen die Aufnahme eines ihrer Versicherten anzeigen oder bei einem Sozialamt Erstattung seiner Kosten beantragen wollte, klebte es auf die dazu eingesetzten Vordrucke das "große Etikett". Dieses Etikett enthält all die Daten, die das Krankenhaus bei regulären Patientenaufnahmen erfragt und damit auch In-

formationen, die für die Abrechnung mit den Kostenträgern nicht benötigt werden, beispielsweise Angaben über die Religionszugehörigkeit eines Patienten oder Telefonnummern von Angehörigen oder sonstigen Bezugspersonen des Patienten, die das Krankenhaus in dringenden Fällen benachrichtigen soll. Deshalb darf das "große Etikett" nicht für den Schriftverkehr mit den Kostenträgern verwendet werden.

Daß dies zum Zeitpunkt unserer Kontrolle trotzdem in der Praxis noch geschah, war besonders ärgerlich, weil wir das betreffende Krankenhaus bereits 1993 schriftlich darauf hingewiesen hatten, daß diese Aufkleber auf den für die Abrechnung eingesetzten Formularen nichts zu suchen haben.

Auf meine Beanstandung hat das Krankenhaus jetzt Abhilfe zugesagt.

- Im Antragsformular für die Kostenerstattung durch Sozialämter waren Erklärungen des Patienten vorgesehen, die das Sozialamt dazu ermächtigen sollten, "bei allen Banken und Sparkassen Auskünfte über seine jetzigen und früheren Guthaben einzuholen". Gleichzeitig sollte er "alle Ärzte, von denen er behandelt oder denen er vorgestellt worden ist", von ihrer Schweigepflicht gegenüber dem Sozialamt entbinden. Es verwundert schon ein wenig, daß solche unbestimmten und deshalb unwirksamen Erklärungen heutzutage immer noch auf Formularen zu finden sind. Das Krankenhaus will es künftig besser machen.
- Schließlich verwendete das Krankenhaus für Entlaßanzeigen an die Krankenkassen Formulare, auf denen es ankreuzte, ob der Patient arbeitsfähig oder arbeitsunfähig entlassen wurde. Diese Informationen gehören aber nicht zu den Daten, die den Krankenkassen nach dem abschließenden Katalog in § 301 Abs. 1 SGB V zu Abrechnungszwecken mitgeteilt werden dürfen.

  Das Krankenhaus hat zugesagt, künftig in Entlaßanzeigen darauf zu verzichten.

1.1.7 Vakanz beim Beauftragten für den Datenschutz

Bei dem Zentrum für Psychiatrie war zudem zum Zeitpunkt unseres Kontrollbesuchs seit über einem Jahr kein Beauftragter für den Datenschutz mehr bestellt, obgleich dies in § 51 des Landeskrankenhausgesetzes zwingend vorgeschrieben ist. Inzwischen hat das Krankenhaus mitgeteilt, es würde demnächst Vertragsverhandlungen mit einem Bewerber führen, um die Vakanz alsbald zu beenden.

1.2 Die Behandlungsdaten und das psychiatrische Gutachten

Es mag in vielen Fällen sinnvoll sein und auch im Interesse des Patienten liegen, wenn ein Gericht, das für seine Entscheidung, beispielsweise eine Anordnung oder Änderung eines Betreuungsverhältnisses, ein ärztliches Gutachten benötigt, damit den Arzt beauftragt, der den Patienten behandelt oder behandelt hat. Denn ein solcher Arzt verfügt über umfassende Kenntnisse über den Patienten, die für eine Begutachtung von Nutzen sein können. Nur: So ohne weiteres geht das nicht. Denn wer sich bei einem Arzt in Behandlung begibt, muß darauf vertrauen können, daß dieser all das, was er während der Behandlung über ihn erfährt, geheimhält und Dritten nur offenbart, wenn er sich entweder damit einverstanden erklärt hat oder eine Rechtsvorschrift die Weitergabe erlaubt. Das gilt auch für den Fall, daß der behandelnde Arzt zum Gutachter bestellt ist. Da es keine Rechtsvorschrift gibt, die den Arzt berechtigt, bei der Behandlung gewonnene Informationen dem Gericht mitzuteilen, darf er diese nur in Gutachten verwerten, wenn der Patient dazu seine Einwilligung gegeben hat. Darauf hat unser Amt schon in seinem 15. Tätigkeitsbericht 1994, LT-Drs. 11/5000, S. 73/74, hingewiesen.

Leider findet diese Rechtslage hin und wieder keine Beachtung. So auch in einem Zentrum für Psychiatrie. Ohne weiter nachzufragen, hatte der zum Gutachter bestellte Arzt die schriftlichen Behandlungsunterlagen des Krankenhauses für die Erstellung des Gutachtens herangezogen und diese bei der Erstellung des Gutachtens verwertet. Auf meine Beanstandung räumte die Klinik den Datenschutzverstoß ein und sicherte zu, daß sich solche Fehler dort künftig nicht mehr wiederholen werden. Am besten ließe sich dies freilich sicherstellen, wenn Gerichte behandelnde Ärzte von vornherein nur dann als Gutachter bestellen würden, wenn feststeht, daß ihre Patienten mit der Einbeziehung der Behandlungsdaten in das Gutachten einverstanden sind. Ist dies nicht der Fall, sollten von vornherein nur Ärzte als Gutachter bestellt werden, die an der Behandlung nicht beteiligt waren.

1.3 Die Auskunft an den Haftpflichtversicherer

Ziemlich verärgert reagierte ein Bürger, als ihm die Haftpflichtversicherung seines Unfallgegners ein ärztliches Attest des städtischen Krankenhauses präsentierte, in dem er direkt nach seinem Unfall behandelt worden war. Der ärztliche Bericht enthielt nämlich nicht nur Angaben über seine dortige unfallbedingte Behandlung, sondern auch einen Hinweis darauf, daß der Patient später in einer ganz anderen Klinik wegen bestimmter weiterer Beschwerden stationär aufgenommen worden war, die jedoch nicht im Zusammenhang mit dem Unfall stünden. Von diesem weiteren stationären Aufenthalt hatte das Krankenhaus

Kenntnis erhalten, weil ihm die andere Klinik einen Entlaßbericht zugesandt hatte, ohne daß der Patient etwas davon wußte.

Das städtische Krankenhaus hatte der Haftpflichtversicherung die Auskunft gegeben, obwohl diese zu diesem Zeitpunkt noch gar nicht im Besitz einer Einwilligungserklärung des Bürgers war, sondern nur behauptet hatte, eine solche liege ihr vor. Die Krankenhausärzte hatten diese Angabe nicht nur ungeprüft geglaubt, sondern sich auch für verpflichtet gehalten, in ihrem Attest auf die spätere Behandlung in der anderen Klinik und ihre Auffassung über den Zusammenhang dieser späteren Behandlung mit dem Unfall kundzutun.

Damit hat sich das Krankenhaus in doppelter Hinsicht falsch verhalten:

- Auskünfte über die Behandlung eines Patienten dürfen Krankenhäuser nach dem Landeskrankenhausgesetz an private Dritte und damit auch an Haftpflichtversicherer nur geben, wenn der Patient zuvor im Einzelfall schriftlich in die Übermittlung dieser Daten eingewilligt hat. Auf die Versicherung, eine solche Einwilligung liege vor, darf sich ein Krankenhaus nur verlassen, wenn Patientendaten von einer Behörde erfragt werden. Erbittet eine private Versicherung - und sei es auch, um dem Patienten unfallbedingte Behandlungskosten ersetzen zu können - vom Krankenhaus ein Attest, muß dieses sich zumindest eine Kopie der schriftlichen Einwilligung des Patienten vorlegen lassen, bevor es die Bescheinigung ausstellt. Auch wenn, wie die Klinik einwandte, die Patienten üblicherweise bereit sind, zum Nachweis ihres Schadens Versicherungen ärztliche Gutachten zur Verfügung zu stellen, kann und darf ein Krankenhaus nicht ungeprüft davon ausgehen, daß diese Bereitschaft bei jedem Patienten vorliegt. Es kann nämlich für einen Patienten durchaus Gründe geben, im Einzelfall eher auf eine Versicherungsleistung zu verzichten, als bestimmte Informationen über seinen Gesundheitszustand preiszugeben.
- Darüber hinaus war auch die Einbeziehung der sog. Fremdbefunde der später behandelnden Klinik in das Attest des städtischen Krankenhauses unzulässig, weil sie von der Einwilligung des Patienten, deren Existenz die Versicherung behauptet hatte, nicht umfaßt war. Der Patient wußte nämlich nichts davon, daß die später behandelnde Klinik dem städtischen Krankenhaus einen Entlaßbericht zugeschickt hatte. Deshalb konnte sich seine Einwilligung auch nicht auf die darin enthaltenen Befunde beziehen.

Ich habe das städtische Krankenhaus aufgefordert, in Zukunft darauf zu achten, daß Patientendaten nur bei Vorliegen einer schriftlichen Einwilligungserklärung

und nur in dem Umfang an private Stellen weitergegeben werden, den die Erklärung auch wirklich abdeckt.

1.4 Was ist aus dem Patienten geworden?

Bei meiner Beratungstätigkeit werde ich immer wieder mit dem Problem konfrontiert, wie Krankenhäuser, in denen auch medizinische Forschung betrieben wird, z.B. Universitätskliniken, Tumorzentren und onkologische Schwerpunkte, auf legale Weise in Erfahrung bringen können, ob ehemalige Patienten noch leben oder wann und woran sie gestorben sind. Dies zu wissen ist überaus wichtig, um beurteilen zu können, welche Therapie bei welcher Erkrankung am erfolgreichsten ist bzw. dem betroffenen Patienten die längste Überlebenschance eröffnet. Informationen über den sog. Vitalstatus, also darüber, ob jemand noch lebt, haben in aller Regel die Meldebehörden, die Todesursache ist auf den Leichenschauscheinen, die bei den Gesundheitsämtern aufbewahrt werden, verzeichnet.

Wenn Krankenhäuser Auskunftsersuchen über den Vitalstatus bzw. die Todesursache ehemaliger Patienten an Meldebehörden oder Gesundheitsämter richten, teilen sie damit jedoch zwangsläufig zugleich mit, daß die Personen, auf die sich ihre Anfragen beziehen, schon einmal ihre Patienten waren. Teilweise, z.B. bei Tumorzentren oder Psychiatrischen Krankenhäusern, ergibt sich sogar allein aus der Anfrage die Art der Erkrankung, die den stationären Aufenthalt der Patienten notwendig gemacht hat.

Solchen Auskünften aber steht die ärztliche Schweigepflicht entgegen. Danach müssen die Ärzte und Kliniken bereits über die Tatsache Stillschweigen bewahren, daß jemand überhaupt jemals ihr Patient war. Anfragen über den Vitalstatus und die Todesursache ehemaliger Patienten dürften die Krankenhäuser daher nur dann an Meldebehörden oder Gesundheitsämter richten, wenn eine Rechtsvorschrift ausdrücklich eine derartige Durchbrechung der ärztlichen Schweigepflicht erlauben würde.

Eine gesetzliche Regelung, die solche Datenübermittlungen erlaubt, gibt es jedoch bisher nicht. Zwar enthält das Landeskrankenhausgesetz in § 46 eine Reihe von Tatbeständen, bei deren Vorliegen Patientendaten übermittelt werden dürfen, doch ist die Frage, ob ein ehemaliger Patient noch lebt bzw. wann oder woran er gestorben ist, von keiner der dort genannten Alternativen erfaßt. Auch das Landesdatenschutzgesetz hilft hier nicht weiter: Dieses erlaubt zwar unter bestimmten Voraussetzungen die Weitergabe von Daten für Zwecke wissenschaftlicher Forschung, doch lassen diese Regelungen die Bestimmungen zum Schutz der ärztlichen Schweigepflicht ausdrücklich unberührt, d.h. die ärzt-

liche Schweigepflicht geht insoweit vor. Mit anderen Worten: Fragen Krankenhäuser, um wichtige Forschungen über lebensbedrohliche Krankheiten weiterzubringen, bei Meldebehörden oder Gesundheitsämtern nach dem Vitalstatus bzw. der Todesursache ehemaliger Patienten, so ist dies zwar sinnvoll, notwendig und deshalb unterstützenswert, aber nach jetziger Rechtslage unzulässig.

Um hier eine Änderung herbeizuführen, habe ich gegenüber dem Sozialministerium angeregt, die Datenübermittlungsvorschriften des Landeskrankenhausgesetzes um einen Erlaubnistatbestand zu ergänzen, der solche Anfragen ermöglichen und zugleich sicherstellen würde, daß die Krankenhäuser hierbei nur die unabdingbar notwendigen Informationen über ihre Patienten nach außen geben und daß solche Anfragen unterbleiben, wenn überwiegende schutzwürdige Interessen der Patienten entgegenstehen.

Das Sozialministerium hat auf diese Anregung positiv reagiert und in Aussicht gestellt, meinen Vorschlag bei passender Gelegenheit aufzugreifen.

1.5 Datenschutz zu Unrecht am Pranger

Leider ist immer wieder festzustellen, daß Informationsdefizite und Mißstände, die in Wirklichkeit andere Ursachen haben, dem Datenschutz angelastet werden.

So erfuhr ein Bürger aus Norddeutschland, dessen hochbetagte Mutter nach einem Sturz in Baden-Württemberg in ein Krankenhaus eingeliefert worden war, das dortige Pflegepersonal dürfe ihm am Telefon aus Gründen des Datenschutzes keine Informationen über den Gesundheitszustand seiner Mutter geben. Dabei stand auch für das Pflegepersonal zweifelsfrei fest, daß es sich bei dem Anrufer um den Sohn der Patientin handelte. Tragischerweise führte in diesem Fall das Informationsdefizit zusammen mit verschiedenen weiteren Umständen dazu, daß die Patientin kurz darauf im Krankenhaus verstarb, ohne daß ihr Sohn sie dort noch einmal besucht hatte. Die Schlagzeile: "Datenschutz - 88jährige stirbt allein", die daraufhin in der Presse zu lesen war, wurde dieser Situation in keiner Weise gerecht:

Die Datenschutzvorschriften des Landeskrankenhausgesetzes lassen es ausdrücklich zu, daß Angehörige und sonstige Bezugspersonen eines Patienten in dessen Versorgungsinteresse über seinen Gesundheitszustand informiert werden. Auch ist es zulässig und in vielen Krankenhäusern tägliche Praxis, die Patienten bereits bei ihrer Aufnahme zu fragen, wer in dringenden Fällen benachrichtigt werden soll, um später entsprechend zu verfahren. Im konkreten Fall

kam dazu, daß die Patientin trotz ihrer körperlichen Beschwerden geistig rege war und ohne weiteres hätte gefragt werden können, welche Informationen ihr Sohn erhalten soll.

Hierauf und darauf, daß es keine Frage des Datenschutzes, sondern der medizinisch-fachlichen Verantwortlichkeit ist, wer innerhalb der Hierarchie eines Krankenhauses entsprechend seiner Ausbildung welche Auskünfte über den Gesundheitszustand eines Patienten erteilen darf, mußte ich das Krankenhaus erst aufmerksam machen.

2. Die Aktenführung beim Gesundheitsamt

Bei der Kontrolle der verschiedensten Behörden fällt mir immer wieder auf, wie wichtig es für einen effektiven Datenschutz ist, daß der Informationsfluß zwischen und innerhalb von einzelnen Organisationseinheiten richtig organisiert wird. Mit den Entscheidungen über den Postlauf und die Anlage und Aufbewahrung der Akten und sonstigen Unterlagen werden auch die Weichen für einen datenschutzgerechten Umgang mit den personenbezogenen Daten der betroffenen Bürger gestellt. So auch bei einem Gesundheitsamt im badischen Landesteil.
Erfreulicherweise konnte ich dort feststellen, daß die Verantwortlichen nach der Eingliederung des Gesundheitsamts in das Landratsamt den Postlauf so organisiert hatten, daß Dienstpost für das Gesundheitsamt, die zentral beim Landratsamt einging, aber erkennbar Gesundheitsdaten einzelner Bürger enthalten konnte, ungeöffnet zum Gesundheitsamt weitergeleitet und ihr Inhalt erst dort zur Kenntnis genommen wurde. Umgekehrt hat das Gesundheitsamt Post an Bürger direkt von dort versandt. Dies trägt sowohl dem Datenschutzinteresse der Bürger als auch der Schweigepflicht der beim Gesundheitsamt beschäftigten Ärzte Rechnung.
Die Beratungsstellen des Gesundheitsamtes, z.B. die Gesundheitshilfe für Behinderte, für psychisch Kranke, für Suchtkranke, für chronisch Kranke oder für AIDS-Gefährdete, konnten die Bürgerinnen und Bürger direkt aufsuchen, ohne sich vorher zentral anmelden und so noch weitere Personen über ihr Anliegen informieren zu müssen. Personenbezogene Daten in Beratungsangelegenheiten wurden außerdem nur in der jeweils zuständigen Beratungsstelle festgehalten.
Anders sah es leider bei den amtsärztlichen Untersuchungen aus:
Hier führte das Gesundheitsamt für jede untersuchte Person grundsätzlich nur eine Akte. In diesen "Personenakten" waren, ausgenommen bestimmte Untersuchungen nach dem Bundesseuchengesetz, alle Unterlagen über amtsärztliche Untersuchungen der betreffenden Person zusammengefaßt, gleich aus welchem Rechtsgrund, für welchen Zweck und für welche Stelle die Untersuchung auch erfolgt war. Hatte sich z.B. ein Bürger wegen einer Führerscheinangelegenheit amtsärztlich untersuchen

lassen und benötigte später aus einem ganz anderen Grund ein amtsärztliches Zeugnis, beispielsweise um in den öffentlichen Dienst eingestellt zu werden oder eine Deputatsermäßigung zu erhalten, so wurde beim Gesundheitsamt über all diese Untersuchungen nur eine Akte angelegt. Die Amtsärzte zogen somit bei späteren Untersuchungen derselben Person stets die komplette Akte bei, ohne danach differenzieren zu können, welche Informationen hieraus sie für die momentane Untersuchung eigentlich benötigten. Enthalten die Akten Aufzeichnungen über Untersuchungen für verschiedene Zwecke, führt das System der "Personenakte" fast zwangsläufig dazu, daß in die aktuelle Untersuchung auch Daten einbezogen werden, deren Kenntnis für den Zweck dieser letzten Untersuchung nicht erforderlich ist und die das Gesundheitsamt nach § 15 des Gesetzes über den öffentlichen Gesundheitszdienst hierzu auch nicht nutzen darf. Um solche Datenschutzverstöße von vornherein zu verhindern, muß das Landratsamt daher die Aktenführung im Gesundheitsamt umorganisieren und dafür sorgen, daß die Unterlagen nach den einzelnen Zwecken getrennt werden, für die die Daten erhoben und gespeichert wurden. Auf einen entsprechenden Hinweis meines Amtes hat das Landratsamt prompt reagiert und zugesagt, die Akten im Gesundheitsamt künftig nach Untersuchungszwecken zu trennen.

3. Einmal berufsunwürdig - immer berufsunwürdig?

Ärzte, Zahnärzte, Tierärzte und Apotheker haben sich, wenn sie gegen die Pflichten verstoßen haben, die ihnen zur Wahrung des Ansehens ihres Berufs obliegen, vor Berufsgerichten zu verantworten. So bestimmt es das Gesetz über die öffentliche Berufsvertretung, die Berufspflichten, die Weiterbildung und die Berufsgerichtsbarkeit der Ärzte, Zahnärzte, Tierärzte, Apotheker und Dentisten, kurz: Kammergesetz. Weder in diesem Gesetz noch in der Verordnung des Sozialministeriums zur Durchführung der berufsgerichtlichen Verfahren nach dem Kammergesetz, der sog. Berufsgerichtsordnung, ist allerdings geregelt, wie lange berufsgerichtliche Maßnahmen gegen die betroffenen Kammermitglieder berücksichtigt werden können und wie nach Abschluß dieser Verfahren mit den hierüber angelegten Akten, Unterlagen und Vorgängen zu verfahren ist.
Meine Frage an die Kammern der Ärzte, Zahnärzte, Tierärzte und Apotheker, wie es in puncto Nutzung, Aufbewahrung und Löschung solcher Daten in der Praxis aussieht, ergab ein sehr unterschiedliches Bild: Die eigentlichen Verfahrensakten werden überwiegend bis heute aufbewahrt. Auch Hinweise in anderen Akten auf berufsgerichtliche Verfahren gegen ihre Mitglieder haben die Kammern meist noch nicht gelöscht. Teilweise existieren interne Verwaltungsanordnungen, die Fristen für die Vernichtung der Akten vorgeben, teils werden Regelungen aus dem Bereich des Strafprozeßrechts bzw. Aufbewahrungsbestimmungen für die Justizverwaltung in Strafsachen entsprechend angewandt. Dabei wird zum Teil noch weiter unterschie-

den, ob die berufsgerichtliche Ahndung im Einzelfall auf Geldbuße oder Warnung bzw. Verweis lautete. Mit anderen Worten: Die berufsgerichtlichen Maßnahmen selbst können den Kammermitgliedern gegenüber 2, 5, 10 Jahre oder unbegrenzt vorgehalten werden, die Akten werden - bei unter Umständen gleichgelagertem Sachverhalt - bei den verschiedenen Kammern 10, 30 Jahre oder unbegrenzt aufbewahrt.
Mit dem Grundrecht auf informationelle Selbstbestimmung ist dies freilich so nicht vereinbar. Die Grundsätze, die für den Schutz dieses Rechts maßgebend sind, verlangen auch bei der Verarbeitung der Daten über berufsgerichtliche Entscheidungen und Verfahren Geltung. Dies bedeutet, daß der Gesetzgeber auch für diesen Bereich normenklar regeln muß, wie lange personenbezogene Daten im überwiegenden Allgemeininteresse aufbewahrt und gegen Kammermitglieder verwendet werden dürfen und wann sie zu vernichten sind.
Bei anderen Berufsgruppen ist dies längst geschehen. So bestimmt z.B. das Architektengesetz im einzelnen, wann bei den Architektenkammern Eintragungen über einen Verweis, eine Geldbuße oder die Aberkennung der Befähigung zu ehrenamtlicher Tätigkeit in der Kammer in den Akten, die die Kammern über ihre Mitglieder führen, zu tilgen und die hierüber entstandenen Vorgänge aus den Akten zu entfernen und zu vernichten sind und ab wann der jeweilige Architekt als von berufsgerichtlichen Maßnahmen nicht mehr betroffen gilt.
Auf meine Frage an das Sozialministerium, ob es beabsichtige, für Ärzte, Zahnärzte, Tierärzte und Apotheker ähnliche Regelungen auf den Weg zu bringen, habe ich bisher nur die Antwort erhalten, man werde die Angelegenheit dort in Abstimmung mit den berührten Ministerien und unter Beteiligung der betroffenen Kammern prüfen.

2. Abschnitt: Soziales

1. Von Abgleichen und Detektiven

Eine Entwicklung, die mein Amt schon im 14. und 17. Tätigkeitsbericht (LT-Drs. 11/2900, S. 20 ff., und LT-Drs. 12/750, S. 55) aufgezeigt hat, schreitet voran: Unter dem Diktat leerer Kassen und ständig steigender Aufwendungen im Sozialleistungsbereich müssen alle Einsparpotentiale ausgeschöpft und die öffentlichen Gelder möglichst zielgenau verteilt werden. Um dies zu erreichen, fordern immer mehr Politiker aller Ebenen, Medienvertreter und Repräsentanten von Sozialleistungsträgern weitere Maßnahmen zur Bekämpfung des Sozialleistungsmißbrauchs. Besondere Popularität genießt dabei der Ruf nach zusätzlichen Datenabgleichen und nach dem Einsatz sog. Sozialdetektive.

1.1 Datenabgleiche und ihre Grenzen

Verfolgt man die Berichterstattung in den Medien, werden Datenabgleiche ohne Anlaß und der regelmäßige Datenaustausch mit den verschiedensten Behörden und Stellen immer öfter als Allheil- und Wundermittel gegen den Leistungsmißbrauch und als wichtiges Element für Einsparungen im Sozialbereich beschrieben. Wie leicht solche Verfahren aber die Grenze der Verhältnismäßigkeit überschreiten und welchen Preis anlaßunabhängige Datenabgleiche haben, rückt immer weiter in den Hintergrund. Selten verweist jemand auf die Gefahr, daß zusätzliche Datenerhebungs- und -abgleichsverfahren zum "gläsernen Sozialleistungsempfänger" führen und mit der wachsenden Zahl derjenigen, die aufgrund der Lage auf dem Arbeitsmarkt zu Sozialhilfeempfängern werden, auch die Zahl der rechtstreuen Bürger steigt, die Objekt staatlicher Mißbrauchskontrolle und damit als potentielle Betrüger behandelt werden. Das Ziel, Sozialleistungen nur an wirklich Bedürftige zu verteilen und ungerechtfertigten Leistungsbezug zu bekämpfen, ist legitim. Die Mittel zur Erreichung dieses Zieles müssen aber verhältnismäßig sein.

1.1.1 Die Datenabgleiche nach § 117 Abs. 1 und 2 BSHG

Daß die Entwicklung zentraler Datenabgleichsverfahren nicht einfach ist, zeigt schon die mühsame Geburt der Rechtsverordnung zur Durchführung des § 117 Abs. 1 und 2 des Bundessozialhilfegesetzes (BSHG). Immerhin hat es, seit die Einführung dieser Maßnahmen mit dem Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms beschlossen wurde, über vier Jahre gedauert, bis dem Bundesrat die für die Durchführung der Datenabgleiche nach § 117 Abs. 1 und 2 BSHG erforderliche Rechtsverordnung zur Zustimmung vorgelegt wurde. In der Praxis wird es jetzt voraussichtlich 1998 erstmals dazu kommen, daß die Träger der Sozialhilfe Daten ihrer Hilfeempfänger unter Einschaltung der Datenstelle der Rentenversicherungsträger als Vermittlungsstelle automatisch mit Daten der Rentenversicherungsträger und der Bundesanstalt für Arbeit abgleichen, ohne daß für solche Prüfungen im Einzelfall ein konkreter Anlaß erforderlich wäre. Auch zwischen einzelnen Sozialhilfeträgern wird es auf diesem Wege zu regelmäßigen anlaßunabhängigen Datenabgleichen kommen.

Abgesehen von den Problemen und Kosten, die die praktische Umsetzung dieser automatisierten Datenabgleiche mit sich bringen wird, gab es bei der Kreation des Abgleichsverfahrens auch einige Rechtsfragen zu lösen. So bestimmte beispielsweise ein meinem Amt zugeleiteter Entwurf der Durchführungsverordnung, daß die Datenstelle der Rentenversicherungsträger und die Deutsche Post AG im Datenabgleichsver-

fahren Aufgaben erhalten sollten, die ihnen nach den einschlägigen Fachgesetzen bisher überhaupt nicht zugewiesen sind. Auch sah der Entwurf Löschfristen von zum Teil mehreren Monaten vor, die beim besten Willen nicht mehr mit der gesetzlichen Vorgabe, die Daten und Datenträger nach Durchführung des Abgleichs unverzüglich zurückzugeben, zu löschen oder zu vernichten, in Einklang zu bringen waren. Hierauf und auf einige andere datenschutzrechtliche Unzulänglichkeiten des Entwurfs habe ich in einer Stellungnahme an das Sozialministerium hingewiesen. Was die Datenstelle der Rentenversicherungsträger anbelangt, soll das Bundessozialhilfegesetz inzwischen nachgebessert werden. Auch bei den Löschfristen und in einigen anderen Bereichen konnten auf Bundesebene inzwischen Verbesserungen erreicht werden. Nachdem die Verordnung nun 1998 trotz der grundsätzlichen Bedenken, die mein Amt seit 1993 immer wieder geäußert hat, in Kraft treten wird, bleibt nur zu hoffen, daß die Städte und Landkreise, die die Datenabgleiche als Sozialhilfeträger durchführen werden, von dieser Möglichkeit verantwortungsbewußt und mit Augenmaß Gebrauch machen werden.

1.1.2 Neue Datenabgleiche?

Noch bevor die automatisierten Datenabgleichsverfahren nach § 117 Abs. 1 und 2 BSHG praktiziert und Erfahrungen mit den Auswirkungen dieses neuen Kontrollinstruments gesammelt werden konnten, wird auf Bundes- und Landesebene schon nach Möglichkeiten gesucht, das System der Datenabgleiche im Sozialleistungsbereich weiter auszubauen und voranzutreiben.

So hat die Konferenz der Arbeits- und Sozialminister (ASMK) bereits im Herbst 1995 eine länderoffene Arbeitsgruppe "Verbesserter Datenaustausch bei Sozialleistungen" mit dem Auftrag eingesetzt, umfassend zu prüfen, ob und in welchem Umfang im Bereich der Sozialleistungen Verbesserungen des Datenaustausches gefordert werden sollen. Die Arbeitsgruppe hat inzwischen einen Bericht vorgelegt, in dem sie nicht nur in speziellen Sozialleistungsbereichen die Ermächtigungen zur Erhebung und Übermittlung von Daten wesentlich erweitern will, sondern auch weitreichende Änderungen der allgemeinen Datenerhebungs- und -übermittlungsvorschriften des Zehnten Buches des Sozialgesetzbuchs vorschlägt. Zur "Schaffung effektiver Generalklauseln für die Mißbrauchskontrolle" soll das Gesetz nach dem Bericht so geändert werden, daß Daten zur Mißbrauchskontrolle stets ohne konkreten An-

fangsverdacht im Einzelfall erhoben werden können und selbst private Dritte grundsätzlich schon dann befragt werden können, wenn dies der Überprüfung der Angaben der Hilfeempfänger auch nur "dient".

Neue Datenabgleiche dürfen aber nur eingeführt werden, wenn sie die verfassungsmäßig garantierten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit wahren. Insoweit ist der Beschluß, den der Deutsche Bundestag zu den kritischen Einwänden des Bundesbeauftragten für den Datenschutz in dessen 14. Tätigkeitsbericht, Nr. 1.1, gefaßt hat, aktueller denn je. Dort heißt es:

> "Die Bundesregierung wird aufgefordert, vor der Einrichtung von Datenabgleichsverfahren jeweils zu prüfen, ob sie im Interesse des Gemeinwohls zur Erreichung eines konkreten Zieles erforderlich und verhältnismäßig sind." (BT-Drs. 13/1636)

Wie dies gemeint war, kann man in der Begründung zur Beschlußempfehlung des Innenausschusses nachlesen:

> "Im Berichtszeitraum ist die Tendenz zur Kontrolle und Überwachung von Leistungsbeziehern mit Hilfe pauschaler automatisierter Datenabgleichsverfahren deutlich gewachsen. Selbst wenn die einzelnen Abgleiche und Kontrollvorgänge für sich eine gewisse Berechtigung, z.B. zur Bekämpfung von Leistungsmißbrauch, haben, hat der Innenausschuß die Gefahr gesehen, daß ein umfassendes Netz von Überwachungs- und Überprüfungsmöglichkeiten geschaffen und vergrößert wird."
> (BT-Drs. 13/1636, S. 6).

Angesichts ständig neuer Forderungen nach Schaffung weiterer Datenerhebungs- und Abgleichsmöglichkeiten sind diese Aussagen von brennender Aktualität. Man scheint zu vergessen, wie differenziert und ausbalanciert das derzeitige System der Datenerhebungsvorschriften im Zehnten Buch des Sozialgesetzbuchs ist und wie wichtig ein solches System ist, wenn es darum geht, die verfassungsrechtlich garantierten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit öffentlichen Handelns zu wahren. Wollen Sozialleistungsträger die nötigen Informationen über ihre "Kunden" einholen, müssen sie nach geltendem Recht grundsätzlich nach einem abgestuften System vorgehen: Ausgangspunkt und Grundsatz ist dabei die Datenerhebung beim Hilfeempfänger selbst. Grundlage der Entscheidung sind damit nicht nur seine eigenen Angaben, sondern auch die Nachweise, die er, um seine Bedürftigkeit zu untermauern, selbstverständlich vorlegen muß. Bestehen danach noch Zweifel, ob im konkreten Einzelfall die Leistungsvoraussetzungen

vorliegen, kann der Leistungsträger die notwendigen Daten bei Dritten mit und unter Umständen auch ohne Mitwirkung des Hilfeempfängers erheben. Wie dabei vorzugehen ist, ist im einzelnen gesetzlich geregelt. Dieses System gewährleistet, daß die Behörde die für ihre Entscheidung erforderlichen Informationen erhält, dabei jedoch so wenig wie möglich in das Grundrecht des Hilfeempfängers auf Datenschutz eingreift.

Schon die nach § 117 BSHG zugelassenen regelmäßigen Datenabgleiche bilden in diesem System bereits einen Fremdkörper, weil hier kein konkreter Anlaß im Einzelfall mehr für die Überprüfung bestehen und den Grundrechtseingriff rechtfertigen muß. Einen gewissen Ausgleich hat der Gesetzgeber bei § 117 BSHG jedoch immerhin noch dadurch geschaffen, daß die Daten, die nach dieser Vorschrift ausgetauscht werden dürfen, im einzelnen konkret und abschließend festgelegt wurden und die Sozialhilfeträger klare Verfahrensregelungen des Gesetz- bzw. Verordnungsgebers einhalten müssen.

Aber auch diese Schranken würden aufgegeben, würde der Gesetzgeber der Empfehlung der Arbeitsgruppe der ASMK folgen und bei den allgemeinen Datenerhebungsvorschriften des Zehnten Buchs des Sozialgesetzbuchs zusätzlich Generalklauseln für anlaßunabhängige Mißbrauchskontrollen schaffen.

Neue Datenabgleiche zu Kontrollzwecken wären nur dann verhältnismäßig, wenn zumindest einigermaßen gesichert feststünde, daß tatsächlich ein erheblicher Teil der Leistungsempfänger unzutreffende oder unvollständige Angaben macht. Hierüber gehen aber, wie der Presse immer wieder zu entnehmen ist, die Meinungen selbst bei Experten noch weit auseinander. Außerdem müßten verläßliche Feststellungen darüber vorliegen, in welchen Sozialleistungsbereichen ein derart erhöhter Mißbrauch vorliegt, so daß beurteilt werden kann, ob, wenn es überhaupt weiterer Datenabgleiche bedarf, hier nicht bereichsspezifische Regelungen ausreichen würden. Das gleiche gilt hinsichtlich der Frage, ob Inhalt und Umfang der Daten, die man zu Kontrollzwecken austauschen müßte, nicht klarer eingegrenzt werden könnten und welche Verfahrensregeln im einzelnen vorgegeben werden könnten, um das unverhältnismäßige Ausufern der Datenabgleiche zu verhindern.

Solange all diese Fragen nicht ausreichend geklärt sind, dürften weitere Datenabgleiche im Sozialleistungsbereich, erst recht aber Generalklauseln zur Mißbrauchsbekämpfung, eigentlich kein Thema sein.

Angesichts dieser Situation haben die Datenschutzbeauftragten des Bundes und der Länder intensiv über die Vorschläge der Arbeitsgruppe der ASMK beraten und am 20. Okt. 1997 die im Anhang dieses Berichts abgedruckte Entschließung (Anhang 6) verabschiedet. Die Arbeits- und Sozialminister der Länder haben die Bundesregierung hierauf gebeten, nicht nur den Bericht der Arbeitsgruppe, sondern auch die Entschließung der Datenschutzbeauftragten in die Prüfung einzubeziehen, welche Schritte zur Realisierung eines verbesserten Datenaustauschs im Sozialbereich notwendig sind.

1.2 Der Sozialdetektiv

Immer öfter, so berichteten die Medien in diesem Jahr, setzen auch in Baden-Württemberg Städte und Landkreise "Sozialdetektive" ein, um Mißbrauch von Sozialhilfe aufzuspüren. Von einer härteren Gangart gegen Sozialhilfeempfänger ist da die Rede, von unangemeldeten Hausbesuchen, von Beschattung und von der Erwartung, in vielen Fällen Sozialhilfebetrug aufzudecken.

Was also sind Sozialdetektive, und vor allem wie müssen sie bei ihrer Arbeit vorgehen, um nicht mit dem Datenschutz in Konflikt zu kommen?

- Der Sozialdetektiv - ein Mitarbeiter des Sozialamts
  Sozialdetektive sind Außendienstmitarbeiter der Sozialhilfeträger, die vor Ort überprüfen, ob im Einzelfall die gesetzlichen Voraussetzungen der Sozialhilfe gegeben sind, also insbesondere, ob Antragsteller oder Hilfeempfänger wirklich bedürftig sind. Typischerweise ermitteln sie, ob die Hilfeempfänger mit anderen Personen in Wohn- und Wirtschaftsgemeinschaften leben, erwerbstätig sind oder über nicht angegebenes Vermögen verfügen. Die Ermittler erheben daher Sozialdaten und sind genau wie Mitarbeiter der Sozialämter im Innendienst an die gesetzlichen Vorschriften über den Sozialdatenschutz gebunden.

  Für ihre Ermittlungsarbeit ist daher § 67a des Zehnten Buches des Sozialgesetzbuchs (SGB X) maßgebend. Sozialdetektive dürfen also nur unter den in dieser Vorschrift genannten Voraussetzungen tätig werden und müssen sich an das dort vorgeschriebene Verfahren halten.

Die allgemeinen Verfahrensgrundsätze des Sozialgesetzbuchs, nach denen die Sozialhilfeträger beispielsweise Auskünfte einholen, Beteiligte anhören, Zeugen vernehmen und Augenschein einnehmen dürfen, erweitern diese Befugnisse nicht: Im Sozialgesetzbuch ist ausdrücklich vorgeschrieben, daß § 67a SGB X diesen allgemeinen Grundsätzen vorgeht.

- Nur bei konkretem Verdacht
  Sozialdaten dürfen nach § 67a Abs. 1 SGB X nur erhoben werden, wenn ihre Kenntnis im Einzelfall für die Erfüllung der Aufgaben des Sozialleistungsträgers erforderlich ist. Die Sozialämter dürfen daher Sozialdetektive nur einsetzen, wenn im konkreten Einzelfall bereits tatsächliche Anhaltspunkte für Leistungsmißbrauch vorliegen. Nachforschungen, die erst zur Verdachtsschöpfung führen sollen, sind also unzulässig.

- Der Grundsatz: Offene Ermittlung beim Hilfeempfänger
  Sozialdaten sind nach § 67a Abs. 2 SGB X grundsätzlich beim Hilfeempfänger mit seiner Kenntnis zu erheben. Auch für das Verfahren im einzelnen gibt das Gesetz klare Vorgaben: Der Sozialdetektiv muß sich danach gegenüber dem Hilfeempfänger als Mitarbeiter des Sozialamts zu erkennen geben und ihm erklären, weshalb er was bei ihm überprüft, ob er zur Auskunft verpflichtet ist und welche Folgen es hat, wenn er die Mitwirkung verweigert. Nicht erforderlich ist, daß sich der Ermittler vor seinem Besuch anmeldet.

  Soll eine Wohnung betreten werden, müssen auch Sozialdetektive das Grundrecht auf Unverletzlichkeit der Wohnung beachten. Sie dürfen daher die Wohnung eines Hilfeempfängers nur mit dessen Zustimmung betreten und sein Einverständnis auch nicht mit falschen Angaben oder unter einem Vorwand erschleichen. Außerdem müssen sie eindeutig klarstellen, daß er nicht verpflichtet ist, ihnen Einlaß zu gewähren.

- Wann dürfen andere befragt werden?
  Ermittlungen bei Mitbewohnern, Bekannten, Nachbarn, Vermietern, Hauseigentümern, Hausmeistern etc. der Hilfeempfänger sind nur unter den engen Voraussetzungen des § 67a Abs. 2 Satz 2 Nr. 2 SGB X zulässig. Insbesondere dürfen keine Anhaltspunkte dafür bestehen, daß im Einzelfall überwiegende schutzwürdige Interessen des Hilfeempfängers beeinträchtigt werden. Da die Befragung Dritter zwangsläufig mit der Mitteilung verbunden ist, daß der Hilfeempfänger Kontakt zum Sozialamt hat und es dort Anlaß für Nachfragen gibt, müssen die Sozialhilfeträger im Regelfall zunächst versuchen, die nötigen Informationen und Nachweise von ihm selbst zu erhalten. Vor Nachfragen bei Dritten muß in die Interessenabwägung einbezogen werden, daß

mit der Befragung anderer Personen oder Stellen Informationen über den Hilfeempfänger preisgegeben werden, die unter Umständen geeignet sind, diesem zu schaden, beispielsweise seine Kreditwürdigkeit oder seinen Ruf zu beeinträchtigen. Das Sozialamt muß daher sorgfältig überlegen, wer im Einzelfall befragt werden darf; keinesfalls darf ein Sozialdetektiv einfach an die nächstbeste Person aus dem Umfeld des Hilfeempfängers herantreten, der er bei seinem Einsatz gerade begegnet. Auch muß er seine Fragen so beschränken, daß er möglichst nur die Informationen erhält, die wirklich zur Ermittlung der Bedürftigkeit erforderlich sind.

Befragt ein Sozialdetektiv Privatpersonen oder andere private Stellen, ist er gesetzlich verpflichtet, sie darauf hinzuweisen, daß es ihnen freisteht, Angaben zu machen, und daß ihnen keine Nachteile entstehen, wenn sie dies unterlassen. Hierzu muß sich der Ermittler als Außendienstmitarbeiter des Sozialamts zu erkennen geben und darf seine Gesprächspartner nicht unter falschen Angaben oder sonstigen Vorwänden zu Äußerungen über den Hilfeempfänger verleiten.

- Die heimliche Beobachtung: Grundsätzlich nicht!
  Datenerhebungen beim Hilfeempfänger ohne seine Kenntnis, d.h. verdeckte oder heimliche Beobachtungen, sind im Sozialgesetzbuch nicht vorgesehen. Sie greifen massiv in das Grundrecht auf informationelle Selbstbestimmung ein, da der Ermittler dabei hinter dessen Rücken vorgeht und Informationen sammelt, die ihm niemand bewußt oder gar nach einer rechtlichen Belehrung preisgibt. Außerdem liefern verdeckte Beobachtungen regelmäßig nicht nur Informationen über die Bedürftigkeit des Hilfeempfängers, sondern zugleich eine Vielzahl weiterer Daten und Erkenntnisse aus seiner Privat- und gegebenenfalls Intimsphäre, die das Sozialamt zur Erfüllung seiner Aufgaben überhaupt nicht benötigt. Gegen verdeckte Beobachtungen bestehen daher größte Bedenken. Als Regelmaßnahme von Sozialdetektiven sind sie in jedem Fall unzulässig.

  Andererseits kann es in der Praxis Fälle geben, in denen es zulässig wäre, private Dritte über den Hilfeempfänger zu befragen, das Sozialamt aber die nötigen Informationen mit hoher Wahrscheinlichkeit auch durch eine kurzfristige Beobachtung des Hilfeempfängers selbst gewinnen könnte. Dies kann beispielsweise der Fall sein, wenn es darum geht, nachzuprüfen, ob der Hilfeempfänger in einem Bereich einem Erwerb nachgeht, der der Öffentlichkeit zugänglich ist, z.B. an einer Kasse im Supermarkt, an einer Tankstelle, in einer Gaststätte oder an ähnlichen Orten. Hier würde sein Selbstbestimmungs-

recht unter Umständen durch eine kurzfristige verdeckte Beobachtung deutlich geringer beeinträchtigt als durch die Befragung des Dritten, der dann ja zwangsläufig vom Kontakt zum Sozialamt und der Überprüfung erfährt.

In eng begrenzten Ausnahmefällen kann es daher nach dem Grundsatz des geringstmöglichen Grundrechtseingriffs noch hinnehmbar sein, den Hilfeempfänger kurzfristig verdeckt zu beobachten. Ob ein solcher Ausnahmefall vorliegt, müßte allerdings im Einzelfall sehr sorgfältig geprüft werden. Voraussetzung hierfür wäre jedenfalls, daß

- es im konkreten Einzelfall rechtlich zulässig wäre, einen privaten Dritten zu befragen,
- die Befragung des Dritten für den Hilfeempfänger deutlich schwerer wiegen würde als die kurzfristige verdeckte Beobachtung durch einen Mitarbeiter des Sozialamts,
- hierdurch mit hinreichender Wahrscheinlichkeit die notwendigen Informationen gewonnen werden könnten,
- der aufzudeckende Mißbrauch in einer Größenordnung läge, die einen derart intensiven Grundrechtseingriff rechtfertigen würde,
- zuvor sorgfältig abgewogen wurde, ob in diesem Einzelfall nicht vorzuziehen wäre, die Sozialhilfe nach § 66 SGB I zu entziehen oder zu versagen oder aber an Polizei oder Staatsanwaltschaft einen Ermittlungsauftrag zu geben, und
- die Beobachtung zeitlich und vom Umfang her eng begrenzt bliebe.

Angesichts der Problematik solcher Maßnahmen sollten sie nur vom Leiter des Sozialamts selbst angeordnet werden.

- Last but not least: Mindeststandards für die Auftragserteilung und Dokumentation

  Um die Erforderlichkeit und Verhältnismäßigkeit der Ermittlungen zu gewährleisten, müssen Sozialdetektive, die nicht selbst für die Sachbearbeitung zuständig sind, über die von ihnen zu beachtende Rechtslage informiert werden. Sie müssen genau definierte Aufträge erhalten und sollten schriftlich angewiesen werden, wie sie bei ihren Ermittlungen vorzugehen haben. Außerdem sind Auftragserteilung und Einsätze zu dokumentieren. Hierzu gehören Notizen über die Vorlage des Dienstausweises, die Informationen und Belehrungen, die die Ermittler den Hilfeempfängern und anderen Gesprächspartnern gegeben haben, sowie über Verlauf und Ergebnis der Einsätze. Die Dokumentationen müssen Eingang in die Sozialhilfeakten finden, damit auch die Arbeit der Sozialdetektive stets transparent und überprüfbar bleibt.

Nur wenn sich sowohl die Träger der Sozialhilfe als auch die Ermittler selbst an diese Regeln halten, ist der Einsatz von Sozialdetektiven zur Aufdeckung von Sozialhilfemißbrauch überhaupt mit dem Recht der Hilfeempfänger auf Datenschutz vereinbar.

2. Sozialversicherung

Wenn in diesem Tätigkeitsbericht nur wenig über Aktivitäten meines Amts im Bereich der Sozialversicherung zu lesen ist, dann bedeutet dies nicht etwa, daß wir uns damit nicht befaßt hätten. Im Gegenteil: Nur ging es dabei weniger um die Aufdeckung von Fehlern und Verstößen, sondern mehr darum, Aufklärungsarbeit zu leisten, Versicherten, aber auch Ärzten und Zahnärzten und anderen Leistungserbringern das komplizierte Beziehungsgeflecht der an der gesetzlichen Krankenversicherung beteiligten Personen und Institutionen zu erklären und ihre gegenseitigen Rechte und Pflichten beim Umgang mit Versichertendaten aufzuzeigen.

2.1 Die Sozialversicherung der Landwirte

Die Landwirtschaftliche Berufsgenossenschaft, die Landwirtschaftliche Alterskasse, die Landwirtschaftliche Krankenkasse und die Landwirtschaftliche Pflegekasse Württemberg führen die gesetzliche Unfallversicherung, Alterssicherung, Krankenversicherung und Pflegeversicherung der Landwirte durch. Sie sind jeweils selbständige landesunmittelbare Körperschaften des öffentlichen Rechts, haben jedoch gemeinsame Organe, eine gemeinsame Geschäftsführung und eine Gesamtverwaltung mit zum Teil gemeinsamen Referaten und Abteilungen. Was lag da näher als eine Datenschutzkontrolle? Schon bei der Vorbereitung zeigte sich, daß die Landwirtschaftliche Sozialversicherung Württemberg (LSV) durchaus auf Datenschutz Wert legt, und dies bestätigte sich auch vor Ort. Da jedoch niemand perfekt ist, stellten wir auch hier einige Mängel fest, die die LSV im Interesse der Persönlichkeitsrechte ihrer Versicherten beheben muß.

2.1.1 Die Zusammenarbeit zwischen der Kranken- und Pflegekasse

Wenn ein in der Landwirtschaftlichen Pflegekasse (LPK) Versicherter pflegebedürftig wird, schaltet die Kasse, wie dies gesetzlich vorgeschrieben ist, den Medizinischen Dienst der Krankenversicherung (MDK) ein, um prüfen zu lassen, ob im Einzelfall die Voraussetzungen der Pflegebedürftigkeit erfüllt sind und welche Stufe der Pflegebedürftigkeit vorliegt. Da die Pflegekasse zu diesem Zeitpunkt regelmäßig nur wenige Informationen über den Versicherten hat, bei der Krankenkasse, bei der er ja ebenfalls versichert ist, jedoch Leistungsdaten vorliegen, die auch für die Beurteilung der Pflegebedürftigkeit relevant sein

können, beschafft sich die LPK in diesen Fällen die entsprechenden Leistungsdaten von der Landwirtschaftlichen Krankenkasse (LKK) und teilt sie dem MDK als Grundlage für seine Begutachtung mit. Einwilligungen ihrer Versicherten zu diesem Vorgehen holte die LPK bisher allerdings nicht ein.

Auf solche Einwilligungen darf die Pflegekasse aber, wenn sie die Daten der Krankenkasse nutzen will, nicht ohne weiteres verzichten: Krankenkasse und Pflegekasse sind, so hat es der Gesetzgeber entschieden, trotz ihrer engen Verbindung rechtlich selbständige Institutionen und dürfen daher die Daten ihrer Versicherten nicht beliebig austauschen. Zwar können die beiden Kassen nach § 96 Abs. 1 SGB XI bestimmte personenbezogene Daten gemeinsam verarbeiten und nutzen, doch ist ein entsprechender Datenkatalog bisher noch nicht abschließend festgelegt worden. Unabhängig hiervon unterliegt die Zusammenarbeit der beiden Kassen bei besonders schutzwürdigen Versichertendaten, insbesondere solchen, die einer der beiden Kassen von einem Arzt zugänglich gemacht worden sind, weiteren Einschränkungen. Diese Informationen muß die Kasse grundsätzlich wie ein Arzt geheimhalten, sie dürfen daher auch zwischen Kranken- und Pflegekasse nur unter den strengen Voraussetzungen des § 76 SGB X ausgetauscht werden. Will die LPK daher beispielsweise Abrechnungsdaten von Krankenhäusern oder Diagnosen aus Arbeitsunfähigkeitsbescheinigungen, die zwar bei der LKK, nicht jedoch bei ihr selbst vorhanden sind, für ihre Aufgaben nutzen, benötigt sie hierzu regelmäßig die vorherige Einwilligung der Antragsteller.

Dem kann die LPK dadurch Rechnung tragen, daß sie in ihre Antragsformulare auf Pflegeleistungen auch eine entsprechende Einwilligungserklärung ihrer Versicherten aufnimmt. Entschließt sich ein Versicherter, die Einwilligung nicht zu erteilen, dürfen diese Leistungsdaten der Krankenversicherung nicht an die Pflegeversicherung übermittelt werden, und der MDK muß den Gesundheitszustand des Antragstellers selbst umfassend aufklären, ihn also gegebenenfalls intensiver untersuchen. Hierauf sind die Versicherten in den Antragsformularen hinzuweisen.
Nach Erläuterung der Rechtslage war die LPK sofort bereit, ihre Formulare entsprechend zu ändern.

2.1.2 Die mikroverfilmten Leistungskarten

Die Landwirtschaftliche Krankenkasse (LKK) hat die Leistungsdaten ihrer Versicherten bis ca. 1990 auf Karteikarten festgehalten und diese Leistungskarten später zur Archivierung mikroverfilmt. Die Mikrofilme bewahrt sie noch heute auf, obgleich die auf den Karten gespeicherten Versichertendaten zum Teil Zeiträume von ca. 30 Jahren umfassen. Dies ist bei weitem zu lang: Wann die LKK Sozialdaten ihrer Versicherten löschen muß, regelt das Zweite Gesetz über die Krankenversicherung der Landwirte (KVLG 1989) i.V. mit § 304 SGB V und § 84 Abs. 2 SGB X. Danach sind insbesondere Angaben über Leistungen, die die Krankenkasse zur Prüfung der Voraussetzungen späterer Leistungsgewährung benötigt, sowie Diagnosen im Falle der Arbeitsunfähigkeit nach spätestens 10 Jahren zu löschen. Die LKK sah schnell ein, daß sie die alten Daten, bei denen diese Frist längst überschritten ist, löschen muß, und sagte zu, die Mikrofilme alsbald zu vernichten.

2.1.3 Probleme mit dem Löschen

Zu einem ordentlichen EDV-Verfahren gehören Löschfunktionen, damit die datenverarbeitende Stelle ihrer Pflicht zur fristgerechten Löschung gespeicherter personenbezogener Daten auch nachkommen kann. Das von der LSV eingesetzte EDV-Verfahren verfügte aber nicht über Löschfunktionen. Diesen Mangel mußte ich beanstanden. Auf meine Forderung, das Verfahren alsbald mit geeigneten Löschfunktionen auszustatten, teilte die LSV mit, eine Arbeitsgruppe sei derzeit damit beschäftigt, eine entsprechende Konzeption auszuarbeiten und den Realisierungsaufwand abzuschätzen.

2.1.4 Die Datenerfassung durch ein privates Unternehmen

Die Landwirtschaftliche Berufsgenossenschaft (LBG) hat ein privates Unternehmen mit verschiedenen Datenerfassungsarbeiten betraut und dazu mit diesem einen Vertrag abgeschlossen. Im Rahmen dieses Auftragsverhältnisses übergibt die LBG dem Unternehmen in regelmäßigen Zeitabständen Papierbelege. Dessen Mitarbeiter erfassen sodann die Daten und erstellen die entsprechenden Datenbänder für die LBG. Eine solche Verarbeitung von Sozialdaten im Auftrag durch ein privates Unternehmen ist datenschutzrechtlich unter gewissen Voraussetzungen zulässig. Verbesserungsbedürftig war dabei folgendes:

- Notwendig wäre gewesen, in dem schriftlichen Auftrag präzise zu regeln, was das Unternehmen im einzelnen zu tun hat. In dem Vertrag war aber nur ganz allgemein von diversen Datenerfassungsarbeiten

die Rede. Somit blieb völlig unklar, welche personenbezogenen Daten das Unternehmen erhielt und welche es erfassen mußte.

- Die Verarbeitung von Sozialdaten durch eine Firma ist nur dann zulässig, wenn das Unternehmen die Sozialdaten so schützt wie dies auch die LSV selbst tun muß. Notwendig ist daher, daß im Vertrag festgelegt werden muß, welche technischen und organisatorischen Maßnahmen zum Schutz der bei ihm verarbeiteten Sozialdaten zu treffen sind. Der Vertrag enthielt aber dazu keine Festlegungen.

Die LSV hat inzwischen zugesichert, den Vertrag zu überarbeiten.

2.1.5 Zugriffsrechte zu weitgehend

Verbesserungsbedürftig war die Ausgestaltung der Zugriffsrechte beim optischen Archivierungssystem, das die LSV in ihrem Beitrags- und Mitgliederbereich einsetzte. Dieses EDV-System ermöglichte allen dort Beschäftigten Zugriff auf die gesamte in der Posteingangsstelle gescannte Post. Jeder im Beitrags- und Mitgliederbereich Beschäftigte war aber nur für ganz bestimmte Aufgabenbereiche zuständig. Ausgereicht hätte daher, daß jeder lediglich die für ihn bestimmte Post zu Gesicht bekommen hätte. Diese zu weitgehenden Zugriffsrechte mußte ich beanstanden. Die LSV hat mitgeteilt, sie werde die Zugriffsrechte auf das dienstlich erforderliche Maß beschränken.

2.2 Dürfen Krankenkassen Arztberichte lesen?

Immer wieder beschweren sich Ärzte und Krankenhäuser bei mir darüber, gesetzliche Krankenkassen würden bei ihnen Befund-, Entlaß- oder sonstige Arztberichte über Patienten anfordern. Meist würden sie dabei gebeten, die gewünschten Unterlagen direkt an den Medizinischen Dienst der Krankenversicherung (MDK) zu schicken, teilweise gingen die Kassen aber auch davon aus, die Berichte seien an sie selbst zu versenden.

Wie also dürfen Krankenkassen vorgehen, wenn sie beurteilen wollen, ob einer ihrer Versicherten wirklich stationär behandelt werden muß, noch arbeitsunfähig ist, Maßnahmen zur Wiederherstellung seiner Arbeitsfähigkeit einzuleiten sind oder die Kasse sonst Leistungen erbringen muß?

Eine Rechtsvorschrift, die die Kassen berechtigen würde, in diesen Fällen von Ärzten oder Krankenhäusern Arztberichte anzufordern, existiert nicht. Dies bedeutet jedoch noch nicht, daß sie ohne Einwilligung der Versicherten keine Möglichkeit haben, diese Fragen zu klären. Wenn hierzu im Einzelfall Anlaß besteht, sind sie vielmehr nach § 275 SGB V verpflichtet, sich an den MDK zu wenden

und dort eine gutachtliche Stellungnahme über den Versicherten einzuholen. Sind die Voraussetzungen dieser Vorschrift gegeben und haben die Kassen eine solche Prüfung veranlaßt, sind die sog. Leistungserbringer, also insbesondere die behandelnden Vertragsärzte und Krankenhäuser, nach § 276 Abs. 2 SGB V verpflichtet, Patientendaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für seine gutachtliche Stellungnahme und Prüfung erforderlich ist. Einer Einwilligung der betroffenen Patienten bedarf es hierzu nicht. Den Krankenkassen darf der MDK nach § 277 SGB V am Ende nur das Ergebnis der Begutachtung und die Angaben über den Befund mitteilen, die für die Entscheidung der Kasse erforderlich sind. Der Gesetzgeber hat hier bewußt Spezialregelungen zum Ausgleich zwischen den Interessen der Versicherten und den Interessen der gesetzlichen Krankenkassen geschaffen. Durch die strikte Trennung zwischen den Kassen und dem MDK und die genauen Vorgaben des SGB V, wie der MDK mit den medizinischen Daten der Versicherten zu verfahren hat, sollen einerseits das Interesse der Patienten an der Geheimhaltung ihrer Behandlungsdaten gewahrt und andererseits die gesetzlichen Krankenkassen in die Lage versetzt werden, in begründeten Einzelfällen zu prüfen, ob sie zur Leistung verpflichtet sind.

Wenn daher in der Praxis entgegen dem Gesetzeswortlaut nicht der MDK, sondern die Krankenkassen an Ärzte und Krankenhäuser herantreten und bestimmte Unterlagen anfordern, darf dies nicht dazu führen, daß die bewußte Entscheidung des Gesetzgebers unterlaufen wird, wonach den gesetzlichen Krankenkassen längst nicht alle Informationen über den Gesundheitszustand ihrer Versicherten zustehen, die der MDK erhalten darf. Die Krankenkassen dürfen daher in diesen Fällen Arztberichte nur anfordern, wenn ihre Anforderung als Aufforderung des MDK interpretiert werden kann, ihm bestimmte Daten zu übermitteln, d.h. die Kassen im Einzelfall im Auftrag des MDK für diesen tätig werden. Dies setzt voraus, daß jeweils zwischen der Kasse und dem MDK Einigkeit darüber besteht, daß der MDK die angeforderten Unterlagen zur Erstellung seines Gutachtens benötigt. Es muß dann auch in der Aufforderung der Kasse zum Ausdruck kommen, daß nicht sie, sondern der MDK die Unterlagen benötigt und daß sie deshalb auch nur diesem vorzulegen sind.

Außerdem dürfen nur solche Daten angefordert werden, die der MDK im Einzelfall wirklich für seine Stellungnahme benötigt. Ob danach beispielsweise komplette Krankenblattunterlagen oder Entlaßberichte erforderlich sind, muß in jedem Einzelfall neu geprüft und entschieden werden. Bestehen daran Zweifel, sollte sich der Arzt oder das Krankenhaus die Erforderlichkeit durch den MDK näher darlegen lassen.

3. Sozial- und Jugendhilfe

Rund 2,7 Mio. Menschen bezogen im Jahr 1996 in Deutschland Sozialhilfe. Auch die öffentliche Jugendhilfe rückt angesichts der wachsenden Jugendkriminalität immer stärker ins Blickfeld des öffentlichen Interesses. Kein Wunder, daß auch wir uns immer wieder Datenschutzfragen aus diesem Bereich stellen mußten.

3.1 Die Anfrage des Sozialamts beim behandelnden Arzt

Weil sich ein Sozialamt nicht sicher war, ob einer Antragstellerin wegen ihrer Behinderung Eingliederungshilfe für Behinderte nach §§ 39 ff. des Bundessozialhilfegesetzes (BSHG) zu gewähren war, wandte es sich an den Arzt, bei dem die Hilfesuchende in Behandlung war, und bat diesen, auf einem Formblatt zu attestieren, ob und inwieweit bei dem bei seiner Patientin vorliegenden Krankheitsbild Maßnahmen der Eingliederungshilfe in Betracht gezogen werden könnten. Das Formblatt sah Angaben zur Vorgeschichte und zum seitherigen Verlauf der Krankheit, zur Art, Schwere und voraussichtlichen Dauer der Behinderung, zur Diagnose und zu den aus ärztlicher Sicht erforderlichen Eingliederungsmaßnahmen nach § 40 BSHG und deren Erfolgsaussichten vor. Ob die Patientin mit einer solchen Begutachtung einverstanden war oder nicht, war dem Schreiben des Sozialamts ebensowenig zu entnehmen wie ein Hinweis darauf, ob und, wenn ja, nach welcher Rechtsvorschrift der Arzt dem Sozialamt gegenüber zur Erstattung des Attestes verpflichtet war.

Auf meine Nachfrage erklärte das Sozialamt, die Angelegenheit sei mit der betroffenen Hilfesuchenden ausführlich besprochen worden und diese habe im übrigen darin eingewilligt, daß das Gesundheitsamt bei den sie behandelnden Ärzten Daten über ihren Krankheitszustand anfordert.

Bei dieser Sachlage war die Anfrage des Sozialamts gleich aus mehreren Gründen fehlerhaft:
Das Sozialamt kann sich zur Rechtfertigung seiner Anfrage beim behandelnden Arzt nicht darauf berufen, daß die Hilfesuchende der Einholung der Auskünfte über ihren Krankheitszustand durch das Gesundheitsamt zugestimmt hatte.
Das Sozialamt und das Gesundheitsamt sind zwar beides Organisationseinheiten des Landratsamts, jedoch haben sie wegen ihrer unterschiedlichen Aufgaben bei der Datenverarbeitung jeweils andere gesetzliche Regelungen zu beachten. Wenn nur eine dieser Stellen zur Erhebung bestimmter Daten ermächtigt ist, ist deshalb nicht gleichzeitig auch die andere Stelle berechtigt, diese Daten anzufordern. Für das Sozialamt gilt: Benötigt es Auskünfte über einen Hilfesuchenden, muß es die Datenerhebungsvorschriften des Zehnten Buchs des Sozialgesetzbuchs (SGB X) beachten. Deshalb hat es nach § 67a Abs. 2 SGB X

die Daten grundsätzlich bei diesem selbst einzuholen, ihn also, wenn es ein ärztliches Attest braucht, unter Hinweis auf seine Mitwirkungspflicht nach § 60 SGB I aufzufordern, das ärztliche Zeugnis selbst beizubringen. Will das Sozialamt das Attest direkt beim behandelnden Arzt anfordern, ist dies nur zulässig, wenn hierfür eine wirksame Einwilligung des Patienten vorliegt. Nur wenn dies der Fall ist, darf im übrigen der Arzt wegen der ihm auferlegten Schweigepflicht gegenüber Dritten - und damit auch gegenüber dem Sozialamt - Angaben über seine Patienten machen und muß dies nach § 100 SGB X auch tun, wenn die Angaben vom Sozialamt benötigt werden. Außerdem muß das Sozialamt, wenn es die Informationen statt beim Hilfesuchenden selbst beim behandelnden Arzt einholt, diesen nach § 67a Abs. 4 SGB X auf seine Auskunftspflicht und die Rechtsvorschrift, die zur Auskunft verpflichtet, hinweisen.

In unserem Fall fehlten somit sowohl die Einwilligung der Hilfesuchenden in die Einholung von Auskünften beim sie behandelnden Arzt als auch der Hinweis des Sozialamts an diesen Arzt nach § 67a Abs. 4 SGB X. Nachdem ich dem Sozialamt die Rechtslage erläutert hatte, versprach es, sich in Zukunft daran zu halten.

3.2 Die Strafanzeige bei Kindesmißbrauch

Dürfen Jugendämter, wenn sie von der Mißhandlung oder dem Mißbrauch eines Kindes oder Jugendlichen erfahren, die Strafverfolgungsbehörden unterrichten? Anlässe, diese Frage zu stellen, gibt es leider immer wieder. In der Öffentlichkeit wird dann schnell die Forderung laut, die Einrichtungen der Jugendhilfe sollten jeden Fall von Kindesmißbrauch, der ihnen bekannt wird, sofort der Polizei oder Staatsanwaltschaft melden. Die Gegenmeinung verweist meist ebenso pauschal auf das Sozialgeheimnis und die berufliche Schweigepflicht der staatlich anerkannten Sozialarbeiter, Sozialpädagogen und Diplompsychologen. Wer die Datenübermittlungsvorschriften, die für die Einrichtungen der Jugendhilfe gelten, genauer ansieht, merkt freilich schnell, daß die Frage nicht so einfach und allgemein zu beantworten ist.

Haben Mitarbeiterinnen oder Mitarbeiter von Jugendämtern im Rahmen ihrer dienstlichen Tätigkeit von einer Kindesmißhandlung oder einem Kindesmißbrauch erfahren, dürfen sie dies nur dann an die Strafverfolgungsbehörden weitergeben, wenn eine Rechtsvorschrift dies erlaubt. Als derartige Rechtsvorschrift kommt § 69 Abs. 1 Nr. 1 SGB X i.V. mit § 64 Abs. 2 SGB VIII in Betracht. Danach ist die Weitergabe zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe der Träger der Jugendhilfe nach dem Sozialgesetzbuch erforderlich ist. Da das Jugendamt, wie sich aus verschiedenen Vorschriften des Achten

Buchs des Sozialgesetzbuchs ergibt, auch die Aufgabe hat, Mißhandlungen und Mißbrauch von Kindern und Jugendlichen zu verhindern, bedeutet dies konkret, daß es eine solche Tat bei der Polizei oder Staatsanwaltschaft anzeigen und die notwendigen Informationen zur Durchführung des Strafverfahrens übermitteln darf, wenn damit die Straftat bzw. ihre Fortsetzung verhindert und dieser Erfolg nicht auch durch eine weniger belastende Maßnahme erreicht werden kann. Zu beurteilen, ob diese Voraussetzungen im Einzelfall vorliegen, ist in erster Linie Sache des Jugendamts, das seine Entscheidung nach den für seine Aufgabenerfüllung maßgeblichen fachlichen Gesichtspunkten zu treffen hat. Dabei ist allerdings zu bedenken, daß das Kinder- und Jugendhilferecht eine ganze Reihe von Hilfen und Maßnahmen zur Bewältigung von Problemsituationen in Familien und zum Schutz der Kinder und Jugendlichen vorsieht, angefangen von der Beratung bis hin zur Anrufung des Vormundschaftsgerichts bei Gefährdung des Kindeswohls und zur Inobhutnahme des Kindes oder Jugendlichen. Dies schließt freilich nicht aus, daß die Jugendämter als ultima ratio auch die Strafverfolgungsbehörden einschalten können, zumal diese Behörden umfassendere Ermittlungsmöglichkeiten als das Jugendamt und das Vormundschaftsgericht haben, die dann beispielsweise auch für Maßnahmen des Vormundschaftsgerichts und des Jugendamts im Interesse des Kindeswohls nutzbar gemacht werden können. Ob die Benachrichtigung der Polizei und Staatsanwaltschaft in diesem Sinne erforderlich ist, kann also nicht generell, sondern muß in jedem Einzelfall nach sorgfältiger Abwägung aller Umstände entschieden werden.

Bejaht das Jugendamt nach pflichtgemäßer Prüfung die Erforderlichkeit, liegen auch regelmäßig die Voraussetzungen des rechtfertigenden Notstands nach § 34 StGB vor. Deshalb steht der Einschaltung der Strafverfolgungsbehörden in diesen Fällen auch weder der besondere Vertrauensschutz in der persönlichen und erzieherischen Hilfe nach § 65 SGB VIII noch die berufliche Schweigepflicht der Sozialarbeiter, Sozialpädagogen und Berufspsychologen nach § 203 Abs. 1 StGB entgegen.

3.3 Die Betreuungspauschale

Erwachsene behinderte Menschen haben es vielfach schwer, sich so in das Leben in der Gemeinschaft einzugliedern, daß sie selbständig, ohne Betreuung in der eigenen Wohnung leben können. Ein Weg, dieses Ziel zu erreichen, ist die vorübergehende Aufnahme in eine Wohngemeinschaft oder andere Betreute Wohnformen. Der Landeswohlfahrtsverband Baden, zu dessen Aufgabe die Behindertenfürsorge und die Eingliederungshilfe gehört, unterstützte solche Betreute Wohnformen bis 31. Dez. 1996 dadurch, daß er den Trägern derartiger Einrichtungen als freiwillige Leistung Personalkostenzuschüsse gewährte. Mit

dem 1. Jan. 1997 stellte er sein Fördersystem jedoch um: Statt den Trägern Zuschüsse zu gewähren, zahlt er jetzt eine Betreuungspauschale als individuelle Eingliederungshilfe für die Behinderten, die in solchen Wohnformen leben. Mit der Betreuungspauschale werden jedoch nach wie vor ausschließlich Kosten bei den Trägern der Betreuten Wohneinrichtungen abgegolten. Deshalb zahlt der Landeswohlfahrtsverband die Förderung auch wie bisher direkt an die Träger der Einrichtungen aus.

Eine Folge der Umstellung des Fördersystems war: Solche Behinderte im Betreuten Wohnen, die bisher noch keine Sozialhilfe bezogen hatten, wurden quasi über Nacht zum Sozialhilfeempfänger. Damit nicht genug: Während die Einrichtungsträger bisher, um Personalkostenzuschüsse zu erhalten, neben Daten über ihr Fachpersonal nur anonymisierte Bescheinigungen über die Erkrankungen, Behinderungen und den Betreuungsbedarf dieser Behinderten vorlegen mußten, verlangt der Landeswohlfahrtsverband jetzt, daß ihm über die Sozialämter der Stadt- und Landkreise die Namen und Anschriften aller im Betreuten Wohnen lebenden erwachsenen Behinderten mitgeteilt werden. Wer von ihnen bisher noch keine Sozialhilfe bezog, mußte also erstmals sowohl dem örtlichen Sozialamt als auch dem Landeswohlfahrtsverband seinen Namen und seine Adresse und damit natürlich auch seine Behinderung offenbaren. Dies hat, wie mir ein Träger Betreuter Wohneinrichtungen mitteilte, gerade bei psychisch Kranken im Betreuten Wohnen, die bisher gegenüber den Sozialhilfeträgern anonym geblieben waren, teilweise erhebliche Ängste ausgelöst.

Auf meine Frage, weshalb sich der Landeswohlfahrtsverband auch bei dem neuen Fördersystem nicht wie bisher mit anonymisierten Daten der Behinderten begnügt, erhielt ich die Antwort, mit der Umstellung könnten die in diesem Bereich aufgewandten Mittel zielgenauer eingesetzt und ein größerer Einfluß auf die Belegung der Betreuten Wohnangebote ausgeübt werden. Im übrigen zwinge schon die neue Rechtsform zur Angabe der Personalien der betroffenen Behinderten. Individuelle Sozialhilfeleistungen könnten nicht für anonyme Personen gezahlt werden, Anträge und Bescheide müßten Namen und Anschrift der Hilfeempfänger nennen.

Formalrechtlich mag diese Argumentation des Landeswohlfahrtsverbands nicht zu beanstanden sein. Daß es dem Landeswohlfahrtsverband aber erst durch die zusätzlichen Namens- und Adressenangaben möglich geworden sein soll, größeren Einfluß auf die Belegung der Betreuten Wohnangebote auszuüben, kann ich nach wie vor nicht erkennen. Ob und gegebenenfalls wie lange das Betreute Wohnen im Einzelfall gerechtfertigt ist, hängt von der Behinderung,

nicht aber von der Identität des einzelnen Behinderten ab. Da auch nach dem früheren Verfahren schon - wenn auch in anonymisierter Form - fachärztliche Bescheinigungen über die Behinderung vorgelegt und die Notwendigkeit der Betreuung nachgewiesen werden mußte, wäre es auch nach diesem - für viele Behinderte erheblich datenschutzfreundlicheren - System möglich gewesen, zu überprüfen, ob das Betreute Wohnen im Einzelfall noch erforderlich ist.

3.4 Warum erst jetzt?

"Weshalb muß ich akzeptieren, daß die Mitarbeiter der Banken, die an der Überweisung meines Landesblindengeldes durch den Landeswohlfahrtsverband Baden beteiligt sind, jeweils erkennen können, daß ich blind bin und Landesblindenhilfe beziehe?", beklagte sich ein Bürger bei mir. Die Klage war berechtigt, denn um das Landesblindengeld zu überweisen und dem Empfänger deutlich zu machen, wofür der überwiesene Betrag bestimmt ist, ist es nun wirklich nicht notwendig, "Blindenhilfe" als Verwendungszweck auf dem Überweisungsträger einzutragen. Dazu reichen neutrale Formulierungen wie "Bescheid vom ..." oder nichtsprechende Aktenzeichen völlig aus. Der Landeswohlfahrtsverband sah dies, nachdem ich ihn mit der Klage des Bürgers konfrontiert hatte, auch so und stellte sein Verfahren um. Die Frage bleibt freilich, warum er dies nicht schon längst von sich aus getan hatte, zumal schon seit Jahren höchstrichterlich anerkannt ist, daß Vermerke auf Überweisungsvordrucken wie "Sozialleistungen" oder gar "Sozialhilfe" auf den Überweisungsträgern nicht zulässig sind und er bei der Überweisung von Leistungen nach dem Bundessozialhilfegesetz daraus schon selbst die gebotenen Konsequenzen gezogen hatte.

4. Teil: Rathaus und Landratsamt

1. Das Einwohnermeldeamt

Das Melderegister, in dem das Einwohnermeldeamt alle Einwohner der Gemeinde registriert, ist eine vielgenutzte Datenquelle für andere Behörden ebenso wie für Privatleute. Angesichts einer so intensiven Verarbeitung von Einwohnerdaten kann nicht verwundern, daß immer wieder Datenschutzprobleme auftreten. Eines davon, das Jahr für Jahr in trauriger Regelmäßigkeit wiederkehrt, ist die Personenverwechslung bei Melderegisterauskünften. Auch in diesem Jahr erfuhr ich durch Bürgereingaben, daß zwei Einwohnermeldeämter - das eine in einem Stadtkreis, das andere in einer 10 000-Einwohner-Gemeinde - auf Anfrage von Gläubigern, wohin ihre Schuldner weggezogen waren, versehentlich die Anschrift jeweils einer anderen gleichnamigen Person mitteilten. Diese anderen Personen erfuhren dadurch von den Zahlungsschwierigkeiten der eigentlich gesuchten Schuldner und hatten überdies Mühe, den Gläubigern klarzumachen, daß sie bei ihnen an der falschen Adresse waren. Immerhin redeten sich die beiden Gemeinden auf meine Beanstandung nicht damit hinaus, bei einem solchen Massenverfahren seien eben Pannen unvermeidlich, sondern räumten ihren Fehler unumwunden ein, entschuldigten sich bei den betroffenen Personen und erließen Anordnungen, um ähnlichen Fehlern vorzubeugen.
Aber mein Amt hatte sich auch mit anderen Problemen zu befassen.

1.1 Die Melderegisterbereinigung

Betroffene Bürger machten mich darauf aufmerksam, daß in einem Stadtkreis und in einer Großen Kreisstadt in Nordbaden das Einwohnermeldeamt eine Befragungsaktion zur Bereinigung des Melderegisters durchführt. Unsere Ermittlungen ergaben, daß beide Ämter unabhängig voneinander jeweils weit über 1 000 ihrer Einwohner angeschrieben hatten, die im Melderegister mit Nebenwohnung gemeldet waren und bei denen bestimmte weitere Kriterien zutrafen. Sie baten die ausgewählten Einwohner, einen Fragebogen mit gezielten Detailfragen zu ihrer Wohnsituation auszufüllen und zurückzusenden. Anhand der Antworten wollten die Einwohnermeldeämter jeweils prüfen, ob der Einwohner die Wohnung tatsächlich noch als Nebenwohnung oder vielleicht inzwischen als Hauptwohnung bewohnt oder ob er gar ganz weggezogen ist, und gegebenenfalls den Melderegistereintrag entsprechend ändern. Hätten sich die Einwohnermeldeämter darauf beschränkt, diese Einwohner vorsorglich an ihre Meldepflicht zu erinnern für den Fall, daß sich die tatsächlichen Wohnverhältnisse seit der Anmeldung geändert haben, so wäre dagegen nichts einzuwenden gewesen. Klar ist auch, daß die Ämter wegen ihrer Verantwortlichkeit für die Richtigkeit des Melderegisters sich um Aufklärung des Sachverhalts hätten bemühen

dürfen, wenn sie konkrete Anhaltspunkte dafür gehabt hätten, bestimmte Daten könnten unrichtig sein. So aber war es hier nicht; gegen keinen der angeschriebenen Einwohner richtete sich ein konkreter Verdacht im Einzelfall. Diese waren vielmehr nur deshalb in die Befragungsaktion einbezogen worden, weil sie zu einem Personenkreis gehörten, bei dem die Ämter aufgrund ihrer Erfahrungen mehr als bei anderen damit rechneten, daß eine Veränderung der Wohnverhältnisse nicht gemeldet wurde. Ob derartige Ermittlungen aufs Geratewohl bei einer Vielzahl für sich unverdächtiger Einwohner noch verhältnismäßig sind, ist sehr die Frage. Auf jeden Fall aber war zu kritisieren, daß die Städte den angeschriebenen Einwohnern nicht, wie es das Landesdatenschutzgesetz verlangt, klar und deutlich sagten, daß sie zwar bei der Aufklärung des Sachverhalts mitwirken sollen, aber rechtlich nicht verpflichtet sind, Angaben zu machen, wenn sie ihrer Meldepflicht korrekt nachgekommen sind. Die Städte erweckten im Gegenteil den Eindruck, die Einwohner seien aufgrund von § 20 des Meldegesetzes zur Auskunft verpflichtet. Diese Vorschrift verpflichtet einen Einwohner aber nur zu ergänzenden Auskünften, die das Einwohnermeldeamt zur Bearbeitung seiner Anmeldung oder Abmeldung benötigt; sie ist dagegen nicht anwendbar, wenn das Einwohnermeldeamt nach Jahren wissen möchte, ob sich an den tatsächlichen Wohnverhältnissen seit der Anmeldung inzwischen etwas geändert hat. Eine der beiden Städte drohte sogar mindestens einem der betroffenen Einwohner an, wenn er nicht antworte, müsse er mit einer Ordnungswidrigkeitenanzeige rechnen und werde von Amts wegen abgemeldet. Das ging nun wirklich zu weit: Wo keine Auskunftspflicht besteht, kann die Verweigerung der Auskunft natürlich auch keine Ordnungswidrigkeit sein; und von Amts wegen abmelden darf ein Einwohnermeldeamt einen Einwohner nur dann, wenn für es eindeutig feststeht, daß er nicht mehr unter der angegebenen Wohnung wohnt. An dieser Gewißheit fehlte es, wie die Befragungsaktion zeigt, in diesem Fall gerade.

1.2 Direktzugriff auf Melderegister

Gewissermaßen zu den Großkunden der Einwohnermeldeämter gehören die Landratsämter: Sie benötigen zur Veranlagung der Abfallbeseitigungsgebühren in großem Umfang Einwohnerdaten aus dem Melderegister und bekommen diese auch regelmäßig von den Einwohnermeldeämtern geliefert. Der bequeme Direktzugriff auf die Melderegister ihrer Kreisgemeinden war den Landratsämtern jedoch in der Vergangenheit noch verwehrt, weil es dazu einer Rechtsverordnung des Innenministeriums bedurfte und dieses sich damit, durchaus auch im Sinne des Datenschutzes, Zeit ließ. Die fünf Landratsämter der Region Stuttgart hatten freilich die Rechtsverordnung nicht abgewartet, sondern sich bereits vorher vom gemeinsamen regionalen Rechenzentrum Online-

Zugriffsmöglichkeiten auf Meldedaten einrichten lassen. Diese widerrechtlich eingerichteten und genutzten Online-Anschlüsse hatten wir seinerzeit daraufhin beanstandet (vgl. 16. Tätigkeitsbericht 1995, LT-Drs. 11/6900, S. 73).

Seit Juli 1996 erlaubt nunmehr die neue Meldeverordnung, daß Landratsämter für Zwecke der Abfallgebührenveranlagung und der Zulassung von Kraftfahrzeugen online auf ausgewählte Meldedaten zugreifen. Die Verordnung legt genau fest, welche Datenarten für den Direktabruf zugelassen sind, und schreibt vor, daß und wie die Abrufe stichprobenweise zu protokollieren sind. Auch wenn das Innenministerium beim Erlaß der Meldeverordnung, wie im 17. Tätigkeitsbericht 1996 (LT-Drs. 12/750, S. 61 f.) dargestellt, nicht allen unseren Vorschlägen entsprochen hat, stellt sie nun die Richtschnur dar, wenn es darum geht, zu prüfen, ob Online-Zugriffe der Landratsämter auf Meldedaten datenschutzrechtlich zulässig sind oder nicht.

Im Januar, also ein halbes Jahr nach Inkrafttreten der Meldeverordnung, ergaben unsere Recherchen, daß die fünf Landratsämter auch nach Inkrafttreten der Meldeverordnung geradeso im alten Trott weitermachten, wie sie es schon getan hatten: Sie riefen im gleichen Umfang wie früher Meldedaten ab, ohne daß, wie von der Meldeverordnung gefordert, die Abrufe protokolliert wurden. Ein Protokollierungsverfahren stand nämlich überhaupt noch nicht zur Verfügung. Deshalb war eine erneute Beanstandung nicht zu umgehen.

Im September schauten wir uns die Sache bei zwei der fünf Landratsämter vor Ort an.

- Diese machten von der Abrufmöglichkeit in großem Umfang Gebrauch. Bei einem von ihnen konnten 10, beim anderen gar 30 Mitarbeiter online auf Meldedaten zugreifen und zwar jeweils auf die Melderegister aller Kreisgemeinden, obwohl die einzelnen Mitarbeiter jeweils nur für die Abfallgebührenveranlagung in einzelnen Gemeinden zuständig waren. Sie konnten jeweils mehr Datenarten ansehen, als die Meldeverordnung zuläßt, beispielsweise Angaben zu früheren Wohnungen, ferner Angaben über Personen, die schon vor mehr als fünf Jahren weggezogen oder verstorben waren. Eines der Ämter kam auf durchschnittlich über 350 Abfragen pro Werktag.
- Ein Protokollierungsverfahren war jetzt zwar im Einsatz, aber es arbeitete nicht so, wie es die Meldeverordnung verlangt. Ein Fehler war, daß das Verfahren von vornherein gar nicht alle Abfragemöglichkeiten erfaßte. Hinzu kam: Anstatt jeden 50. Abruf jedes einzelnen Landratsamts zu protokollieren, wie es die Meldeverordnung verlangt, zählte das Verfahren die Abrufe aller fünf Landratsämter und sogar noch der Polizeidienststellen der Region fort-

laufend durch und zeichnete jeden 50. auf; dadurch war nicht sichergestellt, daß jedes einzelne Landratsamt auf die vorgegebene Quote kam. Schließlich erfaßte die Protokollierung stets nur eine Bildschirmmaske, auch wenn eine Abfrage aus mehreren sachlich zusammengehörenden Masken bestand. Daß diese Art der Protokollierung den Anforderungen nicht entsprach, merkte wohl auch das Rechenzentrum, denn ab Mitte September 1997 protokollierte es **alle** Abrufe; dies aber ist nun wiederum zuviel.

- Damit nicht genug: Die Landratsämter gaben nur bei den wenigsten Abrufen einen Hinweis auf den Anlaß des Abrufs ein, wie es die Meldeverordnung verlangt, und dann war der Eintrag zumeist auch noch wenig aussagekräftig. Da paßt ins Bild, daß auch keines der beiden Landratsämter je die Protokolldaten daraufhin ausgewertet hatte, ob die einzelnen protokollierten Abrufe zur Aufgabenerfüllung erforderlich und damit zulässig waren; ja sie hatten noch nicht einmal ein Konzept für die Auswertung erstellt.

Das ernüchternde Fazit: Auch über ein Jahr nach Inkrafttreten der Meldeverordnung lief das Abrufverfahren noch lange nicht so, wie es die Meldeverordnung verbindlich vorschreibt. Eine effektive Kontrolle, ob die außergewöhnlich zahlreichen einzelnen Abrufe auch tatsächlich zur Abfallgebührenveranlagung erforderlich und damit zulässig waren, fand nicht statt. Auf meine Beanstandungen hin reagierte bislang erst eines der beiden Landratsämter. Es teilte mit, es habe ein Auswertungskonzept erarbeitet und sich zur Beseitigung der Verfahrensmängel mit dem Rechenzentrum in Verbindung gesetzt. Auch wenn hoffentlich bald alles in Ordnung gebracht wird, muß es nachdenklich stimmen, daß die Landratsämter und das Rechenzentrum über einen langen Zeitraum hin gegenüber zwingenden, dem Schutz von Bürgerdaten dienenden Rechtsvorschriften eine solch nonchalante Haltung an den Tag legten.

2. Die Stadtbibliothek

In etwa jeder zweiten Stadt oder Gemeinde unseres Landes gibt es eine kommunale Bibliothek. Mehr und mehr von ihnen setzen den Computer ein, um ihren Bestand an Büchern und anderen Medien zu katalogisieren, die Leser und Benutzer zu verwalten und den Leihverkehr zu verbuchen. Die Bibliotheken können dabei unter mindestens 20 verschiedenen EDV-Verfahren kommerzieller Anbieter auswählen. Jedes dieser Verfahren daraufhin zu überprüfen, ob es die Daten der Benutzer, also der Entleiher, datenschutzgerecht verarbeitet, kann meine kleine Dienststelle natürlich nicht mit vertretbarem Aufwand leisten. Aber bei einem Stadtkreis im badischen und einer Großen Kreisstadt im württembergischen Landesteil, die je eines der häufiger verbreiteten EDV-Verfahren einsetzen, schauten wir uns doch vor Ort näher an, wie das Ver-

fahren arbeitet und wie die Stadtbibliothek mit den Daten der Benutzer umgeht. Dabei kam es uns schwerpunktmäßig auf folgendes an:

- Die Bibliothek darf von einem Benutzer nur diejenigen Angaben erfragen und speichern, die sie für den Ausleihverkehr tatsächlich braucht. Will sie für interne statistische Zwecke zusätzliche Angaben erheben, muß sie dem Benutzer sagen, daß seine Angaben freiwillig sind, und ihm den Zweck nennen.
- Es dürfen keine Benutzerprofile entstehen, die über das Ausleih- und Leseverhalten und die Interessengebiete der einzelnen Benutzer Aufschluß geben. Um eine solche elektronische Überwachung zu verhindern, darf dann, wenn ein Buch zurückgegeben worden ist und sich die Bibliothek davon überzeugt hat, daß alles seine Ordnung hat, nicht länger gespeichert sein, wer das Buch entliehen hatte.
- Wie bei jedem Computereinsatz müssen ausreichende Datensicherungsmaßnahmen ergriffen werden. Werden Computer zur Selbstbedienung durch die Benutzer bereitgestellt, so muß durch einen wirksamen Schutzmechanismus, z.B. durch ein Paßwortverfahren, gewährleistet sein, daß jeder Benutzer nur auf sein eigenes Benutzerkonto zugreifen kann.

Nach Ausräumung einiger kleinerer Mängel, auf die ich hingewiesen habe, genügt die Vorgehensweise beider Stadtbibliotheken den datenschutzrechtlichen Anforderungen.

3. Das Gemeindearchiv

In den Archiven so mancher Stadt oder Gemeinde befinden sich Unterlagen über Opfer der NS-Herrschaft, beispielsweise über deportierte Juden oder über ausländische Zwangsarbeiter. Darüber, wie die Archive mit diesen Unterlagen umgehen können, besteht hin und wieder Unsicherheit. Dazu drei Beispiele:

- In einer Gemeinde am Hochrhein regte ein privates "Komitee zum Schutz der Zeugnisse jüdischen Lebens" an, an einem ehemaligen Altersheim eine Gedenktafel mit den Namen der 105 jüdischen Bewohner anzubringen, die 1940 von dort in das Konzentrationslager deportiert worden waren. Im Zusammenhang damit stellte sich die Frage, ob es der Datenschutz dem Gemeindearchiv, das eine gesonderte Kartei mit den Namen dieser Opfer aufbewahrte, erlaubt, diese Daten für diesen Zweck herauszugeben. Meine Antwort fiel so aus: Auch wenn die Datenschutzgesetze grundsätzlich nur die Daten von noch lebenden Personen schützen, bedeutet dies nicht, daß mit den Daten von Toten beliebig verfahren werden könnte. Jeder Mensch hat auch noch über seinen Tod hinaus Anspruch auf Achtung seiner Menschenwürde. Dieser nachwirkende Persönlichkeitsschutz hat in verschiedenen gesetzlichen Regelungen seinen Niederschlag gefunden, so im Landesarchivgesetz, das auch für die kommunalen Archive gilt. Nach diesem Gesetz darf

kommunales Archivgut grundsätzlich frühestens 30 Jahre nach seiner Entstehung und zehn Jahre nach dem Tod der Personen, auf die es sich bezieht, genutzt werden; kann der Todeszeitpunkt nicht festgestellt werden, endet die Sperrfrist 90 Jahre nach der Geburt. Auch nach Ablauf dieser Fristen darf das Archivgut nicht genutzt werden, soweit Grund zu der Annahme besteht, daß schutzwürdige Belange von Angehörigen oder sonstigen dritten Personen entgegenstehen. Für die Daten der deportierten Juden folgt daraus, daß die Sperrfristen längst abgelaufen sind und es somit entscheidend darauf ankommt, ob der Anbringung der Namen der Opfer auf einer Gedenktafel schutzwürdige Belange dritter Personen entgegenstehen. Ich habe diese Frage verneint. Die Veröffentlichung würde in keiner Weise diskriminierend wirken. Im Gegenteil läßt sich mit guten Gründen die Meinung vertreten, daß damit die Opfer der Judenverfolgung aus ihrer Anonymität herausgehoben würden und deutlich gemacht würde, daß es sich um konkrete Personen aus Fleisch und Blut gehandelt hat. Ich meine daher, daß das Landesarchivgesetz es rechtlich zuläßt, die Namen der Opfer aus dem Archiv für die Gedenktafel zu verwenden. Eine andere Frage ist, ob es nicht gleichwohl angemessen wäre, vor einer Veröffentlichung der Opfernamen, soweit möglich, die Angehörigen zu befragen, auch wenn dies rechtlich nicht geboten ist.

- Der Internationale Suchdienst interessiert sich für die Unterlagen über während des Zweiten Weltkriegs nach Deutschland verschleppte ausländische Zwangsarbeiter, die in manchen Gemeindearchiven ruhen. Zumeist handelt es sich dabei um Melderegisterkarten aus jener Zeit oder um besonders zusammengestellte Listen. Immer wieder wollen Gemeinden von mir wissen, ob sie dem Internationalen Suchdienst, wie er es wünscht, Kopien der gesamten über diesen Personenkreis vorhandenen Unterlagen zum Verbleib herausgeben dürfen. Hier ist zunächst zu bedenken, daß in solchen Unterlagen auch Personen verzeichnet sein können und werden, die noch leben und deren Geburt noch nicht 90 Jahre zurückliegt. Dies bedeutet, daß die Sperrfrist noch nicht abgelaufen ist. Eine Verkürzung der Sperrfrist läßt das Landesarchivgesetz zu, wenn schutzwürdige Belange der betroffenen Personen nicht entgegenstehen. Ob dies der Fall ist oder nicht, hängt in erster Linie davon ab, in welcher Weise und zu welchem Zweck der Internationale Suchdienst die Daten verwenden will. Seine Aufgabe ist, Vermißte zu suchen und die Unterlagen über Deutsche und Nichtdeutsche, die in nationalsozialistischen Konzentrations- oder Arbeitslagern gefangengehalten, und über Nichtdeutsche, die infolge des Zweiten Weltkriegs verschleppt worden waren, zu sammeln, zu ordnen, aufzubewahren und Regierungen und interessierten Einzelpersonen zugänglich zu machen. Die Bundesrepublik Deutschland hat sich völkerrechtlich verpflichtet, die Fortführung der Arbeiten des Internationalen Suchdienstes zu gewährleisten und ihn bei der Gewinnung von Material für seine Tätigkeit zu unter-

stützen. Diesem humanitären Auftrag des Internationalen Suchdienstes kommt ein hoher Rang zu. Da bis heute eine große Anzahl von Anfragen nach dem noch nicht aufgeklärten Schicksal ehemalig Verfolgter dieser Zeit existiert, kann die Überlassung solcher Unterlagen an den Internationalen Suchdienst zur weiteren Aufklärung beitragen. Dabei ist der Internationale Suchdienst aufgrund internationaler Vereinbarungen verpflichtet, die Auskunftserteilung über eine Person zu unterlassen, wenn sie den Interessen dieser Person oder ihrer Angehörigen abträglich sein könnte. Angesichts dessen stehen schutzwürdige Belange der betroffenen Personen und ihrer Angehörigen der Herausgabe der genannten Unterlagen auch vor Ablauf der Sperrfristen nicht entgegen. Ich halte es deshalb für vertretbar, daß ein kommunales Archiv dem Internationalen Suchdienst Mehrfertigungen über Ausländer aus jener Zeit zur Verfügung stellt, wenn der Internationale Suchdienst zur Wahrung der schutzwürdigen Belange der Betroffenen zusichert, die erhaltenen Unterlagen nur für die Beantwortung von Suchanfragen zu verwenden, keine Kopien der Unterlagen weiterzugeben und sie entsprechend gesichert aufzubewahren.

- Anders war in folgendem Fall zu entscheiden: Ein Medienunternehmen beabsichtigte, einen Bericht über die in Industriebetrieben einer bestimmten Stadt beschäftigt gewesenen ausländischen Zivilpersonen und Kriegsgefangenen zu veröffentlichen; zur Illustration wollte es dabei einige Seiten der im Stadtarchiv aufbewahrten Listen dieser Personen wiedergeben. Die Liste enthielt jedoch überwiegend Personen, deren Geburt weit weniger als 90 Jahre zurückliegt, von denen also anzunehmen ist, daß viele noch am Leben sind. Hier liegen die Voraussetzungen für eine Verkürzung der Sperrfrist sicherlich nicht vor. Denn gerade eine Veröffentlichung bedeutet einen besonders starken Eingriff in das Persönlichkeitsrecht der betroffenen Personen. Solange sie noch leben, muß es ihrer Entscheidung vorbehalten bleiben, was über sie öffentlich gemacht wird. Ich riet deshalb der Stadt, allenfalls Ausfertigungen von Listen zur Verfügung zu stellen, die beispielsweise durch Löschen des Namens zuvor anonymisiert worden sind.

4. Das haben wir schon immer so gemacht

   Als üblich, bewährt und unverzichtbar bezeichnete ein Regierungspräsidium seine Praxis, die Gemeinde- oder Stadtverwaltung darüber zu unterrichten, wenn sich ein in der Gemeinde oder Stadt wohnender Bürger mit einer Anfrage oder Beschwerde an die Aufsichtsbehörde wendet. Eine datenschutzrechtliche Problematik habe man bislang in dieser Praxis nicht gesehen. Mag diese Praxis in der Tat noch weitverbreitet und althergebracht sein, korrekt ist sie damit noch lange nicht und wird, wie mir immer wieder Anfragen von Bürgern zeigen, von diesen zu Recht auch nicht so empfunden.

Sie befürchten nämlich, daß ihr Vorstoß bei der Aufsichtsbehörde zu einem Bumerang werden kann. Ein Umdenken in dieser Frage tut not.
Schreibt ein Bürger einer Behörde, so sind nicht nur sein Name und seine Anschrift, sondern schon die Tatsache des Schreibens sowie dessen Inhalt und Form Informationen, die etwas über das Verhalten des Bürgers zu und in einer bestimmten Situation aussagen; mit anderen Worten, das Schreiben insgesamt stellt ein personenbezogenes Datum des Bürgers dar. Daten eines Bürgers darf aber eine Behörde an eine andere Behörde allenfalls dann weitergeben, wenn der Bürger zuvor sein Einverständnis dazu gab oder soweit dies zur Aufgabenerfüllung erforderlich ist. Dies muß jeweils von Fall zu Fall anhand der Umstände des Einzelfalls geprüft werden. Die Weitergabe eines Bürgerschreibens ist also nicht etwa schon immer dann als Regelfall zulässig, wenn nicht wegen besonderer Umstände eine vertrauliche Behandlung angezeigt ist; vielmehr ist eine Weitergabe grundsätzlich ausgeschlossen, es sei denn, daß dies nach den Gesamtumständen erforderlich ist. Dabei reicht nicht aus, daß die Gemeinde möglicherweise ein Interesse daran hat, über Vorgänge aus dem berührten Aufgabenbereich informiert zu werden. Entscheidend kommt es vielmehr darauf an, inwieweit sie Bescheid wissen muß, damit das Anliegen des Bürgers sachgerecht bearbeitet werden kann.
Letzteres kann beispielsweise dann der Fall sein, wenn ein Bürger eine Aufsichtsbehörde bittet, die Bearbeitung gerade seiner Sache durch die Gemeinde zu überprüfen; dann ist es notwendig und damit gerechtfertigt, daß die Aufsichtsbehörde der Gemeinde den Bürger und sein Anliegen benennt, um ihr das Auffinden des Vorgangs, seine Überprüfung und eine Stellungnahme zu dem konkreten Fall zu ermöglichen. Selbst dann bedarf es allerdings in der Regel nicht der Weiterleitung des ganzen Schreibens im Original oder in Kopie, auch wenn dies für die Aufsichtsbehörde sicher der bequemste Weg wäre; die Aufsichtsbehörde sollte sich vielmehr die kleine Mühe machen, das Anliegen des Bürgers im Kern in eigenen Worten wiederzugeben, auch um einem Bürger, der sich weniger gewandt ausdrückt, eine unnötige Bloßstellung zu ersparen.
Anders sieht es dagegen aus, wenn ein Bürger bei der höheren Instanz lediglich eine allgemeine Rechtsauskunft begehrt oder die Überprüfung eines Sachverhalts anregt, an dem er selbst nicht beteiligt ist. In einem solchen Fall tut der Name des Bürgers für die Gemeinde nichts zu Sache, selbst wenn sie gegenüber der Aufsichtsbehörde eine Stellungnahme abgeben muß.
Diese Maßstäbe waren auch bei der Beurteilung der folgenden Einzelfälle zugrunde zu legen, mit denen mein Amt befaßt war:

- Ein Bürger wollte vom Landratsamt wissen, welche "auch für seine Gemeinde gültigen" Vorschriften es darüber gibt, inwieweit Zuwendungen, Gefälligkeiten usw. an Beamte und Gemeinderäte zulässig sind. Das Landratsamt gab ihm die ge-

wünschte Rechtsauskunft und fügte an, im Fall eines konkreten Verdachts auf Unregelmäßigkeiten innerhalb der Gemeindeverwaltung könne er sich erneut an das Landratsamt wenden. Von diesem Schriftwechsel unterrichtete das Landratsamt gleichzeitig - ohne es dem Bürger zu sagen - die Gemeinde. Zu Recht war der Bürger darüber verärgert, als er später davon erfuhr. Denn wer der Bürger war, mußte die Gemeinde wirklich nicht wissen.

- Eine Unterrichtung der Gemeinde war auch nicht erforderlich, als ein Mitglied eines Ortschaftsrats, um bei der Ausübung seines Mandats zu einer sachlich begründeten Entscheidung kommen zu können, beim Regierungspräsidium eine allgemeine Auskunft darüber erbat und erhielt, welche Förderprogramme es für die Gemeinde gibt.
- Dagegen war es vertretbar, daß das Landratsamt die Gemeinde informierte und dabei Roß und Reiter nannte, als ein Gemeinderatsmitglied zu einer im Gemeinderat kontrovers behandelten Rechtsfrage die Auffassung des Landratsamts erfragte, nachdem er mit seiner Auffassung nicht durchgedrungen war. Denn aus der gesamten Vorgeschichte mußte das Landratsamt folgern, daß das Gemeinderatsmitglied eine aufsichtsrechtliche Überprüfung der konkreten Angelegenheit, in der es sich selbst exponiert hatte, erwartete.

5. Der kommunale Alltag

Angesichts der breiten Vielfalt kommunaler Aufgaben kann nicht verwundern, daß Bürger wichtige und weniger gewichtige Datenschutzfragen aus diesem Bereich an mein Amt herantragen. Um einen kleinen Einblick in diese oft aufwendigen und für die betroffenen Bürger durchaus bedeutsamen Fälle zu geben, nachfolgend einige Beispiele:

- Ein fragwürdiger Service
  Wenig erfreut war ein Kurgast, der in einem Heilbad Linderung gesucht hatte, als er in der Kur-Zeitung unter der Rubrik "Wir begrüßen unsere Gäste" seinen Namen samt seiner Kuranschrift lesen mußte. Ihn störte nicht nur, daß überhaupt sein Aufenthalt in der Kurstadt publiziert wurde, sondern daß aus der Erwähnung der Spezialklinik, in der er sich aufhielt, zugleich auf die Art seines Leidens geschlossen werden konnte. Er habe, so schrieb er uns, der Veröffentlichung weder zugestimmt noch sei er überhaupt danach gefragt worden. Bei unseren Nachforschungen stellte sich heraus: Auch der Stadt war klar, daß sie Kurgastdaten nur veröffentlichen darf, wenn der Kurgast dem freiwillig zugestimmt hat. Sie nahm deshalb in den Kurtaxemeldeschein unter der Überschrift "Freiwillige Angaben" die vorgedruckte Frage auf, ob der Gast mit der Veröffentlichung seiner Daten in der Kur-Zeitung einverstanden ist oder nicht. Diesen Meldeschein füllen aber vielfach die Kurkliniken, Hotels, Pensionen usw. für ihre Gäste aus und lassen dann die Frage

nach der Veröffentlichung kurzerhand unbeantwortet, kreuzen also weder "ja" noch "nein" an. In solchen Fällen zog die Stadt aus der fehlenden Äußerung des Kurgastes den Schluß, er habe gegen die Veröffentlichung nichts einzuwenden. Ein unzulässiger Fehlschluß allein schon deshalb, weil nur zustimmen kann, wer von der Möglichkeit, "ja" oder "nein" zu sagen, weiß. Zudem verlangt das Datenschutzrecht, daß eine Einwilligung ausdrücklich erklärt werden muß.

- Das Recht am eigenen Bild
  Einen besonderen Service bietet eine Stadt den Besuchern eines von ihr betriebenen Schaubergwerks an: Bei der Einfahrt mit der Grubenbahn werden die Besucher gruppenweise Wagen für Wagen fotografiert, und nach der Führung werden die fertigen Fotografien zum Erwerb als Erinnerung angeboten. Die meisten Besucher finden dies nett. Aber auch kamerascheue Besucher entgehen dem Auge der Kamera nicht; denn kein Hinweis vor der Einfahrt warnt sie vor, so daß sie von der Situation überrascht werden und keine echte Chance haben, zu verhindern, daß sie mit aufs Bild kommen. Weil aber niemand hinnehmen muß, daß er in einer solchen Situation gegen seinen Willen fotografiert und sein Bild an andere, unter Umständen wildfremde Personen verkauft wird, regte ich bei der Stadt an, ihren Service dementsprechend zu organisieren.
- Wer zahlt den Wasserzähler?
  Entschieden zu hoch geschraubte Erwartungen an den Datenschutz legte ein Bürger in folgendem Fall an den Tag: Ihn störte, daß die von ihm erworbene Doppelhaushälfte über keinen eigenen Wasserzähler verfügte, weil die Bauherren seinerzeit nur einen gemeinsamen Wasserzähler in der anderen Haushälfte einbauen ließen. Ich konnte dem Bürger darin recht geben, daß es kein datenschutzgerechter Zustand ist, wenn sein Nachbar auf diese Weise mitbekommen kann, wieviel Wasser er verbraucht. Bei seinem Hauptanliegen, die Gemeinde solle wegen ihrer Verantwortung für den Datenschutz auch die Kosten der Installation eines eigenen Wasserzählers in seiner Doppelhaushälfte übernehmen, konnte ich ihm freilich nicht helfen. Denn diese Frage hat mit dem Datenschutz nun wirklich nichts zu tun.
- Was kostet uns ein Asylbewerber?
  Empört wandte sich ein Bürger aus einer Großen Kreisstadt an mein Amt, als er in der Presse davon las, ein Asylbewerber erhalte einen ungewöhnlich hohen Betrag an Sozialhilfe, weil er wegen einer chronischen Krankheit auf ein sehr teures Medikament angewiesen ist. Seine Empörung galt nicht der Leistungsgewährung, sondern dem Umstand, daß überhaupt darüber und dazu noch mit so vielen Einzelheiten in der Presse berichtet wird. Müssen künftig auch andere chronisch Kranke, so fragte er, damit rechnen, daß in der Zeitung steht, mit welchen Beträgen sie die Steuerzahler oder die Krankenkassen belasten - und was hätten solche

Menschen dann zu gewärtigen? Es stellte sich heraus, daß ein Stadtrat beim Bürgermeisteramt nach dem Fall, von dem er hatte läuten hören, nachgefragt und dessen schriftliche Antwort, obwohl als vertraulich gekennzeichnet, auf eigene Faust der Presse zugänglich gemacht hatte.

Von mir war allein zu prüfen, inwieweit das Bürgermeisteramt den Stadtrat informieren durfte. Hätte es dessen Anfrage in allgemeiner Form so beantwortet, daß keine Rückschlüsse auf eine bestimmte Person möglich sind, so wäre dagegen nichts einzuwenden gewesen. Tatsächlich aber hat das Bürgermeisteramt seine Antwort, auch wenn es Namen und Anschrift des Asylbewerbers nicht nannte, mit derart vielen Einzelheiten über die persönlichen, familiären und gesundheitlichen Verhältnisse des Asylbewerbers gespickt, daß es in einer Stadt dieser Größe unschwer möglich sein mußte, herauszufinden, um wen es sich handelt. Das Bürgermeisteramt hat an den Stadtrat somit personenbezogene Informationen weitergegeben, und zwar solche, die dem Sozialgeheimnis unterliegen. Dies aber ließ das Sozialgesetzbuch in diesem Fall nicht in diesem Umfang zu. Ich mußte deshalb den Verstoß gegen das Sozialgeheimnis beanstanden.

- Was kostet uns ein Musikschüler?

  Der Bürgermeister einer Gemeinde, die sich mit elf Nachbargemeinden zu einem Zweckverband zur Einrichtung und Unterhaltung einer Musikschule zusammengeschlossen hatte, machte sich Gedanken darüber, ob nicht eine andere Bemessung der Unterrichtsgebühren und eine andere Verteilung des Aufwands auf die einzelnen Zweckverbandsgemeinden in Betracht komme. Als Material für solche Erwägungen erbat er von der Musikschule eine Auflistung aller Musikschüler mit Name und Anschrift, belegten Fächern und Unterrichtsart. Zu Recht hatte die Musikschule Bedenken, diese Daten an den Bürgermeister herauszugeben. Denn Voraussetzung wäre gewesen, daß der Bürgermeister diese Daten zur Aufgabenerfüllung braucht. Um aber über die Entgeltregelung und die Kostenverteilung nachdenken zu können, reichen Angaben ohne Namen über die Gesamtzahl der Musikschüler aus jeder einzelnen Gemeinde, aufgegliedert nach Fächern und Unterrichtsarten, völlig aus. Eine namentliche Liste mit Einzelangaben über die einzelnen Schüler hat demgegenüber keine erhöhte Aussagekraft für die zu entscheidende Frage und ist deshalb nicht erforderlich.

- Akteneinsicht für den Nachbarn

  Die beiden Gesellschafter einer Schrottverwertungs-GmbH staunten nicht schlecht, als ihr Nachbar, gegen den sie einen Zivilprozeß führten, plötzlich dem Gericht Kopien aus einer Akte des städtischen Umweltamts vorlegte. Dieses hatte gegen die Schrottverwertungsfirma Ermittlungen durchgeführt, weil sie in dem Verdacht stand, ihr Betriebsgrundstück und das Gelände der Nachbarn mit boden- und grundwasserbelastenden Schadstoffen kontaminiert zu haben. Einer der

Nachbarn hatte beim Umweltamt Akteneinsicht erhalten, weil er gegen die Schrottverwertungsgesellschaft eben auch zivilrechtlich vorgehen wollte. Und beim Blick in die Akten hatte der Nachbar gleich ein paar Kopien gefertigt.
Wie ist das datenschutzrechtlich zu bewerten? Das betroffene Amt stellte sich zunächst auf den Standpunkt, das Datenschutzrecht sei hier überhaupt nicht anwendbar, weil das Landesdatenschutzgesetz nur den Schutz von Daten natürlicher Personen, nicht aber auch von Gesellschaften bezwecke. Letzteres ist zwar im Prinzip zutreffend. Jedoch hatte es außer acht gelassen, daß dann, wenn eine Gesellschaft aus einigen wenigen Mitgliedern besteht, jede Angabe über sie auch etwas über die einzelnen Gesellschafter sagt. Und die Schrottverwertungsgesellschaft bestand eben nur mal aus zwei Gesellschaftern. Nach einem entsprechenden Hinweis schloß sich das Umweltamt dieser Rechtsauffassung an. Ansonsten gab der Fall keinen Anlaß zur Beanstandung: Der Nachbar hatte ein berechtigtes Interesse an der Akteneinsicht glaubhaft dargelegt. Ein dieses Interesse überwiegendes schutzwürdiges Interesse am Unterbleiben der Akteneinsicht war nicht erkennbar. Im übrigen: Soweit der Nachbar Akteneinsicht nehmen konnte, war er auch berechtigt, Kopien und Abschriften von den in Augenschein genommenen Aktenstücken zu erhalten, um sie zur Wahrnehmung seines die Akteneinsicht rechtfertigenden Interesses zu verwenden.

- Greifvögel und Vereinsmitglieder
  Weil nach den Feststellungen eines Landratsamts Greifvögel im Haus des Vorstands eines Vogelschutzvereins unsachgemäß gehalten wurden, es sich aber nicht darüber im klaren war, ob der Vorstand dies in dieser Eigenschaft oder als Privatmann tat, bat es ihn, dem Amt neben einem aktuellen Auszug aus dem Vereinsregister auch eine Liste sämtlicher Vereinsmitglieder zu überlassen. "Warum wollen die die Namen der Mitglieder wissen?", fragte mich der Vorstand, und das mit Recht. Denn eine Mitgliederliste sagt zu der vom Landratsamt zu klärenden Frage überhaupt nichts aus. Ergo: Mit seiner Aufforderung, ihm eine Mitgliederliste zu überlassen, wollte das Landratsamt personenbezogene Daten erheben, die es überhaupt nicht benötigte. Eigentlich ein klarer Fall, sollte man meinen, nicht aber für das Landratsamt und nur deshalb wird er hier überhaupt erwähnt: In seiner ersten Stellungnahme vertrat es allen Ernstes die Auffassung, bei der Mitgliederliste handle es sich um gar keine personenbezogenen Daten. Zudem dienten die Daten der Erfüllung seiner Aufgaben, nämlich der Ermittlung des Adressaten seiner naturschutzrechtlichen Entscheidung. Zur Ehrenrettung des Landratsamts sei's gesagt: Es sah seinen Irrtum schnell ein und verzichtete auf die Mitgliederliste.

6. Vom Schweigen, das sich nicht auszahlt

Manche Datenschutzanliegen sind wahre Dauerbrenner. So schreiben uns in schöner Regelmäßigkeit nahezu Woche für Woche Bürger, es könne doch nicht im Einklang mit dem Datenschutz stehen, wenn die Bußgeldbehörde oder die Polizei die bei einer Geschwindigkeitsüberschreitung oder einem anderen Verkehrsverstoß fotografierte Person mit dem im Paß-/Personalausweisregister enthaltenen Lichtbild vergleiche, um den Verkehrssünder zu ermitteln. Sie hatten nämlich geglaubt, wenn sie als Fahrzeughalter der Bußgeldstelle den verantwortlichen Fahrer nicht nennen würden, könne diese nicht in Erfahrung bringen, wer gefahren ist, und waren deshalb erstaunt, daß die Bußgeldstelle durch den Lichtbildabgleich dem Lenker auf die Spur kam und ihm einen Verwarnungsgeldbescheid oder einen Anhörungsbogen schickte. Neuerdings ist in Briefen auch folgendes zu lesen:

> "Was allerdings meine Aufmerksamkeit, Verwunderung und Ärger auf sich gezogen hat, ist der im beigefügten Bescheid markierte Hinweis, daß persönliche Daten aus dem Paß- oder Personalausweisregister zur Verfolgung dieser Tat genutzt werden können. Ich meine, daß dies gegen den geltenden Datenschutz verstößt."

Sie alle muß ich in ihrem Glauben an die Schutzwirkung des Datenschutzes enttäuschen, denn dieser Hinweis gibt die Rechtslage zutreffend wieder. Weder ist die Bußgeldbehörde gehindert, in diesen Fällen weitere Ermittlungen anzustellen, noch ist es der Ausweisbehörde verboten, ihr unter bestimmten Voraussetzungen Auskünfte aus ihrem Register zu erteilen.

In der Praxis gingen die beteiligten Behörden manchmal dennoch nicht datenschutzgerecht zu Werke. Polizeibeamte wandten sich beispielsweise hin und wieder nicht zuerst an das Paßamt, sondern versuchten, den Fahrzeughalter zuhause anzutreffen. Gelang das nicht, klingelten sie bei Nachbarn und zeigten ihnen das Beweisfoto mit der Bitte, die abgelichtete Person zu identifizieren. Das Herumzeigen des Beweisfotos in der Nachbarschaft ist freilich ein gravierenderer Eingriff in das Persönlichkeitsrecht des Betroffenen als der Paßbildvergleich. Daraus haben das Ministerium für Umwelt und Verkehr und das Innenministerium inzwischen die Konsequenzen gezogen und in Erlassen detailliert geregelt, wie die beteiligten Behörden bei der Ermittlung von Verkehrssündern vorzugehen haben.

Für die Bußgeldbehörde/Polizei gilt:

- Hat der Fahrzeughalter einen Verwarnungsgeldbescheid oder einen Anhörungsbogen erhalten und macht er keine Angaben zur Sache, darf sich die Verfolgungsbehörde über die Meldebehörde an das Ausweisregister wenden.
- Ist für die Bußgeldbehörde/Polizei von vornherein klar, daß der Fahrzeughalter nicht der verantwortliche Fahrer ist (z.B. der Halter ist männlich, geblitzt wurde eine Frau), muß sie sich nicht erst an den Halter wenden, sondern kann anhand des Melderegisters der Meldebehörde herausfinden, ob Ehegatte, Tochter oder Sohn

als Verkehrssünder in Frage kommen und deren Ausweisbild mit dem Beweisfoto abgleichen.
- Der Vergleich der beiden Fotos ist von der Bußgeldbehörde selbst vorzunehmen. Sie muß deshalb eine Kopie des im Ausweisregister hinterlegten Fotos anfordern.
- Erst wenn der Lichtbildvergleich nicht zum Erfolg führt, kann eine Nachbarschaftsbefragung in Frage kommen.

Für die Ausweisbehörde gilt:
- Aufgrund eines auf eine bestimmte Person bezogenen Ersuchens von Bußgeldbehörde oder Polizei darf sie eine Kopie des im Ausweisregister hinterlegten Fotos weitergeben.
- Nur soweit es für die eindeutige Zuordnung des Lichtbilds erforderlich ist, darf sie auch den Namen, das Geburtsdatum und den Geburtsort des Betroffenen mitteilen.

5. Teil: Andere Bereiche

1. Abschnitt: Der Behörden liebe Not mit den Mitarbeiterdaten

1. Routine der Personalstelle

Nicht nur in schwierigen Einzelfällen bereitet der Personaldatenschutz Behörden immer wieder Kopfzerbrechen. Häufig ist es der alltägliche Umgang mit Personaldaten, den vor allem kleinere Personalstellen nicht datenschutzkonform bewältigen, wie sich an folgenden Beispielen zeigt:

1.1 Beschäftigungsbehörden zu gut informiert

Häufig ist ein Bediensteter nicht in der Behörde tätig, die ihn eingestellt hat, sondern gehört einer dieser nachgeordneten Dienststelle an. Bei allen Beamten des höheren Dienstes der Innenverwaltung trifft beispielsweise das Innenministerium die Bewerberauswahl, händigt die Ernennungsurkunde aus und führt die sog. Personalgrundakte des Beamten unabhängig davon, ob dieser bei einem Landratsamt, einem Regierungspräsidium oder beim Ministerium selbst eingesetzt wird. Ähnlich ist es auch bei den Fachhochschulen und der Polizei. Das Wissenschaftsministerium führt die Personalgrundakten aller Professoren und die Landespolizeidirektion die aller Polizeibeamten des mittleren und gehobenen Dienstes, unabhängig davon, wo die Professoren und Beamten Dienst tun. Doch nicht nur die Einstellungsbehörde, sondern auch die Beschäftigungsbehörde benötigt Informationen über den Mitarbeiter. Welche das sind, bereitet in der Praxis aber noch immer Probleme, wie sich beim Besuch einer Fachhochschule und einer Polizeidirektion zeigte:

- Der Personalbogen
  Genau gleich verfuhren die Fachhochschule und die Polizeidirektion, wenn sie zu einem bei ihr tätigen Beamten eine Personalnebenakte anlegten: Beide hefteten dort den vom Beamten ausgefüllten landeseinheitlichen Personalbogen ein. Dabei ließen sie aber völlig außer acht, zu welchem Zweck dieser landeseinheitliche Personalbogen konzipiert ist. Er dient der personalverwaltenden Stelle dazu, den geeigneten Bewerber herauszusuchen und später jederzeit, z.B. wegen einer zu treffenden Personalentscheidung, einen schnellen Überblick über dessen Werdegang zu haben. Für die Beschäftigungsbehörde hat die Speicherung von Personaldaten und die Verwendung eines Personalbogens einen ganz anderen Zweck. Sie muß nur weniges über einen Beamten wissen, nämlich das, was notwendig ist, um ihn sachgerecht einsetzen und die Dienstaufsicht ausüben zu können. Während also die per-

sonalverwaltende Stelle zu Recht danach fragt, wo der Beamte geboren ist, ob er einen Eingliederungs- oder Zulassungsschein besitzt, ob er Wehr-/Zivildienst geleistet hat, welche Berufstätigkeiten er früher einmal ausgeübt hat und wie sein laufbahnrechtlicher Werdegang im einzelnen war, gehen diese Informationen die Beschäftigungsbehörde nichts an, weil sie für die Verwendung des Beamten irrelevant sind. Diese über das erforderliche Maß hinausgehende Datenspeicherung und das Vorhalten dieser Angaben ist ein Verstoß gegen das Personalaktenrecht, den ich gegenüber dem Rektor der Fachhochschule beanstandete. Daß ich diesen Verstoß bei der Fachhochschule und der Polizeidirektion feststellen mußte, ist deswegen ärgerlich, weil genau dieselbe Praxis eines Staatlichen Schulamts schon 1994 beanstandet und im 15. Tätigkeitsbericht (LT-Drs. 11/5000) geschildert wurde.

- Die Personalkartei
  Die Polizeidirektion legte außerdem zu jedem Polizeibeamten eine Karteikarte an. Darin speicherte sie zusätzlich zu den im Personalbogen enthaltenen Angaben noch weitere, die sie zur Erfüllung ihrer Aufgabe, nämlich den Polizeibeamten optimal verwenden und führen zu können, nicht benötigt und die teilweise nicht einmal die Landespolizeidirektion als personalverwaltende Stelle erfragen dürfte. Alle unzulässigen Angaben aufzuzählen, würde zu weit führen. Deshalb nur so viel: Die Polizeidirektion interessiert sich nicht nur für Geburtsort, Schulbildung und den erlernten Beruf des Beamten, sondern auch für den Mädchennamen seiner Ehefrau, deren Geburtstag und -ort sowie die Namen und die Geburtsdaten der Kinder. Sie vermerkte zudem lückenlos, wann der Beamte in die Landespolizei eingetreten ist, ob und welche Berufstätigkeit als Beamter er vor Eintritt in die Landespolizei ausübte und wann er vereidigt, Beamter auf Probe und Beamter auf Lebenszeit wurde. All das sind ebenfalls Angaben, die für die Polizeidirektion ohne Bedeutung sind. Weil diese Karteikarte keine Eigenschöpfung der besuchten Polizeidirektion, sondern ein offenbar landesweit verwendeter Vordruck ist, gibt es für die Polizei noch viel zu tun, um datenschutzgerechte Zustände herzustellen.
- Akten zu umfangreich
  Die besuchte Fachhochschule sammelte freilich noch mehr Informationen über ihre Bediensteten. Weil sie die Entscheidung über die Berufung eines Professors durch das Wissenschaftsministerium ebenso vorbereitet wie die Bewerberauswahlentscheidung der sonstigen Beamten, bekam sie auch die entsprechenden Unterlagen von dem in Aussicht genommenen Bewerber. Dieser mußte insbesondere Geburts- und Heiratsurkunde, eine beglaubigte Kopie des Personalausweises oder Reisepasses, ein Führungszeugnis, eine

Erklärung über die wirtschaftlichen Verhältnisse, ein amtsärztliches Zeugnis, einen Nachweis der Wehr- oder Ersatzdienstzeit, eine Erklärung zum Wohnsitzwechsel, einen handgeschriebenen Lebenslauf und sein Reifezeugnis vorlegen. Diese Unterlagen nahm die Fachhochschule im Original oder in Kopie zur Personalnebenakte. Nach dem Personalaktenrecht gehören sie dagegen allein in die Personalgrundakte des Wissenschaftsministeriums. Zudem führt die Fachhochschule eine sog. Besoldungsakte. Sie dient der Aufbewahrung der Unterlagen, die bei der Gewährung finanzieller Leistungen wie beispielsweise Umzugskostenvergütung, Reisekosten oder Trennungsgeld entstehen. Bei der Durchsicht fanden sich darin aber auch Kopien von Erklärungen zum Ortszuschlag oder die persönlichen Verhältnisse, Lohnsteuerkarten, Kindergeldanträgen oder Heiratsurkunden, die der Beamte der Fachhochschule zur Weiterleitung an das Landesamt für Besoldung und Versorgung gegeben hat. Außerdem enthielt die Akte Versetzungsverfügungen und Planstelleneinweisungen. Die Fachhochschule darf all diese Unterlagen jedenfalls ohne Einwilligung des Beamten nicht in der Besoldungsakte aufbewahren, und Kopien von Versetzungsverfügungen und Planstelleneinweisungen haben allenfalls in der Personalnebenakte ihre Berechtigung. Daß die Fachhochschule mehr Unterlagen als erlaubt zu ihren Akten nahm, habe ich beanstandet. Eine Stellungnahme steht noch aus.

1.2 Quadranglierung von Personalakten

Personalakten sind so zu führen, daß der Betroffene sein Recht auf Einsicht in die vollständige Personalakte, also in die Grundakte und sämtliche Nebenakten, wahrnehmen kann. Deshalb sollten diese fortlaufend durchnumeriert sein. Zwar wird gegen eine Paginierung gerade von Personalakten mitunter eingewandt, bei Entfernung von Vorgängen entstünden sog. "sprechende Lücken". Trotzdem sollte jede Personalakte quadrangliert werden. Dafür spricht nämlich, daß so jederzeit einzelne Unterlagen schnell gefunden werden können und die Vollständigkeit der Personalakte nachgewiesen werden kann. Zudem sind auch die bei der Entfernung von Unterlagen entstehenden Lücken nicht mehr "sprechend", weil in wesentlich größerem Umfang als bisher nicht nur Unterlagen mit für den Bediensteten negativem Inhalt, sondern auch ihn nicht belastende Vorgänge nach bestimmten Fristen aus der Personalakte zu entfernen sind.

1.3 Datenlöschung - noch immer Stiefkind der Behörden

Die besuchte Fachhochschule besteht seit etwa 35 Jahren. Seit ihrer Gründung hat sie noch keine Personalnebenakten, Besoldungsakten oder Berufungsakten ausgesondert. Schied ein Professor oder Verwaltungsbeamter aus ihrem Dienst aus, legte sie nur die ihn betreffenden Akten in der Altregistratur im Keller ab.

Ein Platzproblem hat die Fachhochschule offenbar nicht. Bei dieser Praxis übersah sie freilich, daß Daten nicht nur im Computer, sondern auch in Akten gelöscht werden müssen. Gerade bei den Personalakten der Beamten sind - im Landesbeamtengesetz im einzelnen nachzulesen - für die Aussonderung genaue Fristen bestimmt, die es zu beachten gilt. Die Lagerkapazität kann keinesfalls ein Kriterium für die Aufbewahrungsdauer sein. Eine Beanstandung dieses Datenschutzverstoßes war die Folge.

Nicht in Ordnung war auch, wie die Polizeidirektion ihre sog. Krankheitsliste führte. Dazu verwendete sie einen Vordruck, in den sie für jeden Polizeibeamten gesondert eintrug, von wann bis wann dieser wie viele Tage krank war. Eine der eingesehenen Krankenlisten enthielt beispielsweise 13 Einträge, anhand derer die Polizeidirektion feststellen konnte, daß der betreffende Polizeibeamte seit seiner Aufnahme des Dienstes bei ihr erstmals 1980 und zuletzt 1996 und dazwischen weitere elfmal krank war - ein unhaltbarer Zustand. Krankheitsbedingte Fehlzeiten sind regelmäßig nur für den Zeitraum eines Jahres von Bedeutung. Danach sind sie unter Verschluß zu nehmen und nach Ablauf von drei Jahren auszusondern.

2. Die Überprüfung der Dienstfähigkeit

Ist ein Beamter gravierend in seiner Gesundheit beeinträchtigt, stellt sich für ihn und seine Dienststelle die Frage, ob er dauernd dienstunfähig und folglich in den Ruhestand zu versetzen ist. Damit der Dienstherr darüber befinden kann, braucht er regelmäßig ein amtsärztliches Gutachten des Gesundheitsamts. Wie dieses den Beamten zu begutachten und das amtsärztliche Zeugnis zu erstellen hat, ist seit 1995 in einer Verwaltungsvorschrift des Sozialministeriums detailliert und datenschutzgerecht geregelt. Unter anderem ist folgendes festgelegt: Benötigt der Amtsarzt für sein Zeugnis ein fachärztliches Gutachten, fragt er die auftraggebende Dienststelle, ob sie die Kosten hierfür übernimmt, läßt durch den Beamten den Amtsarzt und Facharzt wechselseitig von der Schweigepflicht entbinden und erteilt schließlich dem Facharzt den Auftrag. Das Fachgutachten arbeitet der Amtsarzt in sein Zeugnis ein und verwahrt es in seinen Akten, ohne daß es die auftraggebende Dienststelle zu Gesicht bekommt. Bei der Abfassung des amtsärztlichen Zeugnisses hat er darauf zu achten, daß Rückschlüsse auf den untersuchten Beamten durch Dritte nicht möglich sind. Grund hierfür ist, daß bei Beamten unter 55 Jahren das Finanzministerium eine anonymisierte Fertigung des Gutachtens erhält, weil es sein Einvernehmen zur Zurruhesetzung des Beamten erteilen muß. Auch der Dienststelle darf der Amtsarzt Einzelheiten über Anamnese und Befund nur mit Einwilligung des Beamten mitteilen, so-

weit dies für die von der Dienststelle zu treffende Entscheidung nach deren Ansicht oder nach Meinung des Amtsarztes notwendig ist.
Bei einem Lehrer spielte sich das Verfahren allerdings anders ab: Als der Amtsarzt dem Oberschulamt die Notwendigkeit eines neurologischen Fachgutachtens darlegte, beauftragte dieses selbst einen Fachgutachter. Der schickte sein Gutachten natürlich unmittelbar an seinen Auftraggeber, das Oberschulamt. Dadurch erfuhr die personalverwaltende Stelle des Lehrers nicht nur, wie der Fachgutachter dessen Dienstfähigkeit beurteilte, sondern eine Vielzahl von Angaben zu Anamnese und Befunderhebung, die sie zur Begründung der von ihr zu treffenden Personalentscheidung gar nicht wissen mußte. Kurz gesagt: Eine unnötige Beeinträchtigung des Persönlichkeitsrechts des Lehrers. Beanstanden konnte ich diese Vorgehensweise des Oberschulamts allerdings nicht, weil sie nicht gegen das Gesetz verstößt.
Nicht nur datenschutzunfreundlich, sondern rechtswidrig war dagegen, wie die Geschichte weiterging. Pflichtgemäß übersandte das Oberschulamt nämlich dem Finanzministerium eine Fertigung des Fachgutachtens, das es zuvor versuchte zu anonymisieren. Dieser Versuch mißlang, denn das Finanzministerium konnte schwarz auf weiß lesen, daß der Betroffene seit 1974 als Grundschullehrer tätig und seit 1976 in einem namentlich genannten Ort mit knapp über 3 000 Einwohnern angestellt ist. Unter diesen Umständen wäre es ihm leicht möglich gewesen herauszufinden, um wen es sich bei dem zur Ruhe zu setzenden Beamten handelt. Das Oberschulamt versprach, künftig bei der Zuziehung von Fachgutachtern nach den Bestimmungen der Verwaltungsvorschrift des Sozialministeriums vorzugehen und bei einer etwa dennoch notwendigen Anonymisierung von ärztlichen Unterlagen sorgfältiger zu Werke zu gehen.

3. Alte und neue Probleme mit dem polizeiärztlichen Dienst

Schon im letzten Jahr habe ich gravierende Datenschutzmängel in verschiedenen Bereichen des polizeiärztlichen Dienstes aufgezeigt. Beseitigt sind sie bis heute nicht. Vielmehr treten neue Schwachstellen zutage.

3.1 Die polizeiärztliche Rundumfürsorge

3.1.1 Was bisher (nicht) geschah

Im letzten Tätigkeitsbericht (LT-Drs. 12/750, S. 70 ff.) habe ich das unrühmliche Ergebnis eines Kontrollbesuchs beim polizeiärztlichen Dienst der Landespolizeidirektion Stuttgart II geschildert. Zur Erinnerung: Dem Polizeiarzt ist ein umfangreiches Aufgabenspektrum übertragen. Er stellt fest, ob ein Polizeibeamter dienstfähig ist, übt die Tätigkeit des Betriebsarztes einschließlich arbeitsmedizinischer Vorsorgeuntersuchungen aus und wirkt bei der Gewährung der Heilfürsorge mit, indem er

Krankenscheine, Rezepte und Krankenhausrechnungen prüft und über Anträge auf genehmigungspflichtige Heilfürsorgeleistungen wie beispielsweise Kuren entscheidet. Fast alle dabei anfallenden Unterlagen sammelt er in einer sog. Krankenakte, auf die er sich bei seiner gesamten Tätigkeit stützt. Im Alltag kann sich ein Polizeibeamter folglich nicht einer ärztlichen Behandlung unterziehen, ohne damit rechnen zu müssen, daß der Polizeiarzt kurze Zeit später seine Dienstfähigkeit in Frage stellt. Diese Praxis, die bei allen Landespolizeidirektionen und bei der Bereitschaftspolizei im wesentlichen dieselbe ist, stellt den Polizeibeamten nicht nur schlechter als andere Beamte und alle Arbeitnehmer innerhalb und außerhalb des öffentlichen Dienstes, sondern steht seit 1. Jan. 1987 (!) in Widerspruch mit der Rechtslage. Seitdem ist nämlich aus gutem Grund durch Rechtsvorschrift bestimmt, daß

- Unterlagen über die Heilfürsorge grundsätzlich nicht für andere Zwecke verwendet werden dürfen und
- Heilfürsorgeakten getrennt von anderen Unterlagen zu führen sind sowie
- Heilfürsorgeunterlagen drei Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, zu vernichten sind.

Bei der Bereitschaftspolizei wirkt sich diese von mir im August 1996 beanstandete Mißachtung der Rechtslage besonders gravierend aus, weil hier der Polizeischüler verpflichtet ist, Krankheiten und Verletzungen vom selben Polizeiarzt behandeln zu lassen, der nach Abschluß der laufbahnrechtlichen Probezeit oder vor der Berufung in das Beamtenverhältnis auf Lebenszeit darüber zu befinden hat, ob er polizeidienstfähig ist.

3.1.2 Wie es (nicht) weiterging

Im Dezember des letzten Jahres räumte auch das Innenministerium, das bis dahin nicht zu einer Stellungnahme zu meiner Beanstandung zu bewegen gewesen war, nach einem ersten Gespräch mit meinem Amt ein, daß die Wahrnehmung von Aufgaben in der Heilfürsorge und im betriebs- und polizeiamtsärztlichen Dienst durch den Polizeiarzt in Personalunion rechtswidrig ist. Die Trennung der Heilfürsorgeakten von den Personalakten sei schon vor über einem Jahr eingeleitet worden. Zwei weitere Monate waren daraufhin ohne konkrete Maßnahmen verstrichen, als das Innenministerium erneut um eine Besprechung bat, diesmal mit dem obersten Polizeiarzt des Landes. Auch dabei bestand

Übereinstimmung über die Rechtswidrigkeit der polizeiärztlichen Rundumfürsorge. In der Folge "vereinbarte" der oberste Polizeiarzt mit dem Leiter des ärztlichen Dienstes der Bereitschaftspolizeidirektion, daß im Bereich der Bereitschaftspolizei ärztliche Behandlung und Dienstuntauglichkeitsuntersuchung zu trennen sind. Die übrigen Polizeiärzte im Land ließ das Innenministerium die bis dahin geübte Praxis fortsetzen. So ging ein weiteres halbes Jahr ins Land, in dem sich nichts änderte. Anfang August wandte ich mich deswegen an den Herrn Innenminister und bat ihn zu veranlassen, daß die längst überfällige organisatorische und personelle Trennung erfolgt. Ende Oktober, als ich schon gar nicht mehr mit einer Antwort rechnete, wurde meine Hoffnung, nun endlich zu erfahren, wann und in welcher Weise diese Trennung erfolgt, erneut enttäuscht. Der Herr Innenminister teilte mir, nachdem er sich für die verspätete Beantwortung meines Schreibens entschuldigt hatte, nämlich nur mit, daß "keine grundsätzlichen Einwendungen" mehr gegen die Trennung bestünden, nachdem die Angelegenheit auch in zwei Polizeichefbesprechungen intensiv diskutiert worden sei. Eine bemerkenswerte Aussage, wie ich meine, weil ja eine nach Art. 20 GG an Gesetz und Recht gebundene Verwaltung die Beachtung von Rechtsvorschriften wohl kaum davon abhängig machen kann, ob diese ihr gefallen oder nicht. Genau davon geht aber offensichtlich die Polizeiverwaltung des Landes aus. Anders kann ich das Hickhack um die vom geltenden Recht zwingend geforderte Trennung nicht mehr verstehen. Ich würde es deshalb begrüßen, wenn sich der Landtag dieser Frage annehmen und dafür sorgen würde, daß den Polizeibeamten des Landes endlich der Schutz gewährt wird, der ihnen zusteht.

3.2 Polizeidiensttauglichkeit

Durch die Praxis des ärztlichen Dienstes der Bereitschaftspolizeidirektion, von allen Bewerbern für den Polizeidienst des Landes Krankenkassenauskünfte zu verlangen, aus denen sämtliche dort bekannten Arbeitsunfähigkeitszeiten und Krankenhausaufenthalte (jeweils mit Diagnosen) sowie Versicherungszeiten ersichtlich sein müssen (vgl. S. 36 des 13. Tätigkeitsberichts 1992 [LT-Drs. 11/1060] und S. 70 des letzten Tätigkeitsberichts [LT-Drs. 12/750]), trat ganz automatisch der Bereich der Bewerberauswahluntersuchung ins Blickfeld. Deshalb nahm mein Amt die Polizeidienstvorschrift "Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit" (PDV 300) und den hierzu ergangenen Einführungserlaß des Innenministeriums unter die Lupe. Dort ist im einzelnen beschrieben, was der Polizeiarzt bei seiner Beurteilung der Polizeidiensttauglichkeit eines Polizeibeamten oder Bewerbers für den Polizeidienst

zu beachten, welche Untersuchungen er vorzunehmen und welche Angaben der (künftige) Polizeibeamte hierbei zu machen hat. Für einen Datenschützer enthält die PDV 300 einige Stolpersteine. Beispielsweise stellen sich folgende Fragen:

- Wozu benötigt der Polizeiarzt für seine Untersuchung Bewerbungsunterlagen wie Lebenslauf und Zeugnisse?
- Aus welchen Gründen schließen welche Tätowierungen die Einstellung des Bewerbers aus?
- Warum schließt bei weiblichen Bewerbern das Vorliegen einer Schwangerschaft die ärztliche Untersuchung aus, und welche Folgerungen sind damit für den Arzt und die für die Einstellungen zuständige Stelle verbunden?
- Welche Schlußfolgerungen zieht der Polizeiarzt aus frühkindlichem Bettnässen und häufigem Wechsel von Freunden und Vorgesetzten des Bewerbers?
- Kann es gerechtfertigt sein, vom Bewerber eine pauschale Erklärung zu verlangen, daß für die Beurteilung benötigte ärztliche Befunde und Unterlagen beschafft und dem Polizeiarzt zur Verfügung gestellt werden können?
- Was passiert mit dem Einstellungsgutachten, wenn der Bewerber später gar nicht eingestellt wird?

Diese und weitere Fragen stellten wir Anfang März dem Innenministerium. Eine Reaktion erfolgte nicht. Mitte Mai bat mein Amt erneut darum, die gestellten Fragen zu beantworten - wieder keine Antwort.
Auf meine Anfang August an den Herrn Innenminister gerichtete Bitte, er möge doch dafür sorgen, daß seine Polizeiabteilung mir die gewünschten Auskünfte rasch erteilt, geschah immer noch nichts. Folglich blieb mir nichts anderes übrig, als diese beharrliche Weigerung des Innenministeriums, mir pflichtgemäß Auskunft zu geben, förmlich zu beanstanden. Erfolg: Fast keiner. Nach sechs Wochen teilte mir der Herr Innenminister folgendes mit:

> "Die Leitenden Polizeiärzte des Bundes und der Länder haben in ihrer Frühjahrstagung im Mai 1997 hinsichtlich der Überarbeitung der Polizeidienstvorschrift 'PDV 300' eine Arbeitsgruppe gebildet, deren Ergebnis wegen der Komplexität der Fragen noch nicht vorliegt. Die Polizeiärzte beabsichtigen, den Ergebnisbericht 1998 dem Arbeitskreis II der Innenministerkonferenz vorzulegen. Über den weiteren Fortgang wird Sie mein Haus gleichfalls unterrichten."

Schön und gut, nur ist damit keine unserer Fragen beantwortet und die Antworten - z.B. wozu der Polizeiarzt bisher diese oder jene Angaben wissen will - können ja wohl kaum von Überlegungen der Leitenden Polizeiärzte für die Zukunft abhängen. Einen Tag später beantwortete das Innenministerium dann

doch noch einen ganz kleinen Teil der gestellten Fragen, nämlich wie der Polizeiarzt mit den Einstellungsgutachten umgeht. Der Rest ist nach wie vor Schweigen.

4. Personalunion - kein Rechtfertigungsgrund

Überrascht und erbost war eine Assessorin des Lehramts über das, was ihr der CDU-Landesvorsitzende, Herr Ministerpräsident Teufel, auf ihre Parteiaustrittserklärung antwortete. In dessen Brief konnte sie nämlich folgendes lesen:

> "Sie selbst haben die Fächer Französisch und Latein studiert und im Staatsexamen die Leistungsziffer ... erreicht. Im Fach Französisch wurde in diesem Jahr kein Bewerber übernommen. Im Fach Latein kam es zu 16 Neueinstellungen. Sie selbst stehen nach Ihrer Leistungsziffer auf Rangplatz ..., also weit entfernt von der Einstellungsgrenze."

Wie kam es dazu? Die Assessorin, nennen wir sie Frau Z., wollte nicht sang- und klanglos aus der Partei austreten, sondern wandte sich über die Geschäftsstelle des Kreisverbands Stuttgart der CDU an deren Landesvorsitzenden, um ihren Schritt zu erläutern. Unter anderem begründete sie, ohne dabei näher auf ihr persönliches Schicksal einzugehen, ihren Austritt damit, daß die CDU vor der Landtagswahl Neueinstellungen im Schulbereich zugesagt, dieses Versprechen aber hinterher Lügen gestraft habe.

Das Persönliche Büro des Herrn Ministerpräsidenten, an das die CDU-Kreisgeschäftsstelle ihr Schreiben weiterleitete, ließ sich vom Kultusministerium die Examensergebnisse von Frau Z. geben, die in das Antwortschreiben des CDU-Landesvorsitzenden Eingang fanden. So kann es natürlich nicht gehen. Soweit das Persönliche Büro des Herrn Ministerpräsidenten Parteiangelegenheiten bearbeitet, darf es hierzu nicht auf von der Landesverwaltung gesammelte Bürgerdaten zurückgreifen. Zu diesem Vorgang befragt, stellte dies auch das Staatsministerium nicht in Abrede. Nur meinte es, Frau Z. habe doch den Herrn Ministerpräsidenten nicht nur als Landesvorsitzenden der CDU, sondern auch als Regierungschef angeschrieben und überhaupt dürfe doch unterstellt werden, "daß derjenige, der über eine bestimmte Verwaltungsentscheidung Klage bei dem Herrn Ministerpräsidenten führt, damit einverstanden ist, daß sich der Herr Ministerpräsident bei den zuständigen Behörden sachkundig macht." Es übersah dabei allerdings, daß Frau Z. beim Herrn Ministerpräsidenten gerade nicht über eine Verwaltungsentscheidung geklagt, sondern ihre Nichtberücksichtigung bei der Lehrereinstellung lediglich als Beleg und Beispiel dafür angeführt hatte, daß ihrer Meinung nach die Zusage der Partei, genügend Lehrerstellen zu schaffen, nicht eingehalten worden sei. Das sah offenbar auch das Persönliche Büro so, indem es die Prüfungsergebnisse von Frau Z. nicht für eine Antwort des Herrn Ministerpräsidenten als Regierungschef verwendete, sondern der Partei zugänglich machte. Daß nämlich Frau Z. die Antwort auf ihr Schreiben auf einem Brief

mit dem Kopfbogen "CDU Baden-Württemberg - Der Landesvorsitzende" erhielt, war konsequent und keineswegs - wie das Staatsministerium auf meine Beanstandung der Datenschutzverstöße meinte - eine Verwechslung.

2. Abschnitt: Wirtschaft

1. Das Korruptionsregister

   Auch die öffentliche Verwaltung ist vor Korruption nicht gefeit. Spektakuläre Einzelfälle, die Schlagzeilen gemacht haben, belegen dies. Deshalb ist seit langem klar, daß dem ein Riegel vorgeschoben werden muß. Rezepte, wie dies am besten zu bewerkstelligen ist, gibt es viele. Eines davon ist die Forderung nach der Einrichtung von Korruptionsregistern, um Unternehmen, die mit Preisabsprachen, Bestechungsgeldern und anderen unlauteren Mitteln bei der Vergabe öffentlicher Aufträge agieren, das Handwerk zu legen. Weil man sich an fünf Fingern abzählen kann, daß ein solches Register von erheblicher datenschutzrechtlicher Relevanz ist, schalteten wir uns schon zu Beginn des Jahres 1996 ein. Die Kernfrage war von Anfang an: Reichen für die Errichtung eines Korruptionsregisters die vorhandenen Regelungen des Landesdatenschutzgesetzes aus, oder muß der Gesetzgeber aktiv werden? Das Innenministerium hielt sich bedeckt. Im Herbst 1996, als das Kabinett die Einführung eines Korruptionsregisters beschlossen und es sich an die Umsetzung des Kabinettsbeschlusses gemacht hatte, hieß es noch immer, Ausgestaltung und Rechtsgrundlage des Korruptionsregisters müßten zunächst noch geprüft werden. Im Frühjahr 1997 präsentierte es uns dann den Entwurf einer Verwaltungsvorschrift der Landesregierung und des Innenministeriums zur Verhütung unrechtmäßiger und unlauterer Einwirkungen auf das Verwaltungshandeln und zur Verfolgung damit zusammenhängender "Straf- und Dienstvergehen" und ließ uns zu der darin vorgesehenen Errichtung eines Korruptionsregisters ohne nähere Begründung wissen, es halte eine spezialgesetzliche Regelung zur Einrichtung des Registers nicht für erforderlich. Diese Auffassung kann ich nicht teilen. Weshalb dies so ist, habe ich dem Innenministerium bereits im Juni und Juli 1997 eingehend dargelegt. Der Herr Innenminister meinte bei der Beratung des Entwurfs der Verwaltungsvorschrift im Innenausschuß des Landtags dazu nur, eine ausführliche Klärung dieser Fragen mit meinem Amt hätte eine Verzögerung der Verwaltungsvorschrift zur Folge, zu dieser sei er aber nicht bereit. Am 1. Okt. 1997 hat das Innenministerium die Verwaltungsvorschrift in Kraft gesetzt. Dies habe ich beanstandet. Die wesentlichen Gründe dafür sind auf einen kurzen Nenner gebracht folgende:
   Alle Behörden und öffentlichen Stellen des Landes und sämtliche kommunalen Auftraggeber (Vergabestellen) müssen der Verwaltungsvorschrift zufolge dem Landes-

gewerbeamt, das das Korruptionsregister führt, solche Bewerber melden, die sie in einem Verfahren zur Vergabe von Bau-, Liefer- oder Dienstleistungen wegen schwerer Verfehlungen ausgeschlossen haben. Als solche Verfehlungen gelten beispielsweise Betrügereien im Geschäftsverkehr, wettbewerbsbeschränkende Absprachen bei Ausschreibungen, Bestechung oder Vorteilsgewährung. Gemeldete Bewerber oder Bieter können die Löschung der Meldung verlangen, wenn sich die Beweislage nachträglich ändert und Zweifel am Vorliegen einer schweren Verfehlung entstehen oder wenn beispielsweise kein oder nur ein geringer Schaden entstanden ist oder wenn sie durch geeignete organisatorische oder personelle Maßnahmen Vorsorge gegen die Wiederholung schwerer Verfehlungen getroffen haben. Ansonsten bleibt jede Meldung mindestens zwei Jahre, mitunter auch länger im Korruptionsregister gespeichert. Bevor eine Vergabestelle einem Anbieter den Zuschlag geben will, muß sie bei Aufträgen mit einem Volumen von über 100 000 DM den Anbieter im Korruptionsregister abchecken; ist das Auftragsvolumen niedriger, steht es in ihrem Ermessen, ob sie dies tun will.

Keine Frage: Nicht bei jeder Meldung zum Korruptionsregister ist der Datenschutz tangiert. Bei Aktiengesellschaften beispielsweise ist er sowieso nicht betroffen. Anders ist es dagegen, wenn es zum einen um Einzelkaufleute, Handelsgesellschaften oder juristische Personen geht, bei denen die sie tragenden Personen im Rechtsverkehr im Vordergrund stehen, und zum anderen, wenn aus der gemeldeten Verfehlung auf den dafür Verantwortlichen geschlossen werden kann. Dann steht deren Grundrecht auf Datenschutz (Art. 1 Abs. 1 i.V. mit Art. 2 Abs. 1 GG) zur Debatte. Eingriffe in dieses Grundrecht dürfen aber nach der seit dem Volkszählungsurteil von 1983 ständigen Rechtsprechung des Bundesverfassungsgerichts - von den übrigen Voraussetzungen einmal abgesehen - nur aufgrund einer klaren gesetzlichen Grundlage erfolgen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben. Eine solche gesetzliche Grundlage für das Korruptionsregister gibt es jedoch nicht. Insbesondere läßt es sich nicht auf das Landesdatenschutzgesetz stützen. Denn dieses Gesetz regelt nur die Verarbeitung personenbezogener Daten im Einzelfall. Für die Einrichtung eines zentral geführten Registers wie das Korruptionsregister, in dem von zahlreichen Stellen mitgeteilte Informationen über schwere Verfehlungen in einem Vergabeverfahren gespeichert werden und bei dem eine Vielzahl von Stellen nach solchen Informationen nachfragen können, ist das Landesdatenschutzgesetz dagegen nicht gemacht. Es enthält für ein solches zentrales Register gar keine Regelungen. Deshalb nutzen alle Hilfskonstruktionen des Innenministeriums nichts:

- Das Innenministerium geht offenbar davon aus, daß eine Anfrage einer Vergabestelle vor der Vergabe des Zuschlags sich eigentlich nicht an das Korruptionsregister, sondern praktisch an alle übrigen Vergabestellen im Land richte und daß um-

gekehrt Adressat einer Mitteilung einer Vergabestelle über eine schwere Verfehlung nicht das Korruptionsregister, sondern alle anderen Vergabestellen seien. Es handele sich deshalb um Datenerhebungen und Datenübermittlungen. Diese Annahme geht jedoch - ganz abgesehen davon, daß sie mit den tatsächlichen Abläufen nun wirklich nichts zu tun hat - von unzutreffenden Prämissen aus. Denn solche praktisch "ins Blaue hinein" erfolgenden Datenerhebungen und Datenübermittlungen der Vergabestellen wären von den einschlägigen Vorschriften des Landesdatenschutzgesetzes (§§ 11, 13 LDSG) gerade nicht gedeckt.

- Der dazu vom Innenministerium gegebene Hinweis auf das Rechtsinstitut der Datenverarbeitung im Auftrag geht fehl. Würde nämlich das Landesgewerbeamt tatsächlich das Korruptionsregister im Auftrag der Vergabestellen betreiben, bedürfte es nach § 7 LDSG schriftlicher Aufträge zwischen diesen und dem Landesgewerbeamt. Darin wären vor allem Gegenstand und Umfang der Datenverarbeitung im Korruptionsregister und die hierfür notwendigen technischen und organisatorischen Maßnahmen festzulegen. Solche Aufträge zwischen Vergabestellen und Landesgewerbeamt gibt es aber nicht. Auch hilft der Weg über § 7 Abs. 2 Satz 4 LDSG nicht weiter. Nach dieser Vorschrift können solche Aufträge zwar auch durch die obersten Fachaufsichtsbehörden mit Wirkung für die ihrer Aufsicht unterliegenden Stellen des Landes erteilt werden. Außer dem Innenministerium ist aber kein anderes Ministerium am Erlaß der Verwaltungsvorschrift beteiligt gewesen - nur sie sind aber nach § 22 des Landesverwaltungsgesetzes oberste Fachaufsichtsbehörden. Hinzu kommt, daß die vielen Vergabestellen der Kommunen von vornherein nicht der Fachaufsicht des Landes unterstehen.

Das Innenministerium half meiner Beanstandung nicht ab. Seit 1. Okt. 1997 gibt es ein zentrales Korruptionsregister beim Landesgewerbeamt, eine tragfähige gesetzliche Grundlage dafür jedoch nicht, jedenfalls nicht, soweit darin personenbezogene Daten gespeichert werden.

2. So nicht

Ziemlich forsch agieren zwei der drei Steuerberaterkammern in Baden-Württemberg. Sie geben in den Kammermitteilungen, ihrer Mitgliederzeitschrift, Namen und Anschriften derjenigen bekannt, deren unerlaubte Hilfe in Steuersachen sanktioniert wurde. Nach dem Grund hierfür befragt, meinten sie nur, die Veröffentlichung der Delinquenten sei allein schon durch ihre Aufgabe, die beruflichen Belange der Gesamtheit der Mitglieder zu wahren, gerechtfertigt und auch "wegen der Wiederholungsgefahr angezeigt". Hier irren die beiden Kammern. Die Bekanntgabe der betroffenen Personen wäre nur erlaubt, wenn sie erforderlich wäre, mit anderen Worten die Kammern ihre Aufgaben ohne die Veröffentlichung überhaupt nicht oder nur mangelhaft erfüllen könnten. Daran fehlt es aber, denn selbst wenn es Kammeraufgabe ist,

Verstöße gegen das Steuerberatungsgesetz aufzuspüren, was keineswegs einhellige Meinung ist, sind sie dabei nicht darauf angewiesen, daß alle ihre Mitglieder von Verfehlungen bestimmter Personen wissen. Halten die Kammern eine besondere Beobachtung der aufgefallenen "Steuerhelfer" für geboten, können sie selbst das Nötige tun. Daß dies ausreicht, zeigt sich schon daran, daß andere Kammern solche Veröffentlichungen nicht vornehmen. Zudem ist die Veröffentlichungspraxis unverhältnismäßig, weil sehr viele Personen und keinesfalls nur Kammermitglieder Kenntnis von den verhängten Sanktionen erhalten und die Veröffentlichung damit eine ganz erhebliche Prangerwirkung entfaltet. Weil die beiden Kammern trotz meiner Erläuterung der Rechtslage an ihrer rechtswidrigen Praxis festhalten wollen, mußte ich diese beanstanden. Ich hoffe, daß sie doch noch einsichtig werden.
Umsichtig verhielt sich dagegen eine Handwerkskammer, die ähnliches vor hatte. Sie wollte "Schwarzarbeitsünder" in der Deutschen Handwerkszeitung bekanntgeben und damit die Schwarzarbeit bekämpfen. Ganz wohl war ihr dabei offenbar nicht, denn sie bat mich, eventuelle datenschutzrechtliche Bedenken mitzuteilen. So konnte ich sie schon vorab von meiner datenschutzrechtlichen Beurteilung unterrichten, worauf die Kammer von ihrem Vorhaben Abstand nahm.

3. Abschnitt: Finanzverwaltung

1. Wer war sonst noch dabei?

   Ein Geschäftsmann besuchte eine Fortbildungsveranstaltung. Tagungsort: Eine Ferieninsel. Die finanziellen Aufwendungen dafür wollte er als Betriebsausgaben von der Steuer absetzen. Doch die Belege, die deren Höhe nachweisen, genügten dem zuständigen Finanzamt nicht. Es machte die Anerkennung von der Vorlage eines Verzeichnisses mit den Namen der übrigen Veranstaltungsteilnehmer abhängig.
   Außer Frage steht: Wer eine Steuervergünstigung begehrt, muß dies beim Finanzamt beantragen und dazu Unterlagen zur Glaubhaftmachung vorlegen. Diese müssen aber zu diesem Zweck auch geeignet und erforderlich sein. Etwas Sinnloses darf das Finanzamt nicht verlangen, schon gar nicht, wenn es auf diesem Wege eine Reihe von Informationen über andere Bürger erhalten würde, die es zur Bearbeitung des konkreten Falles gar nicht benötigt.
   Was hatte das Finanzamt zu seiner Aufklärungsmaßnahme bewogen? Offenbar die Befürchtung, daß sog. Fortbildungsreisen selbst dann als solche abgerechnet werden könnten, wenn sie in Wahrheit "getarnte" Vergnügungsreisen waren. Und Aufklärung in diesem Punkt liegt im Interesse aller, aber nur mit rechtlich zulässigen, insbesondere aber auch tauglichen Mitteln! Daran aber haperte es in unserem Fall.

Zum einen sind Seminarteilnehmer oftmals gar nicht in der Lage, ein Teilnehmerverzeichnis beim Finanzamt vorzulegen, weil sie über ein solches nicht verfügen und ihnen auch kein Anspruch gegen den Veranstalter zusteht, eine Teilnehmerliste nachträglich zu erhalten. Zum anderen ist ihre Vorlage bei der Steuerbehörde ungeeignet, Zweifel am Fortbildungscharakter der Tagung auszuräumen, weil eine solche Liste noch lange nicht sagt, ob die Mitreisenden fortbildungswillig oder "branchenfremd" waren. Dem Namen allein sieht man das Motiv für die Reise nicht an. Aber selbst wenn man auf diesem Wege in Erfahrung bringen würde, daß die Gruppe aus beiden Arten von Reiseteilnehmern zusammengesetzt war, würde dies noch keinen Schluß in die eine oder andere Richtung zulassen. So kann sich ein Teil der Mitreisenden - etwa Familienangehörige - durchaus ausschließlich für das Rahmenprogramm interessieren, was sicher nicht eine steuerliche Anerkennung der Aufwendungen dieser Personen rechtfertigt, während der Steuerpflichtige selbst sich der Fortbildung widmet. Viel sachdienlicher wäre es deswegen, wenn sich das Finanzamt in solchen Fällen ein Veranstaltungsprogramm und ein Verzeichnis der eingesetzten Dozenten vorlegen ließe. Daraus läßt sich der wahre Charakter der Veranstaltung am ehesten entnehmen.
Nachdem auch die Oberfinanzdirektion Stuttgart die Forderung des Finanzamts verteidigte, beanstandete ich die unzulässige Datenerhebung gegenüber dem Finanzministerium, zumal Steuerverwaltungen anderer Länder in solchen Fällen davon absehen, die Vorlage von Teilnehmerverzeichnissen zu verlangen. Das Ministerium sieht die Dinge jedoch anders und will aus mich nicht überzeugenden Gründen die bisherige Praxis beibehalten.

2. Außenprüfung von Arztpraxen

Weil von Ärzten immer wieder die Frage an mich herangetragen wurde, ob die Prüfbeamten des Finanzamts bei Außenprüfungen verlangen können, daß ihnen trotz des Ärzten nach § 102 der Abgabenordnung (AO) zustehenden Auskunftsverweigerungsrechts Einsicht in Patientenunterlagen wie beispielsweise Durchschriften der Rechnungen an Privatpatienten gewährt wird, wandte ich mich damit an das Finanzministerium. In einer ersten Antwort vertrat dieses unter Berufung auf eine Entscheidung des Bundesfinanzhofs aus dem Jahr 1957 folgende Auffassung: Das Finanzamt könne, wenn es berechtigte Zweifel an der Ordnungsmäßigkeit der Aufzeichnungen des Arztes habe, diesem aufgeben, "in geeigneter Form Auszüge und Zusammenstellungen über die einzelnen Besuche und sonstigen Leistungen aus der Patientenkartei mit Namensangabe zu fertigen, welche sich auf die finanziellen Beziehungen beschränken und die das Auskunftsverweigerungsrecht begründende Tatsachen nicht enthalten". Im auch für Normalbürger zu verstehenden Klartext heißt das: Das Finanzamt kann Einsicht in Unterlagen eines niedergelassenen Arztes verlangen, aus

denen die einzelnen Besuche oder sonstigen Leistungen, die dafür in Rechnung gestellten Beträge sowie Name und Anschrift der Patienten ersichtlich sind. Insoweit steht dem Arzt kein Auskunftsverweigerungsrecht zu.
Diese Auffassung kann ich nicht teilen, denn das Auskunftsverweigerungsrecht der Ärzte nach § 102 AO soll es diesen ermöglichen, ihrer ihnen durch die ärztliche Berufsordnung und § 203 Abs. 1 Nr. 1 StGB auferlegten Schweigepflicht auch gegenüber den Finanzbehörden gerecht zu werden. Unter die ärztliche Schweigepflicht fallen aber alle dem Arzt in Ausübung seines Berufs bekannt gewordenen Daten, die auf konkrete Erkenntnisse über den Gesundheitszustand einer Person schließen lassen. Dazu gehört nach einer gefestigten neueren Rechtsprechung auch der Name des Patienten, der den Arzt zur Behandlung aufgesucht hat. Denn schon der Umstand, daß jemand einen Arzt aufsucht, läßt Rückschlüsse auf seinen Gesundheitszustand zu. Erst recht gilt dies, wenn es sich dabei um einen auf eine Behandlung bestimmter Erkrankungen spezialisierten Arzt (Facharzt) handelt. Ich bat deshalb das Finanzministerium darum, seine bisherige Haltung nochmals zu überdenken und mitzuteilen, ob nicht auch anonymisierte Unterlagen für die Durchführung von Außenprüfungen ausreichen. Für das Finanzministerium war dies wiederum Anlaß, die strittige Frage den Referatsleitern Abgabenordnung des Bundes und der Länder vorzutragen. Das Ergebnis der Beratung dieses Gremiums war alles andere als überzeugend. Die Referatsleiter räumen zwar ein, daß Name und Anschrift eines Patienten grundsätzlich unter die ärztliche Schweigepflicht fallen, ziehen daraus aber nicht die gebotene Konsequenz, sondern meinen gleichwohl, das Zeugnisverweigerungsrecht der Ärzte beziehe sich nicht auf Name und Anschrift der Patienten. Dies ergäbe sich aus einem Vergleich der verschiedenen in § 102 AO getroffenen Regelungen zum Schutz bestimmter Berufsgeheimnisse. Sie halten deshalb die Einsichtnahme in ärztliche Unterlagen, die den Namen des Patienten enthalten, für zulässig, soweit sich die Unterlagen auf die Wiedergabe der finanziellen Beziehungen zwischen Arzt und Patienten beschränken. Soweit dagegen aus den Unterlagen Diagnosen und Behandlungsmethoden des Arztes erkennbar seien, sei den Außenprüfern die Einsichtnahme verwehrt, es sei denn, die betreffenden Patienten würden darin einwilligen oder die Unterlagen anonymisiert werden.
Das Finanzministerium sieht sich durch das Ergebnis der Beratung der Referatsleiter Abgabenordnung des Bundes und der Länder bestätigt und bleibt bei seiner bisherigen Auffassung. Ich kann dies nur bedauern, zumal es, obwohl danach befragt, bisher nicht plausibel dargetan hat, weshalb eine wirksame Kontrolle nicht auch durch Einsichtnahme in anonymisierte Unterlagen möglich sein soll.

3. Die Mitwirkung auf Raten

Anfang Februar 1997 wurde mir bekannt, daß das Finanzamt Stuttgart II gegen einen Arzt einen Durchsuchungs- und Beschlagnahmebeschluß erwirkt, die Praxis wegen des Verdachts der Steuerhinterziehung durchsucht und Patientenunterlagen sichergestellt hatte. Daraufhin bat ich das Finanzamt um eine Stellungnahme und um die Übersendung des Durchsuchungs- und Beschlagnahmebeschlusses des Amtsgerichts. Die Stellungnahme ging knapp einen Monat später bei uns ein, nicht aber der Durchsuchungs- und Beschlagnahmebeschluß. Der Bitte, ihn vorzulegen, könne nicht entsprochen werden, da dieser eine gerichtliche Entscheidung darstelle, die nicht der Kontrolle des Landesbeauftragten für den Datenschutz unterliege, bedeutete mir das Finanzamt. Letzteres ist sicher richtig, berechtigte das Finanzamt aber noch lange nicht dazu, den Beschluß zurückzuhalten. Ich bat deshalb, das Versäumte nachzuholen, da dieser Beschluß benötigt werde, um das Vorgehen des Finanzamts und nicht das des Gerichts zu überprüfen. Damit hätte es eigentlich genug sein müssen. Aber weit gefehlt: Das Finanzamt schickte uns daraufhin zwar den Durchsuchungs- und Beschlagnahmebeschluß, aber nur in "gereinigter" Form: "Den Namen des Beschuldigten und die Gründe haben wir wegen § 30 Abgabenordnung geschwärzt." Nun ist es zwar grundsätzlich lobenswert, daß das Finanzamt so großen Wert auf die Beachtung des in § 30 AO geregelten Steuergeheimnisses legt, nur, im konkreten Fall war die Berufung darauf völlig deplaziert. Denn nach § 24 Abs. 2 Satz 1 und Abs. 6 BDSG i.V. mit § 30 Abs. 4 Nr. 2 AO kann das Steuergeheimnis Datenschutzkontrollen nicht entgegengehalten werden. Darauf hat das Finanzministerium die Finanzämter schon vor Jahren hingewiesen. Also forderte ich das Finanzamt unter Hinweis auf diese Rechtslage mit Schreiben vom 30. April 1997 auf, den kompletten Beschluß vorzulegen. Aber auch diese Aufforderung zeitigte noch keinen Erfolg. Jetzt legte das Finanzamt den Fall der Oberfinanzdirektion zur Entscheidung vor, und dort ließ man sich Zeit. Nachdem insgesamt sechs Monate seit meiner ersten Anfrage beim Finanzamt Stuttgart II vergangen waren und mir der Durchsuchungs- und Beschlagnahmebeschluß des Amtsgerichts immer noch nicht vorlag, sah ich mich veranlaßt, diese offenkundige Verletzung der in § 25 Abs. 1 LDSG festgelegten Unterstützungspflicht durch das Finanzamt Stuttgart II zu beanstanden. Daraufhin ging dann alles sehr schnell: Ich erhielt den vollständigen Beschluß des Amtsgerichts, und das Finanzministerium entschuldigte sich für die fehlerhafte Rechtsanwendung durch das Finanzamt Stuttgart II.

4. Die Stillegung des Kraftfahrzeugs eines gewissenhaften Steuerzahlers

Ziemlich verärgert wandte sich ein Bürger an mein Amt, weil ihm seine Kraftfahrzeugzulassungsstelle die zwangsweise Stillegung seines Autos wegen angeblich nicht bezahlter Kraftfahrzeugsteuer angedroht hatte und dies, obwohl er doch dem zuständigen Finanzamt einen Lastschriftauftrag zur Einziehung dieser Steuer erteilt

hatte. Ein unverzüglich vorgenommener Kontrollbesuch bei der Zulassungsstelle ergab, daß das Finanzamt dort in Wirklichkeit die Stillegung des Fahrzeugs eines ganz anderen, tatsächlich säumigen Fahrzeughalters beantragt hatte. Zum Verhängnis war dem Petenten der Umstand geworden, daß sein Fahrzeug ein ähnlich lautendes Kennzeichen hatte und der Zulassungsstelle ein Erfassungsfehler unterlaufen war. Solche können zwar vorkommen, doch hätte die Zulassungsstelle den Fehlgriff in unserem Fall rechtzeitig erkennen können, wenn sie die nötige Sorgfalt hätte obwalten lassen. Ihr Datenverarbeitungssystem ist nämlich so angelegt, daß, wenn das Kraftfahrzeugkennzeichen eingegeben wird, automatisch der Name des Halters auf dem Bildschirm erscheint. Ein einfacher Vergleich der vom Finanzamt genannten und der von der Zulassungsstelle aufgerufenen Personalien hätte den Eingabefehler offenbar werden lassen und alle unangenehmen Weiterungen verhindert. Statt dessen nahm die Zulassungsstelle sogar noch einen Ausdruck der Halterdaten des Petenten in die Stillegungsakte des eigentlichen Steuerschuldners. Die Aktivitäten meines Amts führten zu einer umgehenden Entschuldigung der Zulassungsstelle bei dem Petenten und einer Bereinigung der Akten.

4. Abschnitt: Hochschulen und Schulen

1. Die Studentenwohnheime der Studentenwerke

Die Studentenwerke haben unter anderem die Aufgabe, Studentenwohnheime zu führen und darin insbesondere weniger betuchte Studenten aufzunehmen. Klar, daß sie dazu personenbezogene Daten von Bewerbern und Bewohnern verarbeiten müssen. Wie Kontrollbesuche bei zwei Studentenwerken und eine Umfrage bei anderen ergaben, war dabei einiges zu kritisieren.

1.1 Die Wohnraumvergabe

Ein Studentenwerk, das über die Vergabe einer Wohnung in einem Studentenwohnheim zu entscheiden hat, darf von den Bewerbern die Angaben erfragen, die es für seine Entscheidung benötigt. So simpel sich das anhört, in der Praxis ist es offenbar schwierig, diesen Grundsatz umzusetzen:

- So forderten die meisten befragten Studentenwerke alle Bewerber auf, ein Paßbild vorzulegen. Dabei wird dieses nur benötigt, damit die Heimverwaltung überprüfen kann, ob der Student, mit dem sie den Mietvertrag letztendlich abgeschlossen hat, identisch ist mit der Person, die tatsächlich einzieht. Dazu reicht es aber aus, wenn das Bild später dann von dem angefordert wird, dessen Aufnahme das Studentenwerk akzeptiert hat.

- Angaben zum Familienstand und der Anzahl der Kinder werden ebenfalls nur benötigt, wenn die Familienangehörigen mit aufgenommen werden sollen. Also sollten solche Fragen auch nur für diesen Fall gestellt werden.
- Die Heimverwaltung muß nur wissen, wo der Bewerber erreichbar ist. Deshalb sollte danach und nicht pauschal nach der Wohnanschrift der Eltern gefragt werden.

Darüber hinaus mußten wir aber auch noch weitere Mängel feststellen:

- So sollten sich die Bewerber ausdrücklich damit einverstanden erklären, daß das Studentenwerk die "im Rahmen eines eventuellen Mietverhältnisses erforderlichen personenbezogenen Daten mit Hilfe der Elektronischen Datenverarbeitung" speichern und verarbeiten kann. Dazu besteht keinerlei Notwendigkeit, denn die Speicherung dieser Daten ist schon kraft Gesetzes zulässig. Mit dem Einholen der Einwilligung erweckt ein Studentenwerk nur den unzutreffenden Eindruck, als ob die Bewerber etwas anderes bestimmen könnten.
- Wenn ein Studentenwerk schon die Einwilligung in die Weitergabe von Namen und Wohneinheitsnummer an die Post zur Erleichterung der Zustellung einholen will, dann muß es beachten, daß die Abgabe einer solchen Erklärung der freien Entscheidung des Bewerbers überlassen ist. Deshalb muß es den Bewerber nach § 4 Abs. 2 LDSG darauf hinweisen, daß eine Verweigerung der Einwilligung für die Wohnraumvergabe nicht nachteilig ist.
- Schließlich muß ein Bewerber nach § 11 Abs. 2 LDSG zutreffend darüber informiert werden, welche Folgen es haben kann, wenn er den Antragsvordruck nicht korrekt ausfüllt. Mit anderen Worten: Ihm muß gesagt werden, daß eine Verweigerung von erforderlichen Angaben zu einer Ablehnung des Aufnahmeantrags führen kann. Dagegen kann das Studentenwerk nicht, wie geschehen, damit drohen, der Antrag werde überhaupt nicht bearbeitet.

Ich habe die überprüften Studentenwerke aufgefordert, ihr Vorgehen der geschilderten Rechtslage anzupassen. Sie haben dem weitgehend Rechnung getragen und ihre Formulare für die Wohnheimaufnahme entsprechend geändert.

1.2 Speicherung auf ewig?

Auch für Studentenwerke muß gelten: Personenbezogene Daten, die nicht mehr benötigt werden, sind zu löschen. Wann dies der Fall ist, sollte schon beim Einsatz eines EDV-Verfahrens von vornherein festgelegt werden. Bei den beiden Studentenwerken, denen wir einen Kontrollbesuch abgestattet hatten, war dies nicht geschehen. Sie speicherten Mieterdaten auf ihrem PC, hatten aber bis zum Zeitpunkt der Überprüfung Daten ehemaliger Mieter weder gelöscht noch

festgelegt, wann sie dies tun wollten. Dazu sahen sie keinen Anlaß, weil sie auch noch nach Auszug eines Mieters nachvollziehen wollten, wie lange er im Studentenwohnheim gewohnt hat, um dies berücksichtigen zu können, wenn er möglicherweise Jahre später erneut in das Studentenwohnheim aufgenommen werden will. Dieses durchaus legitime Anliegen entbindet die Studentenwerke jedoch nicht von der Verpflichtung, sich Gedanken darüber zu machen, wie lange ein berechtigtes Informationsinteresse noch besteht und entsprechende Löschungsfristen festzulegen. Die Studentenwerke haben inzwischen zugesagt, die Mieterdaten 10 Jahre nach Beendigung des Mietverhältnisses zu löschen.

2. Studentenwerk als Ausbildungsförderungsamt

Die Studentenwerke haben neben ihren sonstigen Aufgaben auch Anträge auf BAföG-Leistungen zu bearbeiten und darüber zu entscheiden. Bei zwei Studentenwerken überprüften wir an Ort und Stelle, wie sie dabei mit personenbezogenen Daten umgehen.

2.1 Formulare und Akten

Nicht nur die automatisierte, sondern auch die konventionelle Datenverarbeitung in Akten bereitet öffentlichen Stellen immer wieder Probleme. So auch den beiden Studentenwerken:

- Wer BAföG-Leistungen beantragt, muß die für die Gewährung der Leistungen erforderlichen Angaben machen und ihre Richtigkeit durch Vorlage von Urkunden nachweisen. Anstatt, wie dies die Allgemeine Verwaltungsvorschrift zum Bundesausbildungsförderungsgesetz des Bundesministeriums für Bildung und Wissenschaft (BAföG-VwV) vorschreibt, die vorgelegten Urkunden mit den Angaben des Antragstellers zu vergleichen und, bei Übereinstimmung, im Antragsformular einen Bestätigungsvermerk anzubringen und sie anschließend wieder an den Antragsteller zurückzugeben, fertigten beide von allen vorgelegten Urkunden Kopien an und nahmen sie zu den Akten. Dort verbleiben sie, solange die Akte existiert. Die BAföG-VwV verlangt ein solches Vorgehen nur bei Steuerbescheiden und bei Urkunden, die die Angaben des Antragstellers nicht bestätigen oder zumindest an deren Richtigkeit zweifeln lassen. Da die vorgelegten Urkunden vielfach mehr Informationen enthalten, als für die BAföG-Gewährung notwendig ist, führt dieses Vorgehen der Studentenwerke dazu, daß dort noch Informationen in den Akten gespeichert bleiben, die in Wirklichkeit gar nicht benötigt werden und zwar auch nicht für eine spätere Rechnungsprüfung. Da eine derartige generell geübte Praxis nicht zulässig ist und mein Amt darauf in der Vergangenheit schon wiederholt hingewiesen hat, beanstandete ich sie. Das Landesamt für Aus-

bildungsförderung hat inzwischen die Studentenwerke angewiesen, der dargelegten Rechtslage Rechnung zu tragen.

- Bei einem Studentenwerk stellten wir fest, daß in der Registratur noch mehrere tausend Akten mit sensiblen Sozial- und Steuerdaten lagerten, die bereits vor Jahren hätten ausgesondert werden müssen. Dies konnte nicht verwundern, denn dort war nicht einmal bekannt, wann eigentlich die Akten abgeschlossener Fälle ausgesondert werden müssen. Die Angaben der Geschäftsführung des Studentenwerks, des Sachbearbeiters und des Registrators variierten beim Kontrollbesuch zwischen sechs und acht Jahren. Dabei hat das Landesamt für Ausbildungsförderung in einer Verwaltungsvorschrift präzise Aufbewahrungsfristen festgelegt, und zwar 5 Jahre für die Normalfälle und 6 Jahre für die Darlehensfälle. Auch in dieser Frage war eine Beanstandung nicht zu umgehen. Eine abschließende Stellungnahme des Studentenwerks steht noch aus.

2.2 Das alte Lied: Keine Löschung

Um der Fülle der Akten Herr zu werden, setzen beide Studentenwerke ein EDV-Verfahren ein. Dazu speichern sie neben der BAföG-Förderungsnummer auch Name und Vornamen des Antragstellers, dessen Geburtstag sowie das Jahr, in dem die Akte zu vernichten ist. Keines der beiden Studentenwerke hatte jedoch vor, diese Daten zu löschen, und zwar auch nicht nach der Vernichtung der jeweiligen BAföG-Akte. Das Ergebnis war, daß eines der beiden Studentenwerke auch noch Daten von BAföG-Empfängern speicherte, deren Akten bereits vor 15 Jahren zur Vernichtung anstanden. Diesen offenkundigen Verstoß gegen die sich aus § 84 Abs. 2 SGB X ergebende Löschungspflicht beanstandete ich. Das Landesamt für Ausbildungsförderung hat daraufhin alle Studentenwerke des Landes angewiesen, künftig keine Daten über bereits vernichtete Akten mehr zu speichern.

2.3 Auftragsdatenverarbeitung unzulänglich geregelt

Die Studentenwerke erfassen die Angaben aus den BAföG-Anträgen elektronisch und leiten sie einmal monatlich einem Rechenzentrum zu, das daraus BAföG-Bescheide und Zahlungsbelege erstellt. Erstaunlich, aber leider nicht einmalig, war dabei, daß beide nicht angeben konnten, welche Verfahrensschritte das Rechenzentrum im einzelnen ausführt, ob und, wenn ja, welche Falldaten es über die monatlichen Berechnungsläufe hinaus speichert, an wen und in welchen Fällen das Rechenzentrum BAföG-Daten weitergibt und wann es diese Daten löscht. Sie selbst hatten mit dem Rechenzentrum keinen Vertrag über diese Datenverarbeitung abgeschlossen. Daß das Landesamt für Ausbildungsförderung als Aufsichtsbehörde dies getan hatte, war ihnen nicht bekannt.

Allerdings ging auch aus diesem Vertrag nicht hervor, welche Daten das Rechenzentrum im einzelnen verarbeiten und wie lange es sie speichern darf. Zudem läßt es das Zehnte Buch des Sozialgesetzbuchs, das für die Verarbeitung der BAföG-Daten maßgebend ist, anders als das Landesdatenschutzgesetz nicht zu, daß die Aufsichtsbehörde einer datenverarbeitenden Stelle für diese eine Auftragsdatenverarbeitung vereinbart. Ich forderte deshalb die Studentenwerke auf, eigene Verträge mit dem Rechenzentrum abzuschließen und dabei die inhaltlichen Mängel des bisherigen Vertrags auszuräumen. Das Landesamt für Ausbildungsförderung will einen Mustervertrag erarbeiten und diesen den Studentenwerken zur Verfügung stellen.

3. Nicht alles taugt zur Versteigerung

Einfallsreichtum bewies ein Gymnasium bei der Gestaltung seines 25jährigen Jubiläums. Eine Attraktion sollte die Versteigerung persönlicher Utensilien von Lehrern werden und der Erlös einem guten Zweck zukommen. Weil die Lehrer aber offenbar zu knauserig waren, mußten andere Gegenstände her. So kam man auf die Idee, zehn Jahre alte Klassentagebücher zu versteigern, was der Rektor "trotz schwerwiegender Bedenken" schließlich doch zuließ. Bei einem ehemaligen Gymnasiasten wollte bei diesem Programmpunkt allerdings keine rechte Freude aufkommen, wußte er doch, daß er in einem der Klassentagebücher mehrfach erwähnt wurde und keineswegs nur positiv. Daß die Versteigerung der Bücher des Guten zuviel und eindeutig datenschutzwidrig war, sah der Rektor danach auch zerknirscht ein. In der Folge meiner Beanstandung stellte sich aber noch eine Frage: Wie lange darf eine Schule Klassentagebücher überhaupt aufbewahren? Ich meine, bis zum Ablauf des folgenden Schuljahres. Das Kultusministerium ist dagegen der Auffassung, die Schulverwaltung müsse auf sie auch noch viele Jahre später zurückgreifen können. Auf eine konkrete Aufbewahrungsfrist wollte es sich freilich noch nicht festlegen. Hoffentlich tut es das bald und sagt den Schulleitern klipp und klar, wann sie die Klassentagebücher aussondern müssen. Dann hätte der Vorfall, so wenig angenehm ihn der ehemalige Gymnasiast empfunden hat, wenigstens noch etwas Positives bewirkt.

5. Abschnitt: Ausländer

1. Die Ausforschung des Gastgebers

Nach dem Ausländergesetz kann die Erteilung eines Visums davon abhängig gemacht werden, daß der Ausländer eine Erklärung seines deutschen Gastgebers vorlegt, worin dieser sich verpflichtet, für die Kosten für den Lebensunterhalt und für die Ausreise seines Gastes aufzukommen. Von dieser rechtlichen Möglichkeit machen

die Ausländerbehörden und Auslandsvertretungen seit geraumer Zeit regen Gebrauch. Die Art und Weise, wie sie dabei vorgehen, ist freilich nur schwer mit dem Datenschutz in Einklang zu bringen. In Baden-Württemberg setzen die Ausländerbehörden dazu aufgrund einer Weisung des Innenministeriums einen bundeseinheitlichen Vordruck ein. Darin muß sich ein Gastgeber nicht nur zur Übernahme der Kosten verpflichten, sondern zugleich auch verschiedene Angaben über seine persönlichen Verhältnisse machen. So soll er unter anderem seinen Beruf und seinen Arbeitgeber angeben. Darüber hinaus wird er danach befragt, ob seine Wohnung ihm gehört oder ob er nur Mieter ist und wie viele Quadratmeter sie umfaßt. Schließlich muß er noch präzise Angaben zu seinen Einkommens- und Vermögensverhältnissen machen. Mit alledem sollen Ausländerbehörde und Auslandsvertretung prüfen können, ob der Gastgeber auch in der Lage ist, die übernommene Verpflichtung zu erfüllen. Eine solche Prüfung ist sicherlich gerechtfertigt. Nur: Die meisten der erfragten Angaben sind dafür nicht erforderlich. Es macht beispielsweise schlechthin keinen Sinn, pauschal nach den Eigentumsverhältnissen und der Größe der Wohnung zu fragen. Entscheidend ist vielmehr, ob die Wohnung groß genug ist, um den Gast darin neben den bereits dort wohnenden Personen aufzunehmen. Auch ist eine Berufsangabe, wie immer sie auch vorgenommen wird, und die Benennung des Arbeitgebers kaum geeignet, Klarheit darüber zu verschaffen, ob der Einladende in der Lage ist, für den Aufenthalt seines Gastes aufzukommen.

Was freilich aus der Sicht des Datenschutzes noch bedenklicher ist: Die mit dem bundeseinheitlichen Vordruck erfragten Angaben verbleiben keineswegs nur bei der Ausländerbehörde. Vielmehr soll der Einladende eine Fertigung des ausgefüllten Vordrucks dem von ihm eingeladenen Ausländer schicken. Dieser muß ihn dann der deutschen Auslandsvertretung mit seinem Visumantrag vorlegen. Darüber hinaus muß er ihn unter Umständen auch noch beim Grenzübergang den kontrollierenden Beamten vorzeigen. Gerade dieser Umstand veranlaßte eine Reihe von Bürgern, sich an mich zu wenden, weil sie befürchteten, daß diese Informationen im Heimatstaat des Gastes in falsche Hände geraten können. Ich bat daraufhin das Innenministerium, darauf hinzuwirken, daß der Vordruck in seiner derzeitigen Fassung nicht mehr zum Einsatz kommt. Es müsse ausreichen, wenn die Ausländerbehörde, die die Verpflichtungserklärung entgegennimmt, anhand von näheren Vorgaben überprüft, ob der Gastgeber in der Lage ist, der eingegangenen Verpflichtung nachzukommen und nur das Ergebnis auf der Verpflichtungserklärung vermerkt. Die einladenden Gastgeber müßten dann nicht mehr befürchten, daß detaillierte Angaben über ihre persönlichen Verhältnisse im Ausland in falsche Hände geraten können. Die Reaktion des Innenministeriums war mehr als enttäuschend. Es sah keinerlei Notwendigkeit zur Änderung des praktizierten Verfahrens und fand insbesondere nichts dabei, daß der Ausländer dabei Kenntnis von persönlichen Verhältnissen des einla-

denden Gastgebers erlangt. Zwischen Einlader und Eingeladenem bestünde in der Regel ohnehin ein solches Näheverhältnis, daß die Kenntnisnahme des Ausländers als normal erscheinen müsse. Mit anderen Worten: Für das Innenministerium ist es offenbar durchaus in Ordnung, daß deutsche Eltern, die einen ausländischen Schüler als Feriengast einladen wollen, dem eingeladenen Gast mit der Einladung gleich auch noch mitteilen müssen, welchen Beruf sie haben, bei wem sie arbeiten, wie sie wohnen und wie viel sie verdienen. Ich meine, eine solche Aussage spricht für sich. In Bonn zeigt man inzwischen für diese Problematik mehr Verständnis. Das Bundesinnenministerium will in Zukunft auf Einzelangaben über die persönlichen Verhältnisse der Gastgeber im Vordruck selbst weitgehend verzichten.

2. Wo ist der Ausländer?

Es kommt immer wieder vor, daß Ausländer verziehen und unter ihrer bisherigen Anschrift für Vertrags- und Geschäftspartner nicht mehr erreichbar sind. Diese wenden sich dann oftmals an die Behörden, um die neue Anschrift des Ausländers in Erfahrung zu bringen. Erste Adresse für solche Anfragen ist die zuletzt zuständige Meldebehörde. Wurde ihr die neue Anschrift gemeldet, dann darf sie diese im Regelfall ohne weiteres bekannt geben. Insoweit gilt für Ausländer nichts anderes als für Deutsche. Schwieriger wird es, wenn die alte Meldebehörde die neue Anschrift nicht kennt. In diesem Fall kommt das vom Bundesverwaltungsamt in Köln geführte Ausländerzentralregister als Informationsquelle in Betracht. Das Bundesverwaltungsamt darf auf Anfrage die ihm bekannte Anschrift bekannt geben, wenn der Anfragende sein rechtliches Interesse an der Kenntnis des Aufenthaltsortes des Ausländers durch Vorlage

- eines nach deutschem Recht gültigen Vollstreckungstitels oder
- einer Aufforderung eines deutschen Gerichts, Daten aus dem Ausländerzentralregister nachzuweisen, oder
- einer Bescheinigung einer deutschen Behörde, aus der sich ergibt, daß die Daten aus dem Ausländerzentralregister zur Durchführung eines dort anhängigen Verfahrens erforderlich sind,

belegt und die Erfolglosigkeit einer Anfrage bei der zuletzt zuständigen Meldebehörde durch eine höchstens vier Wochen alte Auskunft dieses Amts nachweist.

3. Auskünfte vom Therapiezentrum?

Ein privates Therapiezentrum für Drogenabhängige wandte sich ratsuchend an mich, nachdem es von einer Ausländerbehörde aufgefordert worden war, "zur ausländerrechtlichen Prüfung der Zuständigkeit für die Verlängerung der Aufenthaltserlaubnis" über einen seiner Patienten Auskünfte zu geben. Unter anderem wollte die Ausländerbehörde wissen,

- ob der Ausländer die Therapie aufgrund einer gerichtlichen Anordnung oder aus freien Stücken angetreten hat,
- wie lange eine erfolgreiche Therapie voraussichtlich dauern wird und
- wer Kostenträger ist und für den Lebensunterhalt des Patienten aufkommt.

So verständlich die Unsicherheit des Therapiezentrums war, bei korrektem Vorgehen der Ausländerbehörde hätte sie nicht auftreten dürfen. Denn diese hätte eigentlich nach § 75 Abs. 1 AuslG ihre Informationswünsche an den Ausländer richten und ihn gegebenenfalls auffordern müssen, eine Bescheinigung des Therapiezentrums über die Therapiedauer beizubringen. Wenn sie sich aber schon ausnahmsweise, weil es sich um einen Eilfall gehandelt hat und weil die Informationsbeschaffung bei diesem Personenkreis erfahrungsgemäß schwierig ist, an die Therapieeinrichtung gewandt hat, hätte sie diese nach § 75 Abs. 2 AuslG darauf hinweisen müssen, daß die Beantwortung der Fragen für sie freiwillig ist und dazu nicht zuletzt wegen der von den Mitarbeitern des Therapiezentrums zu wahrenden Schweigepflicht die Einwilligung des Patienten eingeholt werden muß. Zudem hätte sie - die Fragen bezweckten nicht nur die Prüfung der Zuständigkeit - korrekt darüber informieren müssen, für welche Zwecke die geforderten Angaben erfragt werden. Die Ausländerbehörde will künftig so verfahren.

4. Fehlinformation mit Folgen

Die Speicherung unrichtiger Daten kann fatale Folgen haben. Diese Erfahrung mußte eine Bürgerin machen. An ihrer Wohnungstür klingelten nachts um 1 Uhr Polizeibeamte, betraten die Wohnung und erklärten, sie wollten einen Ausländer zur Abschiebung mitnehmen. Dieser sei doch mit ihr verlobt und wohne bei ihr. Diese Information war schlicht falsch, die Bürgerin hatte lediglich zuvor für den Ausländer eine Petition eingereicht. Passiert war der Fehler bei der für Abschiebemaßnahmen zuständigen Bezirksstelle für Asyl. Sie hatte in ihrem Festnahmeersuchen an die Polizei als Anschrift des Ausländers die Anschrift der Bürgerin genannt und sie dabei als dessen Verlobte bezeichnet. Wie es zu dieser Fehlinformation kam, ließ sich nicht aufklären, die Bezirksstelle für Asyl führt den Fehler auf ein Mißverständnis und vielleicht auch eine Verwechslung mit einem anderen Fall zurück. Mir blieb nur, die Bezirksstelle für Asyl und die mit der Durchführung der Festnahmeaktion beauftragte Polizeidirektion aufzufordern, die Fehlinformation in ihren Unterlagen zu berichtigen. Beide haben dem entsprochen.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997

Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für problematisch, daß in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereichs verarbeitet werden. Sie fordern, daß zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, daß außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

1. Ärzte bzw. Krankenhäuser haben z.B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z.B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibarbeiten an selbständige Schreibbüros.

   Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

2. Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), z.B. bei Einschaltung eines externen Inkassounternehmens, bei externem Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externen Beratergesellschaften.

3. Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungs-

zwecke vorgesehen wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestellt, daß die personenbezogenen Patientendaten diesen Ärzten "in ihrer Eigenschaft als Arzt" bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmeschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

Die Datenschutzbeauftragten des Bund und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997

Achtung der Menschenrechte in der Europäischen Union

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17. Sept. 1996 zu den Dateien von EUROPOL unterstützt werden soll.

Das Europäische Parlament hat in seiner Entschließung zur Achtung der Menschenrechte gefordert, "alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen".

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997

Geplante Verpflichtung von Telediensteanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Art. 2 [§ 5 Abs. 3] des Informations- und Kommunikationsdienste-Gesetzes vom 20. Dez. 1996 - BR-Drs. 966/96) sieht vor, daß die Anbieter von Telediensten (z.B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstedatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, daß Anbieter von elektronischen Informationsdiensten (z.B. Diskussionsforen) offenlegen müßten, welche ihrer Kunden welche Dienste z.B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht enthalten hinreichende Möglichkeiten, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisherige Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt.

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Diensteanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Abs. 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997

Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz - DNA-Analyse ("Genetischer Fingerabdruck") - die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersu-

chungsmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z.B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81e und 81f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.
   Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:
   - Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.
   - Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherun-

gen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.
- Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z.B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81f Abs. 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997

Beratungen zum Strafverfahrensänderungsgesetz 1996

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z.B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.
- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages "berechtigtes" statt eines rechtlichen Interesses gefordert.
- Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z.B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fanden in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag.

Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.

Beispiele hierfür sind:
- Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.
- Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.
- Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.
- Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.
- Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.
- Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.
- Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

Anhang 6

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Okt. 1997 zu den Vorschlägen der Arbeitsgruppe der ASMK "Verbesserter Datenaustausch bei Sozialleistungen"

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmißbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich - insbesondere mit veränderten Verfahren der Datenerhebung - erreicht werden soll, muß der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

- Datenerhebungen beim Betroffenen selbst,
- Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen,
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlaß,
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlaß (Stichproben/Datenabgleich).

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z.B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritte erhalten keine Kenntnis von diesen Datenerhebungen.

Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z.B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren der Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß hinreichend geprüft und dargelegt wird, ob minderschwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs,

gehen aber davon aus, daß pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmißbrauch tatsächlich erforderlich sind, muß für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten, daß der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Gegen folgende Vorschläge im Bericht bestehen gravierende Bedenken:

1. **Mitwirkung bei der Ahndung des Mißbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I) - S. 30 und S. 2 -**

   Die vorgeschlagenen Möglichkeiten von anlaßunabhängigen Mißbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

   Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, unter anderem da sie geeignet ist, seine Stellung in der Öffentlichkeit, z.B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im unklaren, welche Daten wann an wen übermittelt wurden.

   Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die vorgeschlagene Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit den allgemeinen Grundsatz, daß Datenerhebungen, die sowohl pauschal und undifferenziert sind als auch ohne Anlaß erfolgen, abzulehnen sind.

   Die Datenschutzbeauftragten weisen schließlich darauf hin, daß gegen eine Ausnutzung der technischen Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen (B.I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. Nachfragen beim Wohnsitzfinanzamt des Hilfesuchenden zu Schenkungen und Erbschaften (zu D.I.1.1) - S. 6 -

Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. § 21 Abs. 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67a SGB X einholen, soweit das erforderlich ist. Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.

3. Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6) - S. 13 -

Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses differenzierte System der Datenerhebung im Sozialbereich überhaupt nicht ein.

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünften gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben.

Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, daß derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden Ergebnis führen und Anhaltspunkte dafür bestehen, daß bei der fraglichen Bank/Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4. Akzeptanz des Datenaustauschs (zu E.IV) - S. 36 -

Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These,

daß anlaßunabhängige Datenabgleiche keiner speziellen gesetzlichen Grundlage bedürften, trifft deshalb nicht zu.

Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu gesprächsbereit.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 23./24. Okt. 1997

Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Okt. 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z.B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;
- dem Datenschutzrecht droht Zersplittung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- Weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;
- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des Bundesdatenschutzgesetzes, z.B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;
- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;
- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

- Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;
- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;
- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Videoüberwachung;
- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;
- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;
- Regelungen für Chipkarten-Anwendungen;
- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;
- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;
- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedsstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereiches verwenden darf;

- möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter, Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;
- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen,

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 23./24. Okt. 1997

Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmend Bedeutung. Die Nutzer wenden diese Technik z.B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z.B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff "Privacy enhancing technology (PET)" eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes be-

reits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm "Forschung und Entwicklung" aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 23./24. Okt. 1997

Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wieder. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrats (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten ("Vermeidung kognitiver Dissonanzen"). Ausgehend von diesen Überlegungen hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z.B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.
2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.
3. Vorbehaltlich des o.g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z.B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.
4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.
5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.

6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.