Landtag von Baden-Württemberg **Drucksache 12 / 4600**

12. Wahlperiode **03. 12. 99**

Mitteilung

des Landesbeauftragten für den Datenschutz

Zwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 3. Dezember 1999:

Anbei übersende ich Ihnen unseren 20. Tätigkeitsbericht, der nach § 27 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 1999 zu erstatten ist.

Schneider

Eingegangen: 03. 12. 99 / Ausgegeben: 21. 12. 99

Zwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

1. Teil: Zur Situation

1. Alles schon einmal da gewesen

Der Datenschutz in Baden-Württemberg kann in diesen Tagen ein Jubiläum feiern. Am 29. November 1979 hat der Landtag das erste Landesdatenschutzgesetz beschlossen. Baden-Württemberg war damals keineswegs Vorreiter, sondern lediglich Vorletzter. Bis auf ein Bundesland hatten alle anderen Länder der alten Bundesrepublik ihre Landesdatenschutzgesetze zuvor bereits erlassen. Auch der Inhalt des neuen Gesetzes war nicht gerade bahnbrechend. Vielmehr benutzte man im Wesentlichen die bereits vorhandenen Datenschutzgesetze als Vorlage. Nichts Revolutionäres also, und gleichwohl begann damit eine kleine Revolution in der Verwaltung in Baden-Württemberg. Ausgelöst wurde sie durch zwei im Landesdatenschutzgesetz getroffene Entscheidungen: Während bis dahin in der Verwaltung beim Umgang mit personenbezogenen Daten erlaubt war, was nicht ausdrücklich verboten oder sonst gesetzlich reglementiert war, wurde dieser Grundsatz von da an umgedreht. Das Landesdatenschutzgesetz ließ in seinem Anwendungsbereich eine Datenverarbeitung nur zu, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene dazu sein Einverständnis gegeben hat. Dies war eine Entscheidung, die bis heute leider Viele noch nicht hinreichend verinnerlicht haben, wie wir immer wieder beim Kontakt mit öffentlichen Stellen feststellen müssen. Noch mehr bewirkte freilich eine andere Entscheidung des ersten Landesdatenschutzgesetzes, nämlich die Einrichtung einer unabhängigen Datenschutzkontrolle, also meines Amtes. Während man es bis dahin nicht so genau mit der Umsetzung von teilweise sehr viel älteren gesetzlichen Regelungen über den Umgang mit personenbezogenen Daten nahm, weil dies weitgehend unkontrolliert blieb, gab es jetzt eine Instanz, die sich um die Einhaltung aller Datenschutzregelungen, ganz gleich, wann und wo sie erlassen worden waren, kümmerte und dann auch Gesetzesverstöße beim Namen nannte. Die Reaktion ließ nicht lange auf sich warten. Schon im Jahr 1981 war die erste Änderung des Landesdatenschutzgesetzes mit einer Beschränkung der Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz fällig. Der Datenschutz geriet in dieser Zeit immer mehr in die Defensive. Offensiver Datenschutz war verpönt. Ein Rollback drohte.

Eine neue Situation entstand durch das am 15. Dezember 1983 ergangene Volkszählungsurteil des Bundesverfassungsgerichts. Mit diesem Urteil wurde der Datenschutz auch in Baden-Württemberg gewissermaßen hoffähig, denn darin stellte das Gericht fest, dass Datenschutz nicht nur eine Frage der politischen Opportunität, sondern ein Verfassungsgebot ist. Die zentralen Aussagen dieses Urteils waren: Jeder hat laut unserer Verfassung das Recht, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Eingriffe in dieses Recht darf nur der Gesetzgeber zulassen. Er darf dies nur im überwiegenden Allgemeininteresse unter Berücksichtigung der Grundsätze der Verhältnismäßigkeit und Normenklarheit tun. Zweckbindung, Vorrang der Datenerhebung beim Betroffenen, Transparenz der Datenverarbeitung und effektive Kontrolle der Datenverarbeitung durch unabhängige Datenschutzbeauftragte waren weitere Forderungen, denen der Gesetzgeber von da an Rechnung zu tragen hatte. Damit war aber schnell klar, dass das erste Landesdatenschutzgesetz reformbedürftig war. Bis es dann allerdings so weit war, darüber vergingen nahezu acht Jahre. Im Land spielte man während dieser Zeit nicht „Warten auf Godot“ von Samuel Beckett, sondern „Warten auf Bonn“, eine Gemeinschaftsproduktion bekannter und nicht bekannter Autoren. Erst als man sich dort auf ein neues Bundesdatenschutzgesetz geeinigt hatte, beschloss auch in Baden-Württemberg der Landtag am 27. Mai 1991 ein neues Landesdatenschutzgesetz. Während in anderen Bereichen Baden-Württemberg zu Recht nach Möglichkeit Spitze sein will, entwickelten Landesregierung und Landtag beim zweiten Landesdatenschutzgesetz nicht diesen Ehrgeiz. Man hielt sich zurück und beschränkte sich im Wesentlichen darauf, nur die Regelungen zu treffen, die nach der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung unbedingt getroffen werden mussten.

Weil Bund und Länder verpflichtet sind, das Datenschutzrecht der EG-Datenschutzrichtlinie vom 24. Oktober 1995 anzupassen, steht eine erneute No-

vellierung des Landesdatenschutzgesetzes vor der Tür. Die Arbeiten an diesem Gesetzentwurf sind nach Auskunft des Innenministeriums weitgehend abgeschlossen, so dass sich voraussichtlich in Bälde der Landtag damit zu befassen hat. Wie bei den beiden vorangegangenen Novellierungen will die Landesregierung sich offensichtlich auch jetzt im Wesentlichen damit begnügen, das vorzuschlagen, was die EG-Datenschutzrichtlinie unumgänglich fordert. Allerdings will man – im Unterschied zur letzten Novellierung – diesmal nicht warten, bis das Bundesdatenschutzgesetz geändert worden ist. Obwohl es in der Begründung des Kabinettsentwurfs noch hieß, es sei unvermeidlich, nach einer Novellierung des Bundesdatenschutzgesetzes zu prüfen, ob das Landesdatenschutzgesetz erneut angepasst werden müsse, vor allem im Interesse der Erhaltung einer möglichst weit gehenden Rechtseinheit im allgemeinen Datenschutzrecht, hat man es offenbar eilig, noch vor dem Bund zum Zuge zu kommen. Hängt dies möglicherweise damit zusammen, dass die zuletzt bekannt gewordene Bundesfassung dem Anliegen des Datenschutzes besser gerecht wird und die Landesregierung mit ihrem Entwurf der Marke „light“ hier in Rechtfertigungszwang käme? Nachdem die Umsetzung der EG-Datenschutzrichtlinie nun schon mehr als ein Jahr überfällig ist, hätte man sich jetzt auch noch die Zeit nehmen und darauf warten können, bis die Änderungen am Bundesdatenschutzgesetz feststehen. Denn den von der Landesregierung erwähnten Gesichtspunkt der Rechtseinheit im allgemeinen Datenschutzrecht halte ich in der Tat für ein äußerst anstrebenswertes Ziel, dem in anderen Bereichen, wie etwa dem allgemeinen Verwaltungsverfahrensrecht, bislang eine weit stärkere Bedeutung beigemessen worden ist. Dass auch nur annähernd zeitnah mit einer Anpassung des Landes- an das voraussichtlich nur wenige Monate später in Kraft tretende Bundesdatenschutzgesetz zu rechnen sein wird, dürften nur ausgemachte Optimisten annehmen.

Wäre die geplante Änderung des Landesdatenschutzgesetzes der „große Wurf“, könnte man sich mit der Kritik an dem Sonderweg ja noch zurückhalten. Das ist indes nicht der Fall. Man begnügt sich vielmehr weitgehend mit einem Einarbeiten dessen, was das Europarecht vorgegeben hat. Dass das Gesetz durch eine solche Flickschusterei lesbarer und verständlicher würde, war von vornherein nicht zu erwarten. Hier setzt aber einer der Hauptkritikpunkte an: Gesetze, die nur schwer zu lesen und zu verstehen sind, haben wenig Chancen, in der Praxis auch richtig angewendet zu werden. Nicht umsonst ist das Landesdatenschutzgesetz selbst für viele gestandene Verwaltungspraktiker nach wie vor ein Buch mit sieben Siegeln. Ich fordere deshalb schon seit langem, das Gesetz von Grund auf zu überarbeiten und es sowohl vom Aufbau wie von der Sprache her so zu gestalten, dass jeder damit umgehen kann. Wie heißt es so schön in den Richtlinien der Landesregierung zum Erlass von Vorschriften: „Es ist das Ziel der Landesregierung, das Recht zu vereinfachen … Deshalb hat jeder, der bei der Vorbereitung von Gesetzen … beteiligt ist, besonders auf die … Verständlichkeit einer Regelung zu achten“. Ein Blick in die eigenen Richtlinien wäre manches Mal nicht verkehrt.

Aber nicht nur mit der Darstellung des Datenschutzrechts im Gesamten muss man unzufrieden sein. Kritik fordern auch einzelne getroffene und nicht getroffene Regelungen heraus. Hier nur einige wenige, aus meiner Sicht hervorzuhebende Punkte:

– Zunehmend beziehen öffentliche Stellen private Unternehmen in ihre Aufgabenerledigung ein. Soweit diese Unternehmen dabei zur Erfüllung ihres Auftrags auch personenbezogene Daten verarbeiten müssen, müssen sie nur die für private Unternehmen geltenden Bestimmungen des Bundesdatenschutzgesetzes beachten. Dies ist aber nicht einzusehen. Warum soll beispielsweise ein Ingenieurbüro, das im Auftrag einer Kommune das von dieser nach dem Wasserrecht zu führende Indirekt-Einleiter-Kataster erstellt, beim Umgang mit den dazu benötigten Bürgerdaten sich nicht an die gleichen Datenschutzbestimmungen halten müssen, die auch für die Kommune gelten würden, wenn sie das Kataster mit eigenen Kräften erstellen würde? Dies zu regeln, wurde abgelehnt.

– Vor allem im kommunalen Bereich werden immer häufiger bislang als Eigenbetrieb geführte Einrichtungen, z. B. Krankenhäuser, in private, aber

nach wie vor im Besitz der Kommune verbleibende Gesellschaften umgewandelt. Für diese gilt dann, wie für andere private Gesellschaften auch, das private Datenschutzrecht des Bundesdatenschutzgesetzes. So weit, so gut. Aber warum soll der Landesbeauftragte für den Datenschutz nicht weiterhin berechtigt sein, die Einhaltung der Datenschutzbestimmungen zu kontrollieren? Außer in Baden-Württemberg ist es in keinem anderen Land so geregelt, dass dessen Kontrollbefugnis mit der lediglich formellen Privatisierung öffentlicher Einrichtungen verloren geht.

– Moderne Speicher- und Verarbeitungsmedien, insbesondere Chipkarten, halten in vielen Bereichen des täglichen Lebens Einzug. Auf die damit verbundenen datenschutzrelevanten Fragen gibt das Gesetz bisher keine Antwort. Dies will der Gesetzentwurf zwar ändern. Was an Regelungen allerdings vorgesehen ist, ist bei weitem zu wenig. Hier hätte man sich ein Beispiel am aktuellen Entwurf des Bundesdatenschutzgesetzes nehmen können, der auf die wesentlichen Probleme eingeht. Aber offenbar ist man nicht bereit, die Risiken, die der Einsatz solcher Chipkarten für das Persönlichkeitsrecht des Einzelnen mit sich bringt, in der erforderlichen Weise zu begrenzen.

– Werden personenbezogene Daten automatisiert verarbeitet, stellen sich eine Reihe sicherheitstechnischer Fragen. Zu dem, was hier zum Schutz der Daten zu tun ist, verharrt der Gesetzentwurf in den Ansätzen, die noch unter den Bedingungen der Großrechnertechnologie entwickelt wurden. Und das, obwohl das Land doch gerade im technologischen Bereich immer Spitze sein will! Es gibt mittlerweile bundesweit akzeptierte Standards, denen man sich, obwohl wir hier ganz konkrete Vorschläge gemacht haben, aber partout nicht annähern will. Warum, bleibt schleierhaft.

– Eines der aus meiner Sicht schwerwiegendsten Versäumnisse des Gesetzentwurfs besteht darin, dass man die Behörden nicht zur Bestellung örtlicher Datenschutzbeauftragter verpflichtet. Jeder Behörde soll es selbst überlassen bleiben, zu entscheiden, ob sie das will oder nicht. Wie das in der Praxis aussehen wird, kann man sich unschwer vorstellen. Folge ist, dass die Datenschutzprobleme nicht dort gelöst werden, wo dies am effektivsten wäre, nämlich vor Ort.

Dies sind, wie gesagt, nur Ausschnitte aus einem ganzen Katalog von Einwänden und Anregungen, die ich der Landesregierung vorgetragen habe. So, wie es aussieht, wird dem wohl weitgehend nicht gefolgt werden. Ich halte das im Sinne eines wirkungsvollen Datenschutzes für außerordentlich bedauerlich.

2. Die Dienststelle

Business as usual. So könnte man in etwa die Arbeit meiner Dienststelle im Berichtsjahr umschreiben. Wie die Jahre zuvor haben wir dabei gute und schlechte Erfahrungen gemacht, sind auf Verständnis und Kooperationsbereitschaft gestoßen, mussten hin und wieder aber auch mangelhafte Unterstützung zur Kenntnis nehmen und deshalb sogar die eine oder andere Beanstandung aussprechen. Das Justizministerium ging dabei, wie ich an anderer Stelle des Berichts ausführen werde (vgl. 4. Teil, 1. Abschnitt), mit schlechtem Beispiel voran. Wir waren bestrebt, uns möglichst oft vor Ort zu informieren und dort auch zu kontrollieren, rund 35 Kontroll- und Informationsbesuche kamen so zusammen. Mehr war mit dem Personalbestand meiner Dienststelle schlicht und einfach nicht möglich. Immer deutlicher zeigt sich, dass sie hoffnungslos unterbesetzt ist. Dabei beweisen allein schon die Ergebnisse unserer Kontrollen, dass insbesondere der technisch-organisatorische Datenschutz und das Bewusstsein um seine Notwendigkeit in der Praxis der Verwaltung im Land nach wie vor unterentwickelt ist. Dies ist umso bedenklicher, als gleichzeitig der Einsatz der modernen Informations- und Kommunikationstechnik bei den öffentlichen Stellen in den letzten Jahren immer mehr zugenommen hat und ganz sicher weiter zunehmen wird. Kontrollen und vor allem auch qualifizierte Beratungen sind deshalb notwendiger denn je. Ich meine, wenn man schon den Einsatz der EDV in Verwaltung und Justiz so forciert, wie es derzeit geschieht, und dafür erhebliche Mittel aufwendet, dann muss man auch dafür sorgen, dass die notwendigen technischen und organisatorischen Rahmenbedingungen vorhanden sind. Denn nur

dann ist es hinnehmbar, die mit dem Einsatz dieser Technik verbundenen Risiken einzugehen. Gerade Beratungen im Technikbereich haben uns im vergangenen Jahr sehr stark beschäftigt und viel Zeit in Anspruch genommen. Meine Dienststelle arbeitet u. a. im Arbeitskreis Informationstechnik der Ministerien, im Lenkungsausschuss „Einheitliches Personalverwaltungssystem“ und im Arbeitskreis „Nutzung neuer Medien im Zulassungsverfahren“ des Bund-Länder-Fachausschusses für Angelegenheiten der Zulassung von Fahrzeugen zum Straßenverkehr mit. Wir beraten das Landeskriminalamt bei der Neugestaltung der automatisierten Datenverarbeitung der Polizei, Ministerien bei der Auslagerung (Outsourcing) ihrer Bürokommunikation auf ein privates Unternehmen und haben u. a. beratende Stellungnahmen zur Networking-Konzeption der Landesverwaltung, zur Einführung eines Landesstandards zur Verschlüsselung elektronischer Post und zur Weiterentwicklung des Landesverwaltungsnetzes abgegeben. Dies sind nur einige wenige Fälle, in denen der technische Sachverstand meiner Dienststelle gefordert war. Hinzu kommen noch Kontakte z. B. mit dem Städtetag wegen der Frage der Internet-Nutzung durch Kommunen, aber auch mit einer ganzen Reihe von Städten im Zusammenhang mit der Einführung dort geplanter elektronischer Bürgerdienste. Diese Aufzählung ließe sich noch erheblich verlängern. Eine solche Beratungstätigkeit ist eminent wichtig, nicht zuletzt weil derzeit in vielen Bereichen Weichen gestellt werden, die für die Zukunft richtungsweisend sind. Sie müsste eigentlich weiter intensiviert werden. Die Bereitschaft, die Beratung einzufordern und anzunehmen, ist zunehmend da. Ich habe deshalb das Innenministerium bei der Aufstellung eines Entwurfs eines Haushaltsplans für die Jahre 2000/2001 gebeten, dort für mein Amt eine neue Stelle für einen Informatiker vorzusehen. Das Innenministerium zeigte zwar Verständnis für mein Anliegen. Dieses Verständnis schlug sich in dem von der Landesregierung beschlossenen Entwurf eines Haushaltsplans bisher leider nicht nieder. Ich hoffe nicht, dass dies das letzte Wort ist. Das Land Baden-Württemberg soll nach dem Willen der Landesregierung beim Einsatz der neuen Medien eine Führungsrolle übernehmen. Unabdingbare Voraussetzung dafür ist aber, wie auch Vertreter der Landesregierung immer wieder betonen, dass die notwendige Datensicherheit gewährleistet ist. Dazu ist jedoch eine effektive unabhängige Datenschutzkontrolle, die in der Lage ist, sowohl zu kontrollieren als auch zu beraten, unerlässlich.

2. Teil: Technik und Organisation

1. Virtuelle Verwaltungswelten – die elektronischen Bürgerdienste kommen

Mittlerweile gehört es fast zur Selbstverständlichkeit, dass sich Kommunen, Landesbehörden und andere öffentliche Stellen im Internet präsentieren. Zunehmend nutzen sie es aber auch, um ihr Dienstleistungsangebot zu verbessern und zugleich Modernität und Bürgernähe zu demonstrieren. Zwei Funktionen des Internet stehen dabei im Mittelpunkt: Zum einen die Möglichkeit, insbesondere über das World Wide Web (WWW) interaktive Bürgerdienste anzubieten, und zum anderen der Austausch elektronischer Post (E-Mail).

1.1 Bürgerdienste im Internet

Wo der Bürger bisher eine Behörde mitunter mehrfach persönlich aufsuchen musste und an die von Fall zu Fall unterschiedlichen Öffnungszeiten gebunden war, soll er künftig die Möglichkeit haben, von Zuhause aus und wann immer es ihm gerade passt, Behördengänge via Internet zu erledigen. Und dies ist keineswegs nur Zukunftsmusik:

- Zahlreiche Antragsformulare lassen sich heute schon aus dem WWW herunterladen und am heimischen PC ausdrucken.
- Steuerpflichtige in Böblingen, Karlsruhe und Emmendingen können ihre Einkommensteuererklärung via Internet an die Finanzverwaltung senden.
- Zieht ein Bürger innerhalb der Stadt Mannheim um, kann er dies dem Einwohnermeldeamt elektronisch mitteilen.
- Wer ein Auto bei seiner Zulassungsstelle anmelden will, kann sich vielerorts vorab per Internet bereits ein Wunschkennzeichen reservieren.

– Wer ein gerichtliches Mahnverfahren gegen einen säumigen Schuldner in Gang setzen will, kann auch dies mittlerweile elektronisch tun.

Was alles in Form eines elektronischen Bürgerdienstes angeboten werden kann, ist Thema einer vom Innenministerium geleiteten Arbeitsgruppe, in der auch die Kommunen vertreten sind. Geht es nach den dort entwickelten Ideen, könnte die elektronische Abwicklung beispielsweise dann in Frage kommen, wenn jemand Briefwahlunterlagen beantragen oder ins Wählerverzeichnis eingetragen werden möchte, ein Gewerbe an-, um- oder abmelden oder Kinder- und Erziehungsgeld beantragen will. Wenn auch der Realisierung einiger dieser Angebote gegenwärtig noch rechtliche Hindernisse entgegenstehen, wird doch deutlich, dass die Bürger künftig vermehrt mit solchen elektronischen Antragsmöglichkeiten rechnen können.

Deshalb müssen frühzeitig die notwendigen Weichen gestellt werden, damit der Einsatz der elektronischen Bürgerdienste datenschutzgerecht erfolgen kann. Je nach Ausgestaltung des Bürgerdienstes muss unterschiedlichen datenschutzrechtlichen Anforderungen Rechnung getragen werden:

1.1.1 Hinweise zum Datenschutz in elektronische Formulare aufnehmen

Stellt eine Behörde im Internet amtliche Formulare zum Abruf bereit, so muss sie dafür sorgen, dass die im gedruckten Formular enthaltenen Hinweise zum Datenschutz dem Bürger auch dann gegeben werden, wenn er das Formular über Internet abruft. Das war bisher jedenfalls nicht immer selbstverständlich.

1.1.2 Übertragene Daten vor unberechtigtem Zugriff schützen

Bietet eine Behörde den Bürgern die Möglichkeit, die am Bildschirm ausgefüllten Formulare per Mausklick gleich an die Behörde zu senden, muss sie in ihrem Angebot berücksichtigen, dass im Internet übertragene Daten nicht nur vom anvisierten Empfänger, sondern auch von anderen gelesen werden können. Um dem einen Riegel vorzuschieben, sollte die Behörde daher vorsehen, dass personenbezogene Bürgerdaten verschlüsselt übertragen werden. Andernfalls muss sie die Bürger, bevor diese damit beginnen Daten einzugeben, wenigstens auf die fehlende Verschlüsselung und die mit der unverschlüsselten Übertragung verbundenen Risiken klar und deutlich hinweisen. Eine solche Ausnahme kann aber nur dann in Frage kommen, wenn wenig sensible personenbezogene Daten zu übertragen sind.

1.1.3 Prüfung der Identität des Antragstellers

Sollen die elektronisch übermittelten Antragsdaten einen eigenhändig unterschriebenen Antrag ersetzen, so muss sich die Behörde Gewissheit über die Identität des Antragstellers verschaffen. Ansonsten wäre dem Missbrauch Tür und Tor geöffnet: Anträge ließen sich dann unter falschem Namen stellen mit der Folge, dass möglicherweise auf deren Grundlage Verwaltungsentscheidungen getroffen und im Zusammenhang damit falsche Angaben über Bürger gespeichert werden, die unter Umständen finanzielle (Verwaltungsgebühren, Mahnkosten) oder andere Nachteile für die vermeintlichen Antragsteller zur Folge haben können.

Bei einem herkömmlichen Antrag auf Papier lässt sich im Zweifelsfall anhand der eigenhändigen Unterschrift entscheiden, ob dieser tatsächlich von dem genannten Antragsteller stammt. Als elektronisches Pendant zur eigenhändigen Unterschrift kommt die digitale Signatur in Frage: Das zu unterzeichnende elektronische Dokument wird dabei mit Hilfe eines kryptografischen Verfahrens in besonderer Weise gekennzeichnet: Jeder kann anhand einer solchen Kennzeichnung überprüfen, von wem diese vorgenommen wurde. Um die gewünschte Fälschungssicherheit und Zuverlässigkeit beim Umgang mit digitalen Signaturen erreichen zu können, müssen zuvor zahlreiche technische und organisatorische Festlegungen über die Erzeugung, Ausgabe und Verwendung der Signa-

turschlüssel getroffen werden. Hierzu gehören beispielsweise Sorgfaltsregeln für die Stellen (Trust-Center), die die Signaturschlüssel herstellen, Vorgaben zur Frage, wie lange einmal vorgenommene Signaturen als sicher angesehen werden können und auf welche Weise man Signaturschlüssel erkennt, die für eine weitere Verwendung gesperrt wurden. Nun muss nicht jede Stelle, die digitale Signaturen nutzen will, alle diese Maßnahmen selbst festlegen. Sie kann vielmehr auf eine Reihe aufeinander abgestimmter und sich gegenseitig ergänzender Maßnahmen zurückgreifen, die im Signaturgesetz und der dazugehörigen Signaturverordnung dargestellt sind und ein verhältnismäßig hohes Maß an Sicherheit bieten. Deshalb empfiehlt es sich, diese zu übernehmen. Wird von einzelnen Vorgaben des Signaturgesetzes abgewichen, muss darauf geachtet werden, dass die Sicherheit des Signaturverfahrens nicht auf der Strecke bleibt. Der Verzicht auf Einhaltung der Anforderungen des Signaturgesetzes kann zwar eine einfachere und billigere Lösung ermöglichen. Damit ist aber nichts gewonnen, wenn sich die realisierte Lösung später als unsicher erweist. Es ist deshalb zu begrüßen, dass das Innenministerium in dem von ihm geplanten Erprobungsgesetz, das die bislang für einige Bürgerdienste bestehenden landesrechtlichen Hindernisse aus dem Weg räumen soll, die Verwendung signaturgesetzkonformer Signaturen vorsehen will.

Die bereits realisierten elektronischen Bürgerdienste und die gegenwärtig geplanten Vorhaben beschreiten bei der Identitätsprüfung unterschiedliche Wege:

– Im Fall der elektronischen Steuererklärung und der Ummeldung in Mannheim beispielsweise wird auf eine elektronische Identitätsprüfung verzichtet. Der Bürger muss daher zusätzlich zum elektronischen Antrag stets auch eine eigenhändige Unterschrift auf einem Papierausdruck seines Antrags leisten. Derartige Dienste weisen zwar, zumindest hinsichtlich der Identitätsprüfung, keine größeren datenschutzrechtlichen Risiken auf als klassische Anträge in Papierform. Sie kommen damit aber auch dem eigentlichen Sinn elektronischer Bürgerdienste, nämlich die klassische Antragstellung überflüssig zu machen, noch nicht viel näher.

– Ganz anders sieht es beim elektronischen Baugenehmigungsverfahren aus, das die Städte Esslingen und Ostfildern anbieten wollen. Dabei sollen die elektronisch eingereichten Bauanträge von Anfang an mit signaturgesetzkonformen Signaturen versehen werden. Ein Antrag in Papierform entfällt dann.

– Schließlich gibt es auch Bürgerdienste, die noch einen anderen Weg einschlagen. So soll es in Mannheim u. a. möglich sein, Anträge auf Ausstellung von Anwohnerparkausweisen elektronisch zu stellen, die weder signaturgesetzkonform signiert noch ausgedruckt und eigenhändig unterschrieben werden müssen. Zur Nutzung der Bürgerdienste soll allerdings nur zugelassen werden, wer zuvor eine Benutzerkennung und ein Passwort erhalten hat. Aber auch diese können auf elektronischem Weg beantragt werden, ohne dass dabei die Identität des Antragstellers letztlich verlässlich geprüft werden kann. Beim Anwohnerparkausweis wird das Missbrauchsrisiko auf Grund weiterer organisatorischer Maßnahmen zwar begrenzt, gleichwohl ist bei Bürgerdiensten dieser Art sehr genau zu prüfen, ob das Risiko, dass Anträge unter falschem Namen gestellt werden, hingenommen werden kann.

1.2 Datenschutz bei der E-Mail-Kommunikation

Viele elektronische Dienstleistungen können durch den Austausch elektronischer Post (E-Mail) zwischen Bürgern und Verwaltung abgewickelt werden. Probleme ergeben sich dabei, weil die Behörden auf der einen Seite sehr großen Wert darauf legen, elektronisch möglichst für jeden erreichbar zu sein, auf der anderen Seite aber das Internet bekanntlich un-

sicher ist und seine Nutzung vielfältige Sicherheitsrisiken mit sich bringt. Auf Bitte des Städtetags habe ich diesem dazu folgendes Vorgehen empfohlen:

Sendet ein Bürger eine unverschlüsselte E-Mail über das Internet an eine Kommune, so sollte sie diese nicht in jedem Fall auf gleichem Weg beantworten, sondern grundsätzlich nur dann, wenn sie in ihrer Antwort nur wenig sensible Daten verschicken muss. Enthält die Antwort auf die Bürgeranfrage allerdings Informationen über andere Personen oder nähere Angaben über den anfragenden Bürger, sollte die Kommune sie verschlüsseln. Die Verschlüsselung kann nicht allein deshalb unterbleiben, weil die E-Mail des Bürgers unverschlüsselt war. Darin kann entgegen einer weit verbreiteten Meinung noch kein wirksamer Verzicht auf eine datenschutzrechtlich gebotene Verschlüsselung gesehen werden, denn der Bürger weiß bei der Anfrage meist noch gar nicht, was über ihn im Antwortschreiben ausgeführt wird.

Manche Kommunen denken auch darüber nach, den Bürgern per E-Mail zusätzliche Dienstleistungen anzubieten, wie z. B. Erinnerungsschreiben, in denen sie darauf hingewiesen werden, dass ihr Personalausweis oder Reisepass in einigen Monaten abläuft. Solche Mitteilungen dürfen die Kommunen nur dann unverschlüsselt verschicken, wenn die Bürger, beispielsweise anlässlich der An- oder Ummeldung ihres Wohnsitzes, sich damit einverstanden erklärt haben. Dabei stellt sich allerdings folgendes Problem: Die Kommunen benötigen für derartige Dienste die jeweils aktuellen E-Mail-Adressen der an diesem Service interessierten Bürger. Da sich die E-Mail-Adressen auf Grund eines Providerwechsels kurzfristig ändern können, können einmal erfragte E-Mail-Adressen nicht unbefristet immer wieder verwendet werden. Vor diesem Hintergrund erscheint es gegenwärtig fraglich, ob sich ein praktikabler Weg für derartige kommunale Anschreiben finden lässt.

2. Es tut sich etwas in Sachen Verschlüsselung

Verschlüsselung ist und bleibt ein Thema, das für den datenschutzgerechten Einsatz der Informations- und Kommunikationstechnik von zentraler Bedeutung ist.

2.1 Die deutsche Kryptopolitik

Seit geraumer Zeit wird in Deutschland eine kontroverse Diskussion darüber geführt, ob der Staat den Einsatz der Verschlüsselungstechnik einschränken soll. Befürworter einer Regulierung der Verschlüsselung verweisen darauf, dass auch Kriminelle ihre Botschaften verschlüsselt austauschen können und der Staat damit die Möglichkeit verliert, im Rahmen legaler Abhörmaßnahmen Kenntnis vom Inhalt ihres Informationsaustausches zu erhalten. Überzeugende Vorschläge, wie sich eine Einschränkung der Verschlüsselung in der Praxis bewerkstelligen lässt, konnten bislang freilich nicht vorgelegt werden. Daher habe ich mich bereits vor zwei Jahren gegen jedwede Einschränkung oder gar ein Verbot der Verschlüsselung ausgesprochen (vgl. 18. Tätigkeitsbericht 1997, Landtags-Drucksache 12/2242, S. 14 bis 16). Mit ihrem Eckpunktepapier vom 2. Juni 1999 hat nun die Bundesregierung ihre Position zur Kryptopolitik dargelegt und die Diskussion auf eine neue Grundlage gestellt. Darin unterstreicht die Bundesregierung, dass sie die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland nicht einschränken wolle und hebt gleichzeitig die Anwendung einer sicheren Verschlüsselung als eine entscheidende Voraussetzung für die Gewährleistung des Datenschutzes hervor. Diese begrüßenswerten Positionen nahmen die Datenschutzbeauftragten des Bundes und der Länder zum Anlass, mit einer Entschließung zu dieser Thematik an die Öffentlichkeit zu treten (vgl. Anhang 11). Das Eckpunktepapier der Bundesregierung ist ein Schritt in die richtige Richtung, dem aber weitere folgen müssen. Vordringlich ist dabei:

– Das Wissen um die mit der Nutzung moderner Informations- und Kommunikationstechniken verbundenen Risiken muss bei Bürgern, der öffentlichen Verwaltung und der Wirtschaft zunehmen. Denn nur

wer um die Gefahren weiß, ist bereit, die notwendigen Sicherheitsmaßnahmen zu treffen.

– Für den Anwender sehr hilfreich ist, wenn eine kompetente, unabhängige und neutrale Stelle Verschlüsselungsprodukte bewertet mit dem Ziel, Verbrauchern Empfehlungen für den Einsatz geben zu können. Ausdrücklich zu begrüßen ist daher, dass das Bundesministerium des Innern inzwischen dem Bundesamt für Sicherheit in der Informationstechnik gestattet, die Öffentlichkeit über die Stärken von Verschlüsselungsalgorithmen zu unterrichten.

– Schließlich sind Anwender aufgerufen, Verschlüsselung in größerem Umgang als dies bislang der Fall war einzusetzen, um zu einer Verbesserung des Datenschutzes bei der Verarbeitung personenbezogener Daten beizutragen.

2.2 Verschlüsselungseinsatz im Land und in Kommunen

Nicht nur auf bundespolitischer Ebene erhält die Verschlüsselung derzeit Rückenwind, auch Land und Kommunen wollen sie verstärkt einsetzen. Beispielhaft hierfür stehen:

– Pilotprojekt des Städtetages zur E-Mail-Verschlüsselung

Auf Initiative des Städtetages erproben mehrere Dutzend Städte in einem Pilotprojekt, elektronische Postsendungen verschlüsselt via Internet auszutauschen. Da das dabei eingesetzte Programm PGP (Pretty Good Privacy) von Privatpersonen kostenlos genutzt werden darf, ist dieses Produkt nicht nur zum Datenaustausch zwischen Behörden, sondern auch zur Kommunikation zwischen Bürgern und Verwaltung geeignet. Im Zusammenhang mit elektronischen Bürgerdiensten (vgl. Nr. 1) gewinnt dies zunehmend an Bedeutung.

– Rahmenvertrag des Landes zu E-Mail-Verschlüsselungsprodukten

Das Land verhandelt gegenwärtig über den Abschluss von Rahmenverträgen zum Einsatz von Produkten, die es gestatten, elektronische Postsendungen zu verschlüsseln und digital zu signieren.

– Verschlüsselung im TESTA-Netz

Seit einiger Zeit gibt es das von einem Privatunternehmen betriebene Computernetz TESTA, das die Verwaltungsnetze der Bundesländer und des Bundes miteinander verbindet. Über dieses Netz sollen Daten verschlüsselt übertragen werden.

– Nutzung der Verschlüsselung beim Outsourcing

Wie in Nummer 3 dargestellt, kommt der Verschlüsselung auch beim Outsourcing erhebliche Bedeutung zu. Sie steht deshalb bei allen dort beschriebenen Vorhaben auf der Tagesordnung.

Die Datenschutzbeauftragten von Bund und Ländern weisen schon seit Jahren darauf hin, dass die Verschlüsselung eine wichtige Maßnahme ist, um die Vertraulichkeit gespeicherter und via Netz übertragener Daten zu gewährleisten. Vor diesem Hintergrund ist es zu begrüßen, dass diese Überlegungen nunmehr auch bei den Verwaltungen zunehmend Resonanz finden. Die hier genannten Projekte können aber nur einen Einstieg in die Nutzung der Verschlüsselung markieren. Denn bislang ist die Verschlüsselung noch alles andere als ein Selbstläufer. Und auch dort, wo ein Fortschritt zu verzeichnen ist, z. B. bei der E-Mail-Kommunikation des Landes, ist mit der Bereitstellung der Verschlüsselungsmöglichkeiten noch lange nicht sichergestellt, dass alle Daten, deren Verschlüsselung geboten ist, auch tatsächlich verschlüsselt werden. Erst kürzlich wurde in einer kontroversen Diskussion im Arbeitskreis Informationstechnik der Ministerien deutlich, wie groß die Auffassungsunterschiede darüber noch sind, in welchen Fällen elektronische Postsendungen zu verschlüsseln sind und wann darauf verzichtet werden kann.

3. Outsourcing

Angesichts knapper Kassen fällt es der öffentlichen Verwaltung immer schwerer, kostenträchtige EDV-Projekte rasch zu verwirklichen. Abhilfe erhofft sich hier mancher vom Outsourcing des EDV-Betriebes. Dabei wird fast immer ein Unternehmen damit beauftragt, die erforderlichen Computer bereitzustellen, zu betreiben und auf Wunsch auch die Benutzer zu betreuen. Während das Outsourcing in der Vergangenheit für die Landesverwaltung kaum eine Rolle gespielt hat, setzt sie gegenwärtig gleich in zwei großen Projekten auf dieses Pferd: bei der Bürokommunikation und dem Landesverwaltungsnetz. Aber nicht nur im Land, auch bei den Kommunen gewinnt das Outsourcing zunehmend an Bedeutung; das Outsourcing der Krankenhaus-EDV der Städtischen Kliniken Esslingen illustriert dies.

3.1 Outsourcing der Bürokommunikation

Die Möglichkeit, Textverarbeitungsprogramme einzusetzen und elektronische Post auszutauschen, gehört zum A und O heutiger Computerarbeitsplätze und ist zugleich Kernbestandteil der sog. Bürokommunikation (BK). Aber noch längst nicht alle Behörden des Landes verfügen über die dazu notwendige zeitgemäße und den Landesstandards entsprechende Ausstattung. Behörden, die ihre BK-Systeme mit eigenen Mitteln betreiben, können diese oft nur Schritt für Schritt modernisieren. Demgegenüber bietet ihnen das Outsourcing die Möglichkeit, ihre gesamte Ausstattung auf einen Schlag zu erneuern, ohne gleich die vollen Anschaffungskosten tragen zu müssen, weil der Outsourcing-Dienstleister insoweit in Vorleistung tritt. Um den Behörden diesen Weg so leicht wie möglich zu machen, schloss das Innenministerium im vergangenen Jahr einen Rahmenvertrag mit einem Outsourcing-Anbieter ab, auf dessen Grundlage alle Ministerien und ihnen nachgeordnete Behörden das Outsourcing ihrer BK-Systeme diesem in Auftrag geben können. Dabei geht es um bis zu 36 000 BK-Arbeitsplätze. Bislang schlossen das Justiz- und das Wissenschaftsministerium Einzelverträge über das Outsourcing der in beiden Ministerien betriebenen ca. 650 PC sowie der darauf eingesetzten BK-Software ab. Es handelt sich hierbei um Pilotprojekte, in denen beide Seiten praktische Erfahrungen mit dem Outsourcing sammeln wollen. Die vom Auftragnehmer durchzuführenden technischen und organisatorischen Datenschutzmaßnahmen wurden zwar – da deren Erarbeitung erst Teil der Outsourcing-Aufträge war – nicht schon vor Vertragsunterzeichnung ausgehandelt. Die Wirksamkeit des gesamten Vertrages wurde jedoch davon abhängig gemacht, dass der Auftragnehmer ein profundes Datenschutz- und Datensicherheitskonzept vorlegt. Doch damit tat sich der Auftragnehmer bislang sehr schwer. Nachdem zwei frühere Entwürfe dieses Konzepts erhebliche Mängel aufwiesen und nicht akzeptabel waren, liegt jetzt dessen dritte Version vor. Darin gibt das Unternehmen seinen ursprünglichen Plan auf, die Netze der von ihm betreuten Dienststellen mit seinem Unternehmensnetz zu koppeln. Vielmehr beabsichtigt es nun, in Räumen des Landes ein exklusiv für Landesbehörden tätiges Betreuungszentrum einzurichten. Um Protokolldaten besser auswerten zu können, ist der Einsatz eines speziellen Programmes vorgesehen. Außerdem bietet das Unternehmen jetzt an, auf von ihm betreuten PC-Arbeitsplätzen ein Verschlüsselungsprogramm zu installieren, mit dem die Mitarbeiter des Landes schutzbedürftige Daten verschlüsseln können. Zweifellos zielen alle diese Schritte in die richtige Richtung. Gleichwohl weist auch diese Fassung des Datenschutz- und Datensicherheitskonzepts grundlegende Defizite auf:

– Die Festlegung dessen, was das Konzept an Schutz bieten muss, beruht teilweise auf der falschen Annahme, dass mit der Bürokommunikation in der Regel nur Daten der Kategorie „keine personenbezogenen oder nicht schutzbedürftige Daten“ bearbeitet werden. Dabei liegt auf der Hand, dass elektronisch gespeicherte Entwürfe oder elektronische Postsendungen sehr wohl Personaldaten oder andere sensible personenbezogene Daten enthalten können. Deshalb sind die technischen und organisatorischen Schutzmaßnahmen an diesem Schutzniveau auszurichten.

– Ein methodischer Mangel der vorgelegten Konzeption liegt darin, dass nicht erkennbar ist, welchen der erkannten Sicherheitsrisiken mit welchen der aufgelisteten Schutzmaßnahmen entgegengewirkt werden soll.

– Trotz des jetzt vorgesehenen Einsatzes eines speziellen Zusatzprogramms zur Auswertung der Protokolldaten bleibt die Protokollierung sicherheitsrelevanter Ereignisse und deren Auswertung unzulänglich. So lässt sich z. B. nicht automatisch erkennen, dass ein Anmeldefehlversuch oder ein anderes sicherheitsrelevantes Ereignis mehrfach kurz hintereinander auftritt. Da aber gerade daraus auf besonders sicherheitsempfindliche Vorgänge geschlossen werden muss, sollten solche Wiederholungen auch automatisch erkannt und bearbeitet werden können. Unklar bleibt auch, in welcher Weise die auftraggebenden Behörden selbst die Protokolldaten lesen und auswerten können.

– Die Verschlüsselung beim BK-Outsourcing soll die von den Behörden verarbeiteten Daten unter anderem auch vor unberechtigten Zugriffen von Mitarbeitern des Outsourcing-Dienstleisters schützen. Das vom Auftragnehmer ausgewählte Verschlüsselungsprodukt wird den an eine solche Verschlüsselung zu stellenden Anforderungen jedoch nicht hinreichend gerecht.

– Auch im Zusammenhang mit den auf Ebene des Betriebssystems zu realisierenden Sicherheitsmaßnahmen sowie dem Teleservice ist noch Manches offen.

Zusammenfassend ist festzustellen, dass das Datenschutz- und Datensicherheitskonzept nach wie vor keinen ausreichenden Schutz insbesondere vor den spezifischen Risiken des Outsourcings bietet. Deshalb wären andere Behörden, die outsourcen wollen, gut beraten, den Betrieb ihrer BK nicht aus der Hand zu geben, solange diese Mängel fortbestehen. Hinsichtlich der Pilotprojekte im Justiz- und im Wissenschaftsministerium ist dafür zu sorgen, dass diese – sei es im Wege des Outsourcings oder wieder durch eigenen Betrieb – möglichst bald auf der Grundlage eines ausreichenden Datenschutz- und Datensicherheitskonzepts betrieben werden.

3.2 Outsourcing des Landesverwaltungsnetzes

Weil immer mehr Behörden Informationen untereinander einfacher und schneller austauschen wollen und die EDV-Ausstattung der Dienststellen zunimmt, wird das Landesverwaltungsnetz (LVN), ein landesweites Computernetzwerk, an das bereits zahlreiche Landesbehörden angeschlossen sind, vermehrt in Anspruch genommen. Der Ausbau des LVN ist deshalb beschlossene Sache. Die Landesverwaltung hatte sich demzufolge mit der Frage zu befassen, ob sie das LVN und dessen über das ganze Land verteilte Netzknotencomputer selbst ausbauen und weiterhin selbst betreiben sollte oder ob ein Outsourcing des LVN-Betriebes günstiger wäre. Nach langem Hin und Her stellte das Land die Weichen in Richtung Outsourcing. Wie beim BK-Outsourcing ergeben sich aber auch bei diesem Vorhaben etliche datenschutzrechtliche Fragen und Probleme, auf die ich im Rahmen meiner Beratungstätigkeit mehrfach hingewiesen habe. Wichtig war dabei insbesondere:

– Anforderung an Verschlüsselung zu vage

Auch beim Outsourcing eines Computernetzwerks ist dafür zu sorgen, dass der Betreiber keine Kenntnis der über das Netz übertragenen personenbezogenen Daten erhält, soweit dies nicht zur Erfüllung seiner vertraglichen Pflichten erforderlich ist. Folgerichtig forderte das Land vom Auftragnehmer, bei Bedarf auch verschlüsselte Leitungswege zur Verfügung zu stellen. Offen blieb dabei aber, ob der Auftragnehmer oder der Auftraggeber die Schlüssel zu verwalten hat. Da die Verschlüsselung den gewünschten Schutz jedoch nur dann bewirken kann, wenn dem Auftragnehmer nicht auch das Schlüsselmanagement übertragen ist, sollte der Outsourcing-Auftragnehmer damit auch nicht betraut sein.

– Mitbenutzung von Räumen des Landes für geschäftliche Zwecke regeln

Das Land will einem Schwester-Unternehmen des favorisierten Dienstleisters gestatten, Netzknotencomputer in Räumen des Landes aufzustellen. Diese sollen aber nicht nur der Vernetzung der Dienststellen des Landes, sondern auch anderer Kunden dienen. Wenn in diesem Fall nicht ausgeschlossen ist, dass fremde Personen die vom Land bereitgestellten Räume betreten, sind zusätzliche Sicherungsmaßnahmen nötig. Dazu bedarf es in jedem Fall noch entsprechender vertraglicher Vereinbarungen.

– Datenschutz- und Datensicherheitskonzept präzisieren

Die Erfahrungen beim Projekt BK-Outsourcing belegen, wie schwer es einem Unternehmen fallen kann, ein Datenschutz- und Datensicherheitskonzept zu erarbeiten, das dem Standard der Landesverwaltung gerecht wird. Damit keine unnötigen Verzögerungen eintreten, habe ich empfohlen, mit diesen datenschutzrechtlichen Anforderungen nicht hinter dem Berg zu halten, sondern sie dem Auftragnehmer, der vertraglich zur Erstellung eines Datenschutz- und Datensicherheitskonzeptes verpflichtet ist, gleich an die Hand zu geben.

– Abnahmemodalitäten genauer beschreiben

Es ist geplant, die Verantwortung für den Betrieb des LVN schrittweise dem Auftragnehmer zu übertragen, soweit dieser dafür ein Datenschutz- und Datensicherheitskonzept vorlegt. Bislang nicht geregelt, jedoch dringend regelungsbedürftig ist, was geschehen soll, wenn eines oder mehrere der vorgelegten Datenschutz- und Datensicherheitskonzepte trotz Nachbesserungen nicht akzeptabel sind.

3.3 Outsourcing bei Krankenhäusern – die Städtischen Kliniken Esslingen am Neckar

Daten, die Krankenhäuser verarbeiten, gehören zu den sensibelsten Daten überhaupt und bedürfen eines besonderen Schutzes. Dies gilt nicht nur, wenn das Krankenhaus die Daten auf EDV-Systemen im Krankenhaus selbst verarbeitet, sondern auch, wenn es eine externe Stelle zur technischen Durchführung seiner Datenverarbeitung heranzieht. Einen solchen Weg beschritten die Städtischen Kliniken Esslingen am Neckar, indem sie ein in Dresden ansässiges privates Unternehmen mit dem Betrieb ihrer SAP-EDV-Verfahren beauftragten. Hierzu gehören die Verfahren für die Patientenverwaltung, die stationäre und ambulante Abrechnung oder die medizinische Dokumentation. Das Zeitalter der Vernetzung und der Datenkommunikation macht es möglich: Die Rechner, auf denen die sensiblen Krankenhausdaten gespeichert sind, stehen in Dresden; die Mitarbeiter im Krankenhaus in Esslingen rufen von ihren PC aus die Daten ab, lassen sie sich am Bildschirm anzeigen oder verändern sie. Es liegt auf der Hand, dass mit einer solchen Form des Outsourcings zusätzliche Gefahren für den Datenschutz einhergehen, allein schon deswegen, weil die räumliche Entfernung zwischen Krankenhaus und Unternehmen es den Mitarbeitern des Krankenhauses erschwert, vor Ort bei der Firma immer mal wieder nach dem Rechten zu sehen, ob auch alles so ordentlich läuft wie es laufen sollte. Gleichwohl: Von vornherein unzulässig ist der von den Städtischen Kliniken beschrittene Weg nicht. Krankenhäuser in Baden-Württemberg dürfen nach dem Landeskrankenhausgesetz auch eine externe Stelle zur Verarbeitung von Patientendaten heranziehen. Voraussetzung dafür ist allerdings, dass das Krankenhaus die externe Stelle schriftlich beauftragt und in dem Vertrag Gegenstand und Umfang der Datenverarbeitung, etwaige Unterauftragsverhältnisse und die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen regelt.

Als mich die Städtischen Kliniken über ihr Outsourcing-Projekt unterrichteten, bat ich sie, mir die für eine datenschutzrechtliche Beurteilung des Vorhabens relevanten schriftlichen Vereinbarungen mit der Firma zukommen zu lassen. Dies entpuppte sich als ein äußerst mühsames Unterfangen. Auf mein erstes Schreiben reagierten die Städtischen Kliniken erst nach Mahnung; die von mir erbetenen und für eine sachgerechte da-

tenschutzrechtliche Beurteilung erforderlichen Unterlagen übersandten sie erst nach und nach im Laufe von Monaten. Immer wieder musste ich nachhaken. Einen weiteren Fauxpas leisteten sie sich dann durch die Art und Weise, wie sie meine umfangreiche Stellungnahme von Mitte Mai 1999 beantworteten, besser gesagt nicht beantworteten. Nachdem sie sich mit einer Antwort rund 2 Monate Zeit gelassen hatten, begnügten sie sich im Wesentlichen damit, lapidar mitzuteilen, dass die von mir kritisierten Punkte „soweit wie möglich“ behoben werden sollen, dass dies aber „noch einige Zeit in Anspruch nehmen wird“. Welche Punkte auf welche Weise behoben werden sollen, blieb damit ebenso unklar wie der zeitliche Rahmen, in dem dies geschehen soll. Zudem übersandten die Städtischen Kliniken wieder nicht die von mir erbetenen Unterlagen und waren damit zum wiederholten Male nicht willens oder in der Lage, mir die für eine sachgerechte Prüfung erforderlichen Unterlagen vollständig zur Verfügung zu stellen. Diese wiederholte Weigerung sowie die fehlende Bereitschaft, inhaltlich auf mein Schreiben einzugehen, stellte eine Brüskierung der Datenschutzkontrolle dar und verstieß eklatant gegen die auch den Städtischen Kliniken obliegende Pflicht, mich bei der Ausübung meiner Aufgaben zu unterstützen. Diesen Verstoß habe ich deshalb beanstandet. Erst Ende August 1999 und damit rund 10 Monate nach meinem ersten Schreiben lagen dann die – in der Zwischenzeit nachgebesserten – Unterlagen endlich vollständig vor!

Diese unschönen Begleitumstände vorausgeschickt sind nunmehr aber die eigentlichen inhaltlichen Aspekte und Defizite bei der Datenverarbeitung im Auftrag zu beleuchten:

Besonderes Gewicht für einen wirksamen Datenschutz kommt den beim Einsatz der EDV zu treffenden technischen und organisatorischen Sicherheitsmaßnahmen zu. Abgesehen von der Regelung, dass die Beschäftigten der Firma auf das Datengeheimnis zu verpflichten sind, sowie selbstverständlichen oder nichts sagenden Aussagen enthielt der im August 1997 zwischen den Städtischen Kliniken und der Firma abgeschlossene Vertrag keinerlei Festlegungen darüber, welche technische und organisatorische Sicherheitsmaßnahmen zu treffen sind! Diesen gravierenden Mangel habe ich ebenfalls beanstandet. Insbesondere in folgenden Punkten versäumten es die Städtischen Kliniken ausreichende Sicherheitsmaßnahmen zu vereinbaren; teilweise bestehen die Defizite immer noch:

3.3.1 Fehlendes Weisungsrecht

Bei einer Datenverarbeitung im Auftrag ist unerlässlich festzulegen, wer als Dirigent den Taktstock schwingt und wer Orchester ist. Es gilt: Die Mitarbeiter des Auftragnehmers dürfen nur entsprechend den Weisungen des Auftraggebers tätig werden. Schließlich bleibt der Auftraggeber als Daten verarbeitende Stelle in vollem Umfang für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Daher muss er die Richtung vorgeben und die Spielregeln definieren. Da ein solches Weisungsrecht aber nicht automatisch vom Himmel fällt, muss sich der Auftraggeber im Vertrag ein Weisungsrecht gegenüber dem Auftragnehmer einräumen lassen. Ein solches suchte man in der Beauftragung der Firma aber vergebens. Erst rund zwei Jahre später holten die Städtischen Kliniken Versäumtes nach.

3.3.2 Zugriff auf personenbezogene Daten nicht unterbunden

Ein wesentliches Ziel des Datenschutzes bei einer Datenverarbeitung im Auftrag ist, dass Mitarbeiter des Auftragnehmers auf personenbezogene Daten nur insoweit zugreifen können, wie dies zur Erfüllung des Auftrags tatsächlich erforderlich ist. Um die EDV-Systeme der Städtischen Kliniken zu betreiben, müssen die Mitarbeiter der beauftragten Firma aber nicht wissen, dass Frau X als Notfall in das Krankenhaus eingeliefert wurde, dass Herr Y sich einer Blinddarmoperation unterziehen musste und dass sich der Krankenhausaufenthalt von Herrn Z wegen akuter Darmbeschwer-

den verlängerte, was die Kosten des Aufenthalts von soundso viel DM erklärt. Dies alles zu wissen ist für die Mitarbeiter der Firma nicht erforderlich, um den Auftrag zu erfüllen. Für den Betrieb der Krankenhaus-EDV-Systeme benötigt die Firma in der Regel keinen Zugriff auf gespeicherte personenbezogene Daten, insbesondere keinen Zugriff auf die durch die ärztliche Schweigepflicht geschützten, besonders sensiblen Patientendaten. Dabei ist zu berücksichtigen, dass das Landeskrankenhausgesetz in dieser Frage die Anlegung eines besonders strengen Maßstabs verlangt. Mitarbeiter des Auftragnehmers dürfen danach nur aus zwingenden Gründen einen Zugriff auf Patientendaten erhalten.

Tatsächlich verfügte aber eine ganze Reihe von Firmenmitarbeitern über eine jederzeitige Zugriffsmöglichkeit auf gespeicherte Patientendaten; zehn Administratoren waren mit den umfassendsten SAP-Berechtigungen ausgestattet. Da diese Personen gleichzeitig auch noch mit den Aufgaben der Datenbankadministration betraut waren, besaßen sie damit de facto eine jederzeitige und uneingeschränkte Zugriffsmöglichkeit auf sämtliche von den Städtischen Kliniken gespeicherten Daten. Ich habe die Städtischen Kliniken aufgefordert, auf technische Weise – beispielsweise durch eine geeignete Abschottung oder durch eine Verschlüsselung der Daten – sicherzustellen, dass Mitarbeiter des Auftragnehmers nur dann auf gespeicherte Patientendaten zugreifen können, wenn dies zur Erfüllung der Vertragspflichten zwingend erforderlich ist. Gleichzeitig habe ich ihnen mitgeteilt, dass entsprechende Anforderungen wie bei den durch die ärztliche Schweigepflicht geschützten Patientendaten auch für sonstige personenbezogene Daten gelten, zumindest dann, wenn sie besonders schutzwürdig sind. Die Städtischen Kliniken haben mich bislang nicht wissen lassen, ob sie meiner Forderung nachkommen werden. Sie haben lediglich mitgeteilt, dass sie wegen der Jahr-2000-Umstellung erst Anfang nächsten Jahres in der Lage seien, zu diesem und anderen, noch offenen Punkten Stellung zu nehmen.

3.3.3 Fehlende Kontroll- und Prüfrechte durch den Auftraggeber

Damit der Auftraggeber nachprüfen kann, ob der Auftragnehmer auch tatsächlich seinen Pflichten nachkommt und so verfährt, wie es vereinbart ist, benötigt der Auftraggeber Kontrollrechte. Über diese verfügt er natürlich automatisch in seinen eigenen Räumlichkeiten, also im Krankenhaus, nicht dagegen in den Räumlichkeiten der beauftragten Firma. Aus diesem Grund wäre bei einem Vorhaben diesen Ausmaßes und den hiervon berührten personenbezogenen Daten unerlässlich gewesen, in dem mit der Firma abgeschlossenen Vertrag eine Kontrollbefugnis für den Auftraggeber oder von ihm beauftragte Revisoren aufzunehmen, die es ermöglicht, Kontrollen in den Betriebs- und Geschäftsräumen des Auftragnehmers durchzuführen. Festzulegen wäre dabei gewesen, welche Personen Prüfungen durchführen dürfen, wann sie der Firma eine bevorstehende Prüfung ankündigen müssen, wie sie Zugang zu den Betriebs- und Geschäftsräumen der Firma erhalten und in welchem Umfang sie im Rahmen der Vor-Ort-Prüfung tätig werden dürfen. All dies unterblieb freilich. Inzwischen haben die Städtischen Kliniken nachgebessert und den Mangel abgestellt.

3.3.4 Schutz des Krankenhausnetzwerks unzureichend

Eine ausreichende Abschottung des Computernetzwerks der Städtischen Kliniken gegenüber unerwünschten Eindringlingen von außen ist eine wichtige Sache. Ganz gegenüber der Außenwelt abschotten können die Städtischen Kliniken ihr Netzwerk natürlich nicht, denn ansonsten würde allein schon die Datenkommunikation zwischen Esslingen und Dresden nicht mehr funktionieren. Es gilt also das richtige Maß zu finden. Ich habe den Städtischen Kliniken dargelegt, in welchen Punkten die bisher vorgesehenen Maßnahmen unzureichend sind und gleichzeitig Vorschläge unter-

breitet, auf welche Weise sich ein ausreichender Schutz erreichen ließe.

3.3.5 Fortschreibung der technischen und organisatorischen Maßnahmen

Getroffene technische und organisatorische Sicherheitsmaßnahmen sind keine einmal festzulegende Größe, die dann zur Salzsäule erstarren und nicht mehr geändert werden sollten. Genau das Gegenteil ist richtig. Im Sinne eines wirksamen Datenschutzes ist unerlässlich, die Sicherheitsmaßnahmen von Zeit zu Zeit auf den Prüfstand zu stellen und sie gegebenenfalls anzupassen. Anpassungen können erforderlich sein, weil sich etwa die eingesetzte Technik verändert hat oder weil mittlerweile noch wirksamere Sicherheitsmaßnahmen verfügbar sind. Im Falle bekannt gewordener neuer Sicherheitslücken ist darüber hinaus sogar eine unverzügliche Reaktion notwendig. Richtig war daher, dass der zwischen den Städtischen Kliniken und der Firma abgeschlossene Vertrag eine Weiterentwicklung der vorgegebenen Sicherheitsmaßnahmen vorsah. Problematisch war aber die Art und Weise, wie dies geschah. Ursprünglich räumten die Städtischen Kliniken der Firma das Recht ein, die Sicherheitsmaßnahmen dem Stand der Technik anzupassen. Weder war dabei aber eine Beteiligung der Städtischen Kliniken vorgesehen noch musste die Firma das Krankenhaus über das, was sie im Einzelnen veränderte, unterrichten, noch die Änderungen schriftlich dokumentieren. Die Befugnis, die die Städtischen Kliniken der Firma einräumte, ging damit viel zu weit. Schließlich ist der Auftraggeber in vollem Umfang für einen wirksamen Datenschutz verantwortlich und muss daher bei der Umsetzung von Sicherheitsmaßnahmen erstens ein Wörtchen mitzureden haben und zweitens wissen, was getan wird. Ich habe den Städtischen Kliniken daher vorgeschlagen, vertraglich zu vereinbaren, dass der Auftragnehmer Vorschläge zur Verbesserung der technischen und organisatorischen Sicherheitsmaßnahmen nach dem Stand der Technik unterbreitet. Änderungen sollen dabei jedoch der vorherigen Zustimmung durch den Auftraggeber bedürfen, sind sodann schriftlich zu dokumentieren und als Vertragsbestandteil zu vereinbaren. Inzwischen erfolgte eine Vertragsanpassung, leider aber in einer unzureichenden Weise. Festgelegt ist nunmehr, dass die getroffenen Sicherheitsmaßnahmen dem Stand der Technik angepasst und dem Auftraggeber zur Kenntnis gebracht werden. Bei kleinen Veränderungen mag dies ja noch angehen. Nicht hinnehmbar ist jedoch, dass der Auftragnehmer nach wie vor berechtigt ist, auch gravierende Änderungen vorzunehmen, ohne sich mit dem Auftraggeber abstimmen oder von diesem eine Genehmigung einholen zu müssen.

3.3.6 Unzureichende Verschlüsselung auf dem Übertragungsweg

Verschlüsselung ist eine wichtige Maßnahme, um für einen ausreichenden Schutz von Daten auf dem Transportweg zu sorgen. Zu begrüßen ist daher, dass die Übertragung der auf den Leitungen zwischen Esslingen und Dresden transportierten Daten verschlüsselt erfolgt. Die Art der Verschlüsselung (DES) und die auf Grund von US-amerikanischen Exportbeschränkungen reduzierte Schlüssellänge des Verfahrens (40 bits), welches die erreichbare Sicherheit noch einmal schmälerte, entsprachen aber nicht dem Stand der Technik und boten nicht das für eine Übertragung sensibler personenbezogener Daten notwendige Sicherheitsniveau. In ihrer Antwort verwiesen die Städtischen Kliniken darauf, dass die Verschlüsselung dem in Europa freigegebenen Standard entspräche. Sie übersahen dabei freilich, dass die Kryptografie in Deutschland nicht reglementiert ist und daher hier zu Lande auch sichere Verschlüsselungsverfahren, die dem Stand der Technik entsprechen, eingesetzt werden dürfen.

3.3.7 Weitere technische und organisatorische Mängel

Schließlich musste ich noch eine ganze Reihe weiterer technischer und organisatorischer Defizite bemängeln. Selbst der Passwortschutz blieb dabei nicht außen vor. Die Umsetzung der allgemein bekannten und anerkannten Regelungen zum Umgang mit Passwörtern müssten bei einem Projekt dieser Bedeutung und Sensibilität eigentlich aber eine Selbstverständlichkeit sein.

4. Nutzung von Internet und Intranets

Internet und Intranets boomen nach wie vor. Entsprechend groß ist die Facette datenschutzrelevanter Fragestellungen, mit denen sich mein Amt auch in diesem Jahr befassen musste.

4.1 Hacker-Angriffe – nicht nur eine theoretische Gefahr

Berichte über Hacker-Angriffe auf Computer der Universität Tübingen waren für uns Anlass, vor Ort zu ermitteln, was vorgefallen war und wie dies aus datenschutzrechtlicher Sicht zu bewerten ist.

Was war geschehen?

Einem Hacker war es gelungen, über das Internet auf einen Computer des Universitätsrechenzentrums, vier Computer der Fakultät Mathematik sowie eine nicht genau bekannte Zahl weiterer Computer anderer Fakultäten zuzugreifen und dort umfassende Systemverwalterberechtigungen zu erlangen. Dabei war er sehr systematisch vorgegangen:

– Im ersten Schritt spürte er etliche Computer auf, die mit einem Betriebssystem ausgestattet waren, das eine Sicherheitslücke aufwies. Da Computer ganz unterschiedlicher Einrichtungen betroffen waren, erscheint es eher unwahrscheinlich, dass es sich jeweils nur um Zufallstreffer handelte. Denkbar ist, dass der Hacker zum Aufspüren der angreifbaren Computer ein Programm einsetzte, das ganze Teilnetze des Internet und der daran angeschlossenen Intranets systematisch daraufhin untersuchen kann, welche Betriebssysteme und sogar welche Versionen dieser Betriebssysteme auf den an diesen Teilnetzen angeschlossenen Computern eingesetzt werden.

– Nach dem Aufspüren der angreifbaren Computer verschaffte sich der Angreifer in einem zweiten Schritt umfassende Systemverwalterberechtigungen auf diesen Systemen und installierte dort ein frei erhältliches Hacker-Programm. Einmal installiert, lieferte es dem Hacker quasi eine Tarnkappe, indem es die vom Hacker angelegten Dateien so im System versteckte, dass sie normalerweise einem Systemverwalter nicht auffallen und schon gar nicht gewöhnlichen Benutzern. Auch andere Spuren, die ansonsten jeder Benutzer während seiner Aktivitäten am Computer hinterlässt, werden von diesem Programm gezielt unterdrückt. Neben dieser Tarnkappenfunktion bot das Hacker-Programm auch noch eine Schnüffelfunktion: Es gestattete, den gesamten Datenverkehr im lokalen Netzwerk der Universität, an das der gehackte Computer angeschlossen war, rund um die Uhr abzuhören. Wann immer sich jemand über das lokale Netz an einem anderen Computer anmeldete oder auf sein elektronisches Postfach zugriff, speicherte das Hacker-Programm jeweils die anfangs dabei übertragenen Daten. Darunter befanden sich auch Benutzerkennungen und im Klartext übertragene Passwörter. Der Hacker konnte sich diese dann, wann immer er wollte, ansehen und so Benutzerkennungen und Passwörter erfahren, die ihm einen Zugriff auch auf Computer ermöglichten, deren Betriebssystem nicht den ursprünglich ausgenutzten Fehler aufweist.

Auf diese Weise war es ihm möglich, gewissermaßen nach dem Domino-Prinzip Zugriff auf immer mehr Computer zu erlangen. Da die Spuren der Hacker-Angriffe beim Kontrollbesuch zum Teil bereits wieder beseitigt waren, blieb es im Dunklen, auf wie viele Computer der Hacker letztlich hätte zugreifen können. Bedenkt man aber, dass bereits eine auf einem angegriffenen Computer gespeicherte Protokolldatei

Informationen über ca. 500 Verbindungen enthielt, so wird erkennbar, dass dem Hacker unter dem Strich die von zahlreichen Benutzern gespeicherten Informationen auf dem Präsentierteller geliefert wurden. Da auf den Computern der Universität auch personenbezogene Daten in vielfältiger Form, beispielsweise in elektronischer Post, gespeichert waren, war der Hacker-Angriff datenschutzrelevant. Folgende Mängel waren im Zusammenhang mit dem Hacker-Angriff festzustellen:

4.1.1 Mängel, die den Angriff erst ermöglichten

Zwei gravierende technische Sicherheitslücken haben den Hacker-Angriff in dieser Form erst möglich gemacht: Der Betrieb von Computern mit fehlerhaftem Betriebssystem und die Nutzung von Programmen, die Benutzerkennungen und Passwörter im Klartext über Netz übertragen.

– Daran, dass Betriebssysteme, wie andere Programme auch, Fehler enthalten, die erst nach und nach bekannt werden, können Anwender in der Regel nichts ändern. Umso wichtiger ist es aber, dass Daten verarbeitende Stellen, vor allem wenn sie die EDV so intensiv nutzen wie eine Universität, organisatorische Vorkehrungen treffen, um nach Bekanntwerden von Sicherheitslücken schnell reagieren zu können. Daran mangelte es jedoch bei der Universität Tübingen.

– Anders sieht es beim Einsatz der Produkte aus, die Passwörter im Klartext übertragen. Hier gibt es vielfach gleichwertige Alternativen, die Passwörter nicht im Klartext übertragen, sondern ein kryptografisch gesichertes Anmeldeverfahren nutzen. Nach Bekanntwerden der Hacker-Angriffe begannen einige Universitätseinrichtungen mit dem Einsatz solcher Produkte. Da dies eine wichtige Maßnahme zur Vermeidung des beschriebenen Domino-Effekts ist, habe ich die Universität aufgefordert, den Einsatz solcher Produkte weiter zu forcieren. Dem will sie nachkommen.

4.1.2 Mängel beim Erkennen und Verfolgen der Hacker-Angriffe

Die Universität hatte nicht genug getan, um Hacker-Angriffe zeitnah erkennen und verfolgen zu können.

– Rasche Reaktion nicht gewährleistet

Nachdem studentische Mitarbeiter des von den Hacker-Angriffen mitbetroffenen Fachbereichs Mathematik nach entsprechenden Hinweisen einer ausländischen Universität feststellten, dass zwei von ihnen betreute Computer angegriffen worden waren, benachrichtigten sie umgehend die Administratoren anderer Computer. In einigen Fällen unterblieb jedoch diese Meldung, da sie nicht wussten, wer die Computer betreut. Nicht einmal beim Universitätsrechenzentrum gab es eine Liste der EDV-Verantwortlichen der einzelnen Fakultäten und Institute. Zudem stellte sich heraus, dass ein anderer Fachbereich bereits zwei Wochen zuvor Hinweise über Hacker-Angriffe auf die Universität Tübingen erhalten hatte, ohne davon das Universitätsrechenzentrum oder andere Universitätseinrichtungen zu informieren. Ganz offenbar wurden auf Grund unzureichender organisatorischer Vorkehrungen die sicherheitsrelevanten Informationen über Hacker-Angriffe nicht gleich an alle für die Systemsicherheit verantwortlichen Uni-Mitarbeiter weitergeleitet. So gewann der Hacker mehrere Tage Zeit, in denen er sein Tun ungehindert fortsetzen und Daten der Universität ausspähen konnte. Um in solchen Fällen künftig besser gewappnet zu sein, forderte ich die Universität auf, einen Alarmplan auszuarbeiten, dem jeder Systemverwalter entnehmen kann, was er im Fall eines entdeckten Hacker-Angriffs zu tun hat und insbesondere, wen er in einem solchen Falle unterrichten muss. Außerdem schlug ich – um im Falle eines Falles nicht erst lange nach den

richtigen Ansprechpartnern suchen zu müssen – die Einrichtung einer Liste vor, in der die Systemverwalter aller Universitätseinrichtungen genannt sind. Die Universität kam dem nach, erarbeitete einen Alarmplan und richtete eine Mailing-Liste ein, die zum Informationsaustausch über sicherheitsrelevante Ereignisse dient.

– Zu wenig Personal für Fragen der IT-Sicherheit

Im Universitätsrechenzentrum, das ca. 300 eigene Computer betreibt und die betriebsfachliche Aufsicht über alle ca. 8500 Computer der Universität zu führen hat, wurden die Fragen der IT-Sicherheit von einem Mitarbeiter bearbeitet, der daneben aber auch noch andere Aufgaben wahrzunehmen hat. Zu seinen sicherheitsbezogenen Aufgaben gehört unter anderem,

- aktuelle Meldungen über Sicherheitslücken zu verfolgen,
- die Fakultäten und Institute in Fragen der IT-Sicherheit zu beraten,
- die uni-interne Mailing-Liste zum Thema IT-Sicherheit zu betreuen,
- an der Erarbeitung und Umsetzung von Sicherheitskonzeptionen mitzuwirken,
- sicherheitsrelevante Ereignisse im Bereich der Universität zu untersuchen sowie
- das Geräte- und Verfahrensverzeichnis des Rechenzentrums zu führen.

Ein Mitarbeiter, der zudem auch noch andere Aufgaben wahrzunehmen hat, dürfte kaum in der Lage sein, all dies zu schultern. Ein ähnliches Bild zeigte sich an den Fakultäten: Bis auf die Informatik setzten alle anderen Fakultäten lediglich studentische Hilfskräfte zur Computerbetreuung ein. Da diese jeweils nur 10 bis 20 Stunden pro Woche arbeiteten, war nicht einmal während der regulären Arbeitszeiten sichergestellt, dass vor Ort stets ein Systemverwalter zu erreichen war. Um hier eine Verbesserung zu erzielen, habe ich angeregt, eine Personalbedarfsanalyse durchzuführen und sie zur Grundlage einer bedarfsgerechten Personalausstattung zu machen. Die Universität sieht sich hierzu allerdings nicht in der Lage. Dies sollte aber noch nicht das letzte Wort gewesen sein.

– Computerbetreuung – Theorie und Wirklichkeit

Dem Universitätsrechenzentrum obliegt, so will es das Universitätsgesetz, „die Betreuung aller der Universität verfügbaren Datenverarbeitungskapazitäten und die betriebsfachliche Aufsicht über alle Rechenanlagen in der Universität“. Trotz dieses unmissverständlichen Wortlauts sah es das Rechenzentrum nicht als seine Aufgabe an, alle Computer der Uni zu betreuen und für sie die betriebsfachliche Aufsicht zu übernehmen. Es mag nun dahingestellt sein, ob es organisatorisch stets die beste Lösung ist, die Verantwortung für alle Universitätscomputer dem Rechenzentrum zuzuweisen. Entscheidend ist aber, dass es eine klare Regelung der Verantwortlichkeiten für die Betreuung und die betriebsfachliche Aufsicht über die Computer der Universität geben muss, denn dies stellt eine grundlegende Voraussetzung dafür dar, dass die Universität ausreichende technische und organisatorische Schutzmaßnahmen für alle automatisierten Verfahren ergreift, mit denen personenbezogene Daten verarbeitet werden. Unzulänglich war daher in jedem Fall, dass auf dem Papier eine klare Verantwortlichkeitsregelung getroffen war, die jedoch in der Praxis nicht angewandt wurde. Die Universität will es jedoch gleichwohl beim Status quo belassen. Bleibt zu hoffen, dass sich im weiteren Gespräch hierüber noch eine Wendung ergibt.

4.2 Was muss der Provider tun?

Neben ihrer lange Zeit eigentlichen Domäne, nämlich dem Betrieb von Großrechneranwendungen und Datennetzen, beschäftigen sich viele Rechenzentren inzwischen intensiv mit dem Thema Internet. So auch das Rechenzentrum Region Stuttgart des Zweckverbands Regionale Datenverarbeitung Region Stuttgart (KDRS/RZRS), das als Internet-Provider seinen Kunden, wie Städten oder Gemeinden, den Zugang zu dem weltweiten Datennetz ermöglicht. Bei einem Besuch überprüften wir die dabei getroffenen Sicherheitsmaßnahmen und stellten Folgendes fest:

- Durch eine Firewall schottete das Rechenzentrum das von ihm betriebene regionale Datennetz vom Internet ab. Dabei konnte jeder, der an einem für die Internet-Nutzung freigeschalteten PC arbeiten durfte, sämtliche für diesen PC freigegebenen Internet-Dienste nutzen, auch wenn er gar nicht alle für die Erledigung seiner dienstlichen Aufgaben benötigt und die umfassende Nutzungsmöglichkeit ihm deshalb gar nicht hätte eingeräumt werden dürfen. Eine Möglichkeit, nach Nutzern zu differenzieren, bestand nicht. Ich habe daher das Rechenzentrum aufgefordert, die Firewall so einzurichten, dass eine solche Differenzierung möglich ist. Das Rechenzentrum hat inzwischen mitgeteilt, es werde eine benutzerbezogene Steuerung für die Kunden umsetzen, die dies ausdrücklich wünschen.
- Das Rechenzentrum vermittelt nicht nur die Auffahrt auf das weltweite Internet, sondern hält auch eigene Informationsangebote zum Abruf im Internet bereit. Diese Angebote speicherte das Rechenzentrum auf seinem Firewall-Rechner. Ein wichtiger Grundsatz bei der Gestaltung einer Firewall-Lösung besagt aber, dass der Firewall-Rechner nur für die Aufgaben eingesetzt werden sollte, die er unbedingt erbringen muss. Dies sind im Wesentlichen die Filterung und Weiterleitung von Datenpaketen sowie die Protokollierung, nicht dagegen die Speicherung von Angeboten. Je weniger Aufgaben ein Rechner erbringen muss, desto weniger Programme sind auf ihm zu installieren mit der Folge, dass der Firewall-Administrator den Rechner besser überwachen kann. Je weniger Programme auf dem Firewall-Rechner ablaufen, desto geringer wird auch die Gefahr von Programmfehlern, die im schlimmsten Fall dazu führen können, dass mehr Daten als erlaubt zwischen dem regionalen Datennetz und dem Internet fließen. Inzwischen speichert das Rechenzentrum seine Internet-Angebote auf einem separaten Rechner.
- Sofern ein Firewall-Rechner nicht ausschließlich lokal vor Ort, sondern auch aus der Ferne administriert wird, sollten die über Datenleitung ausgetauschten Administrationsdaten aus Sicherheitsgründen generell verschlüsselt übertragen werden. Beim KDRS/RZRS war dies nicht der Fall. Inzwischen hat es eine Verschlüsselungslösung in Aussicht gestellt.
- Ein ordentliches schriftliches Sicherheitskonzept ist unverzichtbar, wenn es um die mit erheblichen Risiken für den Datenschutz und die Datensicherheit einhergehende Anbindung an das Internet geht. Aus dem Sicherheitskonzept müssen der vorgesehene Nutzungsumfang, die mit der Anbindung einhergehenden Risiken und die zur Beseitigung der Risiken erforderlichen Sicherheitsmaßnahmen hervorgehen. Zwar verfügte das Rechenzentrum über ein schriftliches Sicherheitskonzept. Dieses war aber unvollständig und teilweise fehlerhaft. Sein Nutzwert war daher eingeschränkt. Diesen Mangel habe ich beanstandet. Das Rechenzentrum hat Abhilfe zugesagt.

4.3 Was muss der Anwender beachten?

Wer sein eigenes Computernetzwerk über einen Provider an das Internet anschließen möchte, darf sich nicht nur auf die vom Provider getroffenen Sicherheitsmaßnahmen verlassen. Eigene Anstrengungen

sind unverzichtbar. Diese können jedoch umso geringer ausfallen, je mehr Sicherheit der Provider bietet. Einem Landkreis habe ich, als ich vom Personalrat eines Kreiskrankenhauses gebeten wurde, mich zu den datenschutzrechtlichen Aspekten einer solchen Anbindung zu äußern, Folgendes mitgeteilt:

– Die Nutzung des Internet-Dienstes World Wide Web kann dazu führen, dass ohne Zutun des Nutzers Programme auf den eigenen PC geladen werden und dort ablaufen (sog. ActiveX-Controls oder Java Applets). Klar, dass damit Sicherheitsrisiken einhergehen, weil ein solch fremdes Programm natürlich auch Schaden stiftende Funktionen enthalten kann. Zur Begrenzung der Risiken verfügt die Java-Technologie – anders als ActiveX – über eine Sicherheitsarchitektur, deren Umsetzung in der Vergangenheit jedoch immer wieder zu wünschen übrig ließ. Da in aller Regel zentrale Firewall-Lösungen ActiveX-Controls und Java Applets nicht herausfiltern, gilt für den Anwender die Devise: Er selbst muss die PC, die über einen Zugang zum Internet verfügen, sicher konfigurieren. Die ActiveX-Unterstützung sollte er gänzlich abschalten; ein restriktiver Umgang empfiehlt sich auch bei Java.

  Weitere Gefahren drohen auch durch JavaScript. Hierbei können JavaScript-Befehle in die WWW-Seite eingebaut werden, die ausgeführt werden, sobald der Nutzer die Seite aufruft. Es empfiehlt sich, die JavaScript-Unterstützung im Browser abzuschalten, wenn im Internet gearbeitet wird.

– Dateiverzeichnisse dürfen nicht für einen Zugriff über das Netz freigegeben werden. Unverzichtbar ist zudem, für einen ausreichenden Virenschutz zu sorgen, auch wenn der Provider entsprechende Vorsorge betreibt. Denn verschlüsselte elektronische Post kann der Provider natürlich nicht auf Viren überprüfen. Das ist erst nach der Entschlüsselung der elektronischen Post beim Adressaten möglich.

– Unverzichtbar ist schließlich, dass nur solche Beschäftigte Zugang zu Internet-Diensten erhalten, die über die mit der Nutzung des Internet einhergehenden Risiken und erforderlichen Sicherheitsmaßnahmen ausreichend unterrichtet sind. Denn nur wenn ein ausreichendes Sicherheitsbewusstsein vorhanden ist, kann davon ausgegangen werden, dass die Nutzer selbst ihrerseits das Erforderliche beachten und tun.

5. Privatsphäre und Computertechnik

Computer sind aus dem Berufsalltag und zunehmend auch aus dem privaten Bereich nicht mehr wegzudenken. Texte mit dem PC zu schreiben oder Adressen zu verwalten, ist heutzutage für Viele selbstverständlich. Der Anschluss an das Internet eröffnet zusätzliche Möglichkeiten: Der Austausch elektronischer Post, E-Commerce, die Erledigung von Bankgeschäften oder der Abruf von Informationen erschließen weitere Lebensbereiche. Bei allen diesen elektronischen Aktivitäten die Privatsphäre der Nutzer zu wahren, ist ein wichtiges Anliegen des Datenschutzes. Dazu gehört, dass der Nutzer weiß, wann welche Angaben dabei über ihn anfallen, wie sie verarbeitet werden sollen und was er selbst tun kann, um solche persönlichen Datenspuren zu vermeiden oder deren Umfang zumindest zu begrenzen. In der Praxis macht dies freilich Mühe. Die moderne Hard- und Software präsentiert sich demjenigen, der von ihren vielfältigen Möglichkeiten Gebrauch machen will, häufig als bunte Fassade mit einem Konglomerat aus ansprechenden Schriftarten, komfortabler Mausbedienung, vielen Masken und unzähligen Einstellmöglichkeiten. Den Überblick darüber zu behalten, welche Einstellungen denn nun für die Privatsphäre relevant sind und an welcher Schraube wie zu drehen ist, um sie möglichst gut zu wahren, fällt allein schon auf Grund des großen Funktionsumfangs der Produkte oft nicht leicht. Hinzu kommt, dass immer wieder Produkte entwickelt und am Markt angeboten werden, deren Abläufe selbst für Fachleute, geschweige denn für die breite Masse der Nutzer, die keine EDV-

Spezialisten sind, kaum nachvollziehbar sind. Wie schwer es ist, Spuren zu vermeiden, illustrieren folgende Beispiele:

5.1 Was Texte so alles verraten können

Ein brauchbares Textverarbeitungsprogramm gehört zur Grundausstattung eines jeden Computerarbeitsplatzes, ob im Büro oder zu Hause. Wer Texte erstellt, konzentriert sich in aller Regel auf den Inhalt und ist froh, wenn sie endlich seinen Vorstellungen entsprechen. Textdokumente können aber weit mehr Informationen enthalten als das, was sich schwarz auf weiß dem Ausdruck entnehmen lässt. So können Textdokumente, die mit dem weit verbreiteten Textverarbeitungsprogramm Word 97 erstellt werden, einiges über ihren Ersteller und ihre Entstehungsgeschichte verraten. Problematisch kann dies bei der Weitergabe eines Textes oder dessen Veröffentlichung, beispielsweise im Internet, sein, weil die Adressaten Interna, die über den reinen Textinhalt hinausgehen, in aller Regel nichts angehen:

– Autorenname:

In Word lässt sich ein Autorenname hinterlegen, der, einmal eingegeben, mit jedem neu erstellten Word-Textdokument verknüpft wird. Bei der Weitergabe eines Textes oder seiner Veröffentlichung kann freilich unerwünscht sein, dass der Empfänger oder derjenige, der den Text abruft, sogleich auch den Namen des Autors erfährt. Das lässt sich verhindern, wenn der Ersteller des Textes vor der Weitergabe oder vor der Veröffentlichung den mit diesem Text verknüpften Autorennamen verändert, indem er ihn mit einer nicht sprechenden Zeichenkette belegt, die keinen Personenbezug aufweist. Weil dies leicht einmal vergessen werden kann, kann man auch den Autorennamen in Word von vornherein mit einer nicht sprechenden Zeichenkette belegen.

– Diverse Angaben zum Textdokument:

Wer ein Word-Textdokument erhält, kann abrufen, wann das Textdokument erstellt und wann es zuletzt geändert, geöffnet und gedruckt wurde. Zudem lässt sich abrufen, wie oft die Datei gespeichert wurde und wie viele Minuten sie zur Bearbeitung geöffnet war. Diese Angaben verraten einiges über die Entstehung des Textdokuments. Die Anzahl der Dateispeicherungen lässt z. B. einen Rückschluss zu, wie häufig der Ersteller über dem Text gebrütet und ihn überarbeitet hat. Verändern oder löschen kann der Nutzer diese Angaben nicht. Wer bei der Weitergabe oder der Veröffentlichung eines Textes dem Bekanntwerden dieser Interna vorbeugen will, dem bleibt deshalb nichts anderes übrig, als das Textdokument unter einem neuen Namen zu speichern. Die Angaben, wann das Textdokument erstellt und wann es zuletzt geändert und geöffnet wurde, werden dabei aktualisiert. Zudem wird die Anzahl der Dateispeicherungen zurückgesetzt.

– Änderungsfunktion:

Die sog. Änderungsfunktion kann nützlich sein, wenn mehrere Personen an der Erstellung eines Textes mitwirken. Wird sie eingeschaltet, so lässt sich dem Textdokument entnehmen, wer wann welche Textpassage eingegeben hat. Was im Rahmen eines internen Dienstbetriebs durchaus sinnvoll sein kann, wird bei der Weitergabe eines Textes an eine andere Stelle oder bei dessen Veröffentlichung freilich problematisch, weil den Empfänger in aller Regel nichts angeht, auf welche Weise der Text entstanden ist. Hier hilft: Die Änderungsfunktion ausschalten und den Textinhalt in ein neues Textdokument kopieren. Denkbar ist natürlich auch, die Änderungsfunktion von vornherein erst gar nicht einzuschalten.

– Textversionen:

Insbesondere dann, wenn ein Autor an langen oder komplizierten Texten feilt, ist er mitunter froh darüber, dass er mit Word mehrere unterschiedliche Versionen eines Textes in einem einzigen Textdokument gemeinsam verwalten kann. Will er den Text weiterbearbeiten, so

kann er sich zunächst die unterschiedlichen Textversionen am Bildschirm anzeigen lassen. Um den Überblick zu behalten, werden zu jeder Version automatisch Datum und Uhrzeit der Erstellung angezeigt. Zudem kann der Ersteller jede Textversion noch mit einem Kommentar versehen, der hilfreich sein kann, um zu erkennen, worin sich die Textversionen denn nun im Einzelnen unterscheiden. Hat der Ersteller schließlich dem Text den letzten Schliff gegeben, so sollte er vor dessen Weitergabe oder Veröffentlichung tunlichst darauf achten, nur die aktuelle Version beizubehalten und die anderen zu löschen. Ansonsten würde er nämlich neben der endgültigen Fassung des Textes auch gleich noch dessen Rohversionen mitliefern.

– Verborgene Informationen:

Wer sein Word-Textdokument mit Hilfe eines sog. ASCII-Editors genauer unter die Lupe nimmt, kann einige Überraschungen erleben. Denn in Word-Textdokumenten können auch Angaben enthalten sein, die bei der regulären Bearbeitung des Textes mit Hilfe von Word nicht am Bildschirm angezeigt werden und die im Text nichts zu suchen haben. Dazu gehören die Namen der Rechner und Verzeichnisse, auf denen und in denen die Datei gespeichert wurde. Schon dies kann unerwünscht sein, weil es Aufschluss über die interne Organisation der Datenverarbeitung gibt. Aber es gibt noch Gravierenderes: Wer eine Textpassage löscht, geht selbstverständlich davon aus, dass sie nicht mehr im Textdokument gespeichert ist. Schließlich wird sie ja auch nicht mehr am Bildschirm angezeigt. Bereits gelöschte Textteile können aber nach wie vor im Textdokument gespeichert sein.

Um dem vorzubeugen, sollte der Nutzer die sog. Schnellspeicherungsfunktion abschalten. Alle Probleme beseitigt dies freilich nicht. Wer vor der Weitergabe oder der Veröffentlichung eines Textes auf Nummer sicher gehen will, dass keine unerwünschten Angaben im Textdokument enthalten sind, dem bleibt nicht anderes übrig, als den Text mit Hilfe eines ASCII-Editors akribisch zu untersuchen. Stellt er dabei Unerwünschtes fest, dann sollte er den Text in einem anderen Dateiformat abspeichern. Ein voller Erfolg ist damit freilich nicht garantiert.

5.2 Die eindeutigen Nummern

Die Privatsphäre ist nicht nur dann tangiert, wenn der Nutzer Angaben hinterlässt, die ihn unmittelbar identifizieren, wie etwa seinen Namen, Vornamen und seine Anschrift. Sie kann auch schon dann berührt sein, wenn er eine eindeutige Nummer hinterlässt, auch wenn diese, für sich allein genommen, keinen Rückschluss auf eine bestimmte Person ermöglicht. Denn wer einmal davon erfährt, welche Person welche Nummer verwendet, der kann in zukünftigen Fällen, auch wenn er nur die Nummer erhält, auf den Nutzer rückschließen. Solche eindeutigen Nummern gerieten dieses Jahr gleich zweimal in die Schlagzeilen:

– Seit Anfang dieses Jahres sind Personal Computer erhältlich, die mit dem neuen Prozessor Pentium III bestückt sind. Bereits bei der Herstellung wird dieser Prozessor mit einer eindeutigen Seriennummer versehen, die sich mit Hilfe von Programmbefehlen auch wieder auslesen und über Datennetze übermitteln lässt. Datenschützer übten weltweit teilweise scharfe Kritik an dieser Seriennummer; die Proteste gipfelten sogar in Boykottaufrufen einzelner US-amerikanischer Datenschutzgruppen. Anlass für die Kritik war die Befürchtung, dass eine solche eindeutige Seriennummer, die den Prozessor und damit den PC identifiziert, sich auch dazu verwenden lässt, Nutzerprofile zu erstellen. Denn wem einmal die Zuordnung zwischen einer eindeutigen Nummer und einer Person bekannt wird, weil etwa der Nutzer auf einer Internet-Seite seinen Namen hinterlässt, um Informationsmaterial anzufordern, der kann in zukünftigen Fällen allein anhand der Nummer auf die Person rückschließen. Stand der Dinge ist nunmehr, dass sich das Auslesen der Seriennummer wenigstens abschalten lässt; PC-Hersteller können ihre Computer auch gleich in diesem Zustand ausliefern.

– Kaum flaute die Diskussion um den Pentium III-Prozessor ab, kam anderes im Zusammenhang mit dem Computerbetriebssystem Windows 98 ans Licht. Der Hersteller dieser Software bietet den Anwendern die Möglichkeit, das Produkt entweder auf herkömmliche Weise per Post oder auch online registrieren zu lassen. Wer davon Gebrauch macht, den unterrichtet der Hersteller beispielsweise über Progammverbesserungen. Bei der Online-Registrierung wurde neben den eigentlichen Registrierungsinformationen auch gleich noch eine bei der Installation des Betriebssystems erzeugte eindeutige Nummer, die den zugehörigen PC identifiziert, heimlich an den Hersteller übertragen. Nachdem dieser Umstand in der Öffentlichkeit bekannt wurde und für einigen Wirbel sorgte, überarbeitete der Hersteller sein Registrierungsprogramm so, dass die eindeutige Nummer nicht mehr heimlich übertragen wird.

  Dies war aber noch nicht alles. Auch weitverbreitete Standardprogramme des gleichen Herstellers, wie das Textverarbeitungsprogramm Word oder das Tabellenkalkulationsprogramm Excel, können eindeutige Nummern erzeugen und in Dokumenten, die mit diesen Programmen erstellt wurden, speichern. Nun liegt es bei der Weitergabe oder der Veröffentlichung eines mit Word geschriebenen Textes oder einer mit Excel erzeugten Tabelle aber beileibe nicht im Interesse eines Dokumentenerstellers, dem Empfänger stets eine eindeutige Nummer mitzuliefern, durch die er unmittelbar auf den PC, auf dem das Dokument erstellt wurde, und unter Umständen auch auf den Ersteller rückschließen kann, auch wenn aus der erhaltenen Datei selbst nicht hervorgeht, wer sie erstellte. Inzwischen bietet der Hersteller ein Korrekturprogramm an, das verhindert, dass die Nummer in den Dokumenten gespeichert wird. Ein zweites löscht die Nummer aus bereits erstellten Dokumenten. Datenschutzbewussten Anwendern ist zu raten, von diesen Programmen rege Gebrauch zu machen.

5.3 Was ist vonnöten?

Um im Zeitalter der Vernetzung den gläsernen Nutzer zu verhindern, der nicht mehr überblickt, wer über welche Informationen über ihn verfügt, ist zweierlei unverzichtbar: Computersysteme sollten von vornherein so konstruiert sein, dass möglichst keine oder so wenig Datenspuren wie möglich über die Nutzer anfallen (vgl. 18. Tätigkeitsbericht 1997, Landtags-Drucksache 12/2242, S. 11 ff.). Da dies leider nur allzu häufig nicht der Fall ist, erlangt besondere Bedeutung, dass der Nutzer nachvollziehen kann, wann welche Angaben über ihn anfallen, gespeichert oder über Datennetze übertragen werden sollen. Nur dann ist er in der Lage, auch selbst steuernd in die Datenverarbeitung einzugreifen und beispielsweise einer vorgesehenen Übertragung persönlicher Angaben über das Internet einen Riegel vorzuschieben. Transparenz über die in den Computersystemen aus Hard- und Software ablaufenden datenschutzrelevanten Vorgänge ist also das Gebot der Stunde. Hinzu kommen müssen Sicherheitsfunktionen, die es dem Nutzer ermöglichen, die Zügel selbst in die Hand zu nehmen und seine Privatheit in dem von ihm gewünschten Maße zu schützen. Voraussetzung für all dies sind freilich entsprechende marktgängige Produkte. Die Datenschutzbeauftragten des Bundes und der Länder haben diese wichtige Thematik zum Anlass genommen, in einer Entschließung die Entwicklung und den Einsatz derartiger Hardware und Software zu fordern (vgl. Anhang 14). Bleibt zu hoffen, dass sich die Datenschutzfreundlichkeit von Produkten mehr und mehr zu einem Wettbewerbsfaktor entwickelt.

6. Technische und organisatorische Mängel – ein Streifzug durch die Praxis

Es ist manchmal schon recht ernüchternd, wenn wir bei unseren Kontrollen vor Ort immer wieder die gleichen, auch in unseren Tätigkeitsberichten schon wiederholt beschriebenen Mängel feststellen müssen. Ganz besonders treffen wir solche Defizite bei den technischen und organisatorischen Sicherheitsmaßnahmen an, und zwar auf allen Ebenen und querbeet im gesamten Kontrollbereich. Die nachstehende, keineswegs vollständige Aufzählung

von im Berichtsjahr festgestellten Mängeln zeigt dies beispielhaft. Ganz offensichtlich schenken die öffentlichen Stellen im Lande, aus welchen Gründen auch immer, dem technisch-organisatorischen Datenschutz noch immer nicht die Beachtung, die ihm eigentlich zukommt, obwohl doch gerade die fortschreitende Computerisierung und Vernetzung und die damit verbundenen Missbrauchsmöglichkeiten und Risiken dazu allen Anlass böten. Wesentliche Verbesserungen scheinen mir nur erreichbar, wenn sich vor Ort mehr als bisher sachverständige, engagierte Mitarbeiterinnen und Mitarbeiter dieser wichtigen Aufgabe stellen.

6.1 Probleme mit dem Telefax

Gleich mehrfach wandte sich eine in Stuttgart ansässige Firma an meine Dienststelle, da sie binnen kürzester Zeit von drei verschiedenen Stellen des Landes eine Reihe von Telefaxsendungen erhielt, die sämtlich eigentlich für die Landesoberkasse in Karlsruhe bestimmt waren. In einem Fall gingen der Firma auch personenbezogene Daten zu. Auf der von der Verwaltung des Landtags initiierten Fehlsendung waren fünf Landtagsabgeordnete mit Name, Vorname, Kontonummer und einem Geldbetrag aufgeführt, den sie für EDV-Anschaffungen erhielten.

Ausgelöst wurde diese Fehlsendung wie so oft durch einen Bedienungsfehler. Bei einem an einer Nebenstellenanlage angeschlossenen Telefaxgerät ist es notwendig, zunächst eine bestimmte Taste zu betätigen, um eine Amtsleitung zu erhalten. Meist ist dies die „0“, so auch beim Telefaxgerät der Landtagsverwaltung. Um ein Telefax nach Karlsruhe zu versenden, wäre folglich zunächst eine „0“ für die Amtsleitung und sodann die „0721“ als Vorwahl für Karlsruhe zu wählen gewesen. Tatsächlich aber unterblieb die Wahl der ersten „0“ mit der Folge, dass die Sendung nicht in Karlsruhe, sondern bei der Firma in Stuttgart landete.

Das gleiche Problem zeigte sich bei der Kontrolle in einer Justizvollzugsanstalt. Deren Telefaxgerät war ebenfalls an eine Nebenstellenanlage angeschlossen, und auch hier musste bei Verbindungen ins öffentliche Netz jeweils eine zusätzliche „0“ vorgewählt werden. Dem Sendejournal des Telefaxgeräts war zu entnehmen, dass sich der jeweilige Absender manchmal erst nach Auftreten eines Übertragungsfehlers daran erinnerte, dass noch eine zusätzliche „0“ zu wählen ist. Außerdem deuteten einige Einträge im Sendejournal darauf hin, dass auch Sendungen der Justizvollzugsanstalt auf Grund der fehlenden zusätzlichen „0“ zu Irrläufern wurden.

Angesichts dieser immer wieder auftretenden Mängel beim Umgang mit dem Telefax und dem sich dabei ergebenden erhöhten Risiko von Fehlleitungen erinnerte ich daran, dass Unterlagen mit personenbezogenen Daten grundsätzlich nicht per Telefax übertragen werden sollten. Sofern wegen einer besonderen Eilbedürftigkeit in einem Ausnahmefall doch einmal eine Übertragung per Telefax unerlässlich ist, ist – etwa durch Kontrolle der gewählten Empfangsnummer in der Anzeige des Telefaxgeräts – peinlich genau darauf zu achten, dass tatsächlich der richtige Empfänger die Daten erhält. Schließlich ist angezeigt, an den Telefaxgeräten jeweils deutlich wahrnehmbare Hinweise anzubringen, dass zunächst stets eine führende „0“ vorzuwählen ist. Die Landtagsverwaltung und die Justizvollzugsanstalt wollen dem Rechnung tragen.

Weitere Informationen zum datenschutzgerechten Umgang mit Telefax-Geräten sind unserem Merkblatt „Datensicherheit beim Telefax“ zu entnehmen, das über das Internet-Angebot meiner Dienststelle unter http://www.baden-wuerttemberg.datenschutz.de abgerufen oder in gedruckter Form bei meiner Dienststelle angefordert werden kann.

6.2 Mängel bei der Zutrittskontrolle

Um unberechtigte Personen davon abzuhalten, dass sie sich an Servern, Routern oder Modems zu schaffen machen, sind derartige Geräte möglichst in einem separaten, abschließbaren Raum unterzubringen. Zugang zu den Geräten dürfen nur diejenigen erhalten, die sie administrieren.

Ein Kreiskrankenhaus stellte einen Server sowie das Fernwartungsmodem samt Fernwartungsprotokollierungseinrichtung in seinem Labor frei zugänglich auf. In einem Landratsamt war zwar ein separater Serverraum vorhanden. Dieser Raum war aber gegenüber den angrenzenden Räumen teilweise nur durch Schränke oder Trennwände abgeteilt, die nicht bis zur Decke reichten.

6.3 Mängel bei der Freigabe und dem Betrieb eines Verfahrens

Die Verarbeitung personenbezogener Daten darf nur mit Hilfe sorgfältig getesteter und von der Dienststelle schriftlich für den Echtbetrieb freigegebener EDV-Verfahren erfolgen. Anders ging ein Landratsamt vor. Es setzte ein EDV-Verfahren ein, das sich zum Zeitpunkt unseres Besuchs nach den Angaben des Landratsamts noch im „Teststadium“ befand und noch nicht zum Echteinsatz freigegeben war. Wohin es führen kann, wenn man Testbetrieb und Echtbetrieb nicht klar voneinander abgrenzt, zeigte sich dann auch gleich: Im Echtdatenbestand speicherte das Landratsamt auch einige Testdaten. Neben der fehlenden Freigabe war dies ein weiterer Mangel, besteht bei einer solchen Vorgehensweise doch die Gefahr, dass Testdaten irrtümlich als Echtdaten verarbeitet werden. Inzwischen hat das Landratsamt die Testdaten gelöscht und das Verfahren schriftlich für den Echteinsatz freigegeben.

6.4 Dokumentation unvollständig

Die baden-württembergischen Justizvollzugsanstalten arbeiten mit mehreren vom Justizministerium entwickelten Verfahren zur Verarbeitung der Gefangenen- und der Besucherdaten. Bei unseren Kontrollbesuchen in den Justizvollzugsanstalten Ravensburg und Schwäbisch Hall stellte sich heraus, dass diese Verfahren über Funktionen verfügten, die in der Verfahrensdokumentation überhaupt nicht genannt waren. Nicht beschrieben waren beispielsweise die Auskunftsfunktionen, mit deren Hilfe Gefangenendaten nur gelesen, nicht aber verändert werden konnten. Nicht beschrieben – und dies war wesentlich gravierender – waren auch die Funktionen, mit deren Hilfe jeder Benutzer die für ihn vorgesehenen Zugriffsbeschränkungen hätte umgehen und auf Daten, die er nicht für seine dienstlichen Aufgaben benötigt, hätte zugreifen können.

Die Unvollständigkeit der Dokumentation erschwerte nicht nur die Kontrolle unnötig. Sie ist auch für die Stelle, die die EDV-Verfahren einsetzt, ein gravierendes Manko. Ohne vollständige Dokumentation kann sie ihrer Aufgabe, die notwendigen technischen und organisatorischen Datenschutzmaßnahmen festzulegen, nicht nachkommen. Die unvollständige Dokumentation stellte daher einen datenschutzrechtlichen Mangel dar. Das Justizministerium hat mitgeteilt, dass es zu diesem und einer ganzen Reihe weiterer bei den Justizvollzugsanstalten Ravensburg und Schwäbisch Hall festgestellter Mängel, die ich ihm Mitte September mitgeteilt habe, voraussichtlich erst im Februar oder März nächsten Jahres antworten kann. Auch so kann man demonstrieren, für wie wenig gravierend man Datenschutz- und Datensicherheitsmängel hält.

6.5 Mängel beim Verfahrensverzeichnis

Jede Stelle, die personenbezogene Daten mit Hilfe eines EDV-Verfahrens verarbeiten will, muss mit der Aufnahme des Echtbetriebs in dem sog. Verfahrensverzeichnis schriftlich dokumentieren, welche personenbezogenen Daten es auf Grund welcher Rechtsgrundlage mit dem EDV-Verfahren verarbeiten darf, welche Personen von der Verarbeitung der Daten betroffen sind, welche anderen Stellen welche Daten regelmäßig erhalten, wann welche gespeicherten Daten zu sperren bzw. zu löschen sind, wer mit welchen Zugriffsrechten auf welche gespeicherten Daten zugreifen darf und welche technischen und organisatorischen Sicherheitsmaßnahmen getroffen sind. Eine solche schriftliche Dokumentation ist allein schon deswegen notwendig, damit die Stelle selbst den Überblick darüber behält, was sie mit Hilfe der EDV eigentlich tut und welche Daten sie auf welche Weise verarbeitet. Nach wie vor tun sich die öffentlichen Stellen mit diesem Verfahrensverzeichnis sehr schwer

(siehe dazu auch meinen 18. Tätigkeitsbericht 1997, Landtags-Drucksache 12/2242, S. 27 sowie 19. Tätigkeitsbericht 1998, Landtags-Drucksache 12/3480, S. 92). Das Kreiskrankenhaus Freudenstadt führte überhaupt kein Verfahrensverzeichnis; die Verfahrensverzeichnisse der Regierungspräsidien Karlsruhe und Freiburg, der Justizvollzugsanstalten Ravensburg und Schwäbisch Hall sowie des Landratsamts Schwäbisch Hall waren unvollständig und enthielten teilweise nichts sagende Angaben.

6.6 Unzureichende oder gar fehlende Löschfunktionen

Die exaktesten Festlegungen, wann welche Daten zu löschen sind, nützen nichts, wenn das EDV-Verfahren keine oder keine praxistauglichen Löschfunktionen zur Verfügung stellt. Die Daten verarbeitenden Stellen dürfen daher nur EDV-Verfahren für die Verarbeitung von personenbezogenen Daten einsetzen, die über geeignete Löschfunktionen verfügen. Das war nicht der Fall bei einem EDV-System eines Kreiskrankenhauses sowie bei einem landeseinheitlichen EDV-Verfahren zur Verarbeitung von Daten von Asylbewerbern.

6.7 Unzureichende Eingabekontrolle

Um einer missbräuchlichen Verwendung personenbezogener Daten wenigstens im Nachhinein noch auf die Schliche kommen zu können, ist es wichtig, dass sich nachträglich überprüfen lässt, wer wann welche Daten in den Computer eingegeben hat. Deshalb muss die Eingabe maschinell protokolliert werden. Zumindest muss in der jeweiligen Akte festgehalten werden, wer wann die Eingabe getätigt hat. Dieser Anforderung trug ein Landratsamt nicht ausreichend Rechnung.

6.8 Start des PC nicht gut genug abgesichert

Wird ein PC eingeschaltet, so muss zunächst einmal das Betriebssystem geladen werden, damit der Rechner in einen betriebsbereiten Zustand gelangt. Der Start des PC sollte dabei über die Festplatte oder über das Netzwerk erfolgen, nicht dagegen über das Diskettenlaufwerk oder das CD-ROM-Laufwerk. Ansonsten besteht zum einen die Gefahr, dass Viren eingeschleppt werden, falls die Diskette oder die CD-ROM solche enthält. Zum anderen könnte der Computerbenutzer sein eigenes Betriebssystem auf Diskette oder CD-ROM mitbringen und auf dem PC installieren mit der Folge, dass er u.U. Sicherheitsmaßnahmen, die die Daten verarbeitende Stelle getroffen hat, unterläuft. Diese Anforderung beachtete das Kreiskrankenhaus Freudenstadt nicht, da sich die PC, an denen Diskettenlaufwerke zur Erledigung dienstlicher Aufgaben verfügbar sein mussten, auch von einer Diskette starten ließen. Das Kreiskrankenhaus hat den Mangel inzwischen abgestellt.

6.9 Mängel beim Passwortschutz

Folgende Passwortmängel trafen wir bei unseren Kontrollen in diesem Jahr an:

– Fehlender Passwortschutz

  Abgesehen von je zwei PC konnten alle in den Justizvollzugsanstalten Ravensburg und Schwäbisch Hall eingesetzten PC nach dem Einschalten gleich genutzt werden. Ein Passwort musste dazu nicht eingegeben werden. Dies war ein Mangel, weil nur berechtigte Personen mit einem PC arbeiten und auf die gespeicherten Daten zugreifen dürfen.

– Passwörter allgemein bekannt

  Wer über das lokale Netz der Justizvollzugsanstalten Ravensburg und Schwäbisch Hall auf freigegebene Daten anderer PC zugreifen oder wer die auf den Servern installierten Programme nutzen wollte, musste sich zunächst am lokalen Netzwerk anmelden. Als Benutzername war dabei jeweils der PC-Name einzugeben und auch als Passwort diente stets der PC-Name. Auch dies war ein Mangel, weil ein Passwort, das alle kennen, nutzlos ist und seine Funktion verfehlt.

– Verfahrensnutzung ohne Verwendung individueller Kennungen und Passwörter möglich

  Um bei der Justizvollzugsanstalt Ravensburg die Programme zur Verarbeitung der Gefangenendaten zu nutzen, musste nur etwa die Hälfte der ca. 90 Benutzer ein Passwort eingeben. Die andere Hälfte konnte ohne Eingabe eines Passworts auf die in dem Verfahren gespeicherten personenbezogenen Daten zugreifen. Welche Benutzer sich mit Passwort anmelden mussten und welche nicht, entschied der Systemverwalter jeweils danach, ob seiner Einschätzung nach der betreffende Mitarbeiter bereits so weit mit der Technik vertraut war, dass er mit der Passworteingabe zurecht kam. Neu eingerichtete Benutzer arbeiteten in jedem Fall erst einmal mehrere Wochen lang ohne Passwort.

  Auch bei der Justizvollzugsanstalt Schwäbisch Hall war die Anmeldung der Benutzer mit individueller Kennung und Passwort die Ausnahme: Die ca. 100 Mitarbeiter des Vollzugsdienstes, des sog. Werkdienstes und der Krankenstation verwendeten keine individuellen, sondern Gruppenkennungen, die ohne Eingabe eines Passwortes nutzbar waren. Die Mitarbeiter der Verwaltung meldeten sich zwar mit individuellen Kennungen an. Jedoch mussten auch hier nicht einmal 10 der insgesamt etwa 40 Mitarbeiter bei der Anmeldung ein Passwort eingeben.

– Administratoren kennen Passwörter

  Das Kreiskrankenhaus Freudenstadt speicherte die Benutzerkennungen und Passwörter sämtlicher Nutzer des dortigen Computernetzwerks im Klartext in einer Datei, auf die die beiden Systemverwalter zugreifen konnten. Das Kreiskrankenhaus begründete die Einrichtung dieser Datei damit, dass sich die Systemverwalter in Fällen, in denen ein Benutzer Probleme mit der EDV hat, unter der Kennung des Benutzers anmelden und den Fehler nachvollziehen wollten.

  Ein ähnliches Bild zeigte sich bei der Justizvollzugsanstalt Ravensburg: Sofern dort Benutzer überhaupt ein Passwort verwenden mussten, wurde dieses zwischen Benutzer und Systemverwalter abgesprochen und vom Systemverwalter auf der lokalen Festplatte seines PC gespeichert.

  Der Benutzerverwalter des Labor-EDV-Systems im Kreiskrankenhaus Backnang kannte sämtliche Benutzerpasswörter und konnte sich die Passwörter jederzeit am Bildschirm im Klartext ansehen.

  Alle diese Vorgehensweisen widersprachen dem Grundsatz, dass Passwörter nur dem jeweiligen Benutzer bekannt sein dürfen. Auch System- und Benutzerverwalter dürfen das Passwort eines Benutzers nicht kennen. Ansonsten können sie sich nämlich ohne weiteres unter falscher Identität am EDV-System anmelden. Die vom Gesetz verlangte Eingabekontrolle, nach der nachvollziehbar sein muss, wer welche Daten in das System eingab, ließe sich nicht gewährleisten. Sofern Benutzerkennungen samt zugehöriger Passwörter sogar im Klartext in einer Datei gespeichert werden, stellt dies ein enormes Sicherheitsrisiko dar. Denn wer Zugriff auf diese Datei erhält, weil etwa das für den Zugriff notwendige Passwort einmal doch einem Unberechtigten bekannt wird, erhält auf einen Schlag alle Informationen, um sich als beliebiger Benutzer anzumelden. Bei allem Verständnis für die Notwendigkeit einer effizienten Administration der eingesetzten EDV-Systeme: Ein ausreichender Datenschutz muss dabei gewahrt bleiben.

– Benutzer konnten ihre Passwörter nicht selbst ändern

  Abgesehen von einem einzigen Mitarbeiter konnten die Computernutzer im Krankenhaus Freudenstadt ihr Passwort nicht selbst ändern, genauso wenig wie die Benutzer des Labor-EDV-Systems im Kreiskrankenhaus Backnang.

  Dies wird den datenschutzrechtlichen Erfordernissen nicht gerecht. Jeder Benutzer muss in der Lage sein, sein Passwort jederzeit zu än-

dern. Von dieser Möglichkeit muss er beispielsweise dann Gebrauch machen, wenn er den Verdacht hegt, sein Passwort sei einer anderen Person bekannt geworden.

Die Passwortmängel in den Kreiskrankenhäusern Freudenstadt und Backnang sowie in den Justizvollzugsanstalten Ravensburg und Schwäbisch Hall musste ich beanstanden. Die Kreiskrankenhäuser haben die Mängel inzwischen abgestellt. Die Antwort des Justizministeriums zu den Mängeln in den Justizvollzugsanstalten lässt noch, wie erwähnt, auf sich warten.

6.10 Keine Bildschirmsperre

Die Systemverwalter der Justizvollzugsanstalten in Ravensburg und Schwäbisch Hall richteten, sofern das von Benutzern so gewünscht wurde, den PC so ein, dass der Bildschirmschoner nur nach Eingabe eines Passworts deaktiviert werden konnte. Nach Auskunft der Systemverwalter war eine solche Bildschirmsperre in beiden Justizvollzugsanstalten an 2 bis 4 PC eingerichtet. Dieses Vorgehen, das es in das Ermessen der einzelnen Benutzer stellte, ob eine solche Sperre eingerichtet wurde oder nicht, war datenschutzrechtlich nicht in Ordnung: Notwendig ist vielmehr, einen Bildschirmschoner an allen Arbeitsplätzen so einzurichten, dass er nach 5 bis 10 Minuten aktiviert wird und die Sperre nur durch die Eingabe des Passworts wieder beseitigt werden kann.

6.11 Mängel beim Umgang mit Dateifreigaben in lokalen Netzwerken

Werden mehrere PC über ein Netzwerk miteinander verbunden, so kann man, ohne einen speziellen Computer (Server) bereitstellen zu müssen, von einem PC aus auf Daten zugreifen, die auf einem anderen gespeichert sind. Voraussetzung ist freilich, dass die Daten auf dem bereitstellenden PC ausdrücklich für einen Zugriff über Netz freigegeben sind.

Wer ein solches Netzwerk betreibt, muss dafür sorgen, dass nur Mitarbeiter auf die personenbezogenen Daten zugreifen können, die sie tatsächlich für ihre Aufgaben benötigen. Hieran ließen es die Justizvollzugsanstalten mangeln: Dort hätte jeder Nutzer eines vernetzten PC alle auf der lokalen Festplatte des PC gespeicherten Daten zum Zugriff über Netz freigeben können. Eine spezielle Dienstanweisung oder sonstige organisatorische Vorgaben zum Umgang mit dieser Möglichkeit gab es in beiden Fällen aber nicht. Zudem war der Passwortschutz, der unberechtigte Zugriffe auf freigegebene Daten, z. B. Laborergebnisse von Urinuntersuchungen bei den Gefangenen, verhindern sollte, unzulänglich. Die Anzahl der möglichen Anmeldefehlversuche war nämlich nicht beschränkt. Zudem läuft jeder Passwortschutz von vornherein ins Leere, wenn die Passwörter – wie in Schwäbisch Hall geschehen – der Einfachheit halber im PC hinterlegt werden. Um diese Probleme vermeiden zu können, sollten personenbezogene oder andere schutzbedürftige Daten, auf die mehrere Mitarbeiter einer Dienststelle zugreifen sollen, nicht mehr über Freigaben, sondern über einen speziellen Server bereitgestellt werden.

6.12 Unzureichender Schutz bei Fehlversuchen

Fehlerhafte Anmeldeversuche, etwa wenn zu einer Benutzerkennung Passwörter ausprobiert werden, können generell ein Indiz dafür sein, dass ein Unberechtigter versucht, sich am EDV-System anzumelden und auf Daten zuzugreifen, die er nicht sehen darf. Fehlversuche dürfen daher nicht ohne Folgen bleiben. Nach drei, maximal fünf Fehlversuchen unter derselben Benutzerkennung in einem Zeitraum von etwa 30 Minuten ist eine dauerhafte Sperre der betreffenden Benutzerkennung vorzusehen. Weiteren Eindringversuchen unter dieser Kennung ist damit ein wirksamer Riegel vorgeschoben. Diese Anforderung beachteten zwei Kreiskrankenhäuser sowie zwei Regierungspräsidien nicht ausreichend.

6.13 Fehlende Transparenz bei den Zugriffsrechten

Um den Überblick darüber zu behalten, wer über welche Zugriffsrechte verfügt, sollte es eigentlich selbstverständlich sein, dass sich der Benutzerverwalter eine Übersicht anzeigen oder ausdrucken lassen kann, aus der hervorgeht, welche Mitarbeiter welche Zugriffsberechtigungen haben. Solche Ausdrucke sind beispielsweise unverzichtbar, um zu überprüfen, ob die aktuell eingerichteten Zugriffsberechtigungen noch den dienstlichen Notwendigkeiten entsprechen.

In den Justizvollzugsanstalten Ravensburg und Schwäbisch Hall war dies jedoch nicht möglich.

6.14 Benutzer konnten sich selbst zusätzliche Zugriffsmöglichkeiten verschaffen

Einen gravierenden Mangel mussten wir bei der Überprüfung der vom Justizministerium entwickelten Programme zur Verarbeitung der Gefangenendaten feststellen, die unter anderem in den Justizvollzugsanstalten Ravensburg und Schwäbisch Hall eingesetzt wurden: Diese boten zwar die Möglichkeit festzulegen, welcher Benutzer welche Programmfunktionen nutzen darf, allerdings konnte jeder Benutzer diese Beschränkung umgehen und sich selbst auch den Zugriff auf Programmfunktionen verschaffen, die er nicht für seine Aufgaben benötigte. Möglich wurde dies, weil die Funktionen zur Berechtigungsverwaltung nicht nur den Systemverwaltern, sondern allen Benutzern zur Verfügung standen. Ein Benutzer, der nur wenige beschränkte Auskunftsfunktionen über Stammdaten der Gefangenen benötigte, hätte sich auf diesem Weg beispielsweise lesenden und schreibenden Zugriff auch auf Besucher- oder Gefangenendaten verschaffen können, die er dienstlich nicht benötigte. Dies verstieß in krasser Weise gegen den datenschutzrechtlichen Grundsatz, wonach jeder Mitarbeiter nur auf diejenigen personenbezogenen Daten zugreifen können darf, die er für seine dienstlichen Aufgaben benötigt. Diesen schwerwiegenden Mangel habe ich gegenüber dem Justizministerium beanstandet. Dessen Antwort steht auch hier noch aus.

6.15 Fehlende Terminalbeschränkung

Jeder Benutzer der Verfahren zur Verarbeitung von Gefangenendaten konnte diese Verfahren von jedem vernetzten Arbeitsplatz aus aufrufen. Es gab dabei keine technische Beschränkung der Art, dass sich die einzelnen Mitarbeiter jeweils nur von bestimmten Arbeitsplatzcomputern aus anmelden dürfen (sog. Terminalbeschränkung).

Existiert keine solche Beschränkung, so kann beispielsweise ein Mitarbeiter, der nur wenige Zugriffsrechte besitzt, aber die Kennung und das Passwort eines Kollegen mit mehr Befugnissen erfährt, sich von seinem Arbeitsplatz aus mit dessen Kennung anmelden und auf diese Weise die für ihn geltenden Zugriffsbeschränkungen umgehen. Im Fall der Justizvollzugsanstalt Ravensburg wäre dies besonders leicht möglich gewesen: Hier hätte man nicht einmal das Passwort eines Kollegen kennen müssen, um mit einer fremden Kennung zu arbeiten. Jeder Benutzer konnte hier nämlich in einer Systemdatei nachlesen, welche Kennungen seiner Kollegen er ohne Passwort nutzen könnte: er hätte alle diese Kennungen, zu denen im Übrigen auch die des Anstaltsleiters gehörte, ohne weiteres von seinem Arbeitsplatz aus verwenden können.

Die fehlende Terminalbeschränkung erleichtert es ferner auch unberechtigten Dritten, durch Ausprobieren das Passwort zu einer ihnen bekannt gewordenen Kennung zu ermitteln. Sie können sich für ihre Tests dann jeden beliebigen Arbeitsplatzcomputer auswählen, der dafür gerade günstig erscheint.

6.16 Defizite beim Virenschutz

Eine besondere Gefährdung im elektronischen Zeitalter stellen Computerviren dar. Das Risiko einer Infektion besteht unter anderem, wenn

Datenträger wie Diskette oder CD-ROM benutzt werden. Im Kreiskrankenhaus Freudenstadt waren an einigen wenigen PC Disketten- und CD-ROM-Laufwerke verfügbar. Weder hatte das Kreiskrankenhaus Freudenstadt festgelegt, dass Mitarbeiter, die über benutzbare Laufwerke verfügen, Datenträger, die ihnen zugehen, erst der EDV-Abteilung zur Virenüberprüfung auszuhändigen haben noch hatte es die Arbeitsplätze dieser Mitarbeiter mit aktuellen Virenschutzprogrammen ausgestattet. Inzwischen hat es wenigstens per Dienstanweisung festgelegt, dass eingehende Datenträger erst nach vorheriger Virenüberprüfung durch die EDV-Abteilung benutzt werden dürfen.

6.17 Wenn aus temporären Daten dauerhafte werden

Mitunter speichern Behörden auf ihren Computern personenbezogene Daten und wissen gar nichts davon. Feststellen mussten wir dies bei der Justizvollzugsanstalt Schwäbisch Hall. Sie hatte an einem PC einen Scanner angeschlossen, der vor allem dazu genutzt wurde, Ausweise oder andere Vorlagen zu kopieren. Hierzu wurden die gescannten Vorlagen jeweils unmittelbar nach dem Scannen ausgedruckt. Auf Nachfragen erklärten sowohl der zuständige Mitarbeiter als auch der Systemverwalter, die gescannten Vorlagen würden nicht auf der Festplatte des PC gespeichert. Bei der Überprüfung stellte sich jedoch gerade das Gegenteil heraus. Die Dateien der gescannten Dokumente wurden automatisch auf der Festplatte des Computers gespeichert. So sammelten sich im Laufe von zweieinhalb Monaten immerhin 167 Dateien gescannter Ausweise oder anderer Unterlagen an. Dies durfte selbstverständlich nicht sein. Noch während unserer Kontrolle löschte daher der Systemverwalter die 167 bei der Kontrolle vorgefundenen Bilddateien.

6.18 Fehlende oder unzureichende Schulungen

Der Datenschutz im EDV-Alltag kann nur klappen, wenn die Mitarbeiter über die zur Bedienung der Systeme und Programme notwendigen Kenntnisse und Fertigkeiten verfügen. Diese müssen sie im Rahmen von Schulungen erhalten. Anders war dies in einer Gemeinschaftsunterkunft des Landratsamts Schwäbisch Hall. Ohne irgendwelche Schulungen erhalten zu haben, mussten sich die dort tätigen Mitarbeiter selbst darum kümmern, wie die Programme am besten einzusetzen und auf welche Weise personenbezogene Daten damit zu verarbeiten sind. Das Landratsamt will in Zukunft ausreichende Schulungen anbieten.

Besonders wichtig sind ausreichende Schulungen für Systemverwalter. Aber auch hiermit steht es, wie wir bei unseren Kontrollbesuchen in den Justizvollzugsanstalten Ravensburg und Schwäbisch Hall feststellen mussten, nicht immer zum Besten: Dort hatte man alte Computer, die mit einem heute nicht mehr gebräuchlichen Betriebssystem arbeiteten, durch vernetzte Computer ersetzt und dabei gleich drei neue Betriebssysteme eingesetzt. Den Systemverwaltern, die über keine EDV-technische Ausbildung verfügten, wurden zwar in einführenden Fortbildungen Grundkenntnisse dieser Systeme vermittelt – diese Kenntnisse genügten aber nicht, um zielgerichtet an Planung, Einrichtung und Betrieb des neuen Systems heranzugehen. Die Systemverwalter mussten sich die notwendigen Kenntnisse, auch was sicherheitsrelevante Funktionen und Einstellungen angeht, vielmehr durch „learning by doing“ selbst aneignen. Dabei liegt auf der Hand, dass fehlende oder unzulängliche Kenntnisse leicht zu handwerklichen Fehlern bei der Realisierung technischer und organisatorischer Datenschutzmaßnahmen führen können.

6.19 Fernwartung

Inzwischen müsste eigentlich allerorten bekannt sein, dass in Fällen, in denen eine Firma mit Fernwartungsarbeiten betraut wird, diese schriftlich zu beauftragen ist und dass in dem Vertrag die notwendigen Datenschutzregelungen präzise festzulegen sind. Schließlich erhält eine fremde Stelle Zugriff auf das eigene DV-System; präzise Spielregeln sind also unverzichtbar. Als Hilfestellung, welche Maßnahmen im Ein-

zelnen zu treffen sind, können meine Hinweise zum Thema Fernwartung dienen, die Interessierte über das Internet-Angebot meiner Dienststelle unter http://www.baden-wuerttemberg.datenschutz.de abrufen oder auch direkt bei meiner Dienststelle anfordern können.

Nach wie vor werden aber oft Firmen lediglich auf der Grundlage eines ganz allgemeinen Wartungsvertrags tätig, in dem dann sinngemäß nur zu lesen ist, die Bestimmungen des Datenschutzes seien zu beachten. Auf welche Weise und durch welche konkreten Maßnahmen dies geschehen soll, bleibt offen. Eine solch unzureichende Beauftragung musste ich bei einem Kreiskrankenhaus feststellen.

Auch wenn fremde Personen im Rahmen einer Wartung vor Ort tätig werden und dem Wartungspersonal auch Einblick in personenbezogene Daten eingeräumt werden muss, ist eine schriftliche Beauftragung mit Regelungen zum Datenschutz unerlässlich. Dies unterblieb bei einem Landratsamt.

6.20 Mängel bei der Vernichtung von Unterlagen

Wer eine Spezialfirma damit betraut, auszusondernde Unterlagen abzuholen und zu vernichten, muss einen schriftlichen Auftrag erteilen und in dem Vertrag die notwendigen Datenschutzmaßnahmen präzise festlegen. Daran hapert es vielfach:

- Aus dem Vertrag, den ein Kreiskrankenhaus mit einer Firma abschloss, ging nicht hervor, wo die sensiblen Krankenhausdaten vernichtet werden.
- Ein Kreiskrankenhaus sowie zwei Landratsämter machten keine oder nur unzureichende Vorgaben hinsichtlich der Art der Vernichtung von Unterlagen. Personenbezogene Daten sind aber stets zumindest nach Stufe 3 der DIN-Norm 32757, Teil 1, zu vernichten.
- Ein Landratsamt regelte nicht, wie rasch die Firma das Vernichtungsgut nach dessen Abholung der Vernichtung zuführen muss und ob und, wenn ja, wie lange die Firma die zu vernichtenden Unterlagen zwischenlagern darf.

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

1. Telemedizin

Der Begriff „Telemedizin“ kennzeichnet eine Entwicklung im Gesundheitswesen, die durch einen zunehmenden Einsatz moderner Informations- und Kommunikationstechnik geprägt ist. Insbesondere die elektronische Speicherung medizinischer Daten und deren Austausch zwischen den an der Behandlung der Patienten Beteiligten rückt immer mehr in den Blickpunkt des Interesses sowohl der Erbringer medizinischer Leistungen als auch, zwangsläufig, der Datenschutzkontrollstellen. Denn der schnelle, effektive und umfassende Informationsaustausch zum Wohle des Patienten ist nur die eine Seite. Die andere Seite ist, dass die Segnungen der Technik allzu oft über den Kopf des Patienten hinweg genutzt werden (können), der immer weniger wissen, geschweige denn steuern kann, wem welche Informationen über seinen Gesundheitszustand zur Verfügung stehen. Das Grundrecht auf Datenschutz kann hier schnell unter die Räder einer ungebremsten Technikbegeisterung geraten. Als zentrale Herausforderungen seien hier nur die wie Pilze aus dem Boden schießenden Verknüpfungen einzelner DV-Systeme zu Netzverbünden sowie die zunehmenden Bestrebungen, medizinische Erkenntnisse aus unterschiedlichen Bereichen zentral zusammenzufassen und zum Abruf durch eine Vielzahl von Personen bereitzustellen, d. h. sog. elektronische Patientenakten anzulegen, genannt. Hier sind vor allem auch die Datenschutzkontrollstellen gefordert, frühzeitig durch qualifizierte Beratung steuernd tätig zu werden, um den Nutzen des Technologieeinsatzes für den Patienten mit dessen Interesse am Schutz seiner persönlichen Daten, die gerade so-

weit es um Gesundheitsdaten geht besonders sensibel sind, in einen angemessenen Ausgleich zu bringen. Die Erfahrung aus der täglichen Arbeit meines Amtes zeigt, dass dieses Thema zunehmend Raum einnehmen wird. So hatten wir uns im Berichtszeitraum mit Überlegungen des Verbandes Stuttgarter Krankenhäuser e.V., den elektronischen Datenaustausch zu intensivieren, befasst und in diesem Zusammenhang Gespräche mit dem Netzanbieter Medizin Verbundnetz Bundesrepublik (MVB) geführt. Auch das (länderübergreifende) Gesundheitsnetz Rhein-Neckar-Dreieck e.V. nahm unsere Beratungsangebote in der Weise in Anspruch, dass Mitarbeiter meines Amtes und ich zu Vorträgen und Diskussionen eingeladen wurden. Welche datenschutzrechtliche Fragestellungen in diesem Rahmen auftreten können, sei beispielhaft an zwei Projekten erläutert, mit denen ich mich näher befasst habe, wobei damit beileibe nicht alle Probleme angesprochen sind:

1.1 Die „gemeinsame“ Kardiologie-Datenbank (Projekt Stuttgarter Telemedizin)

Ein Stuttgarter Krankenhaus wandte sich an mich mit der Bitte, ein Datenschutz- und Datensicherheitskonzept datenschutzrechtlich zu bewerten. Hintergrund war, dass eine private Arztpraxis im Rahmen eines europäischen Projektes an die Kardiologie-Datenbank des Krankenhauses angeschlossen werden sollte. Die Ärzte der kardiologischen Gemeinschaftspraxis nutzen die Räume und Geräte des Krankenhauses, um ihre Patienten dort zu untersuchen. Die dabei angefallenen Patientendaten speichern sie auf einem Rechner des Krankenhauses. Den Ärzten sollte ermöglicht werden, über in ihrer Praxis befindliche PC direkt auf die Daten im Krankenhaus zuzugreifen.

Bei der Überprüfung des Datenschutz- und Datensicherheitskonzepts stellte sich heraus, dass die auf dem Rechner des Krankenhauses gespeicherten Datenbestände der Ärzte einerseits und die Datenbestände des Krankenhauses andererseits nicht gegeneinander abgeschottet waren. Die Praxisärzte konnten also faktisch auf Daten der Krankenhauspatienten ebenso zugreifen wie das Krankenhaus auf die medizinischen Daten, die die Praxisärzte auf dem Krankenhauscomputer gespeichert hatten. Damit war die Wahrung des ärztlichen Berufsgeheimnisses gefährdet, das auch den Informationsaustausch unter Ärzten ohne entsprechende Einwilligung des Patienten grundsätzlich verbietet.

Ich habe das Krankenhaus aufgefordert, durch technische Maßnahmen wirksam zu verhindern, dass gegenseitige Zugriffe auf die jeweiligen Patientendatenbestände möglich sind. Außerdem sollte es übergangsweise die Ärzte der Gemeinschaftspraxis nachhaltig auf die datenschutzrechtliche Situation hinweisen und sie förmlich verpflichten, nicht auf personenbezogene Daten auf dem gemeinsam genutzten Serversystem zuzugreifen, für die sie nicht verantwortlich sind. Das Krankenhaus akzeptierte dies ohne weiteres und ergriff die notwendigen Maßnahmen. Insbesondere sind mittlerweile die Programme den datenschutzrechtlichen Erfordernissen angepasst und beide Datenbankbereiche vollständig voneinander getrennt.

1.2 Verbundprojekt Medi

Wer in den letzten Monaten die Presse im Stuttgarter Raum aufmerksam verfolgt hat, dem wird der Begriff „Medi“ nicht unbekannt sein. Hinter dem Kürzel verbirgt sich ein ehrgeiziges Projekt, das von der Kassenärztlichen Vereinigung Nordwürttemberg und einem Zusammenschluss niedergelassener Ärzte gemeinsam getragen wird. Es geht nämlich darum, dass sich (zunächst) Ärzte und (dann auch) Krankenhäuser aus dem nordwürttembergischen Raum zu regionalen Verbünden zusammenschließen u. a. mit dem Ziel, unter Einsatz moderner Informations- und Kommunikationstechnik effektiver zusammenzuarbeiten.

Das Projekt ist in mehrere Phasen gegliedert. In der ersten Phase geht es im Wesentlichen um die Etablierung des Informationsaustauschs

per elektronischer Post. Die Daten sollen dabei verschlüsselt und digital signiert über das Deutsche Gesundheitsnetz (DGN) übertragen werden. In der zweiten Phase ist die Einrichtung einer zentralen elektronischen Patientenakte (nachfolgend: EPA) vorgesehen. Auf einer Informationsveranstaltung, zu der ich eingeladen war, stellten die Initiatoren das Projekt sowie insbesondere auch das Konzept der EPA vor. Im Hinblick darauf, dass auch meiner Kontrolle unterliegende öffentliche Krankenhäuser in den Verbund integriert werden sollen, wurde ich um eine datenschutzrechtliche Einschätzung des Projekts gebeten. Dies habe ich getan. Einige wenige, mir wesentlich erscheinende Feststellungen möchte ich hier wiedergeben:

Phase 1

– Jeder Anschluss eines EDV-Systems an ein anderes Datennetz zieht Gefährdungen für den Datenschutz und die Datensicherheit nach sich. Vor allem besteht das Risiko, dass aus dem fremden Netz in das eigene EDV-System eingedrungen und auf die dort gespeicherten Daten zugegriffen wird. Eine derartige Gefährdung besteht auch beim Anschluss an das DGN, zumal dieses wiederum mit dem Internet verbunden ist, wodurch die Risiken noch zunehmen.

  Ich wies deshalb darauf hin, dass ein Anschluss an das DGN im Rahmen von Medi aus datenschutzrechtlicher Sicht nur dann akzeptabel ist, wenn der Teilnehmer die technischen und organisatorischen Sicherheitsmaßnahmen trifft, die erforderlich sind, um sein EDV-System wirksam gegenüber dem DGN abzuschotten. Welche Maßnahmen im Einzelnen dazu notwendig sind, lässt sich nicht pauschal sagen, weil dies maßgeblich auch von den im DGN getroffenen Sicherheitsmaßnahmen abhängt, die mir aber weitgehend unbekannt sind.

– Damit die Medi-Teilnehmer elektronische Post verschlüsselt und digital signiert untereinander austauschen können, benötigt jeder Teilnehmer einen geheimen und einen öffentlichen Schlüssel. Einem Trust-Center obliegt dabei, diese Schlüssel zu erzeugen, den geheimen Schlüssel dem Teilnehmer auszuhändigen und den öffentlichen Schlüssel zu veröffentlichen.

  Für Medi ist ein Trust-Center vorgesehen, das nicht nach dem Signaturgesetz zertifiziert ist (vgl. dazu Teil „Technik und Organisation“, Nr. 1). Nähere Informationen, die es erlauben würden, dessen datenschutzrechtliche Qualität zu beurteilen, liegen mir bis jetzt nicht vor. Da aber der Vertrauenswürdigkeit des Trust-Centers eine wichtige Rolle für den Datenschutz bei Medi zukommt, ist mir derzeit eine abschließende Bewertung, ob die Phase 1 einen ausreichenden Datenschutz bietet, noch nicht möglich.

Phase 2

– Aus grundsätzlichen datenschutzrechtlichen Erwägungen stehe ich zentralen Sammlungen von Gesundheitsdaten, wie in Phase 2 vorgesehen, kritisch gegenüber. Auch wenn ich den Wunsch mancher Ärzte nachempfinden kann, in der konkreten Behandlungssituation schnell und unkompliziert auf die komplette Krankengeschichte ihres Patienten zugreifen zu können, sehe ich doch auch die Gefahren, die eine solche Zusammenballung höchst sensibler Daten mit sich bringt. Nicht jeder Patient wird sich bei dem Gedanken wohl fühlen, dass jeder Arzt mit einem Blick auf den Bildschirm alles über seine zurückliegenden Besuche bei anderen Ärzten jedweder Fachrichtung erfährt. Manch einer wird keinerlei Verständnis dafür haben, wenn sich sein Augenarzt, bei dem er seine Sehstärke feststellen lassen will, auf diese Weise darüber informieren könnte, wegen welcher Beschwerden er einen Urologen aufgesucht oder sich einer psychotherapeutischen Behandlung unterzogen hat. Zu bedenken ist aber auch, dass solche Sammlungen, wenn sie einmal bestehen, der Gefahr illegaler Nutzungen unterliegen. Gesundheitsdaten haben in bestimmten Bereichen einen nicht zu unterschätzen-

den wirtschaftlichen Wert. Und wem es gelingt, in das System einzudringen, der ist in der Lage, sich nahezu jede gewünschte Information über die dort Gespeicherten zu beschaffen. Einen absolut sicheren Schutz hiergegen gibt es jedenfalls nicht. Aber nicht nur das. Besteht eine solche Datei erst einmal, werden sehr schnell auch andere Begehrlichkeiten geweckt, denen durch eine Rechtsänderung sehr rasch Rechnung getragen werden kann. Deshalb würde ich es aus Datenschutzsicht begrüßen, wenn man sich auf eine weniger problematische Form der Informationsbereitstellung verständigen könnte, die es durchaus gibt.

– Sollte die EPA doch realisiert werden, muss vor allem Folgendes beachtet werden:

  • Die Rechner, auf denen die Daten gespeichert werden, sollten bei einem Arzt oder in einem Krankenhaus stehen, damit die Beschlagnahmefreiheit der medizinischen Informationen nach der Strafprozeßordnung erhalten bleibt.

  • Soll für einen Patienten eine EPA angelegt werden, bedarf es einer ausführlichen Information über die zentrale Datei sowie über die dem Patienten zustehenden Datenschutzrechte. Der Patient muss schriftlich in die Erstellung der Akte an sich einwilligen. Diese Einwilligung kann aber nicht bereits zur Einspeicherung von Patientendaten berechtigen, die erst im Rahmen der künftigen Behandlungen gewonnen werden. Um seinem Selbstbestimmungsrecht Rechnung zu tragen muss der Arzt, der im konkreten Behandlungsfall Daten in die Akte einstellen will, dem Patienten die für die Aufnahme in die Akte in Betracht gezogenen Daten zuvor mitteilen und ihn fragen, ob er damit einverstanden ist sowie ob und gegebenenfalls für wen der Zugriff auf sie gesperrt werden soll. Solche Sperrungen müssen möglich sein.

  • Der Zugriff auf die EPA muss vom Patienten autorisiert werden. Die systemtechnisch zwingende Verwendung einer im Besitz des Patienten befindlichen Chipkarte als Zugangsvoraussetzung ist dafür ein richtiger Ansatz. Allerdings kann es nicht ausreichen, dass er dazu lediglich die Krankenversichertenkarte (KVK) vorlegt. Denn jeder Kassenpatient ist, wenn er sich behandeln lassen will, gesetzlich gezwungen, diese vorzulegen. Daraus gleichzeitig seine Einwilligung in die Nutzung der EPA zu folgern, geht nicht an. Wenn schon die KVK als Zugangsberechtigung verwendet werden soll, dann ist zumindest zu fordern, dass sie gerade hierfür nochmals eingesetzt wird. Technisch wäre dies abzusichern.

  • Wer zum Arzt geht, hat es bis jetzt selbst in der Hand zu entscheiden, was er diesem sagt und welche Informationen er ihm vorenthält. Bei der EPA funktioniert dies leider nicht mehr so einfach. Wer mit der Hingabe der Chipkarte bekundet, dass er damit einverstanden ist, wenn der Arzt die Akte aufruft, muss in Kauf nehmen, dass dieser auch alles lesen kann, was dort gespeichert ist. In der konkreten Behandlungssituation besteht grundsätzlich keine Möglichkeit mehr, den Arzt von bestimmten, in der Akte enthaltenen Informationen auszuschließen. Man kann dies nur im Voraus veranlassen, indem man Teile der Akte für den Zugriff durch bestimmte Ärzte sperren lässt, wobei noch offen ist, an wen sich der Patient wenden soll, wenn er eine Sperrung veranlassen will. Ob dieses Verfahren allerdings praktikabel ist, darf bezweifelt werden. Bei spontanen Arztbesuchen dürfte eine vorherige Selektion der Zugriffsrechte jedenfalls regelmäßig ausscheiden. Zudem dürfte es mit zunehmendem Umfang der Akte für den Patienten immer schwieriger werden, noch zu überschauen, wem er welche Zugriffsrechte gewährt hat oder gewähren will.

  • Ein weiteres Problem stellt die sog. Notfallzugangsberechtigung dar. Das bisherige Konzept lässt es zu, dass Ärzte, die sich an Medi beteiligen, die EPA auch ohne Einsatz der Patientenchipkarte allein durch Eingabe des Namens oder eines Namensbe-

standteils aufrufen können. Auch wenn die Forderung nach einer Zugriffsmöglichkeit auf möglicherweise lebensnotwendige Informationen im Falle, dass sich der Patient nicht mehr äußern kann, verständlich ist, fragt sich schon, was ein ausgeklügeltes Zugriffssystem nach dem Vier-Augen-Prinzip eigentlich wert ist, wenn es auf einfachste Weise umgangen werden kann. Die Protokollierung solcher Zugriffe stellt jedenfalls keine ausreichende Schranke gegen Missbrauch dar. Zumindest darf es nicht so sein, dass bei einem „Notfallzugriff" die komplette Akte aufgerufen und sichtbar gemacht wird. Über einen im Voraus festgelegten Kerndatensatz, dem der Patient zugestimmt hat, ließe sich reden.

- Bei der Menge der in einer zentral geführten Patientenakte enthaltenen Daten muss es für den Patienten eine einfache Möglichkeit geben, sich über den Inhalt zu informieren und die Sperrung oder Löschung aller oder eines Teils der Daten bewirken zu können. Dies muss sichergestellt sein.

Allein schon diese summarische Bewertung des Vorhabens auf der Grundlage der bisherigen Überlegungen für eine zentrale elektronische Patientenakte zeigt, dass noch eine Vielzahl von Einzelproblemen zu lösen sein wird, bis mit einer datenschutzkonformen Realisierung gerechnet werden kann.

2. Datenschutz im Krankenhaus – Der Kontrollbesuch

Kontrollbesuche in Krankenhäusern haben in meinem Amt Tradition. Der Grund ist einfach: Gerade in Krankenhäusern fallen große Mengen sehr sensibler personenbezogener Daten an. Deshalb muss mit diesen Daten sehr sorgsam umgegangen werden. Die in der Vergangenheit durchgeführten Kontrollen haben gezeigt, dass die Praxis diesem Anspruch oft nicht hinreichend gerecht wird. Auf die Beseitigung solcher Schwachstellen hinzuwirken ist einer der Zwecke solcher Kontrollbesuche. Ein anderer ist, durch die Diskussion der Probleme vor Ort Sensibilität für die Belange des Datenschutzes zu erzeugen und dadurch ein künftiges datenschutzgerechtes Verhalten zu fördern.

Besucht wurde diesmal das Kreiskrankenhaus Freudenstadt, das durch einen Beitrag in einer Fachzeitschrift über ein neues EDV-Verfahren unsere Neugierde geweckt hatte. Beim Besuch fiel manches auf und zwar unter anderem:

2.1 Die Aufnahme

Es erstaunt immer wieder, wie hartnäckig sich bestimmte Missstände halten. Einer davon ist, bei der Aufnahme ins Krankenhaus beim Patienten Daten abzufragen, die weder für seine Behandlung noch für die verwaltungsmäßige Abwicklung des Aufenthalts erforderlich sind. Das Landeskrankenhausgesetz lässt dies nicht zu. Trotzdem, und obwohl ich diesen Punkt jetzt schon wiederholt in unseren Tätigkeitsberichten angesprochen habe (zuletzt 18. Tätigkeitsbericht 1997, Landtags-Drucksache 12/2242, S. 51), verwenden Krankenhäuser immer noch Aufnahmeformulare, die die Rechtslage schlicht ignorieren. So wird beispielsweise auch im Aufnahmebeleg des Kreiskrankenhauses wieder danach gefragt, ob jemand geschieden oder verwitwet ist oder ob er oder sie getrennt lebt. Das Krankenhaus will Beruf und Arbeitgeber wissen, auch wenn Grund der Aufnahme nicht ein Berufsunfall ist. Auch verlangt es immer die Angabe des Hauptversicherten und seines Arbeitgebers, obwohl dies alles allenfalls dann von Interesse wäre, wenn der Patient keine eigene Krankenversichertenkarte vorlegen kann. Das Krankenhaus selbst hat beim Besuch eingeräumt, dass diese Daten meist nicht benötigt würden. Werden die Aufnahmedaten bei den Patienten erfragt und direkt ins Krankenhausinformationssystem eingegeben, ohne dass der Vordruck ausgefüllt wird, stellt das Aufnahmepersonal einzelne Fragen gar nicht erst. Weshalb dann immer noch die zu weitgehenden Fragebögen? Ich habe dies, wie in der Vergangenheit auch in anderen Fällen, beanstandet.

Das Krankenhaus hat hierauf mitgeteilt, es beabsichtige, den Aufnahmebeleg neu zu entwerfen. Einzelne der von mir beanstandeten Fragen sollen weggelassen oder modifiziert werden. Gleichwohl deutet die Antwort des Krankenhauses darauf hin, dass noch nicht in allen Punkten Einigkeit besteht. Um für alle Eventualitäten gerüstet zu sein, scheint man auch Daten erheben zu wollen, deren konkrete Verwendungsnotwendigkeit im Zeitpunkt der Erhebung noch nicht absehbar ist. Ich habe darauf hingewiesen, dass eine solche Datenerhebung auf Vorrat nicht zulässig ist und hoffe, dass auch das Krankenhaus letztlich bereit sein wird, sein Aufnahmeformular datenschutzkonform auszugestalten. Meine Mithilfe hierzu habe ich angeboten.

2.2 Die Krankenhausseelsorge

Auch das Thema Krankenhausseelsorge ist eigentlich ein alter Hut. Allerdings ist es erstaunlich, wie aus diesem alten Hut immer neue Fallgestaltungen gezaubert werden, die datenschutzrechtliche Fragen aufwerfen.

Gerade in größeren Krankenhäusern ist es oft so, dass jede der beiden großen Kirchen jeweils einen Seelsorger als Krankenhausseelsorger bestellt. Anders dagegen im Kreiskrankenhaus: Hier gibt es nur einen Seelsorger der evangelischen Kirche. Dieser kümmert sich, so das Krankenhaus, grundsätzlich um alle Patienten, gleich welcher Konfession sie angehören. Zu diesem Zweck händigt das Krankenhaus dem Pfarrer wöchentlich aktualisierte Konfessionslisten der evangelischen, katholischen und neuapostolischen Patienten aus. Ich habe das Krankenhaus darauf hingewiesen, dass dies nicht mit dem Gesetz in Einklang steht. Nach § 45 Abs. 2 des Landeskrankenhausgesetzes darf das Krankenhaus die Religionszugehörigkeit nur für Zwecke der Krankenhausseelsorge erheben. Krankenhausseelsorge in diesem Sinne meint aber nicht jede seelsorgerische Betreuung durch einen Geistlichen, sondern setzt eine Betreuung durch einen gerade hierfür von der jeweiligen Kirche bestellten Krankenhausseelsorger voraus. Deshalb darf das Krankenhaus nur die Religionszugehörigkeit erheben und speichern, für die Krankenhausseelsorge in diesem Sinne tatsächlich angeboten wird. Dies ist im Kreiskrankenhaus aber nur für evangelische Patienten der Fall. Weiter verlangt das Gesetz, dass bei der Erhebung der Religionszugehörigkeit nicht nur deutlich auf die Freiwilligkeit der Angabe, sondern auch darauf hingewiesen wird, wozu diese Angabe dient, nämlich Zwecken der Krankenhausseelsorge. Wer, so informiert, seine Religionszugehörigkeit mitteilt, gibt zu erkennen, dass er mit einer Weiterleitung der für die Aufnahme der Krankenhausseelsorge erforderlichen Daten an den Krankenhausseelsorger einverstanden ist; einer ausdrücklichen Einwilligung hierzu bedarf es dann nicht mehr.

Im Aufnahmeformular des Kreiskrankenhauses wird, wenn auch unter Hinweis auf die Freiwilligkeit, generell nach dem Glaubensbekenntnis gefragt, und zwar auch dann, wenn von vornherein klar ist, dass hierfür keine Krankenhausseelsorge angeboten wird (z. B. orthodox). Wozu der Patient diese Angabe eigentlich machen soll, bleibt im Dunkeln. Und schon gar nicht wird klar, dass die Information über die Zugehörigkeit zur katholischen oder neuapostolischen Kirche dem evangelischen Krankenhausseelsorger mitgeteilt wird. Ich halte das für einen gravierenden Mangel und habe das Krankenhaus gebeten, ihn abzustellen. Aus seiner Antwort geht hervor, dass es hierzu grundsätzlich bereit ist. Über Einzelheiten wird aber noch zu sprechen sein.

2.3 Die offene Registratur

Wer im Krankenhaus behandelt wird, erwartet zu Recht, dass alle Daten, die im Zusammenhang mit seiner Behandlung erhoben und gespeichert werden, streng vor dem Zugriff Unbefugter geschützt werden. Der Registratur, in der alle Akten der Krankenhauspatienten zentral aufbewahrt werden, kommt hier eine verantwortungsvolle Aufgabe zu. Sie muss so organisiert sein, dass jederzeit kontrolliert werden

kann, wer in welche Akten einsieht, wer welche Akten entnimmt und wo sich entnommene Akten befinden. Die Rückgabe der Akten muss überwacht und ihre Vernichtung nach Ablauf der Speicherfrist organisiert werden. Eine solche datenschutzgerechte Organisation der Registratur ist nur dann zu gewährleisten, wenn die Räumlichkeiten so beschaffen sind, dass das Registraturpersonal tatsächlich auch jederzeit feststellen kann, wer sich an den Akten zu schaffen macht. Dies ist im Kreiskrankenhaus nicht der Fall. Denn dort sind Registratur und zentraler Schreibdienst gemeinsam in einem Raum untergebracht. Immer dann, wenn die Registratur nicht besetzt ist, ist sowohl dem Schreibpersonal als auch denjenigen, die den Schreibdienst aufsuchen, der gesamte Aktenbestand offen zugänglich. Da die Registraturmitarbeiter, wie uns gesagt wurde, ihren Dienst nachmittags regelmäßig vor den Schreibkräften beenden, hat dies zur Folge, dass ab diesem Zeitpunkt der Zugriff auf die Patientenakten nicht mehr kontrolliert wird. Erst wenn die gemeinsame Eingangstür zu Schreibdienst/Registratur in der Regel von der Schreibkraft, die ihren Dienst als Letzte beendet, abgeschlossen wird, gelangt nur noch in die Registratur, wer an der Pforte den Schlüssel abholt und dies auch quittiert.

Diese Art der Aktenaufbewahrung ist mit einer datenschutzgerechten Organisation nicht zu vereinbaren. Ich habe das Kreiskrankenhaus aufgefordert, durch bauliche Maßnahmen sicherzustellen, dass die Registratur gegenüber dem Schreibdienst abgeschottet und dadurch gewährleistet wird, dass auch nach Dienstende des Registraturpersonals niemand unkontrolliert auf die Patientenakten zugreifen kann. Dies gilt grundsätzlich auch für die Schreibkräfte. Zwar erhalten diese in Erfüllung ihres Schreibauftrags regelmäßig Einblick in die jeweils zu bearbeitende Krankenakte. Eine Berechtigung dafür, ihnen generell Zugang zu allen Patientenakten des Krankenhauses zu gewähren, lässt sich daraus aber nicht herleiten.

Das Krankenhaus hat dem entgegengehalten, eine Abschottung der Registratur gegenüber dem Schreibbüro sei nicht notwendig, da alle im Krankenhaus beschäftigten Personen zur Verschwiegenheit verpflichtet seien und es darauf vertrauen müsse, dass niemand dagegen verstößt. Die Praxis zeigt allerdings, dass dieses Vertrauen nicht immer berechtigt ist, zum Schaden der davon Betroffenen. Angesichts der Sensibilität der medizinischen Informationen, die in einem Krankenhausarchiv in konzentrierter Form vorhanden sind, ist es schlichtweg unvertretbar, Sicherungsmaßnahmen allein mit dem Hinweis zu unterlassen, man vertraue seinem Personal. Das Landesdatenschutzgesetz sagt aus guten Gründen ganz eindeutig, dass allein die Existenz von Datenschutzvorschriften nicht ausreicht, sondern dass vielmehr auch Maßnahmen zu treffen sind, die die Einhaltung dieser Vorschriften gewährleisten.

2.4 Die herrenlosen Gutachten

Beim Betreten des zentralen Schreibbüros fällt der Blick unweigerlich auf ein meterlanges, bis zur Decke reichendes Regal, in dem hunderte von Akten offen zugänglich aufbewahrt werden. Die Annahme, dass es sich hierbei bereits um Teile der Krankenhausregistratur handelt, bestätigte sich auf Nachfrage nicht. Vielmehr wurde erklärt, es handle sich um Gutachten, die Krankenhausärzte privat im Rahmen einer Nebentätigkeit angefertigt und dann hier abgelegt hätten. Die weitere Nachfrage, wie denn beispielsweise sichergestellt werde, dass keine Unbefugten auf die Akten zugreifen, ergab, dass sich weder das Registraturpersonal noch sonst jemand für diese Aktensammlung zuständig fühlt und deshalb auch keine Kontrolle stattfindet. Ich halte diesen Zustand für untragbar und habe dies beanstandet.

Auch wenn die Verantwortung für die Geheimhaltung der in diesen Gutachtenakten enthaltenen Patientengeheimnisse in erster Linie den Ärzten, die die Gutachten erstellt haben, obliegt, kann auch das Krankenhaus nicht völlig aus der Verantwortung entlassen werden. Denn wenn es die Akten für die Ärzte aufbewahrt, findet rechtlich eine Da-

tenverarbeitung im Auftrag statt. Daraus erwächst für das Krankenhaus die Pflicht zu einem datenschutzgerechten Umgang mit diesen Akten. Dieser Pflicht kommt es jedenfalls nicht nach, wenn es die Akten sich selbst überlässt.

In seiner Stellungnahme zu meinem Kontrollbericht begnügte sich das Krankenhaus auch in dieser Frage mit dem Hinweis auf die Geheimhaltungspflicht des Krankenhauspersonals.

2.5 Zu weitgehende Zugriffsrechte für die Pforte

Für viele, die kranke Familienangehörige, eine Freundin oder einen kranken Freund im Krankenhaus besuchen möchten, ist die Pforte oft die erste Anlaufstelle. Sie sind dann sehr froh darüber, dass die dort Tätigen ihnen rasch und präzise Auskunft darüber geben können, wo sie den zu Besuchenden finden. Neben dieser ureigenen und allseits geschätzten Aufgabe betraut ein Krankenhaus sein Pfortenpersonal mitunter mit Weiterem. So ist das Pfortenpersonal des Kreiskrankenhauses dafür zuständig, einige wenige Angaben über einen aufzunehmenden Patienten in das Krankenhaus-EDV-System einzugeben, falls die Patientenaufnahme außerhalb der üblichen Öffnungszeiten der Patientenaufnahmestelle erfolgt. Zulässig wäre nun gewesen, wenn das Kreiskrankenhaus seinem Pfortenpersonal genau die Zugriffsrechte im EDV-System eingeräumt hätte, die es benötigt, um diesen seinen beiden Aufgaben nachkommen zu können. Daran hielt sich das Kreiskrankenhaus freilich bei weitem nicht. Auf dem Bildschirm des Pfortenpersonals erscheinen nämlich Name, Vorname und Geburtsdatum aller seit dem 1. Januar 1995 im Kreiskrankenhaus stationär behandelten Patienten und gleich auch noch ihr Aufnahme- und Entlassdatum, die Behandlungsart und die Stationen sämtlicher Krankenhausaufenthalte. Damit kann das Pfortenpersonal aber auf weit mehr zugreifen als für die Erfüllung der ihm übertragenen dienstlichen Aufgaben notwendig und damit zulässig ist. Für die Erteilung von Auskünften an Besucher genügt, wenn das Pfortenpersonal einige wenige Angaben über die Patienten abrufen kann, die gerade in stationärer Behandlung sind. Wegen etwaiger Nachfragen mag es sogar angehen, den Zugriff auch noch für einen gewissen Zeitraum nach der Entlassung eines Patienten aufrechtzuerhalten. Für die Aufnahme eines Patienten außerhalb der üblichen Öffnungszeiten der Patientenaufnahmestelle reicht es aus, wenn das Pfortenpersonal die zu erfassenden Angaben über den Patienten in das EDV-System eingeben kann und nur dann, wenn dieser Patient bereits früher einmal im Krankenhaus in Behandlung war, von dessen früheren Krankenhausaufenthalten erfährt. Auf meine Forderung, die Zugriffsrechte des Pfortenpersonals in dieser Weise auf das zulässige Maß zu beschränken, hat das Kreiskrankenhaus inzwischen mitgeteilt, mit dem eingesetzten EDV-System sei dies nicht machbar. Das Kreiskrankenhaus wolle das System aber im ersten Quartal 2000 ablösen und werde durch eine geeignete Auswahl der Software darauf achten, den Mangel abzustellen.

2.6 Wenn Daten außer Haus gehen

Will ein Beschäftigter des Kreiskrankenhauses Daten mit nach Hause nehmen, um sie etwa an seinem häuslichen PC weiterzubearbeiten, so kann er die Daten zwar nicht selbst auf eine Diskette kopieren, weil im Wesentlichen nur die Arbeitsplätze der EDV-Mitarbeiter mit benutzbaren Diskettenlaufwerken ausgestattet sind. Der Beschäftigte kann sich mit seinem Wunsch aber telefonisch an die EDV-Abteilung des Kreiskrankenhauses wenden. Diese kopiert ihm dann die Daten auf eine Diskette und leitet sie ihm zu. Die Gretchenfrage für den Datenschutz ist nun zunächst, ob die Beschäftigten des Kreiskrankenhauses auch Patientendaten mit nach Hause nehmen dürfen oder nicht. Will das Kreiskrankenhaus solches erlauben, muss es auf geeignete Weise regeln, wie sich ein datenschutzgerechter Umgang mit den Daten auch außerhalb des Krankenhauses sicherstellen und kontrollieren lässt. Dass dies kein einfaches Unterfangen ist, versteht sich von selbst, weil schließlich ein Arbeitsplatz im Krankenhaus und die dort

getroffenen Datenschutzmaßnahmen auf der einen sowie häusliches Umfeld und privater PC auf der anderen Seite zwei völlig verschiedene Paar Stiefel sind. Will das Kreiskrankenhaus solchem Tun dagegen von vornherein einen Riegel vorschieben, muss es seinen Beschäftigten die Mitnahme von Patientendaten zumindest per Dienstanweisung untersagen. Das Kreiskrankenhaus tat weder das eine noch das andere. Eine Regelung, ob die Beschäftigten auch Patientendaten mit nach Hause nehmen dürfen, existierte im Kreiskrankenhaus nicht. Ob im Zuge eines Datentransfers schon einmal Patientendaten das Krankenhaus verlassen haben, konnte das Kreiskrankenhaus nicht sagen. Eine Prüfung, welche Daten das Krankenhaus verlassen, war nicht vorgesehen und erfolgte auch nicht. Damit machte es sich das Kreiskrankenhaus aber entschieden zu einfach. Es schloss nicht aus, dass auch personenbezogene Daten nach außen gelangen, ohne dass es festgelegt hätte, wie mit den Daten datenschutzgerecht umzugehen ist. Diesen Mangel musste ich beanstanden. Inzwischen hat das Kreiskrankenhaus wenigstens per Dienstanweisung festgelegt, dass keine Patientendaten, sondern nur Daten, die nicht auf einzelne Patienten bezogen werden können, das Krankenhaus verlassen dürfen.

3. Datenschutz im Gesundheitsamt

Seit 1. Januar 1995 haben die Gesundheitsämter die Datenverarbeitungsregelungen des Gesundheitsdienstgesetzes zu beachten. Es kann kaum verwundern, dass sich mein Amt immer wieder mit der Praktizierung dieser verhältnismäßig neuen Bestimmungen zu befassen hatte.

3.1 Die Fortbildung der Amtsärzte

Zu den Aufgaben meines Amtes gehört es, öffentliche Stellen im Lande in Fragen des Datenschutzes zu beraten. Dieser Service wird zunehmend in Anspruch genommen, was sehr zu begrüßen ist. Denn werden die Weichen für datenschutzgerechtes Verhalten frühzeitig gestellt, ist dies allemal besser, als nachträglich korrigierend eingreifen zu müssen. In diesem Rahmen ist auch eine ganztägige Informations- und Fortbildungsveranstaltung zum Thema „Datenschutz im Gesundheitsamt“ zu sehen, die zu Beginn des Jahres auf Initiative des Sozialministeriums beim Landesgesundheitsamt stattgefunden hat. Eingeladen waren die Amtsärzte aller Gesundheitsämter im Lande. Anhand eines vom Sozialministerium vorbereiteten Katalogs wurden diverse Fragestellungen aus der Praxis der Gesundheitsämter besprochen. Dem Vernehmen nach empfanden die Teilnehmer die Veranstaltung überwiegend positiv, auch wenn die Ansichten zu bestimmten Themen teilweise kontrovers waren und die Positionen des Datenschutzes nicht immer auf ungeteilte Zustimmung stießen. Die Ergebnisse der Veranstaltung wurden schriftlich zusammengefasst und den Gesundheitsämtern zur Verfügung gestellt. Nachfolgend ein kleiner Ausschnitt aus dem Themenkatalog:

– Breiten Raum in der Diskussion nahm das Thema Aktenführung beim Gesundheitsamt ein. Wie in den Tätigkeitsberichten der beiden letzten Jahre (18. Tätigkeitsbericht 1997, Landtags-Drucksache 12/2242, S. 57 f.; 19. Tätigkeitsbericht 1998, Landtags-Drucksache 12/3480, S. 34 f.) dargestellt, normiert das Gesundheitsdienstgesetz (ÖGDG) eine strenge Zweckbindung für die im Zusammenhang mit einer Untersuchung, Begutachtung oder Beratung vom Gesundheitsamt erhobenen Patientendaten. Für andere Zwecke als den, zu dem sie ursprünglich erhoben wurden, dürfen diese Daten nur unter den engen Voraussetzungen des § 16 ÖGDG genutzt werden. Diese vom Gesetzgeber angeordnete Zweckbindung würde unterlaufen, wenn alle Informationen, die das Gesundheitsamt über einen Patienten im Laufe der Zeit erhebt, in einer Akte zusammengefasst gespeichert werden. Denn wer immer diese Akte zur Hand nimmt, erhält einen vollständigen Überblick über sämtliche Kontakte des Betreffenden mit dem Gesundheitsamt. Eine streng zweckgebundene Datennutzung wäre damit faktisch nicht mehr zu gewährleisten, da

kaum anzunehmen ist, dass die einmal zur Kenntnis genommenen Informationen nicht auch in anderem Zusammenhang verwendet werden. Gerade damit wird aber seitens der Amtsärzte die Notwendigkeit einer Patientenakte begründet. In der Diskussion wurde immer wieder vorgebracht, als Amtsarzt müsse man doch „richtige" Gutachten erstatten und dies setze die Kenntnis des vollständigen Inhalts der über den Patienten bestehenden Akten voraus. Verkannt wird dabei aber, dass es sich zum einen nicht mit der ärztlichen Schweigepflicht verträgt, wenn Kollegen Patientengeheimnisse untereinander austauschen. Denn auch die Amtsärzte haben (untereinander) ihre standesrechtlichen Berufsgeheimnisse zu wahren, wobei sie ebenso der Strafandrohung des § 203 des Strafgesetzbuches unterliegen wie jeder andere Arzt. Der Umstand, dass sie bei einer Behörde beschäftigt sind, ändert hieran grundsätzlich nichts. Zum anderen macht die angeordnete Zweckbindung auch aus einem anderen Grund guten Sinn. Denn wer zum Amtsarzt geht, tut dies nicht, weil er von einer Krankheit oder einem Leiden geheilt werden will. Das Argument, die vollständige Kenntnis der (medizinischen) Vorgeschichte diene dem Wohl des Patienten, trifft also hier nicht ohne weiteres zu. Er tut dies vielmehr, weil er gesetzlich hierzu verpflichtet ist oder weil er ein amtsärztliches Zeugnis als Voraussetzung für eine (in der Regel behördliche) Begünstigung benötigt und im Vertrauen darauf, dass das, was in diesem Zusammenhang über ihn gespeichert wird, nicht später möglicherweise in anderem Zusammenhang zu seinem Nachteil verwendet werden wird. Daran, dass es im Gesundheitsamt nicht um Heilbehandlung, sondern dem Grunde nach um gesetzesgebundene Verwaltungstätigkeit, wenn auch von Ärzten erbracht, geht, muss ebenso immer wieder erinnert werden wie an die ärztliche Schweigepflicht. Aus diesen Gründen ergibt sich zwangsläufig, dass die Akten des Gesundheitsamts jeweils nach Untersuchungszwecken getrennt zu führen sind. Im Übrigen muss es einem Amtsarzt grundsätzlich möglich sein, eine Untersuchung auch dann fachgerecht durchzuführen, wenn er nicht auf Erkenntnisse aus vorangegangenen Untersuchungen zurückgreifen kann – eine Situation, in der er sich in jedem Fall dann befindet, wenn er erstmals mit einem Patienten zu tun hat. Eine Möglichkeit, auf Daten zurückzugreifen, die für andere Zwecke erhoben und gespeichert wurden, hat der Amtsarzt ja nach wie vor, nämlich dann, wenn der Patient damit einverstanden ist. Im Einzelfall kann es durchaus gute Gründe geben, Vorakten beizuziehen, wenn dadurch beispielsweise Doppeluntersuchungen vermieden werden können. Ein einsichtiger Patient wird sich dem wohl nur selten verschließen. Auch ansonsten kann es durchaus sein, dass der Amtsarzt berechtigt ist, ohne Einwilligung des Patienten auf dessen Vorakten zuzugreifen, soweit dies zur Wahrung eines höherwertigen Rechtsguts erforderlich ist und der Widerstreit der rechtlich geschützten Güter nur durch die Preisgabe des einen und nicht auf andere Weise gelöst werden kann.

– Immer wieder gefragt wurde nach Löschungsfristen. Die gesetzlichen Vorgaben verpflichten zu einer Löschung von Daten, wenn diese für die weitere Aufgabenerfüllung nicht mehr erforderlich sind. Insofern lässt sich eine generelle Löschungsfrist nur schwer bestimmen. Abgesehen von den Fällen, in denen sie fachgesetzlich vorgegeben ist (z. B. § 28 Abs. 4 der Röntgenverordnung oder § 66 Abs. 1 der Strahlenschutzverordnung), kann in Anlehnung an die ärztliche Berufsordnung von einer Aufbewahrungsfrist von längstens zehn Jahren ausgegangen werden. Dies sollte allerdings nicht schematisch zu Grunde gelegt werden, da es durchaus auch Fälle geben kann, in denen eine vorzeitige Löschung vertretbar ist.

– Auch Ersuchen des Wirtschaftskontrolldienstes um Datenübermittlungen unterliegen den engen Grenzen des Gesundheitsdienstgesetzes (es muss um die Verfolgung von Verbrechen und von Straftaten gegen die sexuelle Selbstbestimmung von erheblicher Bedeutung oder von Körperverletzungen von erheblicher Bedeutung gehen und

das Strafverfolgungsinteresse muss gegenüber dem Geheimhaltungsinteresse des Betroffenen erheblich überwiegen), soweit nicht speziellere Bestimmungen vorgehen. Dazu gehört aber beispielsweise das Bundes-Seuchengesetz nicht. Dieses lässt einen Datenaustausch nur mit der „zuständigen Behörde“ zu, womit die allgemeinen Polizeibehörden gemeint sind. Der Wirtschaftskontrolldienst als Fachdienst des Polizeivollzugsdienstes gehört nicht dazu. Er kann im Übrigen auch aus § 161 der Strafprozeßordnung keine Mitteilungsansprüche herleiten, da Amtsärzte ein Zeugnisverweigerungsrecht aus beruflichen Gründen haben.

– Wollen Sozialversicherungsträger oder Versorgungsämter Auskünfte aus dem vertraulichen Teil der Leichenschauscheine erhalten, können die Gesundheitsämter diese nach Maßgabe von § 22 Abs. 5 des Bestattungsgesetzes erteilen. Diese Bestimmung lässt die Gewährung von Einsicht in den oder die Erteilung von Auskünften aus dem Leichenschauschein zu, wenn der Antragsteller ein rechtliches Interesse an der Kenntnis über die Todesumstände des Verstorbenen glaubhaft macht und kein Grund zu der Annahme besteht, dass durch die Offenbarung schutzwürdige Belange des Verstorbenen oder der Hinterbliebenen beeinträchtigt werden. Eine Einwilligung der Angehörigen braucht nicht vorzuliegen.

3.2 Sage nicht alles was du weißt, aber wisse immer, was du sagst

Hätte das Gesundheitsamt des Landratsamts Schwäbisch Hall diese Sentenz beherzigt, hätte es einen gravierenden Datenschutzverstoß vermieden. Zugetragen hatte sich dies: Eine Dienststelle bat das Gesundheitsamt um ein amtsärztliches Gutachten zur Frage, ob einer ihrer Mitarbeiter den gesundheitlichen Anforderungen seines Dienstes in vollem Umfang genügt oder zumindest für eine bestimmte Tätigkeit dienstfähig sei. Auf Grund der Untersuchung des Probanden erstattete das Gesundheitsamt formlos das erbetene Gutachten, wobei es detaillierte Ausführungen zum beruflichen Werdegang, zur Entwicklung des Beschwerdebildes, dem psychischen Befund und den Diagnosen des Probanden machte. Bei allem Verständnis für eine gründliche Exploration ging dem Bediensteten die Weitergabe dieser sensiblen Informationen an seine Dienststelle dann doch zu weit, und er hatte völlig Recht damit. Nach dem Gesundheitsdienstgesetz darf der Amtsarzt nämlich bei ärztlichen Untersuchungen der Stelle, welche die Untersuchung veranlasst hat, grundsätzlich nur das Ergebnis der Untersuchung mitteilen. Nur ausnahmsweise darf er Anamnese und einzelne Untersuchungsergebnisse weitergeben, soweit die Auftrag gebende Stelle diese Informationen für ihre Entscheidung über die konkrete Maßnahme, weswegen sie die Untersuchung durchführen ließ, benötigt. Um den Gesundheitsämtern die Beachtung dieser Beschränkungen zu erleichtern, hat das Sozialministerium diesen durch eine Verwaltungsvorschrift Muster von amtsärztlichen Zeugnissen gegeben. Zudem hat es in dieser Verwaltungsvorschrift klar und deutlich geschrieben:

„Einzelheiten aus Anamnese und Befunderhebung werden grundsätzlich nur mit schriftlichem Einverständnis der untersuchten Person mitgeteilt, wenn die das Zeugnis anfordernde Dienststelle dies im Einzelfall ausdrücklich fordert und dabei darlegt, aus welchen Gründen diese Angaben erforderlich sind oder dies vom untersuchenden Arzt für zwingend erforderlich gehalten wird. Angaben aus der Familienanamnese werden nicht weitergegeben.“

Weil keine dieser Voraussetzungen auch nur ansatzweise gegeben war, beanstandete ich die unzulässige Weitergabe der höchst sensiblen Informationen über den Mitarbeiter an dessen Dienststelle gegenüber dem Sozialministerium. In seiner Stellungnahme versicherte dieses, das Gesundheitsamt werde künftig bei der Weitergabe von Untersuchungsergebnissen die Rechtslage beachten.

4. Die gesundheitliche Eignung

Wer den Diätassistentenberuf ergreifen, wer Krankenschwester oder Krankenpfleger oder wer Technischer Assistent in der Medizin werden möchte, braucht eine entsprechende Ausbildung. Zu diesem Zweck kann man sich beispielsweise bei den beim Katharinenhospital der Landeshauptstadt Stuttgart eingerichteten Schulen (Diätschule, Krankenpflegeschule, Schule für Technische Assistenten in der Medizin) bewerben. Wer hier aufgenommen werden möchte, muss neben dem entsprechenden Schulabschluss auch nachweisen, dass er sich gesundheitlich für die Ausübung des Berufs eignet. Dies ist im Gesetz so bestimmt. Nicht geregelt ist dort allerdings, wie dies nachzuweisen ist.

Die Schulen verwenden zu diesem Zweck einen Vordruck „Ärztliches Zeugnis“, den die Bewerberin oder der Bewerber von einem Arzt ausfüllen lassen und der Schule vorlegen muss. Gefragt wird nach Krankenhausaufenthalten, nach körperlichen Mängeln, nach Krankheiten – insgesamt eine sehr ins Einzelne gehende Auflistung sehr persönlicher Informationen. Anhand der Angaben des Arztes prüft die Zulassungskommission der Schule dann, ob gesundheitliche Gründe den Bewerber oder die Bewerberin als für den Beruf ungeeignet erscheinen lassen. Ist dies der Fall, erfolgt schon aus diesem Grund eine Absage. Aufgenommene Schüler müssen sich dann vor Beginn des praktischen Teils der Ausbildung noch vom betriebsärztlichen Dienst des Krankenhauses untersuchen lassen.

Wie beim Einsatz von Vordrucken leider immer wieder festzustellen ist, war auch der von den Schulen verwendete Fragenkatalog entschieden zu umfangreich. Nach den jeweils maßgeblichen gesetzlichen Bestimmungen ist von der Berufsausübung nur ausgeschlossen, wer hierzu wegen eines körperlichen Gebrechens, wegen Schwäche seiner geistigen oder körperlichen Kräfte oder wegen einer Sucht unfähig oder ungeeignet ist. Und wer solchermaßen für die Berufsausübung nicht geeignet ist, darf auch schon zur Ausbildung nicht zugelassen werden. Weshalb es nun aber, um darüber entscheiden zu können, auch darauf ankommen soll zu wissen, welche Kinderkrankheiten man hatte, wogegen man geimpft wurde oder welchem Konstitutionstyp man entspricht, ist nicht nachvollziehbar. Personenbezogene Daten, die für die konkrete Aufgabenerfüllung nicht benötigt werden, dürfen aber nicht erhoben werden. Dies widerspricht den das Datenschutzrecht beherrschenden Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit. Meine Intervention hatte Erfolg, die Schulen haben den Fragenkatalog inzwischen deutlich eingeschränkt und gestrafft. Ich kann dies nur begrüßen.

Nach einer gemeinsamen Besprechung mit den Leiterinnen der drei Schulen habe ich noch auf Folgendes hingewiesen:

– In manchen Fällen wird sich allein schon auf Grund des Schulzeugnisses oder anderer Umstände ergeben, dass jemand für die Ausbildung nicht in Frage kommt. Auf die gesundheitliche Eignung für den Beruf kommt es hier gar nicht mehr an. Folglich wäre die Vorlage eines „Ärztlichen Zeugnisses“ in diesen Fällen an sich unnötig. Deshalb sollte das Verfahren nach Möglichkeit so ausgestaltet werden, dass die Bewerberinnen und Bewerber das „Ärztliche Zeugnis“ erst dann vorlegen müssen, wenn feststeht, dass sie nicht schon aus anderen als gesundheitlichen Gründen abgelehnt werden.

– Die Bewerber müssen über die Verwendung des „Ärztlichen Zeugnisses“ aufgeklärt werden. Dies geschieht bisher nicht. Diese Aufklärung sollte schon bei der Anforderung des Zeugnisses erfolgen.

– Nach Abschluss des Bewerbungsverfahrens hat die Schule für das „Ärztliche Zeugnis“ keine Verwendung mehr. Seine Aufbewahrung in den Bewerberakten ist von da an unnötig, deshalb sollte es zurückgegeben werden.

2. Abschnitt: Die Sozialversicherung

1. Krankenversicherung

Die gesetzliche Krankenversicherung ist der älteste Zweig der Sozialversicherung. Rund 90 % der Bevölkerung des Bundesgebiets gehören ihr an. Über jeden dieser gut 70 Millionen Versicherten werden im Versicherungsfall medizinische Daten verarbeitet. Durch wen und wie dies geschieht, ist Vielen nicht bekannt. Umso notwendiger ist es deshalb, dass es Kontrollinstanzen gibt, die darauf achten, dass sorgsam mit diesen Daten umgegangen wird. Auch im Berichtszeitraum hat sich mein Amt wieder bemüht, dieser Aufgabe im Rahmen seiner Möglichkeiten nachzukommen.

1.1 Novellierung des SGB V – Gesundheitsreform 2000

Nur wenige Gesetzesvorhaben der vergangenen Jahre haben zu einer solchen Mobilisierung weiter Bevölkerungskreise geführt wie der Entwurf des Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000, kurz Gesundheitsreform 2000. Fast überwiegend ging und geht es nach wie vor bei den Protesten ums Geld – Stichwort Globalbudget. Weit weniger beachtet wurde in der öffentlichen Diskussion, dass dabei auch zu entscheiden ist, in welchem Umfang Versicherte, aber auch Ärzte, Zahnärzte und andere sog. Leistungserbringer Eingriffe in ihr Grundrecht auf Datenschutz hinnehmen müssen. Die Gesundheitsreform 2000 will auch hier gravierend in das bisherige Regelungsgefüge eingreifen und neue Strukturen schaffen. Was an den dazu im Regierungsentwurf vorgesehenen Regelungen zu kritisieren war, habe ich dem Sozialministerium in einer umfangreichen Stellungnahme mitgeteilt. An dieser Stelle will ich mich auf einen ganz zentralen Punkt beschränken, der die vielfach beschworene Gefahr des „gläsernen Patienten“ ein erhebliches Stück realer hätte werden lassen – wenn es nicht anders gekommen wäre.

Bisher ist es so, dass die Abrechnung ärztlicher Leistungen grundsätzlich fallbezogen, nicht versichertenbezogen zu erfolgen hat. Die Krankenkasse kann also aus den Abrechnungen der Ärzte und Zahnärzte, die ihr von der Kassen- und Kassenzahnärztlichen Vereinigung vorgelegt werden, nicht erkennen, um welchen Versicherten es konkret geht. Nur in besonderen Ausnahmefällen, vor allem zu Prüfzwecken, ist die Krankenkasse berechtigt, sich Versicherteninformationen personenbezogen zu beschaffen. Apotheken, Krankenhäuser und sonstige Leistungsträger rechnen dagegen immer personenbezogen mit der Krankenkasse ab.

Der Gesetzentwurf sah zunächst folgendes neues Verfahren vor: Es sollten sog. Datenannahmestellen eingerichtet werden. Alle Leistungserbringer sollten diesen Datenannahmestellen ihre Abrechnungsdaten versichertenbezogen übermitteln. Die Datenannahmestellen sollten die Rechnungen prüfen und sie dann, ebenfalls versichertenbezogen, an die Krankenkassen weiterleiten. Im Unterschied zum bisherigen Zustand hätte es demnach künftig Stellen gegeben, deren Rechtsform nebenbei völlig offen blieb, bei denen zentral große Mengen medizinischer Informationen über die Krankenversicherten personenbezogen vorgelegen hätten – eine Horrorvorstellung für jeden, der Datenschutz ernst nimmt. Aber damit nicht genug. Auch die Krankenkassen hätten dann alle Abrechnungsdaten versichertenbezogen erhalten, also auch die, die sie bisher nur fallbezogen bekommen. Sie hätten alle diese Daten unter Einsatz der EDV speichern können und wären damit in der Lage gewesen, über jeden Versicherten ein vollständiges Gesundheitsprofil zu erstellen. Die Datenschutzbeauftragten des Bundes und der Länder haben sich in einer Entschließung vom 25. August 1999 (vgl. Anhang 3) mit Nachdruck dagegen gewandt. Und, was nicht unbedingt zu erwarten war, sogar mit Erfolg.

Die am 4. November 1999 vom Bundestag angenommene Fassung des Gesetzentwurfs sieht nun Folgendes vor: Zwar bleibt es dabei, dass Datenannahmestellen eingerichtet werden sollen. Diesen sollen

auch weiterhin alle Abrechnungs- und Leistungsdaten personenbezogen mitgeteilt werden. Klargestellt ist jetzt aber, dass diese Stellen in keiner Weise mit den Krankenkassen und ihren Verbänden zusammenhängen und dass es keine privaten Stellen sein dürfen. Geregelt ist weiter, dass die Datenannahmestellen die versichertenbezogenen Daten vor der Weiterleitung an die Krankenkassen zu pseudonymisieren haben, wobei eine Reidentifikation nur einer von der Datenannahmestelle räumlich und organisatorisch getrennten Stelle, also einer Art Trust-Center, und nur in den vom Gesetz besonders bestimmten Fällen möglich sein darf. Die Datenannahmestellen sollen verpflichtet werden, die Abrechnungs- und Leistungsdaten unverzüglich zu löschen, wenn diese nicht mehr benötigt werden. Aus Datenschutzsicht ist diese Lösung sehr zu begrüßen (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999; vgl. Anhang 4). Nicht nur würde damit die bisher geplante Verschlechterung des Datenschutzes unterbleiben. Es würde sogar insoweit eine Verbesserung eintreten, als die Krankenkassen auch die Abrechnungs- und Leistungsdaten, die ihnen bisher (beispielsweise von Krankenhäusern) versichertenbezogen zugegangen sind, künftig nur noch unter einem Pseudonym erhalten würden. Es bleibt zu hoffen, dass das Rad im weiteren Verlauf des Gesetzgebungsverfahrens insoweit nicht mehr zurückgedreht wird.

1.2 Fortsetzung folgt: Die Krankenkassen und der Arztbericht

Im letzten Tätigkeitsbericht (Landtags-Drucksache 12/3480, S. 23) habe ich die Anforderung von Arztberichten durch die Krankenkassen als Dauerthema bezeichnet. Die Hoffnung, dass vielleicht doch endlich Schluss sei mit dieser schon mehrfach kritisierten Praxis, erfüllte sich leider nicht. Sieht man die Vielzahl der Eingaben, mit denen sich Ärzte, Krankenhäuser und Bürger im Berichtszeitraum darüber beschwerten, dass ihnen von Krankenkassen medizinische Informationen über ihre Patienten abverlangt wurden, gewinnt man den Eindruck, es gehe munter weiter wie bisher.

Beim näheren Befassen mit den Anfragen zeigte sich allerdings auch, dass es um durchaus unterschiedliche Sachverhalte ging, die rechtlich nicht alle gleich zu bewerten waren. Gerade diese Vielgestaltigkeit der Kassenanfragen führt immer wieder zu Verwirrung. Deshalb der nachfolgende Versuch einer Differenzierung:

– Soweit es die Umstände des Einzelfalles erfordern, muss die Krankenkasse bei Arbeitsunfähigkeit den Medizinischen Dienst der Krankenversicherung (MDK) mit einer Begutachtung des Versicherten mit dem Ziel beauftragen festzustellen, ob der Versicherte der Rehabilitation bedarf, oder um Zweifel an der Arbeitsunfähigkeit zu beseitigen (§ 275 Abs. 1 Nr. 3 SGB V). Werden hierzu medizinische Informationen von Leistungserbringern benötigt, müssen sie diese dem MDK unmittelbar übermitteln (§ 276 Abs. 2 Satz 1, Halbsatz 2 SGB V). Die Krankenkasse kann diese Daten nicht für sich selbst anfordern, um sie dann an den MDK weiterzuleiten. Dies auch dann nicht, wenn der Betroffene eingewilligt hat; eine solche Einwilligung einzuholen, würde die bewusste Entscheidung des Gesetzgebers umgehen, die Krankenkasse von der Kenntnisnahme medizinischer Informationen in den Fällen der zwingenden Beteiligung des MDK auszuschließen. Dass dies so ist, wird mittlerweile auch von den Krankenkassen wohl nicht mehr bestritten. Für die AOK Baden-Württemberg hat uns dies deren Hauptverwaltung ausdrücklich bestätigt. Sie hat darauf hingewiesen, dass sie eine Datenschutz-Verfahrensanweisung herausgegeben habe, in der sie zwei datenschutzkonforme Vorgehensweisen beschreibt: Entweder fordert der MDK selbst die von ihm benötigten Unterlagen unmittelbar beim Leistungserbringer an. Oder er bittet die Krankenkasse darum, diese für ihn anzufordern. In diesem Fall muss sich aus dem Anschreiben der Krankenkasse ergeben, dass die Unterlagen unmittelbar an den MDK zu senden sind. Zum Teil wird es auch so gehandhabt, dass dem Arzt oder dem Krankenhaus ein far-

biger, an den MDK adressierter Umschlag gleich mitgeliefert wird. Die jeweiligen Anschreiben hat die AOK in Form von Textbausteinen vorgegeben. Schließlich wurden die Bezirksdirektionen auf Schulungsveranstaltungen hierauf hingewiesen.

Leider scheinen sich diese Vorgaben in der Praxis nur sehr schleppend im Bewusstsein der Mitarbeiterinnen und Mitarbeiter der Kassen zu verankern. Wiederholt mit Eingaben von Leistungserbringern und Versicherten konfrontiert, in denen nach wie vor Arztberichte an sich selbst angefordert werden, entschuldigen sich die Kassen regelmäßig damit, dass es sich um bedauerliche Einzelfälle handle, in denen noch nach der alten Weise verfahren werde. Es bleibt zu hoffen, dass sich im Laufe der Zeit auch bis zum letzten Mitarbeiter der Krankenkassen herumspricht, dass ihn Arztberichte grundsätzlich nichts anzugehen haben.

– Immer wieder wenden sich Ärzte an mich und legen mir Anfragen von Krankenkassen vor, in denen diese um Auskünfte über einen Patienten bitten unter Hinweis darauf, dass damit ggf. eine körperliche Untersuchung durch den MDK vermieden werden könne oder ggf. Maßnahmen zur Wiederherstellung der Arbeitsfähigkeit eingeleitet werden könnten. Hintergrund ist folgender: Die Frage, ob es in einem konkreten Fall erforderlich ist den MDK einzuschalten, hat die Krankenkasse auf der Grundlage der ihr vorliegenden Informationen zu beantworten. Bestehen insoweit Zweifel, ist die Krankenkasse berechtigt, personenbezogene Daten zu erheben. Können die Zweifel so beseitigt werden, entfällt unter Umständen eine ansonsten erforderliche körperliche Untersuchung durch den MDK. Bei diesen Anfragen gehen die Krankenkassen nach der von ihren Spitzenverbänden als Richtlinie beschlossenen Begutachtungsanleitung „Arbeitsunfähigkeit“ vor. Insbesondere benutzen sie bei ihren Arztanfragen die nach der Vordruckvereinbarung hierfür geschaffenen Vordrucke Muster 52. Der ärztliche Fragebogen soll allerdings überarbeitet werden. Ein entsprechender Vorschlag der Spitzenverbände der Krankenkassen liegt der Formularkommission vor. Die AOK Baden-Württemberg setzt diesen überarbeiteten Fragebogen, der gegenüber dem bisherigen deutlich ausführlicher ausfällt, bereits ein. Nachdem die AOK die Frage nach den Befunden aus dem Formular entfernt hat, bestehen gegen den Inhalt der Erhebung an sich keine durchgreifenden Bedenken mehr.

  Allerdings, und hier gehen die Meinungen auseinander, sehe ich keine Verpflichtung der Ärzte, den Auskunftsersuchen der Krankenkassen nachzukommen. Die AOK meint, eine solche Verpflichtung ergebe sich aus § 100 Abs. 1 Satz 1 Nr. 1 SGB X, wonach der Arzt zur Auskunftserteilung verpflichtet ist, wenn er nach einer anderen Bestimmung hierzu berechtigt ist. Eine solche Berechtigung sieht die AOK in § 73 Abs. 2 Nr. 9 SGB V, wo es heißt: „Die vertragsärztliche Versorgung umfasst die Ausstellung von Bescheinigungen und Erstellung von Berichten, die die Krankenkassen … zur Durchführung ihrer gesetzlichen Aufgaben … benötigen“. Dem Wortlaut nach regelt die Vorschrift also allein den Rahmen der vertragsärztlichen Versorgung, begründet aber keine datenschutzrechtliche Befugnis. Hätte der Gesetzgeber dies gewollt, hätte er es deutlicher zum Ausdruck bringen müssen, denn immerhin geht es dabei auch um eine Durchbrechung der ärztlichen Schweigepflicht. Es wäre auch unsystematisch, die Bestimmung so auszulegen. Die anderen Fälle des § 73 Abs. 2 SGB V berechtigen unzweifelhaft nicht zur Datenverarbeitung. Nun gerade der Nummer 9 eine solche Bedeutung zuzuschreiben hieße, ihr eine Sonderstellung im Regelungsgefüge einzuräumen, die sich durch nichts belegen lässt. Die demzufolge fehlende Berechtigung des Arztes zur Datenübermittlung und Durchbrechung der ärztlichen Schweigepflicht kraft Gesetzes lässt sich allenfalls durch eine Einwilligung des Betroffenen ersetzen. Unter der Voraussetzung, dass sich die Krankenkasse an den jeweiligen Versicherten wendet, ihm die Situation darlegt und dabei insbesondere darauf hinweist, dass durch die Beantwortung

der Anfrage unter Umständen eine Untersuchung durch den MDK vermieden werden kann, und der Betroffene hierauf mit der Auskunftserteilung durch seinen Arzt einverstanden ist, bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Ein solches Einwilligungsverfahren praktizieren übrigens einige Krankenkassen bereits.

– Ein Universitätsklinikum erkundigte sich danach, ob eine Ersatzkasse Recht hat, wenn sie mit dem Ablauf fester Verweildauer-Fristen (bei Ersterkrankungen 21 Tage, bei Wiedererkrankungen innerhalb der letzten zwölf Monate 14 Tage) generell Zwischenberichte über Befund und Behandlung von Patienten fordert. Die Kasse begründete dies mit einer Steigerung der Ausgaben für die stationäre Krankenhausbehandlung auf Grund einer zu hohen Verweildauer und (um dem entgegenzuwirken) der Notwendigkeit einer „besseren Kommunikation". Sie verwendet dabei einen von einem MDK konzipierten Erhebungsbogen. Dazu war zu sagen:

  Die Frage, welche Daten Krankenhäuser über ihre Patienten an die Krankenkassen zu übermitteln haben, ist in § 301 Abs. 1 SGB V geregelt. Diese Bestimmung ist abschließend. Nach ihr ist der Krankenkasse (nur) dann, wenn die ihr vom Krankenhaus zunächst mitgeteilte voraussichtliche Dauer der Krankenhausbehandlung überschritten wird, eine medizinische Begründung zu geben. Es fällt also zunächst in die Verantwortung des Krankenhauses, die voraussichtliche Dauer der Krankenhausbehandlung zu bestimmen, und nicht in die der Krankenkasse. Erst dann, wenn die vom Krankenhaus zunächst angenommene Behandlungsdauer überschritten wird, besteht eine Übermittlungsbefugnis des Krankenhauses. Die Forderung der Krankenkasse, unabhängig von der Prognose des Krankenhauses nach von ihr selbst festgelegten Zeiträumen Patientendaten zu übermitteln, stimmt deshalb nicht mit dem Gesetz überein. Hinzu kommt Folgendes:

  Liegt die Prognose des Krankenhauses über die voraussichtliche Behandlungsdauer unterhalb der von der Krankenkasse angegebenen Drei- bzw. Zwei-Wochen-Frist und wird der Patient fristgerecht entlassen, besteht kein Anlass, sich überhaupt mit den Vordrucken zu befassen. Liegt sie von vornherein darüber und hat die Kasse Zweifel an der Richtigkeit, kann sie nach § 275 Abs. 1 Nr. 1 SGB V den MDK einschalten. Diesem sind dann die erforderlichen Patientendaten unmittelbar zu übermitteln. Stimmt die Prognose dagegen mit den Fristen der Kasse überein und überschreitet die Behandlung dann den ursprünglich angenommenen Zeitraum, liegt ein Fall des § 301 Abs. 1 Satz 1 Nr. 3 SGB V vor. Die Kasse kann dann vom Krankenhaus eine „medizinische Begründung" für die Verlängerung der Behandlungszeit verlangen. Der im konkreten Fall von der Krankenkasse verwendete Fragenkatalog geht weit über das hinaus, was Inhalt einer solchen medizinischen Begründung sein darf. Er ist als Grundlage für eine gutachtliche Stellungnahme des MDK zur Frage der Dauer der stationären Behandlung akzeptabel, für eine Unterrichtung der Krankenkasse dagegen nicht.

  Ich habe dem Klinikum deshalb empfohlen, den Erhebungsbogen nicht auszufüllen. Da die Krankenkasse selbst nicht meiner Kontrolle unterlag, habe ich den zuständigen Datenschutzbeauftragten über meine Rechtsauffassung informiert. Er hat sich dem angeschlossen und wird sich an die Kasse wenden.

1.3 Die Krankenversichertenkarte mit Bild

Die Einführung der Krankenversichertenkarte (KVK) im Jahre 1994 an Stelle der bisherigen Krankenscheine brachte, wie sich sehr schnell herausstellte, der Versichertengemeinschaft und den Krankenkassen nicht nur Vorteile. Neben dem sog. „doctor hopping", der ständig wechselnden Inanspruchnahme verschiedener Ärzte, wurde auch über Missbrauchsfälle berichtet, in denen Versicherte ihre Karte nichtversicherten Dritten zur Nutzung überlassen oder sie sogar verkauft haben sollen. Auch verlorene Karten können von Unbefugten verwen-

det werden. Möglich sind solche Missbrauchsfälle u. a. auch deshalb, weil in den Arztpraxen wohl seltenst die Identität des Patienten überprüft wird. Vor diesem Hintergrund ist es verständlich, dass die Krankenkassen nach Wegen suchen, die Schadensrisiken zu minimieren. Als eine Möglichkeit, dies zu erreichen, kommt die Aufnahme eines Lichtbilds des Versicherten in die KVK in Betracht.

Bereits 1997 wandte sich die AOK Baden-Württemberg an mich und teilte mir ihre Absicht mit, im ersten Halbjahr 1998 im Rahmen eines Modellprojekts eine Krankenversichertenkarte mit Bild einzuführen (Bild-KVK). In meiner Antwort machte ich der AOK bereits damals klar, dass eine solche Bild-KVK auf der Grundlage des geltenden Rechts nicht zulässig ist. Denn § 291 SGB V bestimmt abschließend, welche Daten auf der Karte gespeichert werden dürfen. Ein Lichtbild gehört nicht dazu. Nun erscheint es mir, was den zusätzlichen Informationsgehalt eines Lichtbilds des Versicherten auf der Karte angeht, hier nicht um eine Sache zu gehen, die grundsätzliche Fragen des Datenschutzes aufwirft. Ich erhob deshalb gegen die Bild-KVK unter zwei Voraussetzungen keine Einwendungen: Erstens, dass sie ausschließlich im Rahmen des wissenschaftlich begleiteten Modellprojekts eingesetzt wird. Und zweitens, dass es der freiwilligen Entscheidung der Versicherten überlassen bleiben muss, ob sie teilnehmen wollen oder nicht, dass ihnen bei Nichtteilnahme keine Nachteile entstehen dürfen und dass sie darüber informiert werden, was mit ihrem Lichtbild geschieht.

Mittlerweile ist die Modellphase abgeschlossen. Wie kaum anders zu erwarten war, mit Erfolg. Und wie gleichfalls nicht anders zu erwarten war, folgte die Mitteilung der AOK, man wolle nun die Bild-KVK sukzessive allen Versicherten anbieten. Ich machte der AOK gegenüber erneut deutlich, dass eine Rechtsgrundlage hierfür nach wie vor nicht besteht. War die zeitlich begrenzte, modellhafte Erprobung noch hinnehmbar, so kann ich den nun vorgesehenen flächendeckenden und dauerhaften Verstoß gegen das Gesetz nicht gutheißen. Hier wäre es Sache der Krankenkassen und ihrer Spitzenverbände gewesen, beim Gesetzgeber vorstellig zu werden, damit die notwendigen gesetzlichen Voraussetzungen geschaffen werden.

1.4 Beitragsbemessung bei freiwillig Versicherten

Unter gewissen Voraussetzungen können auch nicht der Versicherungspflicht unterliegende Personen freiwillig Mitglied in der gesetzlichen Krankenversicherung sein. Nach § 240 Abs. 1 SGB V haben die Krankenkassen bei diesen freiwilligen Mitgliedern in ihrer Satzung sicherzustellen, dass die Beitragsbelastung die gesamte wirtschaftliche Leistungsfähigkeit des Mitglieds berücksichtigt. Die wirtschaftliche Leistungsfähigkeit bestimmt sich dabei nach dem Gesamteinkommen, das nach § 16 SGB IV als Summe der Einkünfte im Sinne des Einkommensteuerrechts definiert ist. Um die Beiträge bemessen zu können, müssen die Krankenkassen deshalb ihre freiwilligen Mitglieder nach deren Einkünfte befragen. Dazu sind sie nach dem Fünften Buch des Sozialgesetzbuchs berechtigt und die Mitglieder sind verpflichtet, die erforderlichen Auskünfte zu erteilen.

Eine Umfrage bei den meiner Kontrolle unterliegenden Krankenkassen, wie diese Befragung in der Praxis aussieht, ergab kein einheitliches Bild. Alle Kassen (AOK Baden-Württemberg, IKK Baden-Württemberg sowie die landesunmittelbaren Betriebskrankenkassen) verwenden Erhebungsvordrucke, in denen detailliert nach Einkunftsarten gefragt wird. Nun ist es aber so, dass das Gesetz (§ 240 Abs. 4 Satz 2 SGB V) bei all denjenigen freiwilligen Mitgliedern, die nicht das Gegenteil beweisen, Einkünfte in einer Höhe unterstellt, die den höchsten Beitragssatz zur Folge haben. Wer also, mit anderen Worten, die sog. Beitragsbemessungsgrenze überschreitet (und dies, wie gesagt, unterstellt das Gesetz zunächst), zahlt den Höchstbeitrag, ohne dass es darauf ankäme, wie hoch sein Einkommen tatsächlich ist. Daten-

schutzrechtlich von Bedeutung ist dies, weil die Krankenkassen nur die für die Erfüllung ihrer Aufgaben erforderlichen Daten erheben dürfen. Konkret heißt das, dass die vollständige Offenlegung der Einkünfte eines freiwilligen Mitglieds dann nicht erforderlich ist, wenn diese über der Beitragsbemessungsgrenze liegen, da dann ohnehin der Höchstbeitrag zu entrichten ist. Dementsprechend verzichten die Innungskrankenkasse (IKK) und die Betriebskrankenkassen darauf, vom Mitglied eine genaue Darstellung seiner Einkünfte dann zu verlangen, wenn es erklärt, diese lägen über der Beitragsbemessungsgrenze. Nicht so dagegen die AOK. Ihr muss generell jeder seine gesamten Einkünfte offen legen, auch wenn von vornherein feststeht, dass er mit dem Höchstbeitrag veranlagt wird. Auf die Frage, weshalb man nicht ebenso verfahre wie die IKK und die Betriebskrankenkassen, teilte die AOK mit, sie sei verpflichtet, jeweils zum Beginn des nächsten Jahres die Beitragseinstufung zu überprüfen. Hierzu werde ein gewisser Vorlauf im laufenden Jahr benötigt. Zu diesem Zeitpunkt sei aber die für das folgende Jahr maßgebliche Höhe der Beitragsbemessungsgrenze noch nicht bekannt. Diese könne deshalb auf dem Erhebungsbogen nicht angegeben werden. Da die Mitglieder dann aber nicht feststellen könnten, ob sie über der Beitragsbemessungsgrenze liegen oder noch darunter, seien Fehleinstufungen zu befürchten. Dem ist Folgendes entgegenzuhalten:

Richtig ist, dass sich die Beitragsbemessungsgrenze jeweils zum 1. Januar eines jeden Jahres ändert. Es ist auch so, dass die Rechtsverordnung der Bundesregierung, die diese Grenze festsetzt, jeweils erst im Bundesgesetzblatt des Monats Dezember veröffentlicht wird. Tatsache ist aber auch, dass die Höhe der Bemessungsgrenze regelmäßig bereits etwa drei Monate vor Inkrafttreten der Rechtsverordnung faktisch feststeht. Die Verordnungsentwürfe sind den Spitzenverbänden der Renten- und der Krankenversicherungsträger so frühzeitig bekannt, dass sie sich zeitgerecht auf die aktualisierten Rechengrößen einstellen können. Es wäre der AOK deshalb trotz des erforderlichen Vorlaufs durchaus möglich, die Erhebungsformulare rechtzeitig so auszugestalten, dass jedenfalls in den Fällen, in denen detaillierte Angaben zu den Einkünften letztlich völlig überflüssig sind, diese auch nicht abverlangt werden. Zumal die Praxis der IKK und der Betriebskrankenkassen zeigt, dass es tatsächlich auch so geht. Das Argument der AOK, diese hätten weniger freiwillige Mitglieder und benötigten deshalb kürzere Vorlaufzeiten, erscheint nicht stichhaltig. Zudem ist kein Mitglied daran gehindert, dieses Risiko einer Fehleinstufung dadurch zu vermeiden, dass es Angaben über seine Einkommensverhältnisse macht.

Die Praxis der AOK bei der Beitragsermittlung war aber noch in zwei weiteren Punkten zu kritisieren:

– So fragt sie, und zwar ebenfalls abweichend von den anderen Krankenkassen, immer danach, bei welcher Krankenkasse der Ehepartner versichert sei. Auf die Frage, warum man denn dies wissen müsse, antwortete die AOK, Einkünfte des Ehegatten seien für die Beitragseinstufung nur dann nicht zu berücksichtigen, wenn dieser Mitglied einer Krankenkasse sei und dort schon Beiträge entrichte. Da den Versicherten aber, so die AOK, oft nicht bekannt sei, „welche Krankenkassen als gesetzliche Krankenversicherung anzusehen sind“, stelle die Forderung, die Krankenkasse anzugeben, eine „Hilfe“ für den Versicherten dar, um eine korrekte Beitragseinstufung zu gewährleisten. Dieser Argumentation vermag ich nicht zu folgen. Von Versicherten kann durchaus erwartet werden, dass sie wissen, ob sie gesetzlich oder privat krankenversichert sind. Allenfalls dies hat die AOK zu interessieren. Zu wissen, bei welcher Krankenkasse die Versicherung erfolgt, ist für die Erfüllung der Aufgaben der AOK hier nicht erforderlich und geht sie deshalb auch nichts an. Würde die AOK in ihrem Formular darauf hinweisen, dass diese Angabe freiwillig ist, wäre nichts einzuwenden. Der Hinweis zum Datenschutz und zur Auskunftspflicht auf dem Formular bezeichnet aber alle Angaben als zwingend.

– Als Nachweis dafür, dass die Angaben zu den Einkünften zutreffen, wird grundsätzlich die Vorlage des aktuellen Steuerbescheids verlangt. Dies wäre nicht nötig. Der Bundesbeauftragte für den Datenschutz hat bereits in seinem 15. Tätigkeitsbericht 1993 – 1994 zu Recht darauf hingewiesen, dass auch eine vom Finanzamt bestätigte Erklärung des Versicherten oder eine vom Finanzamt bestätigte Erklärung eines Steuerberaters des Versicherten über sein beitragsrelevantes Einkommen ausreichen würde. Allerdings sehen sich einige Krankenkassen, die dies akzeptieren würden, daran gehindert, da ein Arbeitspapier der Prüfdienste der Aufsichtsbehörden von Bund und Ländern die strikte Auffassung vertritt, eine objektive Ermittlung des Einkommens sei ohne die Heranziehung amtlicher Unterlagen der Finanzverwaltung nicht möglich. Die Krankenkassen fühlen sich hierdurch gebunden.

  Während nun die IKK und die Betriebskrankenkassen die Vorlage des Steuerbescheids nur dann verlangen, wenn überhaupt Angaben zu den Einkünften gemacht werden, also bei Unterschreiten der Beitragsbemessungsgrenze, verlangt die AOK den Steuerbescheid generell. Und nicht nur das. Während die anderen Krankenkassen das Mitglied ausdrücklich darauf hinweisen, dass es berechtigt sei, Angaben im Steuerbescheid, die die Krankenkasse nicht benötigt, zu schwärzen, wie dies auch das Arbeitspapier der Prüfdienste ausdrücklich vorsieht, meint die AOK darauf verzichten zu können. Als Grund gibt sie auch hier an, man könne von dem Versicherten nicht erwarten, dass er weiß, welche Angaben er schwärzen darf und welche nicht, „die Komplexität dieser Variationsmöglichkeiten muss zwangsläufig zu irrtümlichen Schwärzungen und damit zu Fehleinstufungen führen; dies ist deshalb nicht realisierbar“. Es ist schon merkwürdig, welches Bild die AOK von ihren Versicherten hat. Es kann jedenfalls nicht sein, dass eine Krankenkasse zur Zweckerfüllung nicht erforderliche Daten mit dem Argument erhebt, der Betroffene könne die Bedeutung der Informationen ja nicht erkennen und deshalb solle er vorsichtshalber lieber zu viel als zu wenig angeben. Entweder man sagt ihm klipp und klar, welche Daten von Bedeutung sind, damit er die übrigen Daten unterdrücken kann, oder man sagt ihm gleich, welche Daten er unterdrücken darf (die IKK nennt hier beispielhaft die Daten über die Höhe der Steuerschuld). Möglich wäre es ja schließlich auch, dann, wenn tatsächlich einzelne Angaben irrtümlich geschwärzt wurden, dies nachträglich korrigieren zu lassen.

1.5 Krankenkassen im Wettbewerb

Das im Januar 1993 in Kraft getretene Gesundheitsstrukturgesetz führte erstmals das Kassenwahlrecht für alle Versicherten ein. Damit kamen die Krankenkassen verstärkt in die Situation, in Wettbewerb miteinander treten zu müssen. Ihre Bemühungen, neue Mitglieder zu werben, führten seitdem immer wieder dazu, dass sich auch mein Amt mit den hierbei auftretenden datenschutzrechtlichen Fragestellungen zu befassen hatte.

1.5.1 Die Imagestudie

Wer für sich werben will, hat meist ein Interesse daran zu wissen, welches Image einem anhaftet, wie man bei der Zielgruppe „ankommt“. Erkenntnisse hierzu können wertvolle Hinweise für gezielte Werbemaßnahmen liefern. Durch Zufall erfuhr ich von einem Schreiben der Hauptverwaltung der AOK Baden-Württemberg an ihre Bezirksdirektionen, in dem diese aufgefordert wurden, einem privaten Wirtschaftsforschungsunternehmen Name, Adresse, Geburtsdatum und Telefonnummer ehemaliger AOK-Mitglieder sowie deren neue Krankenkasse einschließlich Versicherungsart zu übermitteln. Das Unternehmen war von der AOK beauftragt worden, eine sog. Imagestudie durchzuführen. Die Namenslisten dienten als Grundlage für die Befragung. So kam es, dass bei etlichen ehemaligen Versicher-

ten der AOK eines Tages Interviewer des Marktforschungsunternehmens vor der Tür standen. Die aus der Befragung gewonnenen Erkenntnisse will die AOK als Grundlage für Maßnahmen zur Stärkung ihrer Wettbewerbsfähigkeit nutzen. Nachdem mir die AOK auf Anfrage weitere Einzelheiten zu dem Projekt mitgeteilt hatte, kam ich zu folgendem Ergebnis:

Datenschutzrechtlich sehe ich die Weitergabe der Daten ehemaliger Versicherter durch die AOK an das Privatunternehmen als eine Übermittlung von Sozialdaten. Dem Argument der AOK, das Unternehmen habe die Daten nur im Auftrag verarbeitet, rechtlich sei dies als eine reine Datennutzung durch die AOK selbst zu werten, kann ich nicht folgen. Denn hier war es so, dass das Marktforschungsunternehmen die Untersuchung von der Auswahl der Teilnehmer über die Befragungsmethode bis zur Auswertung und Aufarbeitung der Ergebnisse weitestgehend selbst bestimmt hat. Die AOK hatte auf die Durchführung des Auftrags keinen entscheidenden Einfluss. In der Literatur wird bei solchen Befragungen danach unterschieden, ob der Auftraggeber Fragenprogramm, Auswahlverfahren und die Art der Auswertungen bestimmt und der Auftragnehmer lediglich die Befragung der Betroffenen und/oder die technische Aufbereitung des Datenmaterials vornimmt; dann soll eine Datenverarbeitung im Auftrag vorliegen. Übernimmt der Auftragnehmer dagegen die Gesamtdurchführung einschließlich der Erstellung des Befragungs- und Auswertungskonzepts, erfülle er einen eigenen Geschäftszweck und werde selbst zur speichernden Stelle. Ähnlich grenzt das Innenministerium Baden-Württemberg bei Kundenbefragungen für Kreditinstitute ab. Diese Abgrenzung halte ich für überzeugend.

Werden im Rahmen einer solchen „Funktionsübertragung“ Sozialdaten übermittelt, bedarf es einer gesetzlichen Grundlage hierfür. Dies war im gegebenen Zusammenhang deshalb problematisch, weil es letztlich um eine Datenweitergabe für Wettbewerbszwecke (im weitesten Sinne) ging. Hierfür hat der Gesetzgeber bisher jedenfalls zweifelsfrei keine Datenverarbeitungsbefugnis vorgesehen. Dies soll jetzt in der derzeit im parlamentarischen Verfahren befindlichen Novellierung des Rechts der gesetzlichen Krankenversicherung geändert werden. Ungeachtet dessen ist nicht zu verkennen, dass mit der Einführung von Wettbewerbselementen in die gesetzliche Krankenversicherung die Krankenkassen ein verständliches und dem Grunde nach auch anerkennenswertes Interesse daran haben, ihren Mitgliederbestand zu erhöhen. Ich habe deshalb die Datenverarbeitung durch Krankenkassen für Wettbewerbszwecke bisher in der Regel nicht kritisiert, wenn ansonsten die datenschutzrechtlichen Rahmenbedingungen gestimmt haben. Dies war hier nicht in jedem Punkt der Fall. Zwar hatte die AOK mit dem Marktforschungsunternehmen einen „Datenschutzvertrag“ abgeschlossen, der die wesentlichen Pflichten des Auftragnehmers zum Schutz der ihm anvertrauten Sozialdaten festschreibt. Dieser Vertrag enthielt allerdings auch Mängel und Lücken, die ich der AOK aufgezeigt habe. Insbesondere war die Frage der Löschung der Daten beim Unternehmen und durch dieses nur mangelhaft geregelt. Dies habe ich beanstandet. Die AOK hat mitgeteilt, nachdem die Studie abgeschlossen sei, habe das Unternehmen mittlerweile alle Daten gelöscht. Den „Datenschutzvertrag“ will sie unter Berücksichtigung der von mir aufgezeigten Gesichtspunkte überarbeiten. Dies ist zu begrüßen.

1.5.2 Not macht erfinderisch: Die „verdeckte“ Werbung

Beim Versuch, für Werbezwecke an persönliche Daten potentieller Kunden zu kommen, legen die Krankenkassen eine erstaunliche Kreativität an den Tag. Nicht selten werden dabei elementare datenschutzrechtliche Grundsätze missachtet, was

immer wieder dazu führt, dass sich Bürger an mich wenden und nach der Zulässigkeit solcher Werbemaßnahmen fragen. So auch in den beiden nachfolgenden Fällen.

– Die Lehrstellenvermittlung

Ein Vater legte mir ein Schreiben einer Bezirksdirektion der AOK an seinen 15-jährigen Sohn, einen Schüler, vor. Darin stellte sich eine Mitarbeiterin der Bezirksdirektion als persönliche Beraterin des Jungen vor. Dem Angebot, ihm Adressen von Ausbildungsbetrieben geben zu können, was seine Chancen auf einen Ausbildungsplatz verbessern könne, folgte die Bitte um Beantwortung einer Reihe von Fragen über Schulbesuch, Berufswunsch, eventuell vorhandenem Ausbildungsplatz und (für diesen Fall) Arbeitgeber.

Bei allem Verständnis für die schwierige Wettbewerbssituation der Krankenkassen konnte ich dieses Vorgehen nicht gutheißen. Hier wurde versucht, unter dem Vorwand, bei der Lehrstellensuche behilflich zu sein, an persönliche Informationen des Schülers zu gelangen, um ihn dann gezielt als Mitglied zu werben. Nicht nur dass die Lehrstellenvermittlung eindeutig nicht zum Aufgabenkreis der Krankenkassen gehört. Es ist auch kaum anzunehmen, dass sich die Chancen, einen Ausbildungsplatz zu erhalten, dadurch nennenswert erhöhen, dass der Bewerber die Adresse des Ausbildungsbetriebs von einer Krankenkasse erhalten hat. Vor diesem Hintergrund halte ich es für bedenklich, wenn bei jungen Menschen nicht zu erfüllende Hoffnungen geweckt werden, um sie so zur Angabe persönlicher Umstände zu bestimmen. Ich habe dies deutlich kritisiert und darauf hingewiesen, dass eine Datenerhebung für Zwecke der Mitgliederwerbung nur unter der Voraussetzung akzeptabel sei, dass im Anschreiben dieser Zweck klipp und klar mitgeteilt, auf die Freiwilligkeit hingewiesen und auch die weitere Datenverarbeitung verständlich beschrieben wird. Die Bezirksdirektion hat hierauf mitgeteilt, sie werde künftig solche Lehrstellenaktionen nicht mehr durchführen und deshalb auch das kritisierte Schreiben nicht mehr verwenden.

– Die „Pfundskur“

Erhält man aus heiterem Himmel einen Anruf eines Krankenkassenmitarbeiters, der um Mitgliedschaft wirbt, oder findet man persönlich adressierte Werbesendungen von Krankenkassen im Briefkasten, fragt man sich mitunter, wie die Kasse eigentlich an die Adresse gekommen ist. Ein Beispiel dafür habe ich durch einen Bürger erfahren, der an einer sog. „Pfundskur“-Aktion einer AOK-Bezirksdirektion teilgenommen hatte. Was war geschehen?

Im Rahmen einer an einem Krankenhaus durchgeführten „Pfundskur“-Aktion waren Gespräche mit Ernährungsberatern angeboten worden. Wer teilnehmen wollte, konnte einen Fragebogen zu seinen Essgewohnheiten ausfüllen. Der Bogen wurde ausgewertet und die Ergebnisse wurden mit dem Teilnehmer besprochen. Womit der Teilnehmer aber nicht rechnete, war, dass die auf dem Bogen ebenfalls erfragten Identifizierungsdaten (Name, Adresse, Geburtsdatum) später gezielt dazu verwendet wurden, auf die Betroffenen zuzugehen und zum Beitritt zur AOK aufzufordern.

Neben der Ernährungsberatung veranstaltete die AOK-Bezirksdirektion gleichzeitig auch noch ein Preisausschreiben. Um teilnehmen zu können, mussten auf einer Karte ebenfalls die Identifizierungsdaten angegeben werden. Zusätzlich wurden weitere Angaben erwartet (bei welcher Krankenkasse versichert, Schule/Arbeitgeber usw.). Auch hier wurden die

Adressdaten für eine spätere Kontaktaufnahme verwendet, nicht aber etwa um Gewinne mitzuteilen, sondern um zum Beitritt zur AOK aufzufordern. Dies alles war so nicht in Ordnung.

Am unteren Rand des für die Ernährungsberatung verwendeten Fragebogens war folgender – unscheinbarer – Hinweis angebracht: „Ich bin damit einverstanden, dass ich von der AOK Informationen und Beratung erhalte“. Die AOK meinte, dies reiche als Einverständniserklärung für die Nutzung der persönlichen Daten des Befragten zu Werbezwecken aus. Ich habe demgegenüber darauf hingewiesen, dass im Zehnten Buch des Sozialgesetzbuches eindeutig geregelt ist, wie eine Einwilligung auszusehen hat. Danach muss die Einwilligungserklärung, wenn sie zusammen mit anderen Erklärungen schriftlich eingeholt werden soll, im äußeren Erscheinungsbild hervorgehoben werden. Außerdem muss sie schriftlich erfolgen, was bedeutet, dass sie handschriftlich unterschrieben sein muss. Der Erklärung vorausgehen müssen der Hinweis auf den Zweck der Speicherung, die Freiwilligkeit der Angaben und die Folgen ihrer Verweigerung. Nichts davon findet sich in dem Fragebogen wieder. Die Datenerhebung und insbesondere deren Speicherung und weitere Nutzung für Werbezwecke war deshalb rechtswidrig. Ich habe die AOK aufgefordert, diesen Fragebogen künftig nicht mehr zu benutzen.

Die dem Fragebogen anhaftenden Mängel trafen im Grundsatz auch auf den für das Gewinnspiel verwendeten Coupon zu. Für solche Gewinnspiele hatte die AOK allerdings Datenschutz-Verfahrenshinweise erlassen, die im konkreten Fall leider nicht beachtet worden waren. Es handelte sich wieder einmal um einen dieser allseits bedauerten Einzelfälle, die gleichwohl für die Betroffenen außerordentlich ärgerlich sind.

2. Unfallversicherung

Auch wenn es in der Mehrzahl der an mich herangetragenen Fälle Krankenkassen waren, die von Ärzten und Krankenhäusern medizinische Informationen über ihre Versicherten anforderten, ging es in einem Fall um ein entsprechendes Ersuchen eines Unfallversicherungsträgers. Eine Unfallkasse hatte einen Krankenhausarzt gebeten, ihr den stationären Entlassungsbericht über einen ehemaligen Patienten zu übersenden, weil unklar war, ob die Krankenhausbehandlung überhaupt etwas mit dem Unfall zu tun hatte und die Kasse dies überprüfen wollte. Der Arzt wandte sich an mich, weil er meinte, dies sei nicht zulässig. Er irrte sich.

Bevor ein Unfallversicherungsträger Leistungen erbringt, hat er zu prüfen, ob diese berechtigt sind. Die hierfür erforderlichen Daten darf er sich beschaffen, wobei § 201 Abs. 1 Satz 1 und 2 des Siebten Buchs des Sozialgesetzbuchs (SGB VII) die Ärzte, die an einer Heilbehandlung beteiligt sind, verpflichtet, dem Unfallversicherungsträger diese Daten zu übermitteln. Dabei trägt der Arzt die Verantwortung für die Zulässigkeit der Übermittlung, er muss also vor allem prüfen, welche Daten er der Kasse mitteilen darf, damit diese ihre Aufgaben erledigen kann, und welche nicht. Die Kasse hat ihm die hierfür benötigten Angaben zu machen. Und noch eins: Nach § 201 Abs. 1 Satz 5 SGB VII muss der Arzt den Patienten von vornherein nicht nur darauf hinweisen, dass er im Rahmen einer Heilbehandlung nach dem Unfallversicherungsrecht tätig wird und alle Daten, die damit zusammenhängend erhoben und gespeichert werden, nur diesem Zweck dienen. Er muss ihn auch darauf aufmerksam machen, dass er als behandelnder Arzt gesetzlich verpflichtet ist, dem Unfallversicherungsträger gegebenenfalls Auskünfte über die Behandlung zu erteilen und dass der Unfallversicherungsträger verpflichtet ist (§ 201 Abs. 1 Satz 3 SGB VII), dem Patienten auf Verlangen mitzuteilen, welche Auskünfte er über ihn beim Arzt eingeholt hat.

Bleibt nur zu hoffen, dass diese Belehrung in der Praxis tatsächlich auch erfolgt!

3. Datenschutz in der gesetzlichen Rentenversicherung

Weist man als Datenschutzbeauftragter darauf hin, dass die eine oder andere Verfahrensweise mit dem Datenschutzrecht nicht im Einklang steht, stößt man nicht immer sofort auf Verständnis. Umso mehr erfreut es, wenn man einmal gleich auf Anhieb Erfolg hat. So etwa im Fall der Landesversicherungsanstalt Württemberg (LVA). Es ging um einen Fragebogen.

Ein Bürger hatte uns einen Versichertenfragebogen zugesandt, den er vor einer Untersuchung durch die ärztliche Untersuchungsstelle der LVA ausfüllen und dieser vorlegen sollte. Hintergrund war, dass er die Bewilligung einer ambulanten Kur wegen einer Sehnenscheidenentzündung beantragt hatte. Bei der Durchsicht des Fragebogens drängte sich die Frage auf, ob die LVA möglicherweise das falsche Formular versandt hatte. Denn was um alles in der Welt sollte beispielsweise das Alter der Eltern, die Zahl der Geschwister, die Schulbildung, der Umstand, dass der Antragsteller verwitwet ist oder ob und ggf. seit wann er Sozialhilfe empfängt mit dem Anspruch auf Rehabilitationsleistungen wegen einer Sehnenscheidenentzündung zu tun haben? Auch dieser Fragebogen erschien wieder – wie so oft – viel zu ausführlich. Dies sah die LVA, hierauf angesprochen, wohl ebenso. Denn sie war sofort bereit, den Fragebogen zu überarbeiten und dabei auf manche Frage ganz zu verzichten, manche einzuschränken. Ansonsten meinte sie, vor Bewilligung von Rehabilitationsleistungen müsse sie die medizinische und psychosoziale Gesamtsituation des Versicherten beurteilen können; deshalb sei die verhältnismäßig umfassende Datenerhebung erforderlich. Unser Argument hierauf, dass nicht ausnahmslos immer alle erhobenen Informationen benötigt würden, was gerade der konkrete Fall deutlich zeige, und dass aus Gründen der Verhältnismäßigkeit ja zunächst nur ganz bestimmte, in jedem Fall erforderliche Daten erhoben werden könnten, die dann unter Umständen nachträglich zu vervollständigen wären, nahm die LVA auf. Sie teilte mit, sie werde ihren Versichertenfragebogen so umgestalten, dass zunächst nur die in jedem Fall erforderlichen Grundinformationen erfasst würden. Darüber hinaus würden dem Versicherten vorab bereits die Fragestellungen mitgeteilt, auf die es im weiteren Verlauf des Verfahrens unter Umständen noch ankommen könne. Die Fragestellungen, auf die es dann tatsächlich noch ankomme, würden erst in der Untersuchung durch die ärztliche Untersuchungsstelle der LVA Württemberg konkret bezeichnet und die entsprechenden Daten auch erst dann erhoben werden. Eine Lösung ganz in unserem Sinne und ohne viel Aufhebens – so etwas wünscht man sich häufiger.

4. Die Privatisierung bei den Jugendämtern

Kinder haben gegen ihre Eltern Anspruch auf Unterhalt. Leben diese getrennt, kommt es oft vor, dass der unterhaltsverpflichtete Elternteil nicht zahlt. Um sich daraus ergebende finanzielle Belastungen des Elternteils, bei dem das Kind lebt, zu vermeiden, hat der Gesetzgeber einen Anspruch des Kindes auf Unterhaltsvorschuss oder Unterhaltsausfallleistung gegen den Staat geschaffen. Geregelt ist dies im Unterhaltsvorschussgesetz. Erbracht werden diese Leistungen vom Jugendamt als Unterhaltsvorschusskasse. Dieses wird allerdings nicht auf eigene Rechnung tätig. Denn getragen werden die Geldleistungen je zur Hälfte von Bund und Land. Die Kommunen sind dagegen nur für die verwaltungsmäßige Abwicklung zuständig.

Leistet das Jugendamt einen Unterhaltsvorschuss, geht der Unterhaltsanspruch des Kindes gegen den unterhaltspflichtigen Elternteil insoweit auf das Land über. Das Jugendamt ist nun zwar kraft Gesetzes verpflichtet, diesen Anspruch im Wege des Rückgriffs „rechtzeitig und vollständig“ durchzusetzen. In der Praxis werden die Rückgriffsmöglichkeiten offenbar aber nicht konsequent genutzt. Um diese potentielle Einnahmequelle des Landes stärker als bisher auszuschöpfen, denkt die Landesregierung

nun daran, private Inkassobüros mit dem Einzug zu beauftragen. Diesen müssten dazu natürlich zumindest personenbezogene Daten des Unterhaltsschuldners mitgeteilt werden. Ich habe dem Sozialministerium mitgeteilt, dass die Jugendämter hierzu nicht befugt sind.

Auch die personenbezogenen Daten des unterhaltsverpflichteten Elternteils, gegen den die Jugendämter nach Leistung des Unterhaltsvorschusses an das Kind im Wege des Rückgriffs vorgehen, sind Sozialdaten im Sinne des Sozialgesetzbuches. Erst recht gilt dies für personenbezogene Daten anderer Personen, die den Jugendämtern bei der Ermittlung und Geltendmachung des Unterhaltsanspruchs bekannt werden. Denn hierfür ist allein maßgeblich, dass die Daten im Zusammenhang mit der Wahrnehmung einer Aufgabe nach dem Sozialgesetzbuch verarbeitet werden. Und da das Unterhaltsvorschussgesetz Teil des Sozialgesetzbuches ist, unterfallen alle personenbezogenen Daten, die den Jugendämtern in Ausführung ihrer Aufgaben nach diesem Gesetz zugänglich werden, dem Sozialgeheimnis. Ihre Verarbeitung hat sich nach den datenschutzrechtlichen Bestimmungen des Sozialgesetzbuches zu richten. Wie im gesamten übrigen Datenschutzrecht ist auch dort der Grundsatz der Erforderlichkeit das die Zulässigkeit einer Datenverarbeitung bestimmende Element. Konkret heißt das, dass eine Übermittlung von Sozialdaten an private Dritte nur zulässig ist, wenn diese Übermittlung zur Aufgabenerfüllung der übermittelnden Stelle erforderlich ist. Erforderlich wäre die Mitteilung persönlicher Informationen über Unterhaltsschuldner an private Inkassobüros hier nur dann, wenn die Jugendämter ohne die Einschaltung solcher Büros ihre Aufgabe, nämlich die übergegangenen Ansprüche einzutreiben, nicht oder nur unter unverhältnismäßig großen Schwierigkeiten erledigen könnten. Davon kann aber keine Rede sein. Die Jugendämter wären sehr wohl in der Lage, diese Aufgabe rechtzeitig und vollständig selbst wahrzunehmen. Sie haben dazu sogar mehr rechtliche Möglichkeiten als private Gläubiger, also auch Inkassobüros. So können sie anders als diese andere Sozialleistungsträger, wie z. B. Krankenkassen und Rentenversicherungsträger, um Auskünfte angehen. Selbst das Kraftfahrt-Bundesamt in Flensburg muss ihnen auf Anfrage die Anschrift von säumigen Unterhaltsschuldnern mitteilen. Das eigentliche Problem ist, dass sie, weil sie an den so eingenommenen Mitteln nicht beteiligt werden, kein eigenes wirtschaftliches Interesse an einer Erhöhung der Rückgriffquote haben und sich deshalb, das jedenfalls meint das Land, nicht im gebotenen Maße in dieser Frage engagieren. Beklagt wird, die Kommunen würden die Unterhaltsvorschusskassen personell nicht so ausstatten, dass eine effektive Arbeit möglich wäre. Deshalb würden wohl auch nicht alle bestehenden Rückgriffsmöglichkeiten konsequent genutzt. Allein dies führt offenbar dazu, dass eine potentielle Einnahmequelle nicht so genutzt wird, wie das Land dies wünscht. Und nur deshalb sollen nun private Inkassobüros eingeschaltet werden. Um es nochmals deutlich zu sagen: Die Vollzugsdefizite beruhen hier nicht auf objektiven Umständen und schon gar nicht darauf, dass der Datenschutz die Aufgabenerledigung behindern würde. Die Defizite sind vielmehr selbst verursacht und können nun nicht dafür herangezogen werden, die Erforderlichkeit einer Offenbarung von Sozialgeheimnissen gegenüber privaten Dritten zu begründen. Ich habe dem Sozialministerium deshalb deutlich gesagt, dass die Mitteilung von Sozialdaten an private Inkassobüros zur Einziehung von Unterhaltsvorschüssen unzulässig ist.

3. Abschnitt: Sozialhilfe

1. Die Missbrauchsbekämpfung

Sozialhilfemissbrauch darf nicht tabuisiert werden, so wurde der Herr Sozialminister wiederholt in den Medien zitiert, und er hat Recht damit. Betrug bleibt Betrug, ganz gleich in welchem Bereich er begangen wird, sei es in der Wirtschaft, in der Verwaltung, wenn es ums Steuer zahlen geht oder sei es in der Sozialhilfe, und muss deshalb bekämpft werden. Nur, besteht die Gefahr einer Tabuisierung wirklich? Verfolgt man die Medienberichte über dieses Thema, kann man es kaum glauben. Landauf, landab diskutieren Kreistage und Stadträte über Sozialhilfemissbrauch und die Möglichkeiten, ihn zu bekämpfen. Auch der Landtag nahm sich

dieses Themas an, die Landesregierung stand nicht zurück. Alle sind sich darüber einig, Bekämpfung muss sein. Recht unterschiedlich waren freilich die Angaben zur Höhe des vermuteten Missbrauchs, recht unterschiedlich aber auch die Erfolgsmeldungen über einzelne Kontrollmaßnahmen. Für die einen sind die automatisierten Datenabgleiche das non plus ultra, andere versprechen sich noch mehr vom Einsatz von Sozialdetektiven. Sozialämter mussten aber auch einräumen, dass sich manche Maßnahmen kaum gelohnt haben. Bei all diesen Meldungen und Berichten ging es, sei es ausgesprochen oder nicht ausgesprochen, immer auch um ein spezielles Thema, nämlich den Datenschutz. Für die einen ist Datenschutz ein hinderliches Ärgernis, das man tunlichst aus dem Weg räumen sollte, andere zucken bedauernd mit der Schulter und betrachten ihn als unvermeidbares Übel. Ab und zu gibt es dann aber auch noch Stimmen, die seine Notwendigkeit gerade in diesem Bereich verteidigen. Und das mit Recht. Denn nach § 1 des Bundessozialhilfegesetzes ist es zentrale Aufgabe der Sozialhilfe, dem Hilfeempfänger die Führung eines Lebens zu ermöglichen, das der Würde des Menschen entspricht. Zu einem Leben in Würde gehört aber auch, dass ihm größtmögliche Selbstbestimmung zugebilligt wird und er Kontrollmaßnahmen (also Eingriffe in sein Recht auf informationelle Selbstbestimmung) nur hinnehmen muss, wenn dies im überwiegenden Allgemeininteresse unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit zwingend geboten ist.

Mit einigen der damit zusammenhängenden Fragen hatte ich mich im Berichtsjahr zu beschäftigen.

1.1 Die Kontoauszüge

Wer sich einmal bewusst seine Kontoauszüge anschaut, wird überrascht sein, was dort alles verzeichnet ist. Dabei sind es nicht einmal so sehr die einzelnen Beträge von Gut- oder Lastschriften, die ins Auge fallen, sondern die Zweckangaben über die einzelnen Buchungen. Wer sie liest, erhält einen recht informativen Überblick über die Lebensführung des Kontoinhabers. Verständlich ist deshalb, dass die Sozialämter ein Auge auf diese Kontoauszüge geworfen haben und regelmäßig von Hilfesuchenden die Vorlage solcher Unterlagen verlangen. Das ist eine Vorgehensweise, die aus meiner Sicht immer noch schonender ist, und deshalb auch den Vorzug verdient, als die Anforderung von Auskünften über Kontobewegungen unmittelbar bei den Banken. Bei der Einholung von Bankauskünften auf der Grundlage einer zuvor abgegebenen Einwilligungserklärung lässt sich nämlich kaum vermeiden, dass die Bank Kenntnis vom Sozialhilfebezug erhält. Erst recht ist dies der Fall, wenn, was leider immer noch häufig vorkommt, im Auskunftsersuchen ausdrücklich der Sozialhilfebezug erwähnt wird. Allerdings kann ein Sozialamt die Vorlage von Kontoauszügen auch nicht unbegrenzt verlangen. Eine solche Forderung muss, sofern kein Verdachtsfall vorliegt, nur akzeptiert werden, wenn für einen längeren Zeitraum laufende Hilfe für den Lebensunterhalt oder ein größerer einmaliger Betrag bewilligt werden soll und sich das Sozialamt auf die Kontoauszüge der letzten drei bis sechs Monate beschränkt. Ob es aber, wie mir von einem Kreissozialamt bekannt ist, bei Müttern, die im Rahmen des Mutter-Kind-Programms unterstützt werden und noch einen kleinen Zusatzverdienst haben, gerechtfertigt ist, prinzipiell alle drei Monate alle Kontoauszüge anzufordern, erscheint mir doch fraglich. Bis zu einem gewissen Grade kann ich bei einer solchen Totalkontrolle verstehen, dass eine davon betroffene Mutter mir gegenüber Zweifel äußerte, ob ihre Entscheidung für das Kind richtig war. Dass das Sozialamt dazu noch meinte, diese rigorose Kontrollpraxis liege letztlich auch im Interesse der Mütter selbst, wird sie noch mehr in ihren Zweifeln bestärken.

Wenn ich schon meine Kontoauszüge vorlegen muss, kann ich dann nicht wenigstens die Zweckangaben schwärzen? Diese Frage stellen mir Sozialhilfeempfänger häufig. Aber auch dazu kann ich nur sagen: Das Sozialamt kann zwar, muss sich aber nicht mit der Vorlage von Kontoauszügen mit geschwärzten Zweckangaben begnügen. Denn ihm geht es nicht nur um die nackten Zahlen über Einnahmen und

Ausgaben, sondern es will auch wissen, wofür Geld eingenommen und ausgegeben worden ist. Denn diese Angaben können durchaus für die Sozialhilfegewährung von Bedeutung sein, weil sie z. B. Aufschluss über das Halten eines Kraftfahrzeugs, das Bestehen einer Lebensversicherung o. Ä. geben. Bei besonders sensiblen Informationen wie etwa der Zugehörigkeit zu einer Religionsgemeinschaft oder Mitgliedschaft in einer Partei kann es aber unverhältnismäßig sein, wenn eine Schwärzung nicht akzeptiert würde.

Wenn schon vom Hilfesuchenden die Vorlage von kompletten Kontoauszügen verlangt wird, dann muss aber wenigstens sichergestellt sein, dass die Kontoauszüge nach der damit vorgenommenen Überprüfung seiner Angaben wieder zurückgegeben und neben einem entsprechenden Prüfvermerk nur Kopien der Kontoauszüge zu den Akten genommen werden, die für die letztlich getroffene Entscheidung unmittelbar relevante Informationen enthalten. Dazu zählen insbesondere solche, aus denen sich ergibt, dass er unzutreffende Angaben gemacht hat. Würde das Sozialamt sich nicht darauf beschränken, würde es in seiner Akte höchst sensible Daten speichern, die es zur Erfüllung seiner Aufgaben nicht benötigt. Das aber ist schlicht unzulässig.

1.2 Die Bankvollmacht

Ob jemand Sozialhilfe in Anspruch nehmen will, hängt in aller Regel von seiner persönlichen Entscheidung ab. Benötigt das Sozialamt zur Prüfung der dazu notwendigen Voraussetzungen Informationen Dritter, ist es Sache des Hilfesuchenden, diese entweder selbst beizubringen oder aber sich damit einverstanden zu erklären, dass das Sozialamt diese Auskunft selbst beim Dritten einholt. Kommt ein Hilfesuchender einer derartigen Aufforderung nicht nach, ist das Sozialamt nach Verstreichen einer festgesetzten Frist berechtigt, die Sozialhilfe allein schon wegen dieser fehlenden Mitwirkung zu verweigern. Allerdings, nicht in jedem Fall besteht eine Mitwirkungspflicht. Vielmehr muss ein Hilfesuchender nur der Erteilung der erforderlichen Auskünfte durch Dritte zustimmen. Außerdem muss die Einwilligung den in § 67 b Abs. 2 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) näher beschriebenen Anforderungen entsprechen.

In der Praxis der Sozialämter spielt die Einwilligung zur Einholung von Bankauskünften eine große Rolle. Entweder schon im Antragsvordruck oder in einer diesem angeschlossenen Beilage verlangen Sozialämter Hilfesuchenden die Abgabe einer solchen Erklärung ab. Bei Licht besehen sind die meisten dieser Erklärungen unwirksam, weil sie nicht den Anforderungen Rechnung tragen, die an eine wirksame Einwilligungserklärung zu stellen sind:

– Häufig geforderte Erklärungen wie „Ich ermächtige Sparkassen, Banken und sonstige Kreditinstitute, dem Kreissozialamt jede von ihm gewünschte Auskunft zu erteilen“ sind viel zu unbestimmt. Aus ihnen kann der Erklärende nicht ersehen, welche Bedeutung die Erklärung hat und welche Konsequenzen sich daraus für ihn ergeben. Das aber ist notwendige Voraussetzung einer wirksamen Einwilligungserklärung. Soweit mir bekannt, sind die Banken und Sparkassen in aller Regel auch gar nicht bereit, auf der Grundlage einer derart pauschalen Erklärung, die einer Blankovollmacht gleichkommt, Auskünfte zu geben. Notwendig ist vielmehr, dass die Bank oder Sparkasse, die zur Auskunftserteilung ermächtigt werden soll, konkret benannt wird. Außerdem muss der Zeitraum angegeben sein, über den auf Anforderung des Sozialamts Auskunft gegeben werden soll.

– Es fehlt meist ein Hinweis darauf, welche Folgen eine Verweigerung der Einwilligung hat. Das aber ist notwendiger Bestandteil einer wirksamen Einwilligungserklärung.

– Wenn die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden soll, muss sie im äußeren Erscheinungsbild der Erklärung hervorgehoben sein. Ein Sozialamt darf also die Einwilli-

gungserklärung nicht gewissermaßen im Kleingedruckten verstecken. Demjenigen, der eine solche Erklärung abgeben soll, muss dies also deutlich bewusst gemacht werden. Auch daran hapert es des Öfteren.

Allerdings, auch bei der Einholung von Bankauskünften gilt: Es wird nichts so heiß gegessen wie es gekocht wird. Obwohl die Bankvollmacht regelmäßig in den Antragsunterlagen auftaucht, machen die Sozialämter davon zu Recht kaum Gebrauch, zumal sie ja auch Kontoauszüge anfordern können. Fast muss man den Eindruck gewinnen, es handle sich dabei um eine reine Drohgebärde. Deshalb frage ich mich, ob es nicht der Sache besser gerecht würde, wenn die Sozialämter eine Bankvollmacht nur in den Fällen anfordern, in denen sie die Einholung von Bankauskünften tatsächlich auch beabsichtigen. Die dazu notwendige Einwilligungserklärung könnte dann so konkretisiert und abgefasst werden, dass sie hieb- und stichfest ist.

1.3 Vorsicht beim Datenabgleich

Wenn man überhaupt von einem „Erfolg“ der in § 117 des Bundessozialhilfegesetzes (BSHG) geregelten automatisierten Datenabgleiche zur Erkennung von unberechtigter Inanspruchnahme von Sozialhilfeleistungen sprechen kann, dann beim Datenabgleich mit der Datenstelle der Rentenversicherungsträger in Würzburg. Denn über diesen Datenabgleich haben die Sozialämter, die sich daran beteiligt haben, eine ganze Reihe von Personen festgestellt, die laufende Hilfe zum Lebensunterhalt bezogen und dabei aber ihre Einkünfte aus einer sog. geringfügigen Beschäftigung verschwiegen hatten. Hin und wieder kam es dabei aber auch zu einem Fehlgriff, so im folgenden Fall:

Dem Kreissozialamt des Rhein-Neckar-Kreises war aus Würzburg mitgeteilt worden, eine Sozialhilfeempfängerin sei bei einer Firma im dortigen Landkreis auf einer 620-DM-Basis beschäftigt. Obwohl die Sozialämter vor der Durchführung der Datenabgleiche gewarnt worden waren, dass nicht jede Meldung aus Würzburg für bare Münze genommen werden kann, weil mancher Arbeitgeber es mit der Abmeldung nicht immer genau genommen hat, war der 620-DM-Job für das Kreissozialamt eine Tatsache. Es teilte deshalb der Hilfeempfängerin mit, sie habe entgegen ihrer Mitwirkungspflicht erzielte Einkünfte nicht angegeben, und forderte sie auf, anzugeben, seit wann und in welcher Höhe sie diese Einkünfte erhalte. Außerdem kündigte es die Einstellung der Sozialhilfeleistung zum Ende des Monats an. Der Einwand der Hilfeempfängerin, sie habe entgegen der Behauptung des Kreissozialamts keine Einkünfte erzielt, vermochte diese Haltung nicht zu ändern. Selbst nachdem eine Anfrage bei der Firma, bei der die Hilfeempfängerin beschäftigt gewesen sein soll, mit dem Vermerk „Adressat unbekannt“ zurückgekommen war und auch eine Nachfrage bei der zuständigen Meldebehörde nach den Wohnverhältnissen des Inhabers der Firma ergeben hatte, dass dieser schon im Jahr 1994 verzogen war, sah sich das Kreissozialamt noch nicht veranlasst, den Auszahlungsstopp aufzuheben. Das geschah erst, nachdem die Hilfeempfängerin beim zuständigen Verwaltungsgericht einen Antrag auf Erlass einer einstweiligen Anordnung gestellt und darin darauf hingewiesen hatte, dass sie vor einigen Jahren nur für wenige Monate bei der Firma gearbeitet habe. Damit war des grausamen Spiels allerdings noch nicht genug. Denn das Kreissozialamt stoppte kurze Zeit später die Sozialhilfeauszahlung noch einmal und verband damit die Aufforderung, endlich die geforderten Angaben über ihre Einkünfte aus der von ihm für zutreffend gehaltenen geringfügigen Beschäftigung zu machen. Erst nachdem die Hilfeempfängerin das Verwaltungsgericht erneut in Anspruch genommen und zudem am Monatsende ihren Wohnsitz aus dem Rhein-Neckar-Kreis in einen anderen Landkreis verlegt hatte, überwies das Kreissozialamt die noch ausstehende Sozialhilfe. Da ist einiges schiefgelaufen. Das Kreissozialamt hätte sehr viel früher, als es dies tatsächlich dann getan hat, erkennen müssen, dass die Auskunft aus Würzburg unrichtig war und seine Unterlagen entsprechend berichtigen müssen. Von

mir darauf hingewiesen, versprach es, aus diesem Vorfall die notwendigen Lehren zu ziehen.

1.4 Die Empfehlung zur Strafanzeige

Wer, um Sozialhilfe zu erhalten, unrichtige Angaben macht und damit letztlich auch Erfolg hat, erfüllt den Straftatbestand des Betrugs i. S. v. § 263 StGB und muss die sich daraus ergebenden Konsequenzen tragen. Das kann keine Frage sein. Haben die Sozialämter konkrete Anhaltspunkte dafür, dass ein Hilfeempfänger einen solchen Betrug begangen oder versucht hat, sind sie berechtigt, bei Polizei oder Staatsanwaltschaft Anzeige zu erstatten. Der Datenschutz steht dem ganz sicher nicht entgegen. Eine solche Maßnahme, die unmittelbar an die Verantwortlichkeit des Hilfeempfängers anknüpft, ist aus meiner Sicht sogar eher zu vertreten, als generelle anlassunabhängige Kontrollmaßnahmen, bei denen letztlich alle davon Betroffenen als potentielle Betrüger behandelt werden, ohne dass sie dazu die geringste Veranlassung gegeben haben. Diese Rechtslage ist bei allen Sozialämtern im Land sehr wohl bekannt. Auch habe ich aus meiner langjährigen Erfahrung in der Beratung und Kontrolle von Sozialhilfeträgern den Eindruck gewonnen, dass diese durchaus bereit und in der Lage sind, eigenverantwortlich und sachgerecht darüber zu entscheiden, wann es angebracht ist, sich mit Anhaltspunkten für einen Sozialhilfebetrug an die Strafverfolgungsbehörden zu wenden. Ich habe mich deshalb schon etwas gewundert und dem auch Ausdruck gegeben, als mich das Innenministerium über seine dann auch realisierte Absicht unterrichtete, gemeinsam mit dem Landkreistag und dem Städtetag den kommunalen Sozialleistungsträgern Empfehlungen darüber zu geben, wie sie sich in dieser Frage verhalten sollen. Dies passt so gar nicht in eine Zeit, in der die Herausgeber dieser Empfehlung zu Recht immer wieder die Eigenverantwortlichkeit der Städte und Landkreise und die Dringlichkeit einer möglichst weit reichenden Deregulierung betonen. Von einer Tabuisierung des Sozialhilfemissbrauchs kann dabei nun wahrlich nicht die Rede sein.

1.5 Das Rechnungsprüfungsamt ist kein Sozialamt

Das Rechnungsprüfungsamt hat nicht die Befugnisse eines Sozialamts, darauf musste ich den Leiter eines städtischen Rechnungsprüfungsamts hinweisen. Er war der Meinung, sein Amt sei genauso wie das städtische Sozialamt selbst berechtigt, Daten von Sozialhilfeempfängern mit den Daten des örtlichen Fahrzeugregisters und des Einwohnermelderegisters automatisiert abzugleichen und wollte von mir eine Bestätigung für die Richtigkeit seiner Auffassung erhalten. Er irrte sich. Denn § 117 BSHG erlaubt solche Abgleiche nur dem Sozialhilfeträger. Da im Sozialdatenschutzrecht nach § 67 Abs. 9 SGB X der sog. funktionale Behördenbegriff maßgebend ist, bedeutet dies, dass für die Abgleiche die Organisationseinheit einer Stadtverwaltung zuständig ist, die funktional die Aufgabe der Sozialhilfegewährung durchführt. Das aber ist das Sozialamt und nicht das Rechnungsprüfungsamt. Gegen eine Durchführung von automatisierten Datenabgleichen nach § 117 BSHG durch das Rechnungsprüfungsamt spricht eine weitere Überlegung: Aufgabe eines Rechnungsprüfungsamts ist es zu prüfen, ob das Sozialamt Sozialhilfe nach den dafür maßgebenden Rechtsvorschriften erbringt. In diesem Rahmen hat es auch zu prüfen, ob dieses von der ihm in § 117 eingeräumten Ermächtigung, automatisierte Datenabgleiche vorzunehmen, sachgerecht unter Berücksichtigung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit Gebrauch macht. Dazu ist es nicht erforderlich, selbst automatisierte Datenabgleiche vorzunehmen. Weil das Sozialamt ja dokumentieren muss, ob und in welchen Zeitabständen es die Abgleiche durchführt und welche Fälle es dabei einbezieht, kann das Rechnungsprüfungsamt seine Prüfung mit Hilfe dieser Dokumentation vornehmen. Das Gleiche gilt für die Prüfung der Frage, ob die zum Abgleich eingesetzten EDV-Verfahren korrekt ablaufen. Auch dazu muss es nicht selbst automatisierte Datenabgleiche praktizieren. Nähme es sie

gleichwohl vor, würde dies im Ergebnis bedeuten, dass es Aufgaben des Sozialamts wahrnimmt. Es würde dann nämlich neben dem Sozialamt selbständig den für die Sozialhilfegewährung maßgebenden Sachverhalt ermitteln. Das ist aber nicht Aufgabe der Rechnungsprüfung. Deren Sache ist es nicht, selbst Sozialhilfemissbräuche festzustellen, sondern zu überprüfen, ob das Sozialamt seiner Aufgabe, Missbräuche zu verhindern, sachgerecht unter Beachtung der dafür maßgebenden rechtlichen Rahmenbedingungen nachkommt.

2. Vermittlung von Arbeitsplätzen

Im Sozialhilferecht gilt: Sozialhilfe soll nur der erhalten, der sich nicht selbst helfen kann. Wer arbeiten kann, soll arbeiten und sich nicht vom Steuerzahler unterhalten lassen. Aufgabe der Sozialämter ist es, darauf hinzuwirken, dass sich der Hilfesuchende um Arbeit bemüht und Arbeit findet. Hierzu schalten die Sozialämter nicht selten auch private Arbeitsvermittler ein. Dass dabei nicht immer alles im Sinne des Datenschutzes läuft, musste ich in folgendem, an mich herangetragenen Fall feststellen:

Ein verärgerter Bürger legte mir das an ihn gerichtete Schreiben einer Personalvermittlungsagentur vor, in dem ihm eröffnet wurde, das Sozialamt habe ihr (der Agentur) seine Adresse mitgeteilt, um ihm bei der Suche nach einem geeigneten Arbeitsplatz behilflich zu sein. Er solle zu einem ersten Gespräch in die Agentur kommen. Auf meine Frage an das Sozialamt, weshalb es, ohne den Bürger vorher zu fragen, die Agentur darüber informiert habe, dass er Sozialhilfe bezieht, meinte dieses, es habe sich hier noch um einen Altfall gehandelt. Neuerdings würde es die Sozialhilfeempfänger, die für eine Vermittlung in Frage kämen, um ihr Einverständnis in die Weitergabe ihrer persönlichen Daten an die Vermittlungsstellen bitten. So weit, so gut. Zu meiner Überraschung erhielt ich aber bald darauf ein Schreiben des Landkreistags, in dem das ganz anders klang. Die Sozialämter seien nämlich, so wurde behauptet, kraft Gesetzes befugt, die persönlichen Daten von Sozialhilfeempfängern auch über deren Kopf hinweg an private Arbeitsvermittler weiterzugeben. Dem Erforderlichkeitsgrundsatz widerspreche dies nicht, denn „wenn es der Sozialhilfeträger … für erforderlich hält, so ist dieses erforderlich“. Eine wahrhaft zwingende Logik! So einfach liegen die Dinge aber nicht.

Richtig ist, dass das Sozialamt nach dem Sozialgesetzbuch berechtigt ist, Sozialdaten zu übermitteln, wenn dies zur Aufgabenerfüllung erforderlich ist. Die Erforderlichkeit bestimmt sich aber nicht danach, wie das Sozialamt dies aus seiner (subjektiven) Sicht sieht, sondern richtet sich nach objektiven Kriterien. Erforderlich ist eine bestimmte Form der Datenverarbeitung nämlich nur dann, wenn ohne diese die Behörde ihre Aufgabe nicht oder nur mangelhaft erledigen könnte. Dass ein Sozialamt aber Arbeitsplätze nur dann erfolgreich vermitteln kann, wenn es dem Vermittler die persönlichen Daten des Sozialhilfeempfängers mitteilt, ohne dass dieser zuvor gefragt wird, ob er damit einverstanden ist, trifft nicht zu. Denn es gibt zwei Möglichkeiten, Sozialhilfeempfänger der Arbeitsvermittlung zuzuführen, ohne dass das Sozialgeheimnis durchbrochen wird. Die eine Möglichkeit ist, den Betroffenen zu fragen, ob er mit einer Weitergabe seiner Daten an den Arbeitsvermittler oder an einen potentiellen Arbeitgeber einverstanden ist. Ist er einverstanden, ist alles klar. Ist er nicht einverstanden, kann dies dazu führen, dass sein Sozialhilfeanspruch gekürzt wird. Die andere Möglichkeit besteht darin, dass ihm aufgegeben wird, sich bei dem in Aussicht genommenen Arbeitgeber oder Vermittler selbst zu melden und sich die Meldung zum Nachweis gegenüber dem Sozialamt bescheinigen zu lassen. In beiden Fällen ist sichergestellt, dass Vermittler oder potentielle Arbeitgeber nicht über den Kopf des Sozialhilfeempfängers hinweg von dessen Sozialhilfebezug erfahren und diesem damit noch ein Stück weit Selbstbestimmung erhalten bleibt.

Der Landkreistag wollte sich dem aus verschiedenen Gründen nicht anschließen. Dem Argument, vom potentiellen Arbeitgeber könne ja nicht verlangt werden, „die Katze im Sack“ zu kaufen, sondern er müsse schon vorab wissen, mit wem er zu rechnen habe, kann entgegnet werden, dass es durchaus zulässig ist, ihm die für ihn wichtigen Informationen über den

potentiellen Arbeitnehmer zukommen zu lassen – mit Ausnahme des Namens und sonstiger Identifikationsmerkmale, die für die abstrakte Bewertung der Eignung für eine bestimmte Arbeitsstelle ohne Bedeutung sind. Andererseits ist einzuräumen, dass es Einzelfälle geben mag, in denen es sachgerecht sein kann, anders zu verfahren. Ist dem Hilfeempfänger durch Verwaltungsakt ein konkretes Arbeitsangebot vermittelt worden und ist nach den gesamten Umständen, insbesondere auf Grund der Persönlichkeit des Betroffenen, damit zu rechnen, dass er anders als durch eine persönliche Aufforderung durch einen potentiellen Arbeitgeber nicht dazu gebracht werden kann, sich dort vorzustellen, kann es gerechtfertigt sein, den (potentiellen) Arbeitgeber schon vorab zu informieren. Dies kann aber nicht in den Fällen gelten, in denen es nur darum geht, den Hilfeempfänger einer Vermittlungsagentur zuzuführen, um überhaupt erst Beschäftigungsmöglichkeiten zu erkunden. Hier ist dessen Selbstbestimmungsrecht zu respektieren und es ihm zu überlassen, ob er Dritten seine Hilfebedürftigkeit offenbaren will oder, gegebenenfalls unter Hinnahme von Nachteilen, davon absehen möchte.

3. Die Aufgabendelegation

Die Sozialämter müssen nicht alle ihre Aufgaben selbst wahrnehmen, sondern können daran auch die Verbände der Freien Wohlfahrtspflege beteiligen. Das sieht das Bundessozialhilfegesetz ausdrücklich vor. Machen sie von dieser Möglichkeit Gebrauch, müssen sie jedoch sicherstellen, dass die Rechte und Interessen von Betroffenen gewahrt bleiben. Zu diesen Rechten gehört auch der Sozialdatenschutz. Deshalb muss bei der Aufgabendelegation vereinbart werden, dass der beauftragte Verband bei der Erfüllung seiner Aufgaben die Bestimmungen zum Schutz der Sozialdaten (§ 35 SGB I, §67 bis §84 a SGB X) zu beachten hat. Dies ist notwendig, weil es sich bei den Verbänden der Freien Wohlfahrtspflege nicht um öffentliche Sozialleistungsträger handelt und sie deshalb nicht schon kraft Gesetzes zur Beachtung dieser Bestimmungen verpflichtet sind. Die Praxis tut sich dabei aber hin und wieder schwer. So war z. B. in einer Vereinbarung, in der ein Sozialamt einen Wohlfahrtsverband mit der Prüfung der Heimbetreuungsbedürftigkeit von Hilfesuchenden beauftragt hatte, lediglich bestimmt, der Wohlfahrtsverband habe „die einschlägigen gesetzlichen und behördlichen Bestimmungen zu beachten“. Im Übrigen sei er zur Geheimhaltung ihm „bekannt gewordener Daten und Tatsachen verpflichtet, die dem allgemeinen Datenschutz oder dem besonderen Schutz von Sozialdaten unterliegen“. Dies war entschieden zu ungenau. Aus solch sibyllinischen Festlegungen kann ein Wohlfahrtsverband nicht erkennen, welche gesetzlichen Regelungen er bei der Erhebung, Verarbeitung und Nutzung von Informationen über Hilfeempfänger zu beachten hat. Dabei herrscht, wie mir jeder, der auch nur einigermaßen mit den Verhältnissen vertraut ist, bestätigen wird, gerade in dieser Frage sowohl bei den Wohlfahrtsverbänden als auch bei den Sozialämtern große Unsicherheit. Das Sozialamt trug meinem Hinweis Rechnung und veranlasste eine Präzisierung der Vereinbarung.

4. Ein mühevoller Weg zur Fehlerkorrektur

„Fehler machen wir alle, und glauben Sie mir, gerade im Bereich der Sozialverwaltung habe ich normalerweise großes Verständnis für die Mitarbeiter“, so beschrieb ein Bürger, nennen wir ihn Herrn A., seine Konzilianz gegenüber Ämtern. Wie aber das Kreissozialamt des Landratsamts Bodenseekreis meinte, Fehler kaschieren zu können, dafür konnte er, was ich verstehen kann, keinerlei Verständnis aufbringen. Seine Geschichte begann so: Das Sozialamt des Bodenseekreises gewährte der von Herrn A. geschiedenen Ehefrau seit geraumer Zeit Sozialhilfe. Diese war jedoch mit dieser Situation unzufrieden und wollte ihrer Meinung nach bestehende Unterhaltsansprüche gegenüber ihrem früheren Ehemann geltend machen. Weil aber ihre Unterhaltsansprüche kraft Gesetzes automatisch auf das Sozialamt übergegangen waren, so weit dieses Sozialhilfe geleistet hatte, musste das Amt diese erst wieder an die Frau abtreten, was es auch tat. Hätte es damit sein Bewenden gehabt, wäre alles in Ordnung gewesen. Nun wollte die Frau jedoch auch noch angeblich auf das Sozialamt über-

gegangene Unterhaltsansprüche des gemeinsamen Sohnes an sie rückübertragen haben. Auch dazu war das Sozialamt sofort bereit. Nur hatte es dabei übersehen, dass es dem Sohn überhaupt keine Sozialhilfe gewährt hatte und ihm sehr wohl bekannt war, dass Herr A. regelmäßig Kindesunterhalt bezahlt hatte. Demzufolge waren auch keinerlei Unterhaltsansprüche auf das Amt übergegangen, die das Sozialamt jetzt wieder hätte rückübertragen können. Als Herr A. von der Rückübertragung erfuhr, fiel er natürlich aus allen Wolken und wollte vom Sozialamt unter Hinweis darauf, dass er ja regelmäßig Unterhalt für sein Sohn bezahle, wissen, in welcher Höhe es denn für seinen Sohn Sozialhilfe geleistet habe. Hätte das Sozialamt daraufhin die Sache geprüft, hätte es leicht feststellen können, dass es an den Sohn nie Leistungen erbracht hatte und dass die Rückübertragung auf den Sohn bezogener Unterhaltsansprüche folglich Humbug war. Kurzum, es hätte die Angelegenheit auf einfache Weise wieder ins Lot bringen können. Nicht so das Kreissozialamt. Über jeden Zweifel erhaben, übersandte es Herrn A. die Kopie eines Formblatts, aus dem aber nur zu ersehen war, ab wann und auf welcher Rechtsgrundlage das Sozialamt seiner geschiedenen Ehefrau Sozialhilfe gewährt hatte. Auf den Sohn und an diesen angeblich geleistete Sozialhilfe ging es dagegen mit keinem Wort ein. Damit fing Herr A. natürlich überhaupt nichts an. Deshalb wollte er vom Sozialamt erneut wissen, in welcher Höhe und auf welcher Rechtsgrundlage es denn seinem Sohn Sozialhilfe geleistet habe. Dieses Schreiben stufte das Sozialamt offenbar als unbotmäßig ein, denn Herr A. erhielt jetzt überhaupt keine Antwort mehr. Als dieser sich daraufhin notgedrungen an die Aufsichtsbehörde wandte, konnte diese Licht in das Dunkel bringen und ihn über den Fehler des Sozialamts aufklären. Das nicht gerade bürgerfreundliche Verhalten des Sozialamts hat freilich auch eine datenschutzrechtliche Seite, und die ist schnell erzählt. Dadurch, dass das Sozialamt Herrn A. und seine geschiedene Frau glauben machte, es habe für ihren Sohn Sozialhilfe geleistet, hat es diesen unrichtige Sozialdaten mitgeteilt. Dass dies ein klarer Verstoß gegen die Vorschriften des Sozialgesetzbuchs war, versteht sich eigentlich von selbst. Eine Beanstandung dieses Verstoßes war die gebotene Konsequenz, nachdem sich das Sozialamt in seiner Stellungnahme nicht im Geringsten einsichtig gezeigt hatte. Einmal auf dem falschen Weg, blieb sich das Landratsamt in seiner Reaktion auf die Beanstandung treu. Es meinte lapidar, es könne keinen Datenschutzverstoß erkennen, weil ja alle Personen, die von ihm falsch informiert worden seien, irgendwie mit dem Sozialamt zu tun hätten. Diese Antwort lässt nur einen Schluss zu: Beim Landratsamt fehlt es offenbar an Grundkenntnissen im Sozialdatenschutz.

4. Teil: Justiz und Polizei

1. Abschnitt: Die Justiz

1. Die Zusammenarbeit mit dem Justizministerium

Den aufmerksamen Lesern der Tätigkeitsberichte meines Amtes wird sich schon bisher nicht gerade der Eindruck aufgedrängt haben, dass das Justizministerium zu den Bannerträgern des Datenschutzes im Lande zählt. Nur allzu oft mussten wir berichten, wie es bei Gesetzgebungsverfahren dem „Interesse an einer effektiven Strafverfolgung“ Vorfahrt vor den berechtigten Belangen des Datenschutzes eingeräumt und gebotene verfahrensrechtliche Regelungen zur Sicherung des Grundrechts auf Datenschutz gar in die Rubrik „unnötige bürokratische Hemmnisse“ eingereiht hat. Fehler, die einer seiner nachgeordneten Behörden beim Speichern oder Weitergeben von Informationen über Bürger unterlaufen waren, räumte das Justizministerium nur ein, wenn es gar nicht mehr anders ging. Stets wachte es mit Argusaugen darüber, dass jeder zusätzliche, für die Stärkung des Grundrechts auf Datenschutz der Bürger angesagte Handgriff von der angeblich chronisch überlasteten Justiz ferngehalten wird. Ein Beispiel: In meinem Tätigkeitsbericht für das Jahr 1998 habe ich dargelegt, in welche Bredouille die Staatsanwaltschaften die Bürgermeisterämter dadurch bringen, dass sie diesen bei Mitteilungen zum Wählerverzeichnis das Ende des durch eine strafgerichtliche Verurteilung einge-

tretenen Ausschlusses von der Wählbarkeit nicht mitteilen (vgl. Landtags-Drucksache 12/3480, S. 41 ff.). Meinem Vorschlag, die Staatsanwaltschaften sollten in einem Aufwasch mit ihrer Mitteilung über das Ende des Ausschlusses von der Wählbarkeit, die sie nach dem Bundeszentralregistergesetz sowieso an das Bundeszentralregister absetzen müssen, auch die Bürgermeisterämter davon unterrichten, ist das Justizministerium nicht näher getreten. Es meint vielmehr, die Bürgermeisterämter sollen sog. Behördenführungszeugnisse einholen. Auf meine Replik, dass dieses Ansinnen dem Bundeszentralregistergesetz zuwider läuft, ging das Justizministerium nicht ein, sondern ließ mich kurz und knapp wissen, es bleibe bei seinem Standpunkt. Eine solche Haltung ist mehr als bedauerlich und für mich absolut unverständlich. Genauso wenig akzeptabel, weil gesetzwidrig, war das Verhalten, das das Justizministerium bei einer beabsichtigten Kontrolle 1999 an den Tag legte:

1.1 Die verhinderte Kontrolle bei Amtsgerichten

Nachdem in den jüngsten Berichten des Justizministeriums zum Staatshaushaltsplan zu lesen war, dass es einen Teil der Amtsgerichte im Lande bereits mit moderner EDV ausgestattet hat und die EDV-Verfahren zügig auch bei den übrigen Amtsgerichten installieren will, schien es mir angebracht, der Frage nachzugehen, ob die EDV-Technik datenschutzkonform eingesetzt wird. Dass ich damit ein heißes Eisen anfasse, war mir von vornherein klar. Denn nach § 24 Abs. 4 des Landesdatenschutzgesetzes (LDSG) darf mein Amt die Datenverarbeitung der Gerichte nur kontrollieren, soweit diese in Verwaltungsangelegenheiten tätig werden. Obwohl wir diese Grenze akribisch beachteten, sah sich das Justizministerium aufgerufen, den beabsichtigten Kontrollen einen Riegel vorzuschieben. Doch jetzt der Reihe nach:

Im Mai 1999 baten wir sieben Amtsgerichte jeweils mitzuteilen, welche elektronischen Datenverarbeitungssysteme und welche EDV-Programme sie einsetzen und ob ihre Mitarbeiter private PC zur Erledigung ihrer dienstlichen Aufgaben benutzen. Außerdem fragten wir nach Dienstanweisungen und Datenschutzkonzepten für den Einsatz von Computern und danach, wer bei den Amtsgerichten auf welche EDV-Verfahren Zugriff hat. Diese Fragen gingen dem Justizministerium, das durch eines der angeschriebenen Amtsgerichte auf den Plan gerufen worden war, offenbar zu weit. Es gab den Amtsgerichten mit Erlass vom 9. Juni 1999 Hinweise zum Umfang der Kontrollkompetenz meines Amtes bei Gerichten und hielt sie dazu an, dessen Fragen zum EDV-Einsatz nur für die Bereiche der „Personalverwaltung, Hausverwaltung, den äußeren Geschäftsbereich wie z. B. die Materialbeschaffung, die Auskunft an Nichtverfahrensbeteiligte sowie die Tätigkeiten bei Justizverwaltungsakten gemäß § 23 EGGVG“ zu beantworten. Mich darüber zu informieren, hielt das Justizministerium nicht für geboten. Erst Wochen später, nachdem wir von dritter Seite darauf angesprochen worden waren und das Justizministerium schriftlich darum gebeten hatten, übersandte es uns seinen Erlass. Auf diesen Erlass beriefen sich dann auch die Amtsgerichte und beantworteten die Fragen zu ihrer Hard- und Software-Ausstattung nur für die darin genannten Tätigkeitsfelder.

Die Weisung des Justizministeriums an die Amtsgerichte steht im Widerspruch zu § 25 Abs. 1 LDSG. Ich habe sie deshalb beanstandet. Das Justizministerium hat mit seinem Erlass verhindert, dass die Amtsgerichte ihrer in dieser Vorschrift festgelegten Verpflichtung nachkommen, meinem Amt im Rahmen seiner Kontrollbefugnisse Auskunft zu allen Fragen zur Datenverarbeitung zu geben und Einsicht in alle Datenverarbeitungsprogramme zu gewähren. Auf meine Beanstandung rechtfertigte das Justizministerium seine Vorgehensweise damit, die Rechtspflege sei umfassend vom Kontrollbereich meines Amtes ausgenommen und damit auch der Einsatz der EDV-Technik im Bereich der Rechtspflege. Dem liegt eine Verkennung der Reichweite der meinem Amt gesetzlich eingeräumten Kontrollbefugnis zugrunde. Nach § 24 Abs. 4 LDSG ist allein die nicht auf Verwaltungsangelegenheiten bezogene, das heißt die rechtsprechende Tätig-

keit der Gerichte wegen der verfassungsrechtlich garantierten Unabhängigkeit der Richter von der Datenschutzkontrolle durch mein Amt ausgenommen. Zur rechtsprechenden Tätigkeit gehören die eigentliche Spruchtätigkeit und alle damit im Zusammenhang stehenden Tätigkeiten, sei es dass sie der Vorbereitung der Entscheidung dienen, wie die Terminsbestimmung, die Ladung oder die Verlängerung von Fristen, sei es dass sie während der Verhandlung ausgeübt werden, wie etwa die Vernehmung von Zeugen oder Sachverständigen, oder dass sie nach der gerichtlichen Entscheidung erfolgen, wie etwa die Berichtigung eines Urteils. Um eine solche, der richterlichen Unabhängigkeit unterfallende Angelegenheit geht es bei der EDV-Ausstattung von Gerichten aber gerade nicht. Dabei handelt es sich vielmehr um die Beschaffung und den Einsatz sächlicher Mittel für die Tätigkeit der Gerichte und damit um einen Bereich, der typischerweise zur Gerichtsverwaltung und damit zu den Verwaltungsangelegenheiten i. S. v. § 24 Abs. 4 LDSG gehört. Hinzu kommt: Für Verwaltungsangelegenheiten ist charakteristisch, dass die Gerichte insoweit den Weisungen und Vorgaben des Justizministeriums unterliegen. Agiert dieses also gegenüber Gerichten per Anweisung oder gibt es ihnen in einer Angelegenheit vor, wie sie zu verfahren haben, dokumentiert es damit zugleich, dass es sich um eine Verwaltungsangelegenheit handelt. Gerade so ist das Justizministerium bei der EDV-Ausstattung der Amtsgerichte vorgegangen: Das Justizministerium hat die bei den Amtsgerichten installierten Datenverarbeitungssysteme konzipiert. Das Justizministerium hat bestimmt, welche Hard- und Software-Komponenten zum Einsatz kommen. Das Justizministerium hat bestimmt, wozu und wie die Amtsgerichte die EDV-Systeme nutzen sollen. Irgendwelche Skrupel, es greife mit seinen Vorgaben für die EDV-Ausstattung der Amtsgerichte in die richterliche Unabhängigkeit ein, sind dem Justizministerium dabei nicht gekommen. An dieser Vorgehensweise muss es sich auch festhalten lassen, wenn es um die Ausübung der Datenschutzkontrolle geht. Dass sich das Justizministerium jetzt plötzlich, wo sich mein Amt mit der EDV-Ausstattung der Amtsgerichte befasst und damit inzident auf den Prüfstand stellt, ob die nach seinen Vorgaben und Weisungen bei den Amtsgerichten installierte EDV-Technik den sog. zehn Geboten des technischen Datenschutzes entspricht, auf die richterliche Unabhängigkeit besinnt, kann ich nur als Versuch werten, die als lästig empfundene Datenschutzkontrolle zurückzudrängen und ihre Prüfmöglichkeiten zu beschneiden. Sollte sich das Justizministerium mit seiner Haltung durchsetzen, wären meinem Amt die Hände gebunden, wenn es um datenschutzgerechten EDV-Einsatz bei den Gerichten im Lande – angefangen bei den Richterarbeitsplätzen über die Geschäftsstellen bis hin zum Servicebereich – geht. Weder bei der Einführung und Führung des elektronischen Grundbuchs, auf das in Zukunft eine ganze Reihe öffentlicher und privater Stellen direkt zugreifen und Informationen abrufen werden können, noch beim automatisierten Mahnverfahren, noch bei der Führung des sog. Schuldnerverzeichnisses der Amtsgerichte, in das alle eingetragen werden, die die eidesstattliche Versicherung (früher Offenbarungseid) abzuleisten haben, fände eine Kontrolle darüber statt, ob die zur Verhinderung von Missbräuchen und Nachlässigkeiten notwendigen technischen und organisatorischen Schutzvorkehrungen getroffen worden sind. Alle, die diesen Kurs unterstützen, sollten dabei auch bedenken, dass das Vertrauen in das datenschutzgerechte Funktionieren der EDV eine wichtige Voraussetzung für den Erfolg der Arbeit der Gerichte ist. Dieses Vertrauen wird sicherlich nicht gestärkt, wenn der Eindruck erweckt wird, die Justiz lasse sich bei ihrer EDV von der unabhängigen Datenschutzkontrolle nicht in die Karten schauen. Um einer solchen Blockadehaltung, wie sie das Justizministerium an den Tag gelegt hat, ein für allemal einen Riegel vorzuschieben, sollte im Interesse des Grundrechts auf Datenschutz gesetzlich klargestellt werden, dass Gerichte der Datenschutzkontrolle unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden (so auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober

1998, vgl. Anhang 4 zum 19. Tätigkeitsbericht, Landtags-Drucksache 12/3480, S. 102). Einen entsprechenden Vorschlag habe ich im Zuge der derzeit ohnehin laufenden Novellierung des Landesdatenschutzgesetzes dem dafür federführenden Innenministerium unterbreitet. Wie man hört, auf Veranlassung des Justizministeriums bisher leider vergebens.

1.2 Beratung nicht erwünscht?

Vorbeugen ist besser als heilen – diese Regel gilt auch im Datenschutz. Deshalb steht seit jeher im Landesdatenschutzgesetz, dass der Datenschutzbeauftragte die Behörden und öffentlichen Stellen nicht nur kontrollieren, sondern sie auch in Fragen des Datenschutzes beraten kann, damit es gar nicht erst zu einer Beeinträchtigung des Grundrechts auf Datenschutz kommt. Damit wir bei der Wahrnehmung unserer Beratungsaufgabe nicht nur auf die Konsultationsfreude der Behörden und öffentlichen Stellen im Lande angewiesen sind, hat die Landesregierung in ihren Vorschriftenrichtlinien festgelegt, dass meinem Amt frühzeitig Gelegenheit zu geben ist, zu Entwürfen von Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben, Stellung zu nehmen (vgl. GABl. 1997, S. 365 ff.). Außerdem hat die Landesregierung in der Vergangenheit wiederholt zugesagt, meinem Amt unaufgefordert Referentenentwürfe von Bundesvorschriften zur Äußerung zu übersenden (vgl. Stellungnahme der Landesregierung zum 5. Tätigkeitsbericht; Landtags-Drucksache 9/1475, S. 37). All dies scheint beim Justizministerium in Vergessenheit geraten zu sein. Oft genug müssen wir Entwürfe, auf die uns andere Datenschutzbeauftragte ansprechen und die sie längst von ihren Justizressorts mit der Bitte um eine Stellungnahme erhalten haben, erst einmal schriftlich beim Justizministerium anfordern.

Wenn wir dann den Entwurf erhalten und eine Äußerung abgegeben haben, lässt uns das Justizministerium meist nicht wissen, wie es über unsere Hinweise und Vorschläge denkt. Dass es sich mitunter genau für das Gegenteil dessen einsetzt, wozu wir geraten haben, kann man bei Gesetzgebungsvorhaben auf Bundesebene in den Protokollen des Bundesrats nachlesen.

– Unter keinem allzu guten Stern steht das Gesetz zur Regelung des Vollzugs der Untersuchungshaft. Zu dem von der Bundesregierung vorgelegten Gesetzentwurf habe ich im Frühjahr dieses Jahres gegenüber dem Justizministerium Stellung genommen, ihm Vorschläge für datenschutzrechtliche Verbesserungen unterbreitet und es gebeten, sich bei den Beratungen in den Gremien des Bundesrats dafür einzusetzen. Nach den ersten Beratungen des Gesetzentwurfs im Bundesrat mussten meine Kollegen und ich feststellen, dass unsere Bedenken und Empfehlungen nahezu ungehört geblieben sind. Mehr noch: Der Bundesrat hat sich in seiner Stellungnahme sogar für die Rücknahme einiger durchaus datenschutzfreundlicher Regelungen im Regierungsentwurf ausgesprochen. Diese Entwicklung hat meine Kollegen und mich veranlasst, in einer Entschließung (vgl. Anhang 9) die Bundesregierung und den Deutschen Bundestag aufzufordern, bei den weiteren Beratungen des Gesetzentwurfs vor allem folgende vom Bundesrat mit der Stimme des Justizministeriums empfohlene datenschutzrechtliche Verschlechterungen nicht zu übernehmen:

  • Die inhaltliche Überwachung der Unterhaltung eines Untersuchungsgefangenen mit seinen Besuchern und seines Schriftverkehrs sollte nicht – wie dies aber der Bundesrat vorgeschlagen hat – die Regel sein. Vielmehr sollte es bei dem Konzept des Regierungsentwurfs bleiben und danach differenziert werden, ob jemand wegen Verdunkelungsgefahr oder aus anderen Gründen, beispielsweise wegen Fluchtgefahr, in Untersuchungshaft ist.

  • Das Recht auf ungehinderten und unüberwachten Telefonverkehr zwischen dem Beschuldigten und seinem Verteidiger muss auch in der Untersuchungshaft gewährleistet sein.

- Bei Datenübermittlungen an andere öffentliche Stellen und an Forschungseinrichtungen müssen wegen der Unschuldsvermutung die schutzwürdigen Interessen des Untersuchungsgefangenen berücksichtigt werden.

– Seit Dezember 1994 gibt es im Strafgesetzbuch eine Regelung (§ 46 a StGB) über den Täter-Opfer-Ausgleich. Einem Täter wird damit über die Möglichkeit, eine geringere Strafe zu erhalten oder unter Umständen sogar von Strafe verschont zu bleiben, ein Anreiz gegeben, das mit seiner Tat Angerichtete nachträglich durch Wiedergutmachung oder durch Entschädigung des Opfers auszugleichen. Zugleich wird dem Opfer geholfen, dem mit einem solchen Ausgleich vielfach mehr gedient ist, als mit einer (strengen) Bestrafung des Täters. Um dem Täter-Opfer-Ausgleich einen breiteren Anwendungsbereich zu verschaffen, legte die Bundesregierung Anfang 1999 ein Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs vor, das mittlerweile den Bundesrat passiert hat. Die zentrale datenschutzrechtliche Frage hierbei ist: Unter welchen Voraussetzungen dürfen (öffentliche und private) Schlichtungsstellen zur Durchführung des Ausgleichsverfahrens umfassende Informationen, insbesondere über Opfer von Straftaten, erhalten? Während der Regierungsentwurf dies bei entgegenstehendem Willen des Opfers nur im Einzelfall zulassen will, soll der entgegenstehende Wille des Opfers – wenn es nach der mit der Stimme des Justizministeriums beschlossenen Stellungnahme des Bundesrats zu dem Gesetzgebungsvorhaben geht – ganz und gar unbeachtlich sein. Eine solche Missachtung des Willens des Opfers wäre geradezu kontraproduktiv. Rechtsfrieden und Ausgleich der Tat können nur hergestellt werden, wenn die Strafverfolgungsbehörden bereits bei der Frage der Datenübermittlung an die Schlichtungsstellen den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren und die Einstellung des Beschuldigten zum Täter-Opfer-Ausgleich berücksichtigen. Deshalb sollten Informationen nur mit Einwilligung des Opfers an die Schlichtungsstellen gehen, wie die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 7./8. Oktober 1999 betont haben (vgl. Anhang 8).

– Die Umsetzung der Richtlinie 98/5/EG des Europäischen Parlaments und des Rates vom 16. Februar 1998 zur Erleichterung der ständigen Ausübung des Rechtsanwaltsberufs in einem anderen Mitgliedstaat als dem, in dem die Qualifikation erworben wurde, nahm das Bundesjustizministerium zum Anlass, die bisher verstreut geregelten Vorschriften über Rechtsanwälte aus anderen Mitgliedstaaten in einem einheitlichen Regelungswerk zusammenzufassen. An dem Referentenentwurf für ein Gesetz zur Umsetzung von Richtlinien der Europäischen Union auf dem Gebiet des Berufsrechts der Rechtsanwälte sind mir, wie ich das Justizministerium wissen ließ, folgende Änderungen wichtig:

  - Nach dem Gesetzentwurf teilt die ermittelnde Staatsanwaltschaft bereits nach Abschluss der Ermittlungen und noch vor Einreichung der Anschuldigungsschrift beim Amtsgericht der zuständigen Stelle des Herkunftsstaates des Rechtsanwalts die ermittelten Tatsachen für Zwecke der Prüfung mit, ob berufsrechtliche Maßnahmen zu ergreifen sind. Weil solche Mitteilungen die Persönlichkeitssphäre des ausländischen Rechtsanwalts in besonderer Weise berühren und weil sie in einem so frühen Stadium erfolgen, ist eine gleichzeitige Unterrichtung des Rechtsanwalts geboten.

  - Soweit europäische Rechtsanwälte bei der Verteidigung eines Mandanten nur im Einvernehmen mit einem hiesigen Rechtsanwalt tätig werden dürfen, müssen sie bei der Ausübung der Verteidigung nicht nur die gleichen Pflichten, sondern auch die gleichen Rechte wie ein hiesiger Rechtsanwalt haben. Dazu gehört beispielsweise das Recht auf unüberwachte Besuche eines in

Strafhaft befindlichen Mandanten und das Zeugnisverweigerungsrecht über das, was ihm in seiner Eigenschaft als Rechtsanwalt anvertraut worden ist.

– Wollen die Justizvollzugsanstalten Personen, die bei ihnen tätig werden und in keinem Dienst- oder Arbeitsverhältnis zum Land Baden-Württemberg stehen, einer Zuverlässigkeitsprüfung unterziehen, geht das nur mit deren Einwilligung. Dabei müssen die Justizvollzugsanstalten § 4 LDSG beachten. Nach dieser Vorschrift ist die Einwilligung in die Verarbeitung personenbezogener Daten schriftlich einzuholen. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Die Einwilligung muss sich auf einen genau beschriebenen Datenverarbeitungsvorgang beziehen. Sie kann nämlich die ihr zugewiesene Aufgabe, das Entscheidungsvorrecht der zu überprüfenden Personen zu gewährleisten und zu konkretisieren, nur dann erfüllen, wenn sie hinreichend bestimmt ist und mithin klar zu erkennen gibt, unter welchen Bedingungen sich die zu überprüfenden Personen mit der Verarbeitung welcher Daten einverstanden erklären. Deshalb müssen der Erklärung in jedem Fall nicht nur die Daten, die verarbeitet werden sollen, zu entnehmen sein, sondern auch das Ziel und der weitere Gang der Datenverarbeitung. Insbesondere muss für die zu überprüfenden Personen klar sein, welchen Stellen konkret welche Daten zugänglich gemacht werden und was dort damit geschieht. Darüber und über die ansonsten beabsichtigte Verwendung müssen die zu überprüfenden Personen rechtzeitig und umfassend vor der Überprüfung unterrichtet werden. Erst so werden sie in die Lage versetzt, die Tragweite ihrer Einwilligung zu überschauen. Darauf und dass sein Entwurf diesen Anforderungen nicht entspricht, wies ich das Justizministerium hin, als es mir Anfang 1999 den Entwurf einer Verwaltungsvorschrift für die Überprüfung von Personen, die in Justizvollzugsanstalten tätig werden und in keinem Dienst- oder Arbeitsverhältnis zum Land Baden-Württemberg stehen, zuleitete.

  Mit Nachdruck entgegentreten musste ich dem Hinweis im Entwurf der Verwaltungsvorschrift, die zu überprüfenden Personen könnten der Kontrolle der Verarbeitung ihrer personenbezogenen Daten durch mein Amt widersprechen. Ein solches Widerspruchsrecht räumt § 24 Abs. 2 LDSG, eine Vorschrift, die im Übrigen völlig fehl am Platz und in der Praxis nahezu ohne Bedeutung ist, nur bei Sicherheitsüberprüfungen im Sinne des Landessicherheitsüberprüfungsgesetzes und nicht auch bei solchen Zuverlässigkeitsüberprüfungen ein, wie sie hier beabsichtigt sind.

– Gerichte und Behörden dürfen nach § 36a der Bundesrechtsanwaltsordnung den Rechtsanwaltskammern im Lande Informationen über Rechtsanwälte übermitteln, soweit dies aus ihrer Sicht für die Zulassung zur Rechtsanwaltschaft, die Entziehung der Zulassung oder zur Einleitung eines Rügeverfahrens oder anwaltsgerichtlichen Verfahrens erforderlich ist. Näheres dazu, wie die Gerichte bei Mitteilungen von Klagen und Vollstreckungsmaßnahmen gegen Rechtsanwälte zu verfahren haben, steht seit 1. September 1999 in der Anordnung über Mitteilungen in Zivilsachen (MiZi) – einer bundesweit geltenden Verwaltungsvorschrift der Landesjustizverwaltungen. Bereits im Zuge der Änderung der MiZi habe ich das Justizministerium darauf hingewiesen, dass diese Regelung zu weit geht:

  • Die MiZi unterscheidet nicht zwischen Klagen aus der persönlichen/privaten und der beruflichen Sphäre eines Rechtsanwalts. Dies wäre aber geboten. Klagen aus dem privaten Bereich eines Rechtsanwalts können nämlich keine berufsrechtlichen Maßnahmen nach sich ziehen. Mitteilungen hierüber an die Rechtsanwaltskammern sind mithin überflüssig.

  • Allein der Umstand, dass Forderungsklagen, Räumungsklagen und Arrestgesuche die berufliche Sphäre eines Rechtsanwalts be-

treffen, rechtfertigt keine Mitteilung an die Rechtsanwaltskammer, sondern allenfalls dann, wenn das Gerichtsverfahren zu Ungunsten des Rechtsanwalts ausgegangen ist.

- Die Rechtsanwälte sollten zumindest zeitgleich über eine erfolgte Mitteilung an die Rechtsanwaltskammer unterrichtet werden, damit sie der mit einer solchen Mitteilung einhergehenden Gefahr der Verletzung ihres Persönlichkeitsrechts entgegenwirken können.

Wie leider kaum anders zu erwarten war, blieben auch diese Hinweise am Ende unberücksichtigt.

2. Strafverfahren und andere Justizangelegenheiten

Strafverfahren ohne Informationen über Personen sind undenkbar. Regelungen darüber, unter welchen Voraussetzungen Polizei, Staatsanwaltschaften und Gerichte Informationen im Strafverfahren verarbeiten dürfen, finden sich in der Strafprozeßordnung jedoch nur punktuell – und dies, obwohl spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 klar ist, dass Informationen über Personen wegen des damit einhergehenden Eingriffs in das Recht auf informationelle Selbstbestimmung im Strafverfahren nur verarbeitet werden dürfen, wenn der Gesetzgeber dies in der Strafprozeßordnung zugelassen hat. Anläufe für eine komplette gesetzliche Regelung der Informationsverarbeitung im Strafverfahren hat es schon mehrere gegeben, den Weg ins Gesetzblatt hat jedoch noch keine gefunden.

In unserer täglichen Praxis waren Strafverfahren des Öfteren Anlass für Datenschutzfragen. Von einigen, mit denen sich mein Amt im Berichtsjahr befasst hat, ist hier die Rede:

2.1 DNA-Analysen

Zwei Männer aus dem Bayerischen wandten sich an mein Amt, weil die Landespolizeidirektion Tübingen sie im Zuge ihrer Ermittlungen wegen eines Mordfalles Anfang 1998 um eine Blutprobe für eine DNA-Analyse gebeten hatte. Beide Männer betonten, dass sie die Polizei bei ihrer Suche nach dem Mörder der jungen Frau gerne unterstützen, im Gegenzug aber Klarheit darüber haben wollen, was mit ihrer Blutprobe passiert und welche Informationen die Polizei über sie speichert. Erhellendes dazu hätten sie dem Formular, mit dem die Landespolizeidirektion ihr Einverständnis in die Blutprobe eingeholt habe, nicht entnehmen können. Da lagen sie richtig: Die Landespolizeidirektion war einem Hinweis nachgegangen, wonach ein Sportwagen einer bekannten Marke mit Münchner Kennzeichen in der Gegend der Wohnung der 1992 ermordeten Frau gesehen worden war, und hatte deshalb alle in München wohnhafte Besitzer solcher Sportwagen festgestellt. Männliche Sportwagenbesitzer und Sportwagenfahrer bat sie zur Blutprobe für eine DNA-Analyse; ca. 4 000 sollen es gewesen sein, darunter die beiden Männer, die sich an mein Amt gewandt hatten. Da sie ihre Blutproben schon abgegeben hatten, legten wir unser Augenmerk vor allem darauf, wie die Landespolizeidirektion mit den Blutproben verfahren ist. Hierzu und zu ihrer Vorgehensweise war Folgendes anzumerken:

– Wenn die Landespolizeidirektion schon meinte, Blutproben und DNA-Analysen könnten mit Einwilligung der Sportwagenbesitzer und -fahrer vorgenommen werden, hätte sie diese zuvor so aufklären müssen, dass sie sich eine im Wesentlichen zutreffende Vorstellung von der Verarbeitung ihrer personenbezogenen Daten machen können. Zudem hätte sie alle auf ihr Recht hinweisen müssen, die Blutprobe zu verweigern und was in diesem Fall passiert. Dies war nicht geschehen. Kein Hinweis darauf, welche Stelle mit der DNA-Analyse befasst wird. Nichts auch dazu, welche Informationen die Landespolizeidirektion über die Sportwagenbesitzer und -fahrer in ihren Akten und in ihrer Spurendokumentationsdatei wie lange speichert und auch nichts zur Möglichkeit, zum DNA-Test Nein zu sagen.

– Statt die Sportwagenbesitzer und -fahrer auf die anonymisierte Weitergabe der Blutprobe an die Untersuchungsstelle verzichten zu lassen, hätte sich die Landespolizeidirektion besser an den Vorschriften der Strafprozeßordnung orientieren sollen. Danach sind bei einer richterlich angeordneten DNA-Analyse die Blutproben der Untersuchungsstelle ohne Angabe des Namens, der Anschrift und des Geburtstages und Geburtsmonats zuzuleiten. Diesen Geheimnisschutz haben auch Personen verdient, die wie die Sportwagenbesitzer und -fahrer ohne richterliche Anordnung eine Blutprobe für eine DNA-Analyse abgegeben haben.

– Wichtig war mir vor allem, dass die Blutproben unverzüglich vernichtet werden, wenn die DNA-Analyse ergeben hat, dass die Tatspuren nicht von dem Sportwagenbesitzer/-fahrer herrühren, von dem die Blutprobe stammt. Denn von da an ist klar, dass der jeweilige Sportwagenbesitzer/-fahrer als Tatverdächtiger sicher nicht in Frage kommen kann. Nach Meinung von DNA-Experten kann man nämlich davon ausgehen, dass es mit Ausnahme von eineiigen Zwillingen keine zwei Menschen auf der Welt gibt, die ein vollständig identisches DNA-Muster besitzen. Deshalb und weil die Landespolizeidirektion sich mir gegenüber darauf berufen hatte, die Staatsanwaltschaft Tübingen bestehe auf der weiteren Aufbewahrung der Blutproben, hakte ich dort nach. Nach einiger Bedenkzeit ließ diese mich wissen, dass sie die umgehende Vernichtung der Blutproben bei negativem Untersuchungsergebnis angeordnet hat.

2.2 Akteneinsichtsrecht des Strafverteidigers kontra Datenschutz?

Darf der Verteidiger seinen Mandanten darüber informieren, was in den Akten der Staatsanwaltschaft steht? Darf er ihm dazu eine Kopie der Aussagen von Belastungszeugen oder gar der kompletten Akte aushändigen? Läuft das nicht dem Datenschutz zuwider, weil dem Beschuldigten damit auch all das zur Kenntnis gelangt, was zur Person von Zeugen in den Akten steht, werde ich immer wieder gefragt. Weil mein Amt allein bei Behörden und anderen öffentlichen Stellen und damit von vornherein nicht bei Rechtsanwälten die Einhaltung der Vorschriften über den Datenschutz kontrollieren darf und ich deshalb die an mich herangetragenen Fälle nicht konkret bewerten kann, kann ich den Fragestellern jeweils nur meine generelle Haltung zu dem von ihnen angesprochenen Grundsatzproblem erläutern.

Ausgangspunkt für die Beantwortung der aufgeworfenen Fragen ist § 147 der Strafprozeßordnung (StPO). Zwar befasst sich diese Vorschrift ihrer Überschrift zufolge mit dem Akteneinsichtsrecht des Verteidigers. Aus dem Blickwinkel des Datenschutzes betrachtet, regelt sie jedoch die Frage, unter welchen Voraussetzungen die Strafverfolgungsbehörden einem Verteidiger die in den Akten festgehaltenen personenbezogenen Daten übermitteln dürfen. Dazu muss man Folgendes wissen: Einer der wichtigsten Grundsätze unseres Strafprozesses ist der Grundsatz der Mündlichkeit, weil die Wahrheit – wie es ein Standardkommentar zur Strafprozeßordnung ausdrückt – nur erforscht werden kann, wenn die Zeugen Aug in Aug mit dem Beschuldigten aussagen und ihm auf Fragen und Einwände Rede und Antwort stehen. Dieser Grundsatz ist im Stadium der polizeilichen und staatsanwaltschaftlichen Ermittlungen nur unvollkommen verwirklicht; diese spielen sich zum großen Teil ab, ohne dass der Beschuldigte davon etwas erfährt oder daran mitwirkt. Dadurch kann er in seiner Verteidigung beeinträchtigt sein. Zum Ausgleich sollen ihm Akten und Beweisstücke so frühzeitig wie möglich offen gelegt werden, auf jeden Fall aber, wenn die Ermittlungen abgeschlossen sind, damit er von dem Ergebnis der Ermittlungen Kenntnis erlangen, sich darauf einstellen und, wenn nötig, Verteidigungsmittel beschaffen und vorbringen kann. Lediglich aus Gründen der Vorsicht ist die Akteneinsicht in die Hand des Verteidigers gelegt, damit die Akten bei der Einsichtnahme nicht beschädigt, verfälscht oder vernichtet werden. Aus dem Recht auf Akteneinsicht und der Regelung, dass dem Verteidiger auf Antrag die Akten zur Einsichtnahme in seine Geschäftsräume

oder in seine Wohnung mitgegeben werden sollen, wird gefolgert, dass der zur Akteneinsicht berechtigte Verteidiger auch befugt ist, Auszüge oder Abschriften von Akten oder Aktenteilen zu fertigen oder fertigen zu lassen. Diese muss er keineswegs für sich behalten, bloß weil in § 147 StPO vom Akteneinsichtsrecht „des Verteidigers" die Rede ist. Im Gegenteil: Das Akteneinsichtsrecht dient dem Beschuldigten. Eine sachgerechte Verteidigung setzt voraus, dass der Beschuldigte weiß, worauf sich der gegen ihn gerichtete Vorwurf stützt. Der Verteidiger ist deshalb – wie der Bundesgerichtshof entschieden hat – in der Regel berechtigt, dem Beschuldigten zu Verteidigungszwecken mitzuteilen, was er aus den Akten erfahren hat. Im gleichen Umfang, wie er ihm den Akteninhalt mitteilen darf, ist der Verteidiger grundsätzlich auch berechtigt, dem Beschuldigten zu Zwecken seiner Verteidigung Aktenauszüge und Abschriften aus den Akten auszuhändigen. Mit anderen Worten: Soweit das Akteneinsichtsrecht des Verteidigers und dessen Recht reicht, den Beschuldigten über den Akteninhalt zu unterrichten, ist das Grundrecht auf Datenschutz der Personen, über die Informationen in der Akte stehen, durch § 147 StPO eingeschränkt. Dieser Regelung liegt der Gedanke zu Grunde, dass all das, was für den Staatsanwalt und den Richter im Strafprozess von Bedeutung ist, natürlich auch der Beschuldigte und sein Verteidiger wissen müssen. Stehen deshalb Informationen über Zeugen erst einmal in den Akten, lassen sie sich – abgesehen von eng begrenzten Ausnahmefällen – vor den Augen des Verteidigers und seines Mandanten nicht mehr zurückhalten. Es liefe nämlich den Grundsätzen eines rechtsstaatlichen Verfahrens zuwider, wenn der Beschuldigte nicht erfahren könnte, was die Strafverfolgungsbehörden gegen ihn in den Akten festgehalten haben.

Auf der anderen Seite ist es ein berechtigtes Anliegen von Zeugen, dass ihre Persönlichkeitssphäre im Strafverfahren soweit als möglich geschont wird. Ganz wesentlich würde dazu beitragen, wenn die Strafverfolgungsbehörden sich bei Vernehmungen und vor allem bei Vernehmungen von Zeugen zur Person auf die unerlässlich notwendigen Fragen beschränken würden. Sie müssen keineswegs – wie aber immer wieder behauptet wird – eine ausführliche und sehr detaillierte Vernehmung zur Person durchführen, bei der ein Zeuge auch Angaben zu seinem Einkommen, seinen Schulabschlüssen, seinem Elternhaus und was sonst noch machen muss. § 68 StPO besagt vielmehr, dass ein Zeuge bei der Vernehmung zur Person zur Vermeidung von Personenverwechslungen nach Vornamen, Zunamen, Alter, Stand oder Gewerbe und Wohnort befragt wird. Weitere Fragen dürfen bei der Vernehmung eines Zeugen zur Person nicht routinemäßig, sondern nur gestellt werden, wenn die Prüfung der Glaubwürdigkeit des Zeugen dazu Anlass gibt. Fragen nach Tatsachen, die einem Zeugen zur Unehre gereichen oder dessen persönlichen Lebensbereich betreffen, sollen nach § 68a StPO nur gestellt werden, wenn dies unerlässlich ist. Mit dieser durch das Opferschutzgesetz von 1986 in die Strafprozeßordnung eingeführten Vorschrift wollte der Gesetzgeber namentlich die durch Straftaten gegen die sexuelle Selbstbestimmung Verletzten vor detaillierter Befragung über ihr Sexualleben ohne erkennbaren Zusammenhang mit der Tat schützen. Zum persönlichen Lebensbereich können auch Umstände aus dem Familienleben eines Zeugen fallen. Vorstrafen zu offenbaren, soll ein Zeuge nur angehalten werden, wenn es um die Feststellung der Voraussetzungen seiner Vereidigung oder um die Beurteilung seiner Glaubwürdigkeit geht. Hierfür wiederum sind in der Regel nur solche Verurteilungen von Bedeutung, die – wie beispielsweise Falschaussage oder Meineid – nach ihrer Deliktsart eine indizielle Bedeutung haben können. Allein damit, dass diese Regelungen in der Strafprozeßordnung stehen, ist es jedoch nicht getan. Entscheidend ist vielmehr, dass sie auch praktiziert werden. Dabei kommt es entscheidend darauf an, dass Polizei und Staatsanwaltschaften bei Vernehmungen der Persönlichkeitssphäre von Zeugen den nach unserer Verfassung gebotenen Stellenwert einräumen und die Fragen auf das zur Aufklärung der Straftat wirklich unerlässlich Notwendige beschränken. Tun sie das, dann lassen

sich Akteneinsichtsrecht und Persönlichkeitsrecht durchaus in ein ausgewogenes Verhältnis bringen.

2.3 Das jähe Ende einer Ausflugsfahrt

Ein Mann aus dem Unterland erlebte – wie er mir schrieb – eine böse Überraschung, als er bei seinem Ausflug am Frühlingsanfang 1999 im Elsass in eine Verkehrskontrolle geriet. Nachdem er den französischen Polizeibeamtem seinen Führerschein gezeigt hatte, nahmen diese mit ihren deutschen Kollegen Kontakt auf und hielten ihm dann vor, dass ihm in Deutschland die Fahrerlaubnis entzogen sei. Alles Beteuern, es müsse sich um einen Irrtum handeln, half nichts. Die französische Polizei ließ ihn keinen Meter mehr weiterfahren.

Wie alles gekommen war, klärte sich rasch: Der Mann war Ende Januar 1998 nachts mit einem Lkw von der Straße abgekommen und in den Straßengraben gerutscht. Vier Monate später beantragte die Staatsanwaltschaft Heilbronn beim Amtsgericht Heilbronn, dem Mann wegen Trunkenheit im Verkehr die Fahrerlaubnis vorläufig zu entziehen. Das Amtsgericht wies den Antrag zurück. Auf Beschwerde der Staatsanwaltschaft hob das Landgericht Heilbronn Ende Juli 1998 den Beschluss des Amtsgerichts auf und ordnete die vorläufige Entziehung der Fahrerlaubnis und die Beschlagnahme des Führerscheins an. Ende September 1998 erhob die Staatsanwaltschaft aus Anlass des Verkehrsunfalls gegen den Mann beim Amtsgericht Heilbronn Anklage wegen eines Vergehens der fahrlässigen Trunkenheit im Verkehr und eines Vergehens des unerlaubten Entfernens vom Unfallort. Das Amtsgericht Heilbronn verurteilte den Mann im Januar 1999 wegen unerlaubten Entfernens vom Unfallort zu einer Geldstrafe und sprach ihn im Übrigen frei. Zugleich hob es die vorläufige Entziehung der Fahrerlaubnis auf und händigte dem Mann seinen Führerschein aus. Versäumt hat das Amtsgericht Heilbronn allerdings, das Kraftfahrt-Bundesamt von der Aufhebung der vorläufigen Entziehung der Fahrerlaubnis zu unterrichten, obwohl es dies nach § 28 Abs. 4 des Straßenverkehrsgesetzes (StVG) unverzüglich hätte tun müssen. So kam es, dass im Zeitpunkt der Verkehrskontrolle im Elsass im Computer des Kraftfahrt-Bundesamts, den alle Polizeibeamten rund um die Uhr über das Zentrale Verkehrsinformations-System (ZEVIS) abfragen können, unzutreffenderweise immer noch gespeichert war, dass dem Mann die Fahrerlaubnis vorläufig entzogen ist.

Meine Beanstandung dieses erheblichen Verstoßes gegen § 28 Abs. 4 StVG nahm das Amtsgericht Heilbronn zum Anlass, seine Mitarbeiter darauf hinzuweisen, die Mitteilungspflicht an das Kraftfahrt-Bundesamt pünktlichst zu erfüllen. Selbstverständlich ist der unzulässige Eintrag im Computer des Kraftfahrt-Bundesamts jetzt gelöscht – der Mann hat wieder freie Fahrt.

2.4 Zu viel ging an das Kraftfahrt-Bundesamt

Das Kraftfahrt-Bundesamt in Flensburg betreibt das Verkehrszentralregister, das unter der landläufigen Bezeichnung „Verkehrssünderkartei“ besser bekannt ist. In diesem Register führt es nicht nur das sog. Punktekonto von Verkehrssündern, sondern notiert auf Mitteilung der Staatsanwaltschaften u. a. auch rechtskräftige Entscheidungen der Strafgerichte, soweit es um eine Verurteilung wegen einer Straftat im Zusammenhang mit dem Straßenverkehr geht. Eine Staatsanwaltschaft teilte dem Kraftfahrt-Bundesamt jedoch weit mehr mit, als nach den einschlägigen Vorschriften erlaubt ist. Das kam so: Ein Autofahrer war wegen zweier Tatkomplexe verurteilt worden. Bei der einen Tat ging es darum, dass er ohne eine Fahrerlaubnis zu besitzen Auto gefahren war und dabei auch noch gegen andere Strafvorschriften verstoßen hatte. Die andere Tat hatte mit dem Straßenverkehr nichts zu tun. Aus den für die beiden Taten angesetzten Freiheitsstrafen bildete das Gericht eine langjährige Gesamtfreiheitsstrafe. Statt dem Kraftfahrt-Bundesamt nur das Fahren ohne Fahrerlaubnis, die für diesen Tatkomplex angesetzte Freiheitsstrafe und die Dauer der ange-

ordneten Sperre für die Wiedererteilung der Fahrerlaubnis mitzuteilen, trug die Staatsanwaltschaft die viel längere Gesamtfreiheitsstrafe in das Mitteilungsformular ein. Zudem gab sie dort an, dass gegen den Autofahrer Sicherungsverwahrung angeordnet worden war und dass das Urteil den Verlust der Amtsfähigkeit und der Wählbarkeit sowie das Verbot, Jugendliche auszubilden und zu beschäftigen, nach sich gezogen hatte. Auf meine eingehenden Hinweise auf die nun wirklich klare Rechtslage korrigierte die Staatsanwaltschaft ihre viel zu umfangreiche Mitteilung an das Kraftfahrt-Bundesamt dann doch noch, nachdem sie dies zunächst weit von sich gewiesen und so argumentiert hatte, als sei die Datenschutzdiskussion der vergangenen 20 Jahre und die daraus entstandene Datenschutzgesetzgebung bisher spurlos an ihr vorübergegangen.

2.5 Veröffentlichung von Gerichtsentscheidungen nur bei ausreichender Anonymisierung

Ganz gleich welche der vielen juristischen Fachzeitschriften man zur Hand nimmt, überall kann man unter der Rubrik „Rechtsprechung“ Fälle nachlesen, die von Gerichten entschieden worden sind. Damit liegt das Problem offen zu Tage: Wie steht es dabei eigentlich mit dem Datenschutz?

Keine Frage: Gerichtliche Entscheidungen konkretisieren die Regelungen der Gesetze. Schon deshalb kommt der Veröffentlichung von Gerichtsentscheidungen eine enorme Bedeutung zu. In unserer zunehmend komplexen Rechtsordnung muss jeder zuverlässig in Erfahrung bringen können, welche Rechte er hat und welche Pflichten ihm obliegen; die Möglichkeiten und Aussichten, vor den Gerichten sein Recht zu suchen, müssen für ihn annähernd vorhersehbar sein. Ohne ausreichende Publizität der Rechtsprechung ist dies nicht möglich. Nicht zuletzt dient es auch der Fortbildung des Rechts, wenn über die Veröffentlichung von Gerichtsentscheidungen eine fachwissenschaftliche Diskussion ermöglicht wird. Bei alledem müssen die Gerichte aber darauf achten, dass es nicht zu einer Verletzung des Grundrechts auf Datenschutz der Personen kommt, um die es in den Gerichtsentscheidungen geht. Um dies zu verhindern, müssen die Gerichte die Entscheidungen, die sie an juristische Fachverlage zur Veröffentlichung herausgeben, zuvor so anonymisieren und neutralisieren, dass nach menschlichem Ermessen ein Rückschluss auf Personen unmöglich ist. Dazu kann es ausreichen, wenn sie Namen und Ortsangaben schwärzen oder durch neutrale Bezeichnungen wie beispielsweise „Kläger“, „Beklagter“, „Angeklagter“, „A-Stadt“ usw. ersetzen. Sind trotzdem Rückschlüsse auf Personen möglich, ist es notwendig, darüber hinaus weitere Angaben unkenntlich zu machen.

Diesen Anforderungen an die gebotene Anonymisierung von Gerichtsentscheidungen vor ihrer Herausgabe zur Veröffentlichung hat das Oberlandesgericht Karlsruhe nicht ausreichend Rechnung getragen, als es einen Beschluss in der Sache eines Strafgefangenen Fachverlagen zur Veröffentlichung überlassen hat. Statt darin wenigstens den Namen des Strafgefangenen vollständig zu schwärzen, ließ es die Initialen seines Vor- und Familiennamens stehen. Stehen ließ es u. a. auch den früheren Wohnort des Strafgefangenen, den Namen der Stadt, in der er vor noch nicht allzu langer Zeit eine Straftat verübt hatte, und zu welcher Freiheitsstrafe er deswegen von welchem Gericht verurteilt worden war. Deswegen und weil die Medien über die erwähnte Straftat und das anschließende Strafverfahren vielfältig berichtet hatten, war es nicht ausgeschlossen, den Strafgefangenen als denjenigen zu identifizieren, um den es in dem Beschluss des Oberlandesgerichts Karlsruhe ging.

2.6 Gegen wen erging der Haftbefehl?

Niemand ist erbaut, wenn gegen ihn ein Haftbefehl zur Abgabe der eidesstattlichen Versicherung ergeht. Viel beruhigender wird alles auch dann nicht, wenn man genau weiß, dass es sich um eine Personenver-

wechslung handeln muss. In dieser Situation wandte sich ein Nahverkehrsunternehmer aus dem Badischen Hilfe suchend an mich, weil er bei seinem Versuch, Licht ins Dunkel zu bringen, nicht mehr weitergekommen war. Das verwunderte uns nicht. Die Angelegenheit war – wie sich auf unsere eingehenden Recherchen beim Amtsgericht Karlsruhe, der Industrie- und Handelskammer Karlsruhe und beim Landratsamt Karlsruhe herausstellte – verzwickt genug. Manches ließ sich gar nicht mehr klären.

Um die Sache zu verstehen, muss man Folgendes wissen: Gegen einen Schuldner, der in einem zur Abgabe der eidesstattlichen Versicherung (früher: Offenbarungseid) anberaumten Termin nicht erscheint oder die Abgabe ohne Grund verweigert, hat das Amtsgericht zur Erzwingung der Abgabe auf Antrag einen Haftbefehl zu erlassen. Schuldner, gegen die sie einen solchen Haftbefehl erlassen oder die bei ihnen die eidesstattliche Versicherung abgegeben haben, registrieren die Amtsgerichte in ihren Schuldnerverzeichnissen. Informationen daraus dürfen – grob gesagt – für Zwecke verwendet werden, die mit der Feststellung der wirtschaftlichen Zuverlässigkeit zu tun haben. Dies macht die Schuldnerverzeichnisse zum Ausgangspunkt für einen weit verzweigten Datenfluss. Die Amtsgerichte dürfen beispielsweise den Industrie- und Handelskammern per Datenträgeraustausch laufend Abdrucke aus ihren Schuldnerverzeichnissen überlassen. Die Industrie- und Handelskammern können die Abdrucke in Listen zusammenfassen. Diese sog. Schuldnerlisten dürfen sie wiederum ihren Mitgliedern zum laufenden Bezug überlassen. In diesem reichlich komplizierten Geflecht lief im Falle des Nahverkehrsunternehmers manches schief. Das kam so:

– Das Amtsgericht Karlsruhe hatte in einer Zwangsvollstreckungssache gegen einen Schuldner, der zwar den gleichen Namen wie der Nahverkehrsunternehmer trug, jedoch ganz woanders wohnte, die Haft zur Abgabe der eidesstattlichen Versicherung angeordnet. In dem Abdruck aus seinem Schuldnerverzeichnis, den das Amtsgericht der Industrie- und Handelskammer Karlsruhe zur Erstellung der Schuldnerliste überließ, war dann jedoch aus nicht mehr zu klärenden Gründen der Wohnort des Nahverkehrsunternehmers als Wohnort des Schuldners angegeben; ihre beiden Adressen unterschieden sich jetzt nur noch in puncto Straßenname und Hausnummer. Damit nahm das Unheil seinen Lauf. Das Amtsgericht bedauerte – wie es uns schrieb – diese schwerwiegende Fehlleistung außerordentlich.

– Die Adresse des Schuldners mit der unzutreffenden Ortsangabe tauchte dann natürlich auch in der Schuldnerliste der Industrie- und Handelskammer Karlsruhe auf. Hätte es damit sein Bewenden gehabt, gäbe es hier kein weiteres Wort zu verlieren. Der Industrie- und Handelskammer wurde jedoch zum Verhängnis, dass sie sich beim Weitergeben ihrer Schuldnerlisten von dem Motto leiten ließ: Das haben wir schon immer so gemacht. Anstatt sich darauf zu besinnen, dass sie – wie es seit 1994 in der Zivilprozeßordnung steht – ihre Schuldnerlisten nur ihren Mitgliedern überlassen darf, verteilte die Industrie- und Handelskammer Karlsruhe diese entsprechend ihrer überkommenen Praxis nach wie vor auch an das örtliche Landratsamt und eine Reihe anderer Ämter. Auf meine Beanstandung dieser unzulässigen Streuung der Schuldnerlisten stellte die Industrie- und Handelskammer Karlsruhe ihre Praxis ein und forderte die Ämter auf, die erhaltenen Schuldnerlisten zu vernichten.

– Das Landratsamt Karlsruhe stieß in der ihm – zu Unrecht – überlassenen Schuldnerliste auf den Haftbefehlseintrag. Obwohl danach der Schuldner in einer anderen Straße als der Nahverkehrsunternehmer wohnte, ging das Landratsamt kurzerhand davon aus, der Haftbefehl sei gegen diesen ergangen. Es forderte ihn deshalb schriftlich auf, die dem Haftbefehl zugrunde liegende Angelegenheit aus der Welt zu schaffen und eine Bestätigung des Amtsgerichts über die Löschung des Haftbefehlseintrags im Schuldnerverzeichnis beizubringen; ansonsten stehe die Genehmigung für sein Nahverkehrsun-

ternehmen in Frage. Tatsächlich war aber der Nahverkehrsunternehmer nicht identisch mit dem Schuldner, gegen den der Haftbefehl ergangen war. Als ich das Landratsamt auf die Personenverwechslung ansprach, gelobte es Besserung. Künftig will es in Zweifelsfällen die Frage der Personenidentität sorgfältig prüfen, bevor es Weiteres veranlasst. Das sollte doch wohl selbstverständlich sein. Denn Personenverwechslungen bereiten den betroffenen Personen nicht nur Scherereien, sondern führen auch dazu, dass Unbeteiligte Informationen über Dritte erhalten, die sie nichts angehen.

2.7 Das misstrauische Oberlandesgericht

Ausländer, die in Deutschland heiraten wollen, müssen in der Regel eine Bescheinigung ihres Heimatstaats darüber beibringen, dass nach dessen Recht dieser Absicht keine Ehehindernisse entgegenstehen. Von dieser Verpflichtung kann die Verwaltungsabteilung des zuständigen Oberlandesgerichts Befreiung gewähren. Der heiratswillige Ausländer muss dazu beim Standesamt einen entsprechenden Antrag stellen, der dann dem Oberlandesgericht zur Entscheidung vorgelegt wird.

So geschah es auch im Falle einer Ausländerin, die einen Deutschen heiraten wollte. Weil der Standesbeamte bei der Weiterleitung des Antrags angegeben hatte, die Ausländerin sei nicht berechtigt, sich in der Bundesrepublik aufzuhalten, wurde das Oberlandesgericht Stuttgart, das über den Antrag zu entscheiden hatte, misstrauisch. Es vermutete, es könne eine sog. Scheinehe beabsichtigt sein, also eine Ehe, die ausschließlich auf dem Papier zu dem Zweck geschlossen wird, dem beteiligten Ausländer zu einem Aufenthaltsrecht zu verhelfen. Weil es zu Recht für einen solchen Zweck keine Befreiung vom Erfordernis eines Ehefähigkeitszeugnisses aussprechen wollte, forderte es kurzerhand die gesamte Ausländerakte bei der zuständigen Ausländerbehörde an, um auf diese Weise Aufschlüsse darüber zu bekommen, ob sein Verdacht zu Recht bestand. Das war so nicht in Ordnung. Auch ein Oberlandesgericht muss in solchen Fällen – wie alle anderen öffentlichen Stellen im Lande auch – respektieren, dass personenbezogene Daten nach dem Landesdatenschutzgesetz grundsätzlich beim Betroffenen und nur ausnahmsweise bei Dritten zu erfragen sind. Es hätte also zunächst einmal die Ausländerin mit seinem Verdacht konfrontieren und sie gezielt danach befragen müssen. Erst wenn auf diese Weise die Frage Scheinehe oder nicht offen bleibt, kann es bei anderen Stellen Ermittlungen anstellen. Dabei kann sich das Oberlandesgericht die Sache aber nicht einfach machen und kurzerhand die gesamte Ausländerakte anfordern. Denn darin befindet sich meist eine Vielzahl von teilweise sehr sensiblen Daten, die für die zu klärende Frage von vornherein ohne Bedeutung sind. Das bedeutet: Das Oberlandesgericht muss sich auch in solchen Verdachtsfällen in aller Regel damit begnügen, mit gezielten Fragen an die Ausländerbehörde heranzutreten.

Ich habe das Oberlandesgericht auf diese Rechtslage hingewiesen. Es wird ihr bei der Bearbeitung künftiger Fälle Rechnung tragen.

2.8 Die nichterfüllte Zusage

In meinem letztjährigen Tätigkeitsbericht (Landtags-Drucksache 12/3480, S. 63) hatte ich angeprangert, dass viele Gemeinden nicht datenschutzgerecht verfahren, wenn sie in einem Sterbefall dem Notariat als Nachlassgericht Informationen für die amtliche Erbenermittlung liefern, wie es das Landesgesetz über die Freiwillige Gerichtsbarkeit vorschreibt. Häufig erfragen sie bei den Hinterbliebenen mehr Angaben als notwendig und zulässig, weil sie sich noch weitgehend nach einer längst überholten Verwaltungsvorschrift aus der „Vordatenschutzzeit“ richten. Deshalb hatte ich gefordert, die Mitwirkung der Gemeinden in Nachlasssachen entweder per Gesetz einzuschränken oder aber wenigstens ihre Grenzen durch eine Verwaltungsvorschrift zu verdeutlichen.

Die damalige Reaktion des Justizministeriums ließ hoffen. Es lehnte zwar eine Gesetzesänderung rundweg ab, sagte jedoch zu, in Abstimmung mit dem Innenministerium einen Runderlass an die Notariate, Städte und Gemeinden zu richten, der eine datenschutzrechtlich korrekte Behandlung der Nachlassangelegenheiten sicherstellen soll. Diese Zusage wiederholte die Landesregierung in ihrer Stellungnahme zu meinem Tätigkeitsbericht (Landtags-Drucksache 12/3810, S. 25/26) gegenüber dem Landtag.

Inzwischen ist Ernüchterung eingekehrt. Erst auf Nachfrage ließ mich das Justizministerium im Mai 1999 wissen, es wolle die Frage einer Gesetzesänderung doch nochmals grundsätzlich überprüfen. Fast ein weiteres halbes Jahr dauerte es, bis in der Sache wieder etwas zu hören war.

Anfang November 1999 informierte mich das Justizministerium nachrichtlich über einen von ihm ausgearbeiteten Referentenentwurf eines Erlasses an die Notariate, aber noch nicht an die Städte und Gemeinden. Bedenkt man, dass auch noch das offizielle Anhörungsverfahren durchzuführen ist, dann wird klar, dass einige Zeit vergehen wird, bis sowohl die Notariate als auch die Städte und Gemeinden die notwendigen Hinweise erhalten. Angesichts dessen, dass das Justizministerium auch beim Landtag im Wort steht, eine bemerkenswert nonchalante Behandlung eines drängenden Datenschutzproblems!

3. Strafvollzug

Seit In-Kraft-Treten des Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes am 1. Dezember 1998 ist die Verarbeitung personenbezogener Daten im Strafvollzug nun endlich gesetzlich geregelt. Dass man sich aus der Sicht des Datenschutzes manches anders gewünscht hätte, habe ich bereits im letzten Tätigkeitsbericht (vgl. 19. Tätigkeitsbericht, Landtags-Drucksache 12/3810, S. 48/49) dargelegt. Führen die Regelungen zu mehr Sensibilität und Rechtssicherheit beim Umgang mit Gefangenendaten, wäre einiges erreicht, um dem Recht des Gefangenen auf Datenschutz zum Durchbruch zu verhelfen.

3.1 Automatisierte Datenverarbeitung in den Justizvollzugsanstalten

Anfang der 80er Jahre hielt die EDV Einzug in die Justizvollzugsanstalten. Das Justizministerium stattete damals die Justizvollzugsanstalten mit Anlagen der mittleren Datentechnik aus und stellte ihnen in Eigenregie gefertigte Programme zur Verfügung. Diese Technik ist inzwischen veraltet. Auch können die eingesetzten Systeme den Datumswechsel zum Jahr 2000 nicht verarbeiten. Deshalb ersetzt das Justizministerium sie seit einiger Zeit schrittweise durch Client-Server-Systeme, stellt die Programme mittels eines Übersetzungsprogramms eins zu eins um und macht sie für den Jahrtausendwechsel fit. Weil die Umstellung bei den Justizvollzugsanstalten Schwäbisch Hall und Ravensburg bereits abgeschlossen ist, sahen wir uns an, wie dort die automatisierte Verarbeitung von Gefangenendaten läuft. Um es gleich vorwegzusagen: Dabei ergab sich wenig Erfreuliches. Vor allem im Bereich der technischen und organisatorischen Datenschutzmaßnahmen zeigten sich erhebliche Defizite. Zu Fehlern und Mängeln, die wir schon zum x-ten Mal bei anderen Behörden angetroffen haben und die ich in der Hoffnung, ihnen so ein für allemal den Garaus machen zu können, in meinen Tätigkeitsberichten wiederholt unter Hinweis darauf, wie man es richtig macht, dargestellt habe, gesellten sich Defizite, für die dem Justizministerium, das die Hard- und Softwareausstattung vorgegeben hat, das Urheberrecht zusteht. Die Gravierendsten davon sind, wo sie hingehören, im Teil „Technik und Organisation“ dieses Berichts nachzulesen. Außerdem stießen wir noch auf Folgendes:

3.1.1 Interne Aufnahmemitteilungen

Nimmt eine Justizvollzugsanstalt (JVA) einen Gefangenen auf, legt die Vollzugsgeschäftsstelle für ihn eine Personalakte mit

dem sog. A-Bogen als Kernstück an. Dieser enthält zahlreiche Angaben über den Gefangenen, u. a. Name, Vorname, Religionszugehörigkeit, Staatsangehörigkeit, Familienstand, Name und Wohnort der nächsten Angehörigen, erlernter Beruf, Vorstrafen, Strafmaß und vieles mehr. Außer der Vollzugsgeschäftsstelle benötigen auch andere Stellen in einer JVA Informationen über den Gefangenen. Diese Stellen erhalten dazu von der Vollzugsgeschäftsstelle Aufnahmemitteilungen. Weil nach den Vorschriften des Strafvollzugsgesetzes eine JVA personenbezogene Daten von Gefangenen nur verarbeiten und nutzen und deshalb der einzelne Vollzugsbedienstete sich von solchen Daten nur Kenntnis verschaffen darf, wenn und soweit dies für den Vollzug der Freiheitsstrafe bzw. für die Erfüllung der dem Bediensteten obliegenden Aufgabe erforderlich ist, darf die Vollzugsgeschäftsstelle nicht alles, was sie von einem Gefangenen weiß und auf dem A-Bogen vermerkt hat, unbesehen an die anderen Stellen weitergeben. Dies folgt schon seit jeher aus dem guten alten Grundsatz der Verhältnismäßigkeit und steht jetzt im Strafvollzugsgesetz. Die Praxis ist freilich eine andere.

1995 zeigte sich bei einer Kontrolle des Vollzugskrankenhauses Hohenasperg (vgl. 16. Tätigkeitsbericht, Landtags-Drucksache 11/6900, S. 34 f.), dass die Vollzugsgeschäftsstellen im sog. Umdruckverfahren den A-Bogen auf Karteikarten übertragen und diese an andere interne Stellen verteilten. Weil sich diese Verfahrensweise nicht am jeweiligen Informationsbedürfnis der Empfänger orientierte, sondern allein daran, wie die Vollzugsgeschäftsstelle die anderen Stellen in der JVA am einfachsten und mit dem geringstmöglichen Aufwand über die Aufnahme eines Gefangenen unterrichten kann, wurde dies gegenüber dem Justizministerium beanstandet, zumal eine schon im Jahre 1991 ausgesprochene Beanstandung der gleichen Praxis in einer anderen JVA des Landes keine Änderung bewirkt hatte. Das Justizministerium setzte in der Stellungnahme der Landesregierung zu meinem 16. Tätigkeitsbericht darauf, dass „insoweit lediglich die bereits seit längerem geplante Automation der Vollzugsgeschäftsstellen Abhilfe schaffen könnte“ (vgl. Landtags-Drucksache 11/7081, S. 12). Jetzt sind die Vollzugsgeschäftsstellen der JVA Ravensburg und der JVA Schwäbisch Hall zwar mit Computern ausgerüstet und haben das vom Justizministerium zur Verfügung gestellte EDV-Verfahren für die Vollzugsgeschäftsstellen im Einsatz, gelöst ist das Problem dennoch nicht. Die Programme ermöglichen zwar den Vollzugsgeschäftsstellen Aufnahmemitteilungen für die verschiedenen Stellen automatisiert zu erstellen, sie sind jedoch in der konkreten Anwendung nicht flexibel genug. Das EDV-Verfahren ermöglicht es im Zuge der Aufnahme eines Gefangenen nämlich nicht, individuell die Empfänger von Aufnahmemitteilungen festzulegen und den Datenumfang in den Aufnahmemitteilungen nach den jeweiligen Erfordernissen zu komponieren. Das sollte aber ein Datenverarbeitungsprogramm schon leisten.

3.1.2 Auskunftsprogramme inflexibel

Die bei der Aufnahme eines Gefangenen erfassten Daten sollen mit Hilfe der EDV den einzelnen Stellen in der JVA zur Erledigung ihrer Aufgaben zur Verfügung stehen. Dazu gibt es neben speziellen Auskunftsprogrammen für ganz bestimmte Zwecke ein allgemeines Auskunftsprogramm, das allen Personen zugänglich sein soll, die zur Erledigung ihrer Aufgaben Gefangenendaten brauchen. Das allgemeine Auskunftsprogramm ist mit demselben Manko behaftet wie das EDV-Programm für die Aufnahmemitteilungen: Es hat nämlich einen festen Datenumfang, der weder reduziert noch erweitert werden kann. Zudem ist es vom Programm her nicht möglich, den Zugriff eines Mitarbeiters der JVA auf einzelne Datenfelder zu beschränken.

Weil nun einige Stellen bzw. die dort tätigen Mitarbeiter zur Erfüllung ihrer Aufgabe nicht alle Daten benötigen, die das allgemeine Auskunftsprogramm zur Verfügung stellt, steht jede JVA vor dem Dilemma, dass sie einerseits das allgemeine Auskunftsprogramm einsetzen soll, andererseits aber, wenn sie dies tut, gegen den Datenschutz verstößt. Auch hier liegt die Lösung nahe: Das allgemeine Auskunftsprogramm muss flexibler gestaltet werden.

Der Ausweg, den die JVA Schwäbisch Hall und die JVA Ravensburg gewählt haben, verbietet sich freilich von vornherein: Ohne viel Federlesens räumten beide allen Mitarbeitern, die bei ihrer täglichen Arbeit einen Computer benutzen können, meist den kompletten Zugriff auf die speziellen Auskunftsprogramme ein. So können in beiden Anstalten fast alle Computerbenutzer auf das Auskunftsprogramm der Vollzugsgeschäftsstelle und damit auf die umfassendste Sammlung von automatisiert gespeicherten Gefangenendaten zugreifen, obwohl sie nicht alle diese Daten für ihre eigene Aufgabenerfüllung benötigen. Weil in der Programmdokumentation sogar ausdrücklich steht, dass das Auskunftsprogramm für die Vollzugsgeschäftsstelle außer der Vollzugsgeschäftsstelle anderen Abteilungen nur in begründeten Ausnahmefällen und nur für einzelne Personen zugänglich gemacht werden darf, war eine Beanstandung unvermeidlich. Zu beanstanden war außerdem, dass die beiden Anstalten nicht nur denjenigen Mitarbeitern, die für die Aufbewahrung der Akten ausgeschiedener Gefangener zuständig sind, sondern ebenfalls fast allen anderen Computerbenutzern den Zugriff auf ein Auskunftsprogramm gestatteten, das die Daten von ausgeschiedenen Gefangenen anzeigt. Nach dem Strafvollzugsgesetz dürfen Daten von ausgeschiedenen Strafgefangenen nur dann automatisiert gespeichert und genutzt werden, wenn es für das Auffinden der aufbewahrten Gefangenenpersonalakten erforderlich ist. Deshalb darf dieses Auskunftsprogramm auch nur denjenigen Mitarbeitern zur Verfügung gestellt werden, die für die Aufbewahrung der Akten der ausgeschiedenen Gefangenen zuständig sind.

3.1.3 Abschlussdatensatz zu umfangreich

Scheidet ein Gefangener aus der JVA aus, weil er in die Freiheit entlassen oder in eine andere JVA verlegt wird, sind die automatisiert gespeicherten Gefangenendaten spätestens zwei Jahre danach zu löschen, so steht es im Strafvollzugsgesetz. Nur den Familiennamen, Vornamen, Geburtsnamen, Geburtsort und Geburtstag sowie das Eintritts- und Austrittsdatum des Gefangenen darf eine JVA bis zum Ablauf der Aufbewahrungsfrist der Gefangenenpersonalakte in ihrem Computer weiter speichern, soweit dies für das Auffinden der Gefangenenpersonalakte erforderlich ist. Statt sich auf diese enumerativ im Strafvollzugsgesetz aufgezählten Angaben zu beschränken, produziert das EDV-Verfahren, das ihnen das Justizministerium zur Verfügung gestellt hat, einen Abschlussdatensatz, der darüber hinaus geht. Das Justizministerium habe ich deshalb aufgefordert, im Abschlussdatensatz die Angaben zum Geschlecht, zur Staatsangehörigkeit, zur Austrittsart, zur Haftart sowie die Verlegungs- oder Entlassadresse zu streichen.

3.1.4 Aufbewahrung von Altakten

Mit der Novellierung des Strafvollzugsgesetzes wurden auch die Fristen für die Aufbewahrung der Gefangenenpersonalakten und der Krankenakten von ausgeschiedenen Gefangenen gesetzlich geregelt. Danach dürfen Gefangenenpersonalakten und Krankenakten höchstens 20 Jahre und nicht mehr – wie dies früher in einer Verwaltungsvorschrift festgelegt war – 30 Jahre lang aufbewahrt werden. Diese Änderung hatten die JVA Ra-

vensburg und die JVA Schwäbisch Hall noch nicht in die Tat umgesetzt. Beide habe ich deshalb aufgefordert, sich an die Vernichtung der Gefangenenpersonalakten der bereits vor 20 und mehr Jahren ausgeschiedenen Gefangenen zu machen. Vor kurzem meldete die JVA Schwäbisch Hall bereits Vollzug.

Beim Besuch in der JVA Ravensburg mussten wir zudem feststellen, dass in einem Archivraum, der sich im Keller des Verwaltungsgebäudes befindet und der für alle Mitarbeiter der Verwaltung zugänglich ist, neben allgemeinen Verwaltungsunterlagen auch zahlreiche Krankenakten von Gefangenen gelagert sind. Da es sich bei Krankenakten um besonders sensible Datensammlungen handelt, sind diese nach dem Strafvollzugsgesetz getrennt von anderen Unterlagen zu führen und besonders zu sichern. Weil die JVA Ravensburg dem nicht nachgekommen ist und in einem besonders sensiblen Bereich gegen datenschutzrechtliche Bestimmungen verstoßen hat, kam ich nicht umhin, auch dies zu beanstanden und sie aufzufordern, diesen unhaltbaren Zustand unverzüglich zu beseitigen.

Vom Justizministerium habe ich bisher zu meinen Beanstandungen, Hinweisen und Vorschlägen keine Antwort bekommen. Auf mein Schreiben vom 17. September 1999 hat es mich kurz vor Ablauf der gesetzten Äußerungsfrist nur wissen lassen, eine Stellungnahme sei voraussichtlich erst im Februar/März 2000 möglich, weil die Mitarbeiter des Referats EDV in seiner Strafvollzugsabteilung wegen der noch vor der Jahrtausendwende zwingend notwendigen Komplettierung der EDV in den Justizvollzugsanstalten erheblich überlastet sind. Ist ihm eigentlich bewusst, dass es dabei die festgestellten Fehler und Mängel immer gleich mitliefert?

3.2 Einzelfälle

Auch heuer wandten sich zahlreiche Gefangene an mein Amt, weil sie damit nicht zufrieden waren, wie die Justizvollzugsanstalten mit ihren Datenschutzrechten umgingen. Neben anderem sprachen sie auch folgende grundsätzliche Probleme an:

3.2.1 Die Gefangenenpost

Jeder Gefangene hat grundsätzlich das Recht, unbeschränkt Schreiben abzusenden und zu empfangen. Damit zieht das Strafvollzugsgesetz für den Bereich der schriftlichen Kommunikation der Gefangenen die Konsequenz aus dem Gebot, dass die Situation der Gefangenen auch hier soweit als möglich normalen Lebensverhältnissen entsprechen soll. In der Praxis bereitet das Recht der Gefangenen, Briefkontakte zu pflegen, hin und wieder Probleme:

– Der JVA Bruchsal musste ich schon 1997 einmal in Erinnerung rufen, dass der Schriftwechsel von Gefangenen mit sog. Petitionsstellen seit jeher für die Justizvollzugsanstalt tabu ist (vgl. 18. Tätigkeitsbericht, Landtags-Drucksache 12/2242, S. 33/34). Sie hat daraufhin in ihrer Poststelle eine DIN A4-große Hinweistafel mit einer Auflistung aller Petitionsstellen aufgestellt, damit sie beim Sortieren der Post schwarz auf weiß immer vor Augen hat, welche Briefe nicht geöffnet werden dürfen. Darauf steht, dass u. a. die Schreiben von Volksvertretungen des Bundes und der Länder sowie ihrer Ausschüsse und die Schreiben der Strafvollzugsbeauftragten der Landtagsfraktionen an Gefangene aus der eingehenden Post herauszusortieren und den Gefangenen ungeöffnet auszuhändigen sind. Gefruchtet hat dies und der Hinweis, jetzt darauf peinlichst zu achten, nicht lange. Ende letzten Jahres öffnete die JVA zwei Briefe des Petitionsausschusses des Landtags und zwei Schreiben der Strafvollzugsbeauftragten einer Landtagsfraktion an ein und denselben Gefangenen. Um der Sache auf den Grund zu gehen, sah sich einer meiner Mitar-

beiter den Ablauf des Posteingangs vor Ort an. Dabei war rasch klar, warum die vier Schreiben trotz deutlicher Absenderangaben und Hinweistafel geöffnet worden waren: Das Heraussortieren der Schreiben von Petitionsstellen an Gefangene aus der eingehenden Post erfolgte in der Poststelle. Der damit befasste Mitarbeiter war zugleich für die Vergabe von Besuchsterminen zuständig. Weil bei ihm deswegen das Telefon praktisch nicht still stand, hatte er keine ruhige Minute zum Sortieren der eingehenden Post. Dass das ständige Hin und Her zwischen Post sortieren und Vergeben von Besuchsterminen eine permanente Fehlerquelle darstellte, leuchtete der JVA sofort ein. Sie ordnete auf unseren Vorschlag noch beim Kontrollbesuch an, dass die eingehenden Briefe künftig nicht mehr in der Poststelle, sondern in einem extra Raum und damit ungestört von den ständigen Anrufen in Sachen Besuchsterminen sortiert werden. Klagen über geöffnete Briefe sog. Petitionsstellen sind uns seither nicht mehr zu Ohren gekommen.

PS: Dass die JVA im Oktober/November 1998 auch einen Brief der Europagruppe Die Grünen, der F.D.P.-Fraktion im Deutschen Bundestag, eines CDU-Landtagsabgeordneten, eines Abgeordneten des Europäischen Parlaments und eines Bundestagsabgeordneten an den Gefangenen geöffnet hat, verstieß zwar nicht gegen den Buchstaben der erwähnten Regelungen. Einen rechtfertigenden Grund, in die Briefe von Abgeordneten an Gefangene zu schauen, gab und gibt es indes nicht. Inzwischen hat deshalb der Gesetzgeber im Strafvollzugsgesetz klargestellt, dass auch Schreiben von Abgeordneten an Gefangene nicht geöffnet werden dürfen.

– Eine JVA überwacht den Schriftwechsel eines Gefangenen. Bei der Textkontrolle der ausgehenden Post kopierte sie mehrere an Bekannte und Verwandte adressierte Briefe des Gefangenen vollständig und nahm die Kopien zu seiner Gefangenenpersonalakte, weil der Gefangene in seinen Briefen Vollzugsbedienstete bedroht hatte. Beim Kopieren solcher Briefe muss die JVA auch bedenken, dass dies wegen der besonderen Bedeutung und Tragweite des Briefgeheimnisses, das auch Gefangenen zusteht, nur unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes geschehen darf. Um dem Rechnung zu tragen, sollte die Vollzugsanstalt nur die Passagen kopieren, in denen es um die Bedrohung von Vollzugsbeamten geht.

3.2.2 Auskunftserteilung auf Umwegen

Seit Dezember 1998 ist im Strafvollzugsgesetz das Recht eines jeden Gefangenen auf Auskunft über die zu seiner Person gespeicherten Daten geregelt. Beim Umgang mit dem Auskunftsrecht läuft noch nicht alles rund wie folgender Fall exemplarisch zeigt:

Ein Gefangener hatte sich einer umfangreichen Blutuntersuchung unterziehen müssen. Das Ergebnis der Blutuntersuchung erläuterte ihm die Anstaltsärztin in einem Gespräch. Die Bitte des Gefangenen, ihm schriftlich, am besten durch Aushändigung einer Kopie des Untersuchungsbefundes, Auskunft über das Ergebnis seiner Blutuntersuchung zu geben, lehnte die Anstaltsärztin ab. Auf seine Remonstration ließ ihn die JVA wissen, sie habe inzwischen seiner Verteidigerin eine Kopie des Blutwertebefundes ausgehändigt, obwohl er nicht dargelegt habe, warum er die Kopie zur Wahrnehmung seiner rechtlichen Interessen brauche.

Zwar hat der Gefangene so seine Blutwerte doch noch schwarz auf weiß bekommen. Mit der gesetzlichen Auskunftsregelung stand die Vorgehensweise der JVA jedoch in zweierlei Hinsicht nicht im Einklang:

– Das Auskunftsrecht ist ein höchstpersönliches Recht eines jeden Gefangenen, das dieser selbst oder – wenn er will – durch einen Bevollmächtigten ausüben kann. Seinen Verteidiger braucht ein Gefangener demzufolge für die Wahrnehmung seines Auskunftsrechts nicht einzuschalten; darauf kann die JVA einen Gefangenen auch nicht verweisen. Sie muss ihm vielmehr die erbetene Auskunft persönlich zukommen lassen.

– Eine schriftliche Auskunft setzt keineswegs voraus, dass der Gefangene ein rechtliches Interesse daran geltend macht. Vielmehr ist dem Gefangenen die Auskunft bereits dann schriftlich zu erteilen, wenn er ein berechtigtes Interesse an einer solchen Auskunft hat. Hier kommt es – anders als bei dem Begriff des rechtlichen Interesses – nicht auf das Bestehen eines Rechtsverhältnisses an, das durch die Auskunft über die gespeicherten Daten beeinflusst wird. Es genügt vielmehr ein nach vernünftiger Erwägung durch die Sachlage gerechtfertigtes, also ein tatsächliches, von der Rechtsordnung anerkanntes Interesse, das wirtschaftlicher oder ideeller Natur sein kann. Ein solches Interesse ist einer Bitte um Auskunft über gespeicherte Daten in der Regel immanent, weil kaum jemand in der Lage ist sich zu merken, was alles über ihn gespeichert ist. Deshalb gilt der Grundsatz: Nur eine schriftliche Auskunft ist eine datenschutzgerechte Auskunft.

Kurzum: Statt ihm die Bitte abzuschlagen und den Umweg über die Verteidigerin zu wählen, hätte die JVA dem Gefangenen eine Kopie mit seinen Blutwerten gleich aushändigen müssen.

2. Abschnitt: Die Polizei

In kaum einem Bereich der Landesverwaltung kommt der Einsatz der IuK-Technik so voran, wie bei der Polizei: moderne Telefonanlagen, neue Einsatzleitrechner, PCs auf den Polizeidienststellen allenthalben. Zudem planen Landeskriminalamt und Innenministerium im Zuge des Projekts IKNPOL-Dezentralisierung, die Polizeidienststellen im Lande mit moderner Bürokommunikation auszurüsten. Weil sich dadurch das Gesicht der automatisierten Datenverarbeitung bei der Polizei nachhaltig ändert, wirkt mein Amt an diesem Projekt beratend mit.

Auch im Berichtsjahr haben wir bei Kontrollbesuchen vor Ort die Praxis der polizeilichen Datenverarbeitung stichprobenweise überprüft. Dass solche Kontrollen nach wie vor geboten sind, wird ohne weiteres klar, wenn man sich Folgendes vor Augen führt: 1997 hatten wir bei Kontrollbesuchen festgestellt, dass der notwendige Gleichklang bei der Löschung von Datenspeicherungen über mutmaßlich oder tatsächlich begangene Rauschgiftdelikte in der Personenauskunftsdatei (PAD) und in der bundesweiten, auf dem Rechner des Bundeskriminalamts laufenden Falldatei Rauschgift (FDR) aus dem Takt gekommen war, weil die Polizei nach Ablauf der PAD-Speicherfrist den Rauschgifteintrag zwar in der PAD, nicht jedoch zugleich auch – wie es geboten gewesen wäre – in der FDR gelöscht hat. Eine Datenspeicherung in der FDR ist besonders belastend. Wer nämlich dort registriert ist, muss damit rechnen, dass ihn die Polizei etwa bei Kontrollen nach einer Dateiabfrage als jemanden ansieht, der nach wie vor mit Rauschgift zu tun hat, und dass sie weitere Maßnahmen gegen ihn ergreift. Deshalb legte ich Wert darauf, dass die Polizei ihre FDR-Speicherungen einer Revision unterzieht. Das Ergebnis liegt inzwischen vor: Das Landeskriminalamt hat bei mehr als 20 000 Personen oder anders gesagt bei jeder vierten FDR-Speicherung die Löschtaste gedrückt.

1. IKNPOL-Dezentralisierung

Die Zeiten, in denen die Polizeibeamten ihre Vorgänge umständlich in Tagebüchern, Wachbüchern usw. registrieren und Vorkommnisberichte fertigen oder im Laufe der Sachbearbeitung dieselben Daten immer wieder eintippen mussten, sollen vorbei sein, sobald den Polizeidienststellen das Vorgangsbearbeitungs- und Vorgangsverwaltungssystem zur Verfü-

gung steht, das das Landeskriminalamt im Zuge des Projekts IKNPOL-Dezentralisierung erarbeitet hat. Mit Hilfe dieses Systems sollen die Polizeibeamten

– jedweden Vorgang, angefangen von der Anzeige wegen einer Straftat bis zur Vermisstenmeldung, automatisiert bearbeiten und verwalten,
– Informationen zur Gefahrenabwehr und zur vorbeugenden Bekämpfung von Straftaten abrufen (sog. Kurzinformation),
– Lagebilder erstellen,
– Informationen für Einsätze abrufen und
– einmal erhobene und gespeicherte Daten automatisch für alle weiteren Bearbeitungsschritte nutzen können.

Anfang Juni 1999 hat uns das Landeskriminalamt das Vorgangsbearbeitungs- und Vorgangsverwaltungssystem vorgestellt. Aus der Sicht des Datenschutzes ist dazu vor allem Folgendes zu bemerken:

1.1 Die Kurzinformation

Ganz gleich, ob ein Polizeibeamter gegen einen Beschuldigten wegen des Verdachts einer Straftat ermittelt, ob er wegen einer Verkehrs- oder sonstigen Ordnungswidrigkeit oder wegen eines Verkehrsunfalls tätig wird, ob er jemanden zur Fahndung ausschreibt, weil er beispielsweise als vermisst gemeldet worden ist, ob er jemanden in Gewahrsam nimmt, ob er gegen einen Störer einschreitet oder ob er wegen eines sonstigen Ereignisses tätig wird – in jedem Fall ist er gehalten, darüber sofort eine sog. Kurzinformation in das Vorgangsbearbeitungs- und Vorgangsverwaltungssystem einzustellen. Die Kurzinformation besteht im Wesentlichen aus einer kurzen Schilderung, was sich wann wo zugetragen hat und – je nachdem, um welches Ereignis es sich handelt – aus Angaben zum Tatverdächtigen/Beschuldigten/Betroffenen/Beteiligten/Geschädigten bis hin zu der Person, die einen Fehlalarm ausgelöst hat. Für die Kurzinformationen waren nach dem ursprünglichen Konzept des Landeskriminalamts unterschiedliche Speicherfristen vorgesehen; bei Strafanzeigen und Verkehrsunfällen beispielsweise zwei Jahre, bei Ingewahrsamnahmen sechs Monate, bei einer Personenfahndung nach einer vermissten Person, bei einer Ordnungswidrigkeit oder bei einer Ordnungsstörung durch eine betrunkene oder hilflose Person drei Monate. So lange sollten die Kurzinformationen allen Polizeibeamten der jeweiligen Polizeidirektion über das Vorgangsbearbeitungs- und Vorgangsverwaltungssystem zum jederzeitigen Abruf zur Verfügung stehen.

Diese Gestaltung der Kurzinformation strapaziert das Polizeigesetz, den Grundsatz der Verhältnismäßigkeit und das Gebot der Zweckbindung ganz erheblich:

– Daten über Störer darf die Polizei in einem automatisierten Informationssystem wie dem Vorgangsbearbeitungs- und Vorgangsverwaltungssystem nur speichern, wenn es tatsächliche Anhaltspunkte für die Annahme gibt, dass von ihnen künftig erneut eine Gefahr für die öffentliche Sicherheit oder Ordnung ausgeht und die gespeicherten Daten dann die polizeiliche Arbeit fördern könnten. Informationen über Beschuldigte darf die Polizei zur vorbeugenden Bekämpfung von Straftaten in automatisierten Informationssystemen nur speichern, wenn die Umstände des Einzelfalls die Annahme rechtfertigen, dass der Beschuldigte künftig erneut eine Straftat begehen wird. Diesen gesetzlichen Anforderungen an die Speicherung personenbezogener Daten trägt die beschriebene Gestaltung der Kurzinformation nicht Rechnung, weil die Polizei bei der Einstellung der Kurzinformationen in das Vorgangsbearbeitungs- und Vorgangsverwaltungssystem keine solchen Prognosen zu treffen hat, sondern gehalten ist, ganz unabhängig davon in jedem Fall Informationen über Störer und Beschuldigte zu speichern.

– Die beschriebene Funktionsweise der Kurzinformation führt unausweichlich dazu, dass gespeicherte personenbezogene Daten

auch Polizeibeamten zur Kenntnis gebracht werden, die diese zur Erledigung ihrer Aufgaben gar nicht kennen müssen. Dies sei an folgendem Beispiel verdeutlicht: Besagt eine gespeicherte Kurzinformation, dass die Polizei zu einer nächtlichen Ruhestörung gerufen worden ist und fragt ein Polizeibeamter eines benachbarten Polizeireviers aus einem ganz anderen Anlass zum Zwecke der Bekämpfung von Straftaten das Vorgangssystem nach Kurzinformationen über den Verursacher der Störung ab, wird ihm automatisch die gespeicherte Kurzinformation über die Ruhestörung am Bildschirm angezeigt. Die Kenntnis dieser Informationen ist aber für die Bekämpfung von Straftaten schlechterdings nicht notwendig.

– Daten über Opfer einer Straftat darf die Polizei in automatisierten Informationssystemen nur speichern und nutzen, soweit dies zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist. Darauf ist aber die Speicherung und Nutzung von Daten über Opfer in den Kurzinformationen gerade nicht beschränkt.

Das Landeskriminalamt, das ich auf diese und andere Probleme mit der Kurzauskunft hingewiesen habe, ließ mich vor kurzem wissen, dass es die „zeitliche Verfügbarkeit von Kurzinformationen für die gesamte Polizeidirektion auf die Dauer von einem Monat“ begrenzen will. Das ist zwar ein großer Schritt in die richtige Richtung; dem Buchstaben des Polizeigesetzes entspricht die Kurzauskunft damit aber noch nicht.

1.2 Auswertungsmöglichkeiten

Die IuK-Technik darf den Menschen nicht zum bloßen Objekt der Datenverarbeitung machen. Dies gilt nicht nur für die Personen, über die die Polizei Informationen in ihren Computern verarbeitet, sondern auch für die Polizeibeamten. Sie hinterlassen bei jedem Vorgang, den sie mit dem Vorgangsbearbeitungs- und Vorgangsverwaltungssystem erledigen, Datenspuren, aus denen mit Hilfe entsprechender Auswertungsprogramme durchaus auch Erkenntnisse über ihre Leistungen und ihr Verhalten gewonnen werden können. Solchem steht der Datenschutz nicht a priori entgegen. Freilich darf ein Dienstherr solche Auswertungen nur zum Zweck der Personalverwaltung bzw. Personalwirtschaft vornehmen; zudem muss er den Grundsatz der Verhältnismäßigkeit beachten. Mit diesem Grundsatz wäre beispielsweise eine lückenlose, anlassunabhängige Überwachung von Bediensteten durch technische Maßnahmen nicht zu vereinbaren.

Das Landeskriminalamt geht, wie es mich wissen ließ, davon aus, dass die Auswertungsmöglichkeiten des Vorgangsbearbeitungs- und Vorgangsverwaltungssystems nicht der Leistungs- oder Verhaltenskontrolle von Polizeibeamten dienen, sondern dafür da sind, dass Kollegen und Vorgesetzte zur Sicherstellung eines reibungslosen Geschäftsbetriebs nach Vorgängen suchen können. Dies muss dann im Datenschutzkonzept des Vorgangsbearbeitungs- und Vorgangsverwaltungssystems so festgeschrieben werden.

Inzwischen erprobt das Landeskriminalamt das Vorgangsbearbeitungs- und Vorgangsverwaltungssystem in einer Pilotanwendung bei zwei Polizeidienststellen. Meinem Amt hat es mittlerweile die restlichen Datenschutzkonzepte für das Projekt übersandt, die es Anfang 2000 – wie zu hören ist – mit uns erörtern will.

2. Das Initiativprogramm „Jugendliche Intensivtäter“

„Mehr Härte gegen jugendliche Straftäter – Baden-Württemberg knüpft Netzwerk gegen jugendliche Intensivtäter“, so lauteten im Frühjahr 1999 die Schlagzeilen in der Presse. Polizei, Justiz, Schule, Jugendhilfe und Ausländerbehörden sollen – so war zu lesen – Koordinierungsrunden einrichten, in denen die Behörden die im Einzelfall vorliegenden Erkenntnisse austauschen und die für notwendig befundenen Maßnahmen abstim-

men. Wegen des angesprochenen Informationsaustauschs schaltete ich mich ein. Das Innenministerium bat mich daraufhin wegen der diffizilen Datenschutzfragen um Beratung.

Ausgangspunkt für das Initiativprogramm „Jugendliche Intensivtäter“ des Innenministeriums war eine umfangreiche Sonderauswertung der Personenauskunftsdatei durch das Landeskriminalamt nach Kindern und Jugendlichen, die mit mehr als zehn bzw. mehr als zwanzig Tatvorwürfen oder mit drei und mehr bzw. fünf und mehr Tatvorwürfen eines Gewaltdelikts, wofür bereits eine einfache Körperverletzung ausreichte, erfasst waren. Dabei war es auf rund 500 Kinder und Jugendliche gestoßen. Um sie sollen sich – so die Idee des Innenministeriums – auf Kreisebene Jugendämter, Staatsanwaltschaften, Polizeivollzugsdienst und – soweit es sich um ausländische Kinder und Jugendliche handelt – die Ausländerbehörden mit dem Ziel intensiv befassen, weiterem Fehlverhalten vorzubeugen. Dazu sollen die genannten Stellen und bei Bedarf auch die Schule in sog. Koordinierungsgesprächen jeweils im Einzelfall ihr Wissen über das Kind bzw. den Jugendlichen austauschen und gemeinsam abstimmen, welche Maßnahmen ergriffen werden sollen.

Keine Frage: Ohne Informationen kann ein solches Projekt nicht laufen. Genauso klar ist jedoch, dass die beteiligten Stellen nicht unbesehen alles, was sie über ein Kind oder einen Jugendlichen wissen, in die Koordinierungsgespräche einbringen dürfen, sondern strikt die jeweils für die Datenweitergabe einschlägigen Vorschriften berücksichtigen müssen. Anders gesagt: Jede Stelle, die an den Koordinierungsgesprächen teilnimmt, muss sich – ehe sie Informationen über ein Kind oder über einen Jugendlichen einbringt – im Klaren sein, dass sie damit personenbezogene Daten an alle anderen am Tisch sitzenden Stellen weitergibt. Deswegen kam es mir vor allem darauf an, dass Folgendes klargestellt wird:

– Bei den Koordinierungsgesprächen kommt den Jugendämtern eine herausgehobene Stellung zu, weil die Jugendhilfe zuvörderst ihre Sache und nicht diejenige von Polizei, Staatsanwaltschaften, Ausländerbehörden und Schulen ist. Zentraler Auftrag der Jugendhilfe ist nach dem Achten Buch des Sozialgesetzbuches die Förderung und Entwicklung junger Menschen und ihre Integration in die Gesellschaft mit Hilfe allgemeiner Förderungsangebote und Leistungen. Dieses Ziel müssen Jugendämter bei den Koordinierungsgesprächen stets bedenken. Sie dürfen deshalb Informationen über Kinder und Jugendliche nur insoweit in die Runde einbringen, als dies zur Erfüllung ihres Hilfeauftrags erforderlich ist und der Erfolg einer Jugendhilfeleistung dadurch nicht gefährdet wird. Im Zweifel hat die Effektivität der Jugendhilfeleistung Vorrang vor den Informationsbedürfnissen der anderen Stellen. Dies dient auch der Sache. Diskretion ist eine wesentliche Voraussetzung für den Erfolg der persönlichen Hilfen des Jugendamts.

– Auf die Einwilligung des Kindes bzw. des Jugendlichen und seiner Eltern lässt sich eine Unterrichtung der Koordinierungsrunde nicht stützen. Denn eine Einwilligung kann eine Datenverarbeitung nur so lange legitimieren, wie der Betroffene in Kenntnis seines Weigerungsrechts auch die Möglichkeit hat, selbst darüber zu befinden, ob und unter welchen Bedingungen die Informationen über ihn verwendet werden. Gerade dies ist aber bei einem Informationsaustausch in der Koordinierungsrunde nicht gewährleistet. Denn der Betroffene, der in die Weitergabe seiner Daten einwilligt, hat keine ernsthafte Chance, sich der daran anschließenden Verwendung seiner Daten zu entziehen oder sie zumindest in einer den eigenen Vorstellungen entsprechenden Weise zu steuern. Hinzu kommt: Öffentliche Stellen sind lediglich befugt, bestimmten in der Regel gesetzlich definierten Aufgaben nachzugehen. Sie dürfen dabei personenbezogene Daten verarbeiten, die zur Erüllung dieser Aufgaben erforderlich sind und brauchen mithin dafür nicht das Einverständnis der Betroffenen. Deshalb dürfen öffentliche Stellen bei der Datenverarbeitung nur in Ausnahmefällen, die hier nicht vorliegen, auf die Einwilligung zurückgreifen.

Das federführende Innenministerium hat meine Hinweise zu diesen und zu weiteren Punkten in der gemeinsamen Empfehlung berücksichtigt, die

es zusammen mit Landkreistag, Gemeindetag, Städtetag sowie Justiz- und Sozialministerium zur intensivierten Zusammenarbeit von Jugendämtern, Staatsanwaltschaften, Ausländerbehörden und Polizei im Bereich jugendlicher Intensivtäter Anfang August 1999 in Kraft gesetzt hat. Zugleich hat es den Polizeidienststellen aufgegeben, jährlich einen Bericht über ihre Erfahrungen vorzulegen.

3. Eine Probe aufs Exempel

Die Praxis polizeilicher Datenverarbeitung kann man nicht vom grünen Tisch aus, sondern nur kennen lernen, wenn man vor Ort der Sache auf den Grund geht. Deshalb und weil die Personenauskunftsdatei (PAD), die alle Polizeibeamten im Lande rund um die Uhr in Sekundenschnelle abfragen können, nach wie vor das Hauptinstrument der polizeilichen Informationsverarbeitung ist, hat sich mein Amt im Berichtsjahr bei drei Polizeidienststellen anhand einer nach dem Zufallsprinzip gezogenen Stichprobe die PAD-Speicherpraxis näher angesehen. Bei zwei der drei Polizeidienststellen hat es zugleich deren Lichtbildvorzeigekartei unter die Lupe genommen. Das Ergebnis sieht so aus:

3.1 Mit der Aufnahme in die Lichtbildvorzeigekartei zu schnell bei der Hand

Hat eine Polizeidirektion eine Person, die mutmaßlich oder tatsächlich eine Straftat begangen hat, erkennungsdienstlich (ed) behandelt und – wie vorgeschrieben – dem Bundeskriminalamt einen ed-Fotosatz zur Speicherung in der bundesweiten ed-Datei übersandt, steht sie – ehe sie die übrigen ed-Fotos zu ihrer Akte nimmt – vor der Frage: Aufnahme eines ed-Fotosatzes in die Lichtbildvorzeigekartei Ja oder Nein. Dabei geht es keineswegs um eine Belanglosigkeit. Um dies zu verstehen muss man wissen: Kommt die Polizei bei ihren Ermittlungen wegen einer Straftat nicht weiter und glaubt ein Zeuge den geflüchteten Täter wiederzuerkennen, legt ihm die Polizei ed-Fotos aus der Lichtbildvorzeigekartei vor. Die abgebildeten Personen sind so dem Risiko ausgesetzt, von den Zeugen auch dann erkannt zu werden, wenn sie mit dem Ermittlungsverfahren, in dem die Lichtbildvorlage erfolgt, gar nichts zu tun haben. Wegen des damit einhergehenden gravierenden Eingriffs in das Persönlichkeitsrecht, darf die Polizei unter Beachtung des Grundsatzes der Verhältnismäßigkeit ed-Fotos nur von solchen Personen in die Lichtbildvorzeigekartei aufnehmen, die verurteilt worden oder einer Straftat dringend verdächtig sind und bei denen nach ihrem bisherigen Verhalten Wiederholungsgefahr besteht. Daran haben sich die beiden Polizeidienststellen bei der Aufnahme von ed-Fotosätzen in ihre Lichtbildvorzeigekartei nicht immer gehalten:

3.1.1 Kein dringender Tatverdacht

Dringender Tatverdacht setzt einen stärkeren Verdachtsgrad voraus, als es für die Einleitung eines Ermittlungsverfahrens erforderlich ist. Für Letzteres genügt schon der einfache Anfangsverdacht. Ein solcher ist bereits zu bejahen, wenn es auf Grund konkreter Tatsachen nach kriminalistischen Erfahrungen einen Anhalt dafür gibt, dass eine verfolgbare Straftat vorliegt. Er ist dem Grad nach auch intensiver als der hinreichende Tatverdacht, von dessen Vorliegen die Strafprozeßordnung (StPO) die Eröffnung eines Strafverfahrens vor Gericht abhängig macht und bei dessen Fehlen die Staatsanwaltschaft das Ermittlungsverfahren nach § 170 Abs. 2 StPO einzustellen hat. Dringender Tatverdacht liegt nur vor, wenn nach dem bisherigen Ermittlungsergebnis eine große Wahrscheinlichkeit dafür besteht, dass der Beschuldigte die ihm zur Last gelegte Straftat tatsächlich begangen hat. Daran fehlte es mitunter wie allein schon folgende Fälle zeigen:

– Das erfolglose Haustürgeschäft

Eine Frau, die Sozialhilfe bezog und 1996 einen Teppich für 350 DM per Haustürgeschäft verkaufen wollte, geriet in die

Lichtbildvorzeigekartei, obwohl die Staatsanwaltschaft das Ermittlungsverfahren wegen Betrugs zulasten des Sozialamts umgehend mangels hinreichenden Tatverdachts mit der Begründung eingestellt hatte, dass ein Betrug schon deshalb ausscheidet, weil die Frau gar keinen Erlös erzielt hatte, den sie dem Sozialamt gegenüber hätte angeben müssen, und es reine Spekulation ist, wie sie sich verhalten hätte, wenn sie tatsächlich einen Erlös aus dem Teppichverkauf erwirtschaftet hätte. Auf reine Vermutungen lässt sich aber ein dringender Tatverdacht schlechterdings nicht stützen.

– Eine vertrauliche Anzeige

Ein Mann, der 1993 zusammen mit Komplizen einen Automaten aufgebrochen und aus der Kasse das Bargeld entnommen haben soll, war in der Lichtbildvorzeigekartei, obwohl die Staatsanwaltschaft das Ermittlungsverfahren mangels hinreichenden Tatverdachts eingestellt hatte, weil es keine objektiven Beweise gab und alles auf der Anschuldigung eines Zeugen beruhte, dem sie Vertraulichkeit zugesichert hatte. Bleiben die Anschuldigungen so im Dunkeln, kann von einem dringenden Tatverdacht keine Rede sein.

– In Notwehr gehandelt?

Ein Mann, der 1997 einen anderen Mann mit einem Messerstich in den Oberschenkel verletzt hatte, befand sich in der Lichtbildvorzeigekartei, obwohl die Staatsanwaltschaft das Ermittlungsverfahren wegen gefährlicher Körperverletzung mangels hinreichenden Tatverdachts eingestellt hatte, weil nach dem Ergebnis der Ermittlungen zu seinen Gunsten davon auszugehen war, dass er in Notwehr gehandelt hatte. Fehlt es bereits an einem hinreichenden Tatverdacht, mangelt es erst recht an einem dringenden Tatverdacht.

3.1.2 Erfassung in der Lichtbildvorzeigekartei nicht verhältnismäßig

Selbst wenn jemand wegen einer Straftat verurteilt worden ist, darf die Polizei seine ed-Fotos nicht automatisch in die Lichtbildvorzeigekartei einstellen. Vielmehr muss sie auch dann den Grundsatz der Verhältnismäßigkeit beachten. Dieser Grundsatz verlangt, dass die Aufnahme von ed-Fotos in die Lichtbildvorzeigekartei unterbleibt, wenn die berechtigten Belange des Verurteilten das öffentliche Interesse an der Aufklärung möglicher künftiger Straftaten überwiegen. Deshalb darf die Polizei nur bei Straftaten von Gewicht und nicht schon bei Fällen von geringer Bedeutung ed-Fotos in die Lichtbildvorzeigekartei einstellen. Daran hielten sich die Polizeidienststellen nicht immer. Beispielsweise kam eine Frau in die Lichtbildvorzeigekartei, weil sie gemeinsam mit ihrem Mann in einem Kaufhaus Waren im Wert von 164,05 DM ohne zu bezahlen eingesteckt und das Amtsgericht sie mit einer Geldstrafe in Höhe von 15 Tagessätzen zu je 20 DM belegt hatte. Dies allein rechtfertigte aber die Aufnahme der Frau in die Lichtbildvorzeigekartei nicht. Denn bei dem Ladendiebstahl handelte es sich wegen der geringen Folgen und wegen des geringen Unrechtsgehalts der Tat um einen Fall von geringer Bedeutung, wie auch die am untersten Rand des Strafrahmens angesetzte Geldstrafe belegt. Entscheidend zu Gunsten der Frau fällt ins Gewicht, dass sie bis zu dem Ladendiebstahl polizeilich noch nie in Erscheinung getreten war und dass es keinerlei Anhaltspunkte für die Annahme gab, die Polizei könnte es künftig mit ihr womöglich immer wieder als Ladendiebin zu tun bekommen und müsse deshalb auf die Lichtbildvorzeigekartei zurückgreifen können.

Diese Beispiele zeigen: Die beiden Polizeidienststellen müssen bei der Aufnahme von ed-Fotos in die Lichtbildvorzeigekartei mehr Augenmaß an den Tag legen. Zugleich müssen sie sicher-

stellen, dass die Stelle, die die Lichtbildvorzeigekartei führt, vom Ausgang des Ermittlungsverfahrens erfährt. Nur wenn dies gewährleistet ist, kann sie eine Aufnahme in die Lichtbildvorzeigekartei revidieren, wenn sich aus der Mitteilung der Staatsanwaltschaft über den Ausgang des Ermittlungsverfahrens ergibt, dass es an einem dringenden Tatverdacht fehlt.

3.2 PAD-Speicherfristen zu lange

Praktisch wie ein roter Faden durchzieht die Neigung der Polizei zur Vergabe unangemessen langer Speicherfristen in der PAD die Tätigkeitsberichte meines Amtes. Ich erinnere nur an die ausufernde Vergabe der zehnjährigen PAD-Maximalspeicherfrist (vgl. 17. Tätigkeitsbericht, Landtags-Drucksache 12/750, S. 22 ff.) und die zu lange Speicherung von mutmaßlich oder tatsächlich begangenen Rauschgiftdelikten (vgl. 18 Tätigkeitsbericht, Landtags-Drucksache 12/2242, S. 36). Auch diesmal mussten wir in einer ganzen Reihe von Fällen zu lange PAD-Speicherfristen kritisieren. Dabei hatten die Polizeidienststellen aus dem Auge verloren, dass sie Erwachsene und Jugendliche wegen eines Falles von geringer Bedeutung – dazu zählen insbesondere Beleidigung, Verleumdung, Hausfriedensbruch, Nötigung, einfache Körperverletzung sowie Diebstahl, Unterschlagung, Betrug und Sachbeschädigung bis zu einer Schadenshöhe von 500 DM – allenfalls für drei Jahre und wegen sonstiger Delikte für fünf Jahre in der PAD registrieren dürfen. Abweichend davon dürfen sie Erwachsene wegen eines mutmaßlich oder tatsächlich begangenen Verbrechens, eines in § 100 a StPO genannten Vergehens oder wegen einer anderen überregional bedeutsamen Straftat mit der zehnjährigen PAD-Maximalspeicherfrist registrieren. Damit nahmen es die Polizeidienststellen nicht immer genau, wie schon folgende Beispiele zeigen:

– Drei CDs

Ein 17-jähriger Schüler war wegen des Tatvorwurfs eines Ladendiebstahls für fünf Jahre bis 2003 in der PAD erfasst, weil er in einem Geschäft drei CDs im Gesamtwert von 80 DM in seine Jackentasche eingesteckt hatte und dabei von einer Angestellten beobachtet worden war. Ein solcher Tatvorwurf rechtfertigt eine fünfjährige Speicherfrist nicht. Fälle eines Ladendiebstahls bis zu einer Schadensumme von 500 DM sind – so steht es in der Durchführungsverordnung zum Polizeigesetz – Fälle von geringer Bedeutung, die die Polizei allenfalls für drei Jahre in der PAD registrieren darf.

– Drei Fläschchen Parfum

Ein 22-jähriger Soldat war wegen des Tatvorwurfs eines Ladendiebstahls für fünf Jahre bis Anfang 2002 in der PAD erfasst, weil er in einem Drogeriemarkt drei Fläschchen Parfum im Gesamtwert von 87 DM eingesteckt und ohne zu bezahlen das Geschäft verlassen hatte. Auch hier handelt es sich um einen Fall von geringer Bedeutung, dem mit einer allenfalls dreijährigen PAD-Speicherfrist genüge getan ist, zumal der junge Soldat den Parfum-Diebstahl unumwunden eingeräumt und die drei Fläschchen Parfum wieder herausgerückt hatte, als ihn eine Mitarbeiterin des Drogeriemarkts auf den Diebstahl ansprach.

– Eine Jacke

Ein 30-jähriger Asylbewerber war für fünf Jahre bis 1. März 2003 wegen des Tatvorwurfs eines Ladendiebstahls in der PAD erfasst, weil er in einem Einkaufsmarkt eine Jacke im Wert von 29 DM entwendet haben soll. Auch in diesem Fall ist eine allenfalls dreijährige PAD-Speicherfrist vorschriftsgemäß, weil es sich bei dem dem Asylbewerber zur Last gelegten Ladendiebstahl um einen Fall von geringer Bedeutung gehandelt hatte und weil die Polizei solche Fälle nach der Durchführungsverordnung zum Polizeigesetz nur so lange in der PAD registrieren darf. Daran vermag der Umstand, dass seine Frau in demselben Einkaufsmarkt einen Kerzenständer

und eine Packung Käse entwendet haben soll, nichts zu ändern. Denn selbst wenn der Asylbewerber sich den Diebstahl seiner Frau zurechnen lassen müsste, handelt es sich wegen der geringen Folgen und wegen des geringen Unrechtsgehalts um ein Bagatelldelikt, für das die einschlägigen Vorschriften eine allenfalls dreijährige PAD-Speicherung vorsehen.

– Die Eheleute

Eine Frau war für zehn Jahre bis 1. September 2001 mit dem Tatvorwurf eines Ladendiebstahls in der PAD erfasst, weil sie 1991 mit ihrem Mann in einem Kaufhaus Waren im Wert von 164 DM ohne zu bezahlen mitgenommen hatte. Dieser Tatvorwurf rechtfertigt eine zehnjährige PAD-Speicherfrist schlechterdings nicht. Bei dem Ladendiebstahl handelt es sich keineswegs um eine schwere Straftat, sondern vielmehr um ein Delikt, das die Polizei seit jeher für allenfalls drei Jahre in der PAD erfassen darf. Die Tat hat sich auch nicht durch einen von normalen Fällen eines Ladendiebstahls abweichenden Modus Operandi ausgezeichnet. Irgendwelche Anhaltspunkte, dass die Frau den Diebstahl aus krimineller Neigung oder bandenmäßig zusammen mit ihrem Mann begangen hat, gibt es nicht wie auch die Tatsache belegt, dass die Frau wegen des Ladendiebstahls von 1991 zum ersten und einzigen Mal in der PAD erfasst ist.

– Eine anonyme Anzeige

Ein 40-jähriger Mann indischer Nationalität war für zehn Jahre bis 1. Januar 2007 wegen des Tatvorwurfs des Einschleusens eines Ausländers in der PAD erfasst, weil er einem anonymen, angeblich aus Kalifornien geführten Anruf zufolge einen Landsmann für 22 000 Dollar mit falschem Pass in die USA eingeschleust haben soll. Auch hier war die zehnjährige Maximalspeicherfrist keinesfalls gerechtfertigt. Bei Licht besehen beruht die PAD-Speicherung nämlich allein auf einem anonymen Anruf, für dessen Richtigkeit sich im Zuge der intensiven polizeilichen Ermittlungen keinerlei Anhaltspunkte ergeben haben. Allein ein solcher Anruf kann aber nicht dazu führen, dass die Polizei jemanden in der PAD erfasst und schon gleich gar nicht mit der zehnjährigen Maximalspeicherfrist.

3.3 Keine Konsequenzen aus dem Ausgang des Ermittlungsverfahrens gezogen

Die Polizei ist verpflichtet, jeweils nach Abschluss des Ermittlungsverfahrens anhand der Entscheidung der Staatsanwaltschaft oder des Gerichts zu prüfen, ob sie den in die PAD eingespeicherten Tatvorwurf löschen muss. Um dies zu ermöglichen, vereinbarten Innen- und Justizministerium im Jahr 1981 einen Mitteilungsdienst zwischen Staatsanwaltschaft und Polizei. Inzwischen ist die Benachrichtigung der Polizei über den Ausgang des Verfahrens durch das Justizmitteilungsgesetz von 1997 geregelt. Um der Polizei die Prüfung zu erleichtern, ob sie auf Grund der Benachrichtigung der Staatsanwaltschaft den eingespeicherten Tatvorwurf löschen muss, hat das Innenministerium in seiner Verwaltungsvorschrift über Einzelfalllöschungen in der Personenauskunftsdatei von 1981 detailliert geregelt, in welchen Fällen die gespeicherten Daten zu löschen sind und dabei u. a. bestimmt, dass so zu verfahren ist, wenn die gespeicherten Daten Verhaltensweisen betreffen, die nach der Mitteilung über den Ausgang des Verfahrens nicht strafbar sind. Diese Regelungen waren bei einer der kontrollierten Polizeidienststellen offenbar in Vergessenheit geraten. Nur so kann ich mir erklären, dass sie in Fällen wie dem folgenden, bei dem es sich keineswegs um einen Einzelfall handelt, nach dem Eingang der Mitteilung über den Ausgang des Verfahrens die PAD-Löschtaste nicht gedrückt hat. Die Polizeidienststelle hatte einen jungen Mann aus dem Irak für fünf Jahre bis 1. August 2002 in der PAD wegen des Tatvorwurfs eines Vergehens gegen das Ausländergesetz erfasst, weil er am 30. Juli 1997 unerlaubt in die Bundesrepublik eingereist sein soll. Dabei beließ es die Polizeidienststelle, ob-

wohl die Staatsanwaltschaft das Ermittlungsverfahren umgehend eingestellt und zur Begründung ausgeführt hatte, dass „der Beschuldigte nach der Einreise in die Bundesrepublik unverzüglich einen Asylantrag gestellt hat und aus diesem Grund nach § 92 Abs. 4 des Ausländergesetzes i. V. m. Artikel 31 der Genfer Flüchtlingskonvention nicht strafbar ist“.

3.4 Datenspeicherungen über Opfer in der PAD

Dass die Polizei in großem Stil auch Daten über Opfer in der PAD speichert, war mir bisher neu. Doch darauf stießen wir bei unseren Kontrollen. Es zeigte sich, dass die Polizeidienststellen in einer Vielzahl von PAD-Datensätzen über Personen, die mutmaßlich oder tatsächlich eine Straftat begangen haben, jeweils auch den Vornamen und den Familiennamen, das Geburtsdatum und die Adresse des Opfers der registrierten Straftat suchbar gespeichert haben. Deshalb bekommt jeder Polizeibeamte im Lande, der die PAD danach abfragt, am Bildschirm immer auch angezeigt, wer wann Opfer welcher Straftat geworden ist. Die Angaben über die Opfer bleiben so lange im PAD-Datensatz des mutmaßlichen oder tatsächlichen Straftäters gespeichert, bis die Polizei den PAD-Datensatz insgesamt löscht. Das kann je nach Schwere des gespeicherten Tatvorwurfs drei, fünf oder zehn Jahre und vielfach sogar noch länger dauern. Wozu dies führt, sei an einigen Beispielen illustriert:

– Ein 11-jähriges Mädchen war mit Namen, Geburtsdatum und Anschrift fünf Jahre bis 1. Juli 2003 als Opfer eines sexuellen Missbrauchs im PAD-Datensatz eines Mannes erfasst, der es im Juni 1998 missbraucht haben soll.

– Vier junge Burschen waren mit Namen, Geburtsdatum und Anschrift für elf Jahre bis 1. Dezember 2008 als Opfer einer Körperverletzung im PAD-Datensatz eines Mannes erfasst, der sie zusammen mit seinen Freunden nach einem Diskothekenbesuch 1997 verprügelt haben soll.

– Eine Frau war mit Namen, Geburtsdatum und Adresse für zehn Jahre bis 1. April 2000 als Opfer einer Freiheitsberaubung im PAD-Datensatz eines Mannes erfasst, der sie Anfang 1990 in ihrer Wohnung bedroht und gegen ihren Willen festgehalten haben soll.

– Ein Gastwirt war mit Namen, Geburtsdatum und Anschrift für mehr als dreizehn Jahre bis 1. Dezember 2000 als Opfer eines Diebstahls im PAD-Datensatz eines Mannes erfasst, der im Juli 1987 in seine Gaststätte eingebrochen sein und Bargeld und Zigaretten entwendet haben soll.

Diese PAD-Speicherpraxis steht mit § 38 Abs. 4 des Polizeigesetzes (PolG) in mehrfacher Hinsicht nicht im Einklang. Zum einen speichern die Polizeidienststellen Daten über Opfer entgegen dieser Vorschrift keineswegs nur, wenn gegen das Opfer eine Straftat von erheblicher Bedeutung verübt worden ist, sondern auch bei Straftaten, die diese Schwelle nicht erreichen. Zum anderen ist – was § 38 Abs. 4 PolG aber verlangt – nicht gewährleistet, dass die über Opfer gespeicherten Daten nur genutzt werden können, soweit dies zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist. Zum Dritten wird die in § 38 Abs. 4 PolG vorgeschriebene zweijährige Frist für die Speicherung von Daten über Opfer nicht eingehalten, weil die PAD so programmiert ist, dass die Dauer der Speicherung von Daten über Opfer an die drei-, fünf-, zehnjährige oder noch längere Speicherdauer des PAD-Datensatzes des mutmaßlichen oder tatsächlichen Straftäters untrennbar gekoppelt ist und die Daten über Opfer demzufolge erst nach Ablauf dieser viel längeren PAD-Speicherfristen gelöscht werden.

Weil die Speicherung über Opfer in der PAD keineswegs eine Spezialität der kontrollierten Polizeidienststellen ist, sondern einer weit verbreiteten Praxis der Polizei entspricht, habe ich die Sache an das Innenministerium herangetragen. Dabei habe ich es zugleich darauf

hingewiesen, dass eine Speicherung von Daten über Opfer in der PAD auch mit deren Einwilligung nicht in Frage kommen kann, weil dies eine unzulässige Umgehung von § 38 Abs. 4 PolG wäre.

3.5 Verlängerung von PAD-Speicherfristen

Nach Ablauf der drei-, fünf- oder zehnjährigen PAD-Speicherfrist muss die Polizei die Vorgänge in der PAD löschen. Nur ausnahmsweise darf sie die Speicherfrist um drei Jahre verlängern. Bei unseren Kontrollen trafen wir auf folgende Verlängerungspraxis: Steht ein PAD-Datensatz eines Ausländers nach Ablauf der Speicherfrist zur Löschung heran, schaut die Polizei in der INPOL-Fahndungsdatei nach, ob der Ausländer auf Veranlassung einer Ausländerbehörde zur Festnahme ausgeschrieben ist, weil seine Ausweisung und Abschiebung verfügt worden war oder weil nach erfolgter Abschiebung eine Wiedereinreise verhindert werden soll. Besteht eine solche Fahndungsnotierung, verlängern Polizeidienststellen die PAD-Speicherung über die mutmaßlich oder tatsächlich begangene Straftat bis zum Ablauf der zehnjährigen Speicherfrist für die Fahndungsnotierung. Wohin das führt, sei nur an folgenden beiden Fällen exemplarisch verdeutlicht:

– Eine Polizeidienststelle erfasste im Jahr 1990 einen Mann aus Rumänien für fünf Jahre bis 1995 wegen des Tatvorwurfs eines Vergehens gegen das Ausländergesetz in der PAD, weil er unerlaubt in die Bundesrepublik eingereist sein soll. Nach Ablauf der fünfjährigen Speicherfrist verlängerte die Polizeidienststelle die PAD-Speicherfrist gleich um sechs Jahre, weil inzwischen eine Ausländerbehörde nach der im Oktober 1990 erfolgten Abschiebung den Mann zur Sicherung des Verbots der Wiedereinreise bis Anfang 2001 in INPOL zur Fahndung ausgeschrieben hatte.

– Ein anderer Mann aus Rumänien war wegen des Tatvorwurfs zweier Ladendiebstähle mittlerweile zehn Jahre in der PAD gespeichert. Eine Polizeidienststelle hatte ihn wegen dieses Tatvorwurfs 1991 mit einer fünfjährigen Speicherfrist in der PAD erfasst, weil er als Asylbewerber aus einem Sammelcontainer alte Kleider im Wert von 10 DM und in einem Warenhaus Gegenstände im Wert von 151 DM entwendet haben soll. Obwohl für solche Delikte allenfalls eine dreijährige PAD-Speicherfrist angemessen gewesen wäre, löschte die Polizeidienststelle die Tatvorwürfe in der PAD nach Ablauf der fünfjährigen Speicherfrist nicht, sondern verlängerte die PAD-Speicherfrist um drei Jahre bis 1999 und 1999 nochmals für zwei Jahre bis 2001, weil eine Ausländerbehörde nach der 1994 erfolgten Abschiebung den Mann zur Sicherung des Verbots der Wiedereinreise für zehn Jahre bis 2004 in INPOL zur Fahndung ausgeschrieben hatte.

Diese Verlängerungspraxis muss die Polizei überdenken. Denn allein die Tatsache, dass ein Ausländer auf Veranlassung der Ausländerbehörde in INPOL zur Fahndung ausgeschrieben ist, weil er ausgewiesen oder abgeschoben worden ist, rechtfertigt keine automatische Verlängerung der PAD-Speicherfrist. Die von Ausländerbehörden veranlassten Fahndungsausschreibungen von Ausländern erfolgen nämlich weder zur vorbeugenden Bekämpfung von Straftaten noch zur Strafverfolgung noch zur Abwehr konkreter Gefahr, sondern vielmehr zur Durchsetzung aufenthaltsbeendender Maßnahmen oder zur Sicherung des Verbots der Wiedereinreise. Eine Verlängerung der PAD-Speicherfristen kann deshalb nur in Betracht kommen, wenn der der Ausschreibung zugrunde liegende Vorgang eine weitere Speicherung der mutmaßlich oder tatsächlich begangenen Straftat des Ausländers zu Zwecken der vorbeugenden Bekämpfung von Straftaten oder der Abwehr konkreter Gefahr dringend erforderlich macht. Solche Umstände haben die Polizeidienststellen in der Begründung ihrer Verlängerungsentscheidung nicht angeführt.

Meine Bewertung dieser und weiterer Einzelfälle und der Grundsatzprobleme bei der Registrierung von Opfern in der PAD und bei der Verlänge-

rung von PAD-Speicherfristen habe ich vor kurzem an die Polizeidienststellen und das Innenministerium herangetragen. Das Innenministerium ließ mir inzwischen eine erste Äußerung zukommen: Es bekräftigte, dass eine Aufnahme in die Lichtbildvorzeigekartei derzeit nur bei dringendem Tatverdacht in Frage kommt, eröffnete aber zugleich die Debatte, ob die „Schwelle“ dringender Tatverdacht noch zeitgemäß ist. Datenspeicherungen in der PAD wegen des Tatvorwurfs eines Vergehens gegen das Ausländergesetz werden im Falle einer unter Hinweis auf Artikel 31 der Genfer Flüchtlingskonvention erfolgten Einstellung des Ermittlungsverfahrens gelöscht; bei „Grenzanzeigen“ von Asylsuchenden wird künftig auf eine Speicherung in der PAD verzichtet. D’accord geht das Innenministerium mit mir, dass die Speicherung von Daten über Opfer in der PAD regelmäßig zur polizeilichen Aufgabenerfüllung nicht erforderlich ist und dass eine Verlängerung einer PAD-Speicherfrist durch eine INPOL-Ausschreibung nur dann in Frage kommt, wenn die Ausschreibung in einem inneren Verhältnis zu den zur vorbeugenden Bekämpfung von Straftaten in der PAD gespeicherten Daten steht.

5. Teil: Andere Bereiche

1. Abschnitt: Kommunalwesen

1. Der CDU-Rentenbrief

Als um die Jahresmitte 1999 die Medien ausführlich berichteten, der Bundesvorsitzende der Christlich-Demokratischen Union Deutschlands (CDU) wolle sich mit einem Brief, der sich kritisch mit der Rentenpolitik der Bundesregierung auseinander setzt, an alle Rentner wenden, häuften sich bei meinem Amt Anfragen von Bürgern und verunsicherten Meldebehörden, ob denn etwa die Adressdaten aus den Melderegistern für diesen Zweck zur Verfügung gestellt werden dürfen. Die Frage war deshalb nicht einfach zu beantworten, weil in Baden-Württemberg am 24. Oktober 1999 Kommunalwahlen stattfanden und das Meldegesetz den Meldebehörden die Befugnis einräumt, im Zusammenhang mit solchen Wahlen in den sechs vorangehenden Monaten Adressdaten von nach dem Lebensalter ausgesuchten Gruppen von Wahlberechtigten an Parteien und andere Wählergruppen herauszugeben. Bei rein formaler Betrachtungsweise könnte man deshalb durchaus der Meinung sein, diese Regelung im Meldegesetz erlaube die Herausgabe von Namen und Anschriften von Senioren zur Adressierung des „Rentenbriefes“. Damit würde man freilich ihrem Bedeutungsgehalt nicht gerecht. Im Einzelnen ist dazu zu sagen:

Die Regelung des Meldegesetzes über die Erteilung von Gruppenauskünften an Parteien soll dem Informationsbedürfnis der politischen Parteien und Wählergruppen im Vorfeld von Wahlen Rechnung tragen. Ob damit allein schon von einem überwiegenden Allgemeininteresse, das den mit einer Herausgabe der Adressdaten verbundenen Eingriff in das Recht auf informationelle Selbstbestimmung legitimiert, gesprochen werden kann, ist auch unter Berücksichtigung des den Parteien durch Art. 21 GG eingeräumten Sonderstatus fraglich. Diese haben schließlich in der modernen Medienwelt viele andere Möglichkeiten, den Wahlberechtigten auf ihr Wahlverhalten abzielende Informationen zukommen zu lassen. Wohl auch aus diesem Grund räumt das Meldegesetz deshalb jedem die Möglichkeit ein, der Weitergabe seiner Adresse an Parteien und Wählergruppen zu widersprechen. Damit lassen sich die Zweifel an der Verfassungsmäßigkeit der Auskunftsregelung freilich nicht ausräumen, und zwar nicht zuletzt deshalb, weil die Information über das Widerspruchsrecht die Betroffenen häufig nicht erreicht. Das zeigen die vielen Eingaben, die Datenschutzbeauftragte nach dem Versand von adressierter Wahlwerbung erhalten. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 5./6. Oktober 1998 empfohlen, künftig für solche Fälle die Einwilligungslösung vorzusehen. Solange es aber bei der eingangs geschilderten Regelung bleibt, muss diese aus verfassungsrechtlichen Gründen eng ausgelegt werden. Das bedeutet: Sie kann die Herausgabe von Adressdaten an Parteien und Wählergruppen im Zusammenhang mit Wahlen nur rechtfertigen, wenn es darum geht, Wahlberech-

tigten Informationen zugänglich zu machen, die in einem unmittelbaren sachlichen Zusammenhang mit der Wahl stehen und gezielt auf die Wahlentscheidung Einfluss nehmen wollen. Dafür spricht auch, dass die Meldegesetze die Gruppenauskunft nicht nur zeitlich an Wahltermine binden, sondern ausdrücklich verlangen, dass die Auskunft im Zusammenhang mit Wahlen stehen muss.

Diese Rechtslage ließ eine Herausgabe von Adressdaten von Senioren zum Versand des „Rentenbriefes“ nicht zu. Der „Rentenbrief“ war Teil einer bundesweiten Aktion. Er sollte an alle Rentner im Bundesgebiet ohne Rücksicht darauf versandt werden, ob in dem Bundesland Landtags- oder Kommunalwahlen stattfinden, und befasste sich zudem ausschließlich mit der Rentenpolitik der Bundesregierung und nicht mit einer Angelegenheit, auf die die zu wählenden Kommunalparlamente Einfluss nehmen können. Dass die Rentenbrief-Aktion zeitlich in das Vorfeld der Kommunalwahlen in Baden-Württemberg fiel, war reiner Zufall. Ansonsten hatte sie in der Sache mit diesen Wahlen nichts zu tun.

Ich habe die Städte und Gemeinden in einer Pressemitteilung auf diese Rechtslage hingewiesen und sie aufgefordert, von der Herausgabe von Adressdaten für den Versand der „Rentenbriefe“ abzusehen, und hoffe, dass möglichst viele von ihnen dem gefolgt sind.

2. Die Ertüchtigung des Melderegisters

In die Einwohnermelderegister der Städte und Gemeinden können sich, vor allem weil manche Zeitgenossen es mit ihrer Meldepflicht nicht so genau nehmen, im Laufe der Zeit Fehler einschleichen, sei es dass Einwohner gar nicht erfasst sind, sei es dass weggezogene Personen noch als aktuelle Einwohner geführt werden. Ließen sich in früheren Zeiten solche Fehler hin und wieder dadurch ausmerzen, dass die Ergebnisse der Volkszählungen – gewissermaßen die Inventur vor Ort – mit den Melderegistern abgeglichen und zu deren Bereinigung verwendet wurden, so hat bekanntlich das Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 einer solchen Verwendung von Statistikdaten einen Riegel vorgeschoben. Künftig soll sogar – gerade umgekehrt – die Auswertung der Melderegister an die Stelle einer herkömmlichen Volkszählung treten. Weil aber diese Methode nur dann brauchbare Ergebnisse liefern kann, wenn die Melderegister möglichst auf dem Laufenden sind, sinnen die Innenressorts seit längerem darüber nach, wie die Qualität der Melderegister verbessert werden kann.

In einem ersten Schritt gab das Innenministerium den Städten und Gemeinden mit einem bundesweit abgestimmten Erlass Hinweise auf Maßnahmen, die dazu beitragen können. Beispielsweise sollen die Stellen der Gemeindeverwaltung, die von ihrem Einwohnermeldeamt zur Erfüllung ihrer Aufgabe Einwohnerdaten aus dem Melderegister erhalten haben, das Einwohnermeldeamt unterrichten, wenn sie Anhaltspunkte für die Unrichtigkeit der gelieferten Daten haben. Eine solche Rückmeldung erscheint jedenfalls dann vertretbar, wenn die empfangende Stelle auf richtige Meldedaten angewiesen ist und eigene Ermittlungen nicht möglich sind oder keinen Erfolg versprechen; dann liegt die Unterrichtung des Einwohnermeldeamts zugleich im Interesse der empfangenden Stelle. Deshalb habe ich dieser Erlassregelung nicht widersprochen.

Verbleibende Zweifel, ob das geltende Datenschutzrecht solche Datenübermittlungen in jedem Fall zulässt, sollen in einem zweiten Schritt durch Schaffung einer ausdrücklichen Rechtsgrundlage im Melderecht ausgeräumt werden. Ein Referentenentwurf zur Änderung des Melderechtsrahmengesetzes sieht unter anderem vor, dass alle Behörden, denen regelmäßig Daten aus dem Melderegister übermittelt werden, das Einwohnermeldeamt unterrichten müssen, wenn ihnen konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit übermittelter Meldedaten vorliegen und schutzwürdige Interessen der Betroffenen nicht überwiegen. Ist gegen eine solche Regelung auch im Grundsatz nichts einzuwenden, so begegnet doch Bedenken, dass nach dem Gesetzentwurf das Steuergeheimnis, das Sozialgeheimnis und vergleichbare Geheimhaltungspflichten der Unterrichtung nicht entgegenstehen sollen. Eine Durchbrechung die-

ser besonderen Geheimnisse lässt sich allein mit dem Zweck, die Qualität der Melderegister zu verbessern, schwerlich rechtfertigen. Deshalb bat ich das Innenministerium, sich für die Streichung dieser Durchbrechungsklausel einzusetzen.

An einem validen Melderegister sind aber auch die Städte und Gemeinden selbst interessiert. Sie unternehmen deshalb alles Mögliche, um diese für die gesamte öffentliche Verwaltung so wichtige Datensammlung auf dem Laufenden zu halten. Mit einigen der dazu getroffenen Maßnahmen hatten wir uns zu befassen:

– In einem Stadtkreis, in dem die Abfallbeseitigungsgebühren nach Haushaltsgröße gestaffelt erhoben werden, erhält die für die Gebührenberechnung zuständige Stelle die erforderlichen Einwohnerdaten zulässigerweise aus dem Melderegister. Sie erfährt darüber hinaus auch auf anderem Wege immer wieder von Veränderungen in der Zusammensetzung eines Haushalts, die im Melderegister noch nicht registriert sind, beispielsweise wenn ein Haushalt nachweist, dass ein im Gebührenbescheid noch berücksichtigtes Haushaltsmitglied ausgezogen ist. Darf die Müllgebührenstelle das Einwohnermeldeamt von solchen ihm bekannt gewordenen Änderungen unterrichten? Der nicht ganz eindeutige Wortlaut der einschlägigen Bestimmungen des Landesdatenschutzgesetzes steht wohl nicht zwingend entgegen. Da die Müllgebührenstelle die für sie bedeutsamen Fakten bereits kennt, ist sie für ihre Aufgabe nicht auf weitere Ermittlungen des Einwohnermeldeamts angewiesen und hat kein eigenes Interesse an der Berichtigung des Melderegisters. Besser wäre es deshalb, wenn die Müllgebührenstelle die Bürger an ihre Meldepflicht gegenüber dem Einwohnermeldeamt erinnern würde, anstatt dieses über den Kopf der Bürger hinweg zu informieren.

– In einer Kreisstadt hatte sich im Lauf der Jahre folgende Zusammenarbeit zwischen Stadtwerken und Einwohnermeldeamt entwickelt: Jedes Mal, wenn sich ein neuer Kunde bei den Stadtwerken für den Bezug von Strom und Wasser anmeldete, unterrichteten die Stadtwerke das Einwohnermeldeamt. Dieses überwachte dann anhand dieser Mitteilungen, ob sich für die Wohnung fristgerecht auch ein Einwohner bei ihm anmeldet, und fasste notfalls nach angemessener Frist nach. War diese Methode auch wirkungsvoll, so ging sie doch über das hinaus, was das Landesdatenschutzgesetz zulässt. Für regelmäßige Kontrollmitteilungen dieser Art ohne jegliche Anhaltspunkte dafür, dass die Neukunden der Stadtwerke ihrer Meldepflicht beim Einwohnermeldeamt nicht nachkommen werden, gibt es keine Rechtsgrundlage. Wenn schon die Stadtwerke die Erfüllung der Meldepflicht durch ihre Neukunden fördern wollen, so können sie diese ja an die Meldepflicht erinnern und gar gleich Meldevordrucke für sie bereithalten. Nach Hinweis auf die Rechtslage stellte die Stadt ihre bisherige Praxis ein.

– Auf einen ähnlichen Dreh war man in einer Kleinstadt gekommen: Meldete dort ein Einwohner das Städtische Amtsblatt bei der Vertriebsstelle im Rathaus an eine neue Anschrift innerhalb der Stadt um, so erfuhr dies postwendend auch das Einwohnermeldeamt; dieses wachte mit Argusaugen darüber, dass der Amtsblattummeldung auch eine Ummeldung beim Einwohnermeldeamt folgt. Auch hier musste ich der Stadt sagen: So nicht. Die Amtsblattverwaltung darf nicht einfach davon ausgehen, ein Einwohner, der das Amtsblatt an eine andere Adresse umbestellt, werde seiner Meldepflicht nach dem Meldegesetz nicht fristgerecht nachkommen.

– Über das Ziel hinaus schoss auch eine andere Kreisstadt in dem Bemühen, dass beim Einwohnermeldeamt ja alles seine Ordnung hat. Sie erwartete von Einwohnern, die sich für eine Mietwohnung neu anmeldeten, dass sie außer ihrem ausgefüllten Meldeschein auch zugleich die vom Vermieter zu erstattende Meldung, zumindest aber den Mietvertrag zur Einsichtnahme mit vorlegen. Dafür gibt es freilich keine Rechtsgrundlage. Das Meldegesetz legt die Meldepflicht des Wohnungsinhabers und die des Wohnungsgebers als selbstständige und voneinander unabhängige Verpflichtung fest. Das Einwohnermeldeamt darf den Mieter nicht dafür einspannen, als Vermittler bei der Erfüllung der

Meldepflicht des Vermieters mitzuwirken, oder gar die Bearbeitung seiner eigenen Anmeldung davon abhängig machen. Die Stadt ließ sich überzeugen und trug mit ihrem Hinweis, dass auch andere Einwohnermeldeämter so verfahren, dazu bei, dass das Innenministerium in einem Erlass an alle Städte und Gemeinden die Rechtslage klarstellte.

3. Die kommunale Daseinsvorsorge

Wasserversorgung, Abwasserbeseitigung und Müllabfuhr gehören zum Kernbestand der öffentlichen Einrichtungen, die die Kommunen zum Wohl ihrer Einwohner unterhalten. Weil dabei auch deren Daten verarbeitet werden müssen, gibt es auch dort Datenschutzprobleme.

3.1 Wo bleibt der Gewerbemüll?

Seit Jahren beklagen die Stadt- und Landkreise einen drastischen Rückgang des Aufkommens an Gewerbemüll und damit auch an den mengenabhängigen Gewerbemüll-Gebühren. Den aus der Wirtschaft zu hörenden Beteuerungen, dies sei der Erfolg der Bemühungen um Abfallvermeidung, wollen die Kreise nicht recht Glauben schenken. Sie argwöhnen vielmehr, dass ein großer Teil des Gewerbemülls, als verwertbares Gut deklariert, außer Landes gebracht und anderweitig billiger entsorgt wird. Um die finanziellen Anreize zu einem solchen Verhalten zu verringern, denken die Kreise an die Einführung einer mengenunabhängigen Grundgebühr für Gewerbemüll, der entweder die Branchenzugehörigkeit und Beschäftigtenzahl oder die Nutzfläche der Betriebe als Maßstab zugrunde gelegt werden sollen. Doch weil man dabei Neuland betritt, stehen darüber keine gesicherten Zahlen als Kalkulationsgrundlage für die Bemessung des Gebührensatzes zur Verfügung.

Der Landkreis Böblingen gedachte sich diese Daten bei den Betrieben selbst zu beschaffen und versandte im August 1999 an 16 000 gewerbliche Unternehmen, öffentliche Einrichtungen und freiberuflich Tätige einen Auskunftsbogen, in dem diese angeben sollten, in welche von vier statistischen Kategorien der Betrieb einzustufen ist, wie viele Beschäftigte, aufgegliedert nach Firmeninhabern, Vollzeitbeschäftigten und Teilzeitbeschäftigten, er hat und in welchen Müllbehältern er bislang die Gewerbeabfälle zur Beseitigung bereitstellt. In dem Auskunftsbogen gab der Landkreis zu verstehen, die Betriebe seien auf Grund der Abfallwirtschaftssatzung des Landkreises zur Auskunft verpflichtet. Um der Aufforderung, den Auskunftsbogen auszufüllen, zusätzlichen Nachdruck zu verleihen, bedeutete der Landkreis den Unternehmen, bei Nichtbeantwortung werde sein Abfallwirtschaftsbetrieb eine Eingruppierung „nach unserem Ermessen“ vornehmen. Dieses Vorgehen entsprach gewiss nicht der feinen Art. Denn die in der Abfallwirtschaftssatzung statuierte Auskunftspflicht kann sich nur auf solche Umstände erstrecken, die mit der Durchführung der geltenden Abfallwirtschaftssatzung in konkretem Zusammenhang stehen und für diesen Zweck aus konkretem Anlass erforderlich und verhältnismäßig sind. Dem Landkreis ging es jedoch mit seiner Befragungsaktion um etwas ganz anderes: Er wollte Daten- und Zahlenmaterial als Grundlage für die weiteren Überlegungen zur Einführung der Grundgebühr gewinnen und zusammentragen. Für Angaben, die lediglich der Schaffung von Planungs- und Entscheidungsgrundlagen für kommunalpolitische Entscheidungen über die Fortentwicklung des Abfallwirtschaftssystems dienen sollen, gibt es jedoch keine Auskunftspflicht. Damit aber war der Hinweis des Landkreises, die angeschriebenen Betriebe und Einrichtungen seien auskunftspflichtig, schlicht falsch und deshalb nicht mit § 11 Abs. 2 LDSG vereinbar. Er hätte sie stattdessen darauf hinweisen müssen, dass es ihnen freisteht, die erbetenen Angaben zu machen oder zu verweigern.

Dem Landkreis legte ich meine datenschutzrechtliche Beurteilung mit der Bitte um Stellungnahme dar. Er sieht inzwischen auch, dass er auf dem von ihm eingeschlagenen Weg nicht in den Besitz der gewünsch-

ten Informationen gelangen kann und will jetzt nach anderen Lösungsmöglichkeiten suchen.

Merke: Auch wenn man davon überzeugt ist, das Richtige zu wollen, muss doch der Weg dahin korrekt sein.

3.2 Begehrte Kundendaten

Hausbesitzer und Haushalte, die Wasser, Strom, Gas oder Fernwärme beziehen und an die Kanalisation und die Müllabfuhr angeschlossen sind, werden dafür zur Kasse gebeten und müssen hinnehmen, dass die dafür erforderlichen Daten in Kundendateien gespeichert werden. Auf diese Datensammlungen werfen immer wieder auch andere Unternehmen ein begehrliches Auge. Dafür einige Beispielsfälle:

– Bei einer Gemeinde, die durch ihre Stadtwerke die Einwohner mit Strom versorgt, fühlte der Landkreis vor, ob er nicht für die Veranlagung der Müllgebühren von den Stromkundendaten profitieren könne. Denn da jeder Haushalt einen Stromanschluss habe, stelle die Stromkundendatei der Gemeinde zugleich eine Datei aller Haushalte dar; deren Daten benötige der Landkreis aber ebenfalls für die Erhebung der Müllgebühren. Die Gemeinde hatte Bedenken, ihre Stromkundendaten dem Landkreis für Müllgebührenzwecke herauszurücken, und lag damit nicht falsch. Zwar ist anzuerkennen, dass der Landkreis die Anschriften der Haushalte benötigt, um die Müllgebühren veranlagen zu können, doch sieht das Meldegesetz einen anderen Weg vor, wie der Landkreis an diese Daten kommt: Die Einwohnermeldeämter dürfen bei der Anmeldung eines Einwohners die für die Müllgebühren erforderlichen Daten erfragen – also beispielsweise, an welches Mitglied eines Haushalts der Gebührenbescheid gerichtet werden soll –, diese Daten im Melderegister speichern und sie an das Landratsamt übermitteln. Ich empfahl deshalb der Gemeinde, den Landkreis auf diesen gesetzlich vorgesehenen Weg zu verweisen.

– Von einer anderen Kleinstadt erbat die Neckarwerke Stuttgart AG die Namen und Anschriften von Hausbesitzern, die noch keinen Erdgasanschluss haben, obwohl in ihrer Straße bereits eine Erdgasleitung liegt. Die Neckarwerke wollten diese Hausbesitzer gezielt anschreiben und ihnen den Hausanschluss zu besonders günstigen Bedingungen anbieten. Ich riet der Stadt ab, die Adressdaten für diesen Zweck herauszugeben. Denn bei dieser Aktion stand das werbliche Interesse der Neckarwerke ganz eindeutig im Vordergrund. Dieses Interesse kann jedoch keinen Vorrang haben vor dem berechtigten Interesse der Hausbesitzer, dass ihre Daten, die sie der Stadt auf Grund des Anschluss- und Benutzungszwangs und der Gebührenpflicht zur Verfügung stellen mussten, auch nur für diesen Zweck verwendet und nicht über ihren Kopf hinweg an Private weitergegeben werden. Für vertretbar hielt ich allenfalls, dass die Stadt von den Neckarwerken zur Verfügung gestellte Schreiben mit den Hausbesitzeradressen versieht und die Schreiben selbst versendet.

– Weniger Skrupel hatte eine andere Kleinstadt, die vor einer ähnlichen Frage stand. Sie gab dem Gasversorgungsunternehmen, das die Gasversorgung in der Stadt neu einführen wollte, die Adressdaten der Hauseigentümer heraus, damit es diese persönlich werblich anschreiben kann. Prompt blieben Bürgerbeschwerden bei meinem Amt nicht aus. Aus den gleichen Gründen wie vorstehend beschrieben folgt, dass die Datenweitergabe unzulässig war. An dieser Beurteilung änderte auch der Hinweis der Stadt nichts, sie habe sich um die Einführung der Gasversorgung in der Stadt bemüht und sie mit eigenen Mitteln finanziell gefördert und habe deshalb ein erhebliches eigenes Interesse daran, dass möglichst viele Hausbesitzer auf Erdgasheizung umstellen. Denn auch unter diesem Gesichtspunkt hätte es ausgereicht, wenn die Stadt die Hausbesitzerdaten zur Datenmittlung verwendet hätte, anstatt sie an die Gasversorgungsgesellschaft herauszugeben.

– Eine Stadt und eine Gemeinde aus der Region Stuttgart erbaten unabhängig voneinander meinen Rat, ob sie der Neckarwerke Stuttgart AG, wie von dieser gewünscht, die Wasserverbrauchsdaten für jedes einzelne Gebäude herausgeben dürfen. Meine Antwort fiel so aus: Die Wasserverbrauchsdaten sind auch ohne Namensangaben häufig personenbezogene Daten, weil die Neckarwerke sie, auch wenn sie dies nicht beabsichtigen, in vielen Fällen einzelnen Personen wie Hauseigentümern oder Rechnungsempfängern zuordnen könnten, sei es über eigene Strom-, Gas- oder Fernwärme-Kundendateien, sei es anhand öffentlich zugänglicher Werke wie Adressbücher oder Telefonbücher. Deshalb darf die Gemeinde diese Daten an die Neckarwerke nur weitergeben, wenn deren Interesse an den Daten das entgegenstehende Interesse der Wasserkunden, dass ihre Daten nicht weitergegeben werden, überwiegt. Diese werden generell darauf vertrauen, dass die Gemeinde ihre Verbrauchsdaten nur für Zwecke der Gebühren- oder Entgeltberechnung verwendet und nicht an Dritte weitergibt. Demgegenüber haben sich die Neckarwerke wenig Mühe gegeben, ihr Interesse an der Kenntnis der Daten näher zu begründen: Aus den Daten über den Wasserverbrauch je Gebäude solle der Wärmebedarf als Basis für den weiteren Ausbau der Erdgas-Infrastruktur berechnet und ein Wärmeatlas aufgebaut werden. Diese vagen Ausführungen lassen nicht erkennen, welchen Stellenwert die Erstellung eines Wärmeatlas für die Neckarwerke hat, für welche Maßnahmen genau der Wärmeatlas Grundlage sein soll, warum dazu Wasserverbrauchsdaten überhaupt und warum gebäudescharf benötigt werden und wie sie weiter verwendet werden sollen. Auf dieser Basis konnte man beim besten Willen nicht zu dem Ergebnis kommen, dem Informationsinteresse der Neckarwerke an den Wasserverbrauchsdaten komme der Vorrang zu. Ich riet deshalb von der Datenherausgabe ab.

  Bei meinen weiteren Ermittlungen stellte sich Erstaunliches heraus: Über 20 Städte und Gemeinden aus der Region Stuttgart, die von den Neckarwerken in gleicher Weise angegangen worden waren, hatten bedenkenlos ihrem Rechenzentrum den Auftrag erteilt, die Wasserverbrauchsdaten weiterzugeben. Etliche von ihnen räumten offen, andere eher verklausuliert ein, sie hätten sich nicht viel dabei gedacht, sondern sich mehr oder weniger darauf verlassen, dass schon alles seine Ordnung haben werde, wenn ein Unternehmen wie die Neckarwerke zusichert, den Datenschutz einzuhalten. Auch wenn sich die Datenweitergabe noch stoppen ließ, stellt der Vorgang den beteiligten Kommunen ganz sicher kein gutes Zeugnis in Sachen Datenschutz aus.

– Aufgeschreckt durch diese Affäre fragten die Stadtwerke einer Großen Kreisstadt besorgt an, ob sie denn die Gas- und Wasser-Verbrauchsdaten ihrer Kunden nicht für Berechnungen zur Optimierung des Wasser- und Gasleitungsnetzes verwenden dürften. Ich konnte die Stadtwerke beruhigen: Die Verwendung eigener Kundendaten für einen solchen Betriebszweck lässt das Datenschutzrecht durchaus zu. Daran erinnern musste ich die Stadtwerke allerdings, dass sie, wenn sie eine andere Firma mit den Berechnungen beauftragen, dieser die notwendigen Auflagen zum datenschutzgerechten Umgang mit den Kundenverbrauchsdaten erteilen müssen.

– Darf die Neckarwerke Stuttgart AG die Wasserverbrauchsdaten ihrer Stuttgarter Kunden ohne deren Wissen und Einverständnis an die Stadt Stuttgart weitergeben, damit diese daraus die Abwassergebühr berechnen kann? „Im Prinzip ja“, lautete meine Antwort an einen Bürger, der so fragte. Denn die Hausgebührensatzung der Landeshauptstadt bestimmt, dass sich die Abwassergebühr nach der Frischwassermenge bemisst, und das Kommunalabgabengesetz lässt zu, dass in einem solchen Fall die Stadt die Frischwasserdaten unmittelbar bei dem Wasserversorgungsunternehmen anfordert. Allerdings schreibt das Kommunalabgabengesetz weiter vor, dass dieser Weg der Datenerhebung durch Satzung bestimmt sein muss und dass die gebührenpflichtigen Bürger darüber unterrichtet werden

müssen. Dies hatte die Landeshauptstadt bis zu meiner Nachfrage noch nicht beachtet. Wenigstens hat sie ihr Versäumnis sofort eingesehen und die für ihre Praxis notwendigen rechtlichen Voraussetzungen geschaffen.

4. Sonstiges

4.1 Gebäude-Bild-Datenbank „CityServer“

Ein „spektakuläres Produkt“ präsentierte im Herbst letzten Jahres ein in Niedersachsen ansässiges Unternehmen: Es lässt in deutschen Städten ab 20 000 Einwohnern mit Spezialkameras ausgerüstete Fahrzeuge durch die Straßen fahren und gewissermaßen im Rundumblick die Häuserfronten links und rechts in rascher Bildfolge fotografieren. Die Bilder speichert das Unternehmen zusammen mit den jeweiligen Geokoordinaten in einer Computer-Bild-Datenbank und bietet diese Datensammlung interessierten Stellen zum Kauf an. Diese Geschäftsidee fand ein vielfältiges Echo in den Medien, bei Datenschützern, bei Stadtverwaltungen und nicht zuletzt bei Hausbesitzern und ist nach wie vor umstritten. Auch mein Amt bekam dies zu spüren:

Viele Hausbesitzer wandten sich an mich und baten dabei zu helfen, dass ihr Gebäude nicht in die Bild-Datenbank aufgenommen wird. Sie äußerten teils Bedenken wegen der Missbrauchsmöglichkeiten, teils allgemeines Unbehagen daran, dass ein Stück Privatheit des Wohnumfelds verloren geht. Ich habe sehr viel Verständnis für solche Besorgnisse. Jedoch konnte ich die Hausbesitzer nur an meinen Kollegen in Niedersachsen verweisen, da er allein die datenschutzrechtliche Aufsicht über das Unternehmen führt. Dieser kam zu der rechtlichen Bewertung, dass die elektronische Häuser- und Gebäudedatei derzeit nicht gegen das Bundesdatenschutzgesetz verstößt und dieses somit keine rechtliche Handhabe bietet, die Aufnahmen zu verhindern oder die Löschung von Aufnahmen durchzusetzen.

Städte erkundigten sich bei mir danach, wie es denn mit dem Einsatz der Gebäude-Bild-Datenbank für Zwecke der Stadtverwaltung stehe. Ihnen konnte ich sagen: Wenn eine Stadt die Gebäude-Bild-Datenbank erwirbt und vorhält, so erhebt und speichert sie, da sie die Bilddaten anhand der ihr zur Verfügung stehenden Datenbestände einzelnen Personen wie Hausbesitzern oder Bewohnern zuordnen könnte, personenbezogene Daten. Beides lässt das Landesdatenschutzgesetz nur zu, soweit es zur Aufgabenerfüllung erforderlich ist, d.h. wenn die Stadt eine ihr obliegende Aufgabe ohne diese Datei nicht ordnungsgemäß erfüllen könnte; dagegen reicht nicht aus, dass die Erhebung und Speicherung der Daten nur sinnvoll sein oder künftig werden könnte. Eine städtische Aufgabe, die es in diesem Sinne erforderlich machen könnte, Bild-Daten aller Gebäude im Stadtgebiet ständig vorzuhalten, ist aber nicht ersichtlich.

4.2 GEMA und Rathaus Hand in Hand?

Wer öffentliche Musikdarbietungen mit Werken, an denen noch Urheberrechte bestehen, veranstaltet, muss vorher die Einwilligung der GEMA, der Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte, einholen, damit sie die dafür fälligen Tantiemen einziehen kann. Im 16. Tätigkeitsbericht (Landtags-Drucksache 11/6900, S. 79) berichteten wir darüber, dass die GEMA sich von Städten und Gemeinden jahrzehntelang regelmäßig die Durchschriften der erteilten Tanzgenehmigungen oder Sperrzeitverkürzungen hatte zusenden lassen. Das Innenministerium hatte seinerzeit unsere Auffassung geteilt, dass es für diese Informationsweitergabe keine Rechtsgrundlage gibt, und die Regierungspräsidien und den Städtetag Baden-Württemberg entsprechend informiert. Damit schien das Problem aus der Welt, doch die GEMA gab nicht auf. Erneut wandte sie sich an Städte und Gemeinden mit der Bitte um Zusammenarbeit bei der Anmeldung von Musikveranstaltungen. Nach ihrer Vorstellung sollten diese zumindest die Anmeldevordrucke der

GEMA den Veranstaltern zur Verfügung stellen, noch besser aber die Durchschriften von Veranstaltungsmeldungen an die GEMA weiterleiten oder gar einen gemeinsamen Anmeldevordruck entwickeln. Doch nach wie vor muss es dabei bleiben: Über den Kopf der Veranstalter hinweg darf eine Kommune sich nicht einfach in etwas einmischen, was allein die Veranstalter und die GEMA angeht. Zulässig wäre allenfalls, dass ein Bürgermeisteramt für die Veranstalter, die dort eine Musikveranstaltung anmelden, auch die von der GEMA zur Verfügung gestellten Anmeldevordrucke als Service bereithält, ohne weiteren Einfluss auf die Anmeldung bei der GEMA zu nehmen oder dieser sonst einen amtlichen Anstrich zu verleihen. Erneut informierte das Innenministerium auf meine Bitte hin die Städte und Gemeinden über die Regierungspräsidien und die Kommunalen Landesverbände in diesem Sinne. Ich würde es nicht bedauern, wenn dieses Kapitel damit ein für allemal abgeschlossen wäre.

2. Abschnitt: Ausländer

Das Grundrecht auf Datenschutz ist ein sog. Jedermannsrecht. Es steht also auch Ausländern zu. Sie haben deshalb ebenfalls Anspruch darauf, dass mit ihren Daten nur so umgegangen wird, wie dies das Datenschutzrecht zulässt. Mein Amt hat sich im vergangenen Jahr verstärkt dieser Thematik angenommen und eine Reihe von Überprüfungen an Ort und Stelle durchgeführt.

1. Der Informationsservice

Welche Behörde in Baden-Württemberg in welcher Situation für Asylbewerber zuständig ist, ist jedenfalls für Außenstehende schwer zu überblicken. So muss der Asylantrag bei einer Außenstelle des Bundesamts für die Anerkennung ausländischer Flüchtlinge gestellt werden. Diese hat dann zu entscheiden, ob dem Ausländer in Deutschland politisches Asyl zu gewähren ist. Während der ersten drei Monate des Asylverfahrens wird er in der Regel von einem Regierungspräsidium in einer Gemeinschaftsunterkunft untergebracht, versorgt und ausländerrechtlich betreut. Danach erfolgt die Weiterverteilung auf die Stadt- und Landkreise, die diese Aufgabe dann weiter auf kreisangehörige Gemeinden und Städte delegieren können. Geschieht dies, werden die Ausländerämter der Landratsämter und der Bürgermeisterämter der Stadtkreise und der Großen Kreisstädte für aufenthaltsrechtliche Angelegenheiten zuständig, während es Aufgabe der Regierungspräsidien bleibt, aufenthaltsbeendende Maßnahmen durchzuführen, wenn das Asylverfahren erfolglos geblieben ist. Dabei hat es auch zu prüfen, ob Abschiebungshindernisse vorliegen.

Bei einer Kontrolle mehrerer Regierungspräsidien und Ausländerämter zeigte sich, dass die Außenstellen des Bundesamts für die Anerkennung ausländischer Flüchtlinge die dort im Asylverfahren angefallenen Erkenntnisse, insbesondere die Protokolle über die Anhörung zu den Asylgründen des Ausländers, den Regierungspräsidien übermitteln. Diese leiten diese Unterlagen dann nahezu ausnahmslos an die Ausländerämter weiter. Sie wollen damit, so jedenfalls ihre Begründung, die Ausländerämter in die Lage versetzen, ausländerrechtliche Angelegenheiten parallel zum Asylverfahren zu bearbeiten. Diese Art von Informationsservice geht entschieden zu weit, zumal es sich bei diesen Erkenntnissen des Bundesamts um sensible Daten aus dem höchst persönlichen Bereich der Asylbewerber handelt, die dazu noch besonders schutzbedürftig sind, weil sie unter Umständen Aufschluss über eine Gefährdungssituation geben. Für die Ausländerämter sind sie dagegen weitgehend unerheblich.

Die gebotene Konsequenz aus alledem muss sein: Die Regierungspräsidien dürfen die Informationen aus dem Asylverfahren, die sie von den Außenstellen des Bundesamts für die Anerkennung ausländischer Flüchtlinge erhalten, nicht mehr undifferenziert „nach unten“ weitergeben. Vielmehr ist es Sache der Ausländerämter, von sich aus auf die Regierungspräsidien zuzugehen, wenn sie im Einzelfall zur Wahrnehmung ihrer Aufgaben dort vorhandene Erkenntnisse benötigen.

Ich habe das Innenministerium als oberste Ausländerbehörde des Landes gebeten, dies sicherzustellen. Eine Antwort steht jedoch noch aus.

2. Die grenzenlose Ausschreibung

Nahezu alle Ausländer, die sich in Deutschland aufhalten, unterliegen einem besonderen Regime. Sie müssen sich bei den Ausländerbehörden anmelden, benötigen in der Regel eine Aufenthaltsgenehmigung und können unter bestimmten, im Einzelnen im Ausländergesetz geregelten Voraussetzungen ausgewiesen und abgeschoben werden. Ein solches Kontrollsystem erfordert, um den Überblick nicht zu verlieren, eine leistungsfähige Datenverarbeitung, die es den Ausländerbehörden ermöglicht, sich möglichst „auf Knopfdruck“ über die aufenthaltsrechtlichen Verhältnisse eines jeden Ausländers zu informieren. So kommt es, dass alle ausländischen Mitbürger zumindest im Datenverarbeitungssystem der für sie zuständigen Ausländerbehörde und darüber hinaus bundesweit in dem vom Bundesverwaltungsamt in Köln betriebenen Ausländerzentralregister gespeichert sind. Damit aber noch nicht genug. Sollte ein Ausländer, der kein Aufenthaltsrecht besitzt, nicht rechtzeitig und für die Ausländerbehörde kontrollierbar das Bundesgebiet wieder verlassen haben, lässt ihn das Ausländeramt auch noch im Informationssystem der Polizei (INPOL) zur Festnahme und oftmals auch im Schengener Informationssystem (SIS) zur Einreiseverweigerung ausschreiben.

Das SIS haben die sog. Schengen-Staaten auf der Grundlage des Schengener Durchführungsübereinkommens (SDÜ) eingerichtet, nachdem die Binnengrenzkontrollen zwischen diesen Ländern abgeschafft worden waren. Nach diesem Abkommen muss jeder Mitgliedstaat vor der Gewährung eines Aufenthaltsrechtes an sog. Drittausländer, also Ausländer, die nicht Staatsangehörige eines Schengen-Staats sind, zunächst prüfen, ob in einem der beteiligten Schengen-Staaten Einreisehindernisse bestehen. Um ihnen dies zu ermöglichen, können die Ausländerverwaltungen dieser Staaten solche Drittausländer, die entweder bereits ausgewiesen oder abgeschoben worden sind oder bei denen die Gefahr besteht, dass sie schwere Straftaten begehen werden, in SIS zum Zweck der Einreiseverweigerung ausschreiben lassen.

Diese Voraussetzungen für eine Ausschreibung in SIS scheinen offenbar vielen Ausländerbehörden nicht hinreichend bekannt zu sein. In zahlreichen Fällen haben sie eine Ausschreibung von Ausländern in SIS schon dann veranlasst, wenn diese, obwohl ausreisepflichtig, untergetaucht sind, also die Bundesrepublik entweder noch gar nicht verlassen haben oder aber unkontrolliert ausgereist sind. Diese Ausländer können zwar auch ausgeschrieben werden, aber nicht Schengen-weit in SIS, sondern nur bundesweit im Informationssystem der Polizei (INPOL), nämlich zum Zweck der Festnahme.

Auf meinen Hinweis auf diese rechtswidrige Praxis hat das Innenministerium rasch reagiert und die Ausländerbehörden zur Beachtung der Rechtslage angehalten.

3. Abschnitt: Finanzamt

Kaum jemand zahlt gerne Steuern und wenn es denn schon sein muss, dann möglichst wenig. Deshalb ist jeder bestrebt, möglichst all die steuerrechtlichen Vergünstigungen in Anspruch zu nehmen, die seine Steuerpflicht reduzieren. In keiner Weise zu kritisieren ist, wenn die Finanzämter solche Anträge sorgfältig prüfen. Wie mir eine ganze Reihe von Eingaben zeigen, gehen freilich die Meinungen darüber, ob die Finanzämter dabei nicht doch hin und wieder über das Ziel hinausschießen, ganz erheblich auseinander. Dafür einige wenige Beispiele:

1. Muss man ein Fahrtenbuch führen?

Muss ich tatsächlich ein Fahrtenbuch führen, aus dem sich genau ergibt, wie viele Kilometer ich wann und wo für meine Dienst- und Privatfahrten mit meinem Pkw zurückgelegt habe? Dies fragte mich ein Außendienstmitarbeiter eines Unternehmens. Eine solche Forderung habe sein Finanz-

amt an ihn gerichtet, als er den Teil der für seine Dienstfahrten entstandenen Unkosten, den das Unternehmen nicht erstattet hatte, als Werbungskosten steuermindernd geltend machen wollte. Ihm ging das entschieden zu weit.

Eines ist klar: Wer beim Finanzamt Steuervorteile in Anspruch nehmen will, muss die dafür maßgeblichen Umstände vortragen und gegebenenfalls nachvollziehbar belegen. Aber eben nur in dem Maße, wie dies unbedingt erforderlich ist. Nach Einzelheiten aus dem Privatleben des Steuerpflichtigen, die für die Entscheidung des Finanzamts gar nicht erheblich sind, darf es sich jedenfalls nicht erkundigen.

Auf meine Anfrage beim Finanzministerium nach der Praxis der Finanzämter erläuterte man mir, im Regelfall würden für die Geltendmachung solcher Werbungskosten Aufzeichnungen des Mitarbeiters über die dienstlich zurückgelegten Strecken oder entsprechende Bestätigungen des Unternehmens ausreichen. Nur in außergewöhnlich gelagerten Fällen werde die Führung eines Fahrtenbuchs verlangt, nämlich dann, wenn der Steuerpflichtige nicht in der Lage sei, seine dienstlichen Aufwendungen durch sonstige Belege nachzuweisen. Dabei genüge es aber, wenn darin die nicht für das Unternehmen zurückgelegten Kilometer als Privatfahrt gekennzeichnet sind, Angaben zum Reiseziel und zum Reisezweck seien nicht erforderlich. Geht das Finanzamt so vor, ist dagegen auch aus der Sicht des Datenschutzes nichts einzuwenden.

2. Wer hat bei wem übernachtet?

Einen Fall übler Schnüffelei des Finanzamts in ihren Privatangelegenheiten sahen die Mitarbeiter eines Unternehmens darin, dass sie diesem zum Zweck der Vorlage beim Finanzamt eine Bescheinigung der Gastgeber beibringen müssen, bei denen sie auf Geschäftsreisen übernachten. Grund dafür ist, dass das Unternehmen seinen Bediensteten eine Übernachtungspauschale in Höhe von 39 DM je Übernachtung gewährt. Diese Aufwendungen kann das Unternehmen aber nur dann als Werbungskosten bei der Steuer absetzen, wenn mit eben dieser Bescheinigung gegenüber dem Finanzamt nachvollziehbar belegt wird, dass die Übernachtung tatsächlich stattgefunden hat und die Unterkunft nicht vom Unternehmen unentgeltlich zur Verfügung gestellt worden ist.

Die Vorgehensweise des Finanzamts war jedoch nicht zu beanstanden. Es hat bei der Anforderung von Belegen den Bogen nicht überspannt, denn es will weder wissen, in welchem Verhältnis der einzelne Mitarbeiter zu der Person steht, bei der er übernachtet hat, noch fordert es für jede Übernachtung eine solche Bescheinigung. Vielmehr begnügt es sich stichprobenweise mit Belegen, aus denen sich ausschließlich die Adresse und die Unterschrift des Gastgebers ersehen lassen. Damit hat es insbesondere auch dem Grundsatz der Verhältnismäßigkeit Rechnung getragen.

3. Der Sonderfall

Mit einem erfreulicherweise nicht gerade alltäglichen Sachverhalt konfrontierten mich die Eltern eines volljährigen Sohnes, zu dem sie gewissermaßen alle Brücken abgebrochen hatten. Dieser hatte sich an das Sozialamt gewandt und von dort Sozialhilfe erhalten. Das Sozialamt wiederum hatte, wie es das Bundessozialhilfegesetz zulässt, die ausbezahlte Sozialhilfe von den unterhaltspflichtigen Eltern zurückgefordert. Diese wollten nun wenigstens erreichen, dass der dem Sozialamt ausbezahlte Betrag bei ihrer Veranlagung zur Einkommensteuer als außergewöhnliche Belastung steuermindernd berücksichtigt wird. Dabei hatten sie aber zunächst einmal die Rechnung ohne den Wirt gemacht. Das Finanzamt machte eine solche Berücksichtigung nämlich davon abhängig, dass die Eltern dem Finanzamt die zusätzlich zur Sozialhilfe erzielten Einnahmen ihres Sohnes mitteilen und nachweisen. Da ihnen das nicht möglich war, weil sie ja gar keinen Kontakt mehr mit ihm hatten, wandten sie sich an mich und baten mich um Überprüfung, ob das Verlangen des Finanzamts gerechtfertigt ist. Nun ist es dann, wenn Unterhaltsleistungen als außergewöhnliche Belastung geltend gemacht werden, im Regelfall durchaus gerechtfertigt, dass sich das Finanzamt nach den Einkünften desjenigen erkundigt, der

die Unterhaltsleistungen erhalten hat, denn nicht jede als Unterhaltsleistung deklarierte Zahlung stellt eine außergewöhnliche Belastung dar. Im konkreten Fall aber konnte wegen der Sozialhilfegewährung davon ausgegangen werden, dass die Einkünfte des Sohnes noch in dem Rahmen liegen, der eine volle Berücksichtigung der Unterhaltsleistung der Eltern als außergewöhnliche Belastung rechtfertigt. Von mir darauf aufmerksam gemacht, sah das Finanzamt dies ebenso und trug dem Anliegen der Eltern letztendlich doch Rechnung.

4. Sorgerechtsakten für das Finanzamt?

Offensichtlich ist das Verständnis dafür, dass Behörden und Gerichte mit personenbezogenen Daten sorgsam umzugehen haben, in manchen Amtsstuben noch recht unterentwickelt. Nur so lässt sich ein Aktentransfer zwischen dem Familiengericht beim Amtsgericht Singen und dem Finanzamt Konstanz erklären. Geschehen war dabei Folgendes: Die Steuerfahndungsstelle des Finanzamts verdächtigte einen Mann, der in der Schweiz gearbeitet hatte, er habe seine dort erzielten Einkünfte nicht ordnungsgemäß in der Bundesrepublik versteuert, obwohl er – so die Annahme des Finanzamts – im Veranlagungszeitraum seinen Wohnsitz in Deutschland hatte, und leitete deshalb gegen ihn ein Ermittlungsverfahren ein. Da der Beschuldigte dies bestritt, hoffte die Steuerfahndungsstelle darüber beim Familiengericht Aufschluss zu erhalten. Der Beschuldigte hatte nämlich geltend gemacht, er habe nur deshalb einen inländischen Wohnsitz einrichten müssen, weil dies das Familiengericht zur Voraussetzung für die Einräumung eines Besuchsrechts seiner Kinder, die bei der geschiedenen Ehefrau wohnten, gemacht habe. Anstatt nun gezielt danach zu fragen, was sie wissen wollte, beantragte die Steuerfahndungsstelle beim Familiengericht schlicht und einfach Akteneinsicht und begründete dies mit dem Vorbringen des Beschuldigten. Die Reaktion des Familiengerichts war mehr als erstaunlich. Ohne nachzufragen, was das Finanzamt genau wissen wollte, übersandte es kurzerhand alle im Zusammenhang mit dem Scheidungsverfahren stehende Akten, insgesamt 15 an der Zahl, darunter auch solche, in denen es um das elterliche Sorgerecht und das Umgangsrecht ging.

Hier haben beide Stellen, also sowohl das Finanzamt als auch das Amtsgericht, bei angemessener Berücksichtigung der besonderen Sensibilität der in solchen Akten enthaltenen Informationen des Schlechten zu viel getan. Das Finanzamt hätte sein Informationsbegehren konkretisieren müssen, das Amtsgericht durfte nie und nimmer auf ein solch vages Ersuchen um Akteneinsicht einfach alle bei ihm über die Scheidung und ihre Folgen vorhandenen Unterlagen dem Finanzamt zur Verfügung stellen. Ich habe deshalb vor kurzem sowohl das Vorgehen des Finanzamts als auch das des Amtsgerichts gegenüber dem Finanzministerium und dem Justizministerium beanstandet. Die Stellungnahmen stehen noch aus.

4. Abschnitt: Personalwesen

1. Theorie und Praxis – wie ist es um den Schutz von Beihilfedaten bestellt?

Geht es um die Inanspruchnahme medizinischer Leistungen, sind Beamte in puncto Diskretion gegenüber Arbeitnehmern jedenfalls in der Theorie nicht schlechter gestellt. Auch ein Staatsdiener soll einen Arzt aufsuchen und sich behandeln oder Medikamente verschreiben lassen können, ohne dass sein Dienstherr erfährt, weswegen seine Gesundheit beeinträchtigt ist und er Angst haben muss, dass sich dies auf seine berufliche Stellung auswirkt. Um dies sicherzustellen, lässt das Beihilferecht eine Verwendung von Beihilfedaten für andere Zwecke nur in seltenen Ausnahmefällen zu und schreibt eine größtmögliche Abschottung der Beihilfestelle von der übrigen Personalverwaltung vor. Diese Vorgaben werden landauf landab ganz überwiegend dadurch eingehalten, dass die Beihilfebearbeitung für die Beamten der Landesverwaltung von vornherein dem Landesamt für Besoldung und Versorgung obliegt und die meisten Kommunen diese Aufgabe auf den Kommunalen Versorgungsverband Baden-Württemberg

übertragen haben. Um zu sehen, wie es die Kommunen, die die Beihilfe selbst bewilligen, dabei mit der Einhaltung des Datenschutzes halten, besuchten wir die Beihilfestelle eines Landratsamts und die einer Großen Kreisstadt. Fazit: Theorie und Praxis klafften auseinander.

1.1 Die Ansiedlung der Beihilfestelle

Sowohl beim Landratsamt als auch bei der Stadt sind die Beihilfestellen organisatorisch bei der Personalstelle angesiedelt. Beim Landratsamt sind eine Mitarbeiterin in Vollzeit und eine in Teilzeit mit der Beihilfebearbeitung betraut, bei der Stadt erledigt eine Mitarbeiterin die Aufgabe allein. Beide in Vollzeit tätige Bearbeiterinnen nehmen – zumindest vertretungsweise – auch Aufgaben der Lohn- und Gehaltsabrechnung wahr. Ist beim Landratsamt in einer Beihilfeangelegenheit ein Widerspruchsbescheid zu erlassen, ist dies Sache des Leiters der Personalstelle.

So, wie Landratsamt und Stadt die Beihilfebearbeitung organisiert haben, erfüllen sie die Anforderungen an die Abschottung der Beihilfestelle nicht so, wie es eigentlich wünschenswert wäre. Um der Intention des Gesetzgebers umfassend Rechnung zu tragen, hätten sie die Beihilfestelle völlig aus der Personalstelle herauslösen müssen und mit der Beihilfebearbeitung betraute Mitarbeiterinnen nicht zugleich mit der Bezügeabrechnung beauftragen dürfen. Der Gesetzgeber hat jedoch die organisatorische Trennung nicht absolut festgeschrieben, sondern den Kommunen ein Hintertürchen offen gelassen mit der Begründung, dass in sehr kleinen Behörden ein Sachbearbeiter mit der Bearbeitung von Beihilfevorgängen nicht ausgelastet sein kann. Obwohl eine solche Situation offenbar weder beim Landratsamt noch bei der Stadt vorliegt, ist die Zuordnung der Beihilfestelle zur Personalstelle gerade noch vertretbar, soweit die Mitarbeiterinnen auch im Bereich der Lohn- und Gehaltsabrechnung tätig sind, weil sie bei dieser Arbeit keinen Einfluss auf Personalentscheidungen nehmen können.

Beanstanden musste ich dagegen, dass der Leiter der Personalstelle des Landratsamts über Widersprüche in Beihilfeangelegenheiten entscheidet, denn insoweit ist der rechtswidrigen Verwendung von Beihilfedaten für Zwecke der Personalverwaltung, mag dies auch unbewusst geschehen, Tür und Tor geöffnet.

1.2 Aktenführung

Beihilfeakten sind getrennt von den übrigen Personalakten zu führen, so sieht es das Landesbeamtengesetz schon seit 1986 vor. Das Landratsamt kümmerte das freilich wenig. Es hielt es für praktikabler, Beihilfevorgänge in die Bezügeakten einzusortieren. Ich forderte das Landratsamt deshalb auf, diesen gravierenden, von mir beanstandeten Mangel umgehend zu beseitigen und Beihilfevorgänge als eigenständige Teilakte zu führen.

Auch bei der Stadt war hier nicht alles Gold, was glänzt. Sie bewahrte die Beihilfeunterlagen zwar getrennt von anderen Akten in einem Schrank auf. Der war jedoch für alle Kolleginnen und Kollegen der Bezügestelle zugänglich mit der Folge, dass diese bei Abwesenheit der Beihilfebearbeiterin nachschauen konnten, welcher Mitarbeiter welche Beihilfen beantragt und in welchem Umfang bekommen hat. Hier ist eine bessere Sicherung der Beihilfeakten dringend geboten.

1.3 Aussonderung der Beihilfeakten

Seit Januar 1996 schreibt das Landesbeamtengesetz zwingend vor, dass Unterlagen über Beihilfen drei Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, auszusondern sind. Von dieser Regelung hatten die Beihilfestellen der Stadt und des Landratsamts entweder gar nichts gehört oder sie schlicht ignoriert. Das Landratsamt sonderte jedenfalls keine Beihilfeunterlagen seiner noch aktiven Beamten aus. Auf Grund seiner Akten-

führung wäre ihm das kaum möglich gewesen. Auch dieser Verstoß war so gravierend, dass ich ihn beanstanden musste. Die Stadt machte es zwar besser, aber nicht richtig. In der irrigen Annahme, hierzu gesetzlich verpflichtet zu sein, bewahrte sie die Beihilfeakten zehn Jahre auf. Beide Beihilfestellen forderte ich auf, die auszusondernden Beihilfevorgänge alsbald zu eliminieren.

1.4 Der unbeschränkte PEWES-Zugriff

Damit die Beihilfestelle der Festsetzung der Beihilfe die aktuellen persönlichen Verhältnisse und die bei der Beihilfegewährung zu berücksichtigenden Familienangehörigen zugrunde legen kann, soll sie nach der Beihilfeverordnung diese Angaben mit den für die Bezüge maßgeblichen Daten abgleichen. Das bedeutet natürlich, dass eine Beihilfesachbearbeiterin bei diesem Datenabgleich keinen Zugriff auf andere, für die Beihilfegewährung unerhebliche Personaldaten haben darf. Eine solche Zugriffsbeschränkung sucht man beim Landratsamt allerdings vergeblich, denn auch die Mitarbeiterin, die ausschließlich Beihilfevorgänge bearbeitet, kann Informationen über Fehlzeiten, Leistungsdaten, regelmäßige Zulagen sowie steuer- und sozialversicherungsrelevante Merkmale abfragen. Auch hier muss das Landratsamt bald tätig werden.

2. Akteneinsicht mit Hürden

Dass ein Beamter – wie Arbeitnehmer auch – das Recht hat, in seine vollständige Personalakte Einsicht zu nehmen, ist schon lange Gesetz und weiß jeder. Ein Polizeibeamter rechnete deshalb auch nicht damit, dass ihm seine Landespolizeidirektion (LPD) die Einsicht in die vom Polizeiarzt geführte Krankenakte, die er für einen Teil der Personalakte hielt, verweigern würde. In der Begründung der Ablehnung führte die LPD aber dezidiert aus, warum es sich bei der Krankenakte nicht um eine Teilakte der Personalakte handele. Dies habe zur Folge, dass der Beamte auch nicht in diese Einblick nehmen dürfe, weil die Vorschrift des § 113 c Abs. 2 des Landesbeamtengesetzes (LBG) nur ein Recht auf Einsicht in die Personalakte gewähre.

Hätte die LPD die alte Juristenweisheit beherzigt, wonach man immer den ganzen Paragrafen lesen soll, hätte sie sich diese Mühe sparen können. Mit ihrer Rechtsauffassung, dass die Krankenakte nicht Bestandteil der Personalakte ist und die Bestimmung des § 113 c Abs. 2 LBG nur ein Recht auf Einsicht in die Personalakte gewährt, lag sie zwar völlig richtig. Nur hatte sie übersehen, dass nach § 113 c Abs. 4 LBG der Beamte das Recht hat, auch in andere Akten, die personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet werden, Einsicht zu nehmen soweit gesetzlich nichts anderes bestimmt ist wie z. B für Sicherheitsakten. Diese Voraussetzungen sind bei den Krankenakten des Polizeiarztes gegeben. Ich kann nur hoffen, dass diese Vorschrift, die schon seit Januar 1996 in Kraft ist, bald von allen Personal verwaltenden Stellen zur Kenntnis genommen und beachtet wird.

3. Keine Veröffentlichung von Lehrerdaten ohne Einwilligung

Interessierte sich jemand dafür, wer an welcher Schule welche Fächer unterrichtet und welcher Lehrer befördert oder versetzt wurde, konnte er dies früher den vom Philologenverband und der GEW publizierten Hand- und Jahrbüchern entnehmen. Die Oberschulämter versorgten die Herausgeber mit den gewünschten Daten. Diesen Mitteilungsservice damit zu rechtfertigen, dass dem Informationsinteresse der Öffentlichkeit und der Transparenz der Schulverwaltung gegenüber den schutzwürdigen Interessen der Lehrkräfte der Vorrang einzuräumen ist, war nach damaligem Recht gewiss vertretbar. Seit Januar 1996 ist jedoch das neue Personalaktenrecht in Kraft, das den besonderen Schutz der Personaldaten detailliert regelt. Danach ist eine Weitergabe von Daten eines Bediensteten an Dritte ohne dessen Einverständnis im Wesentlichen nur noch zulässig, wenn dafür ein rechtliches, höherrangiges Interesse besteht. Ein lediglich berechtigtes Interesse genügt also nicht mehr. Gleichwohl sahen sich die

Oberschulämter nicht gehindert, weiterhin Vor- und Nachname, Fächerverbindung und Dienstbezeichnung der Lehrer ohne deren Einverständnis den Herausgebern der Jahrbücher zur Verfügung zu stellen. Dabei gab ihnen das Kultusministerium auch noch Rückendeckung. Noch im letzten Jahr schrieb es dem Oberschulamt Stuttgart, dass nach seiner Auffassung keine datenschutzrechtlichen Bedenken dagegen bestehen, wenn „die Schulen dem Philologenverband im Zusammenhang mit der Herausgabe seines Lehrerhandbuchs Name, Vorname, Fächerverbindung und Dienststellung der bei ihnen tätigen Lehrer mitteilen". Deshalb wies ich es darauf hin, dass seine Rechtsauffassung nicht mehr der Rechtslage entspricht. Zu begrüßen ist, dass das Kultusministerium daraufhin kehrtmachte und an die Oberschulämter appellierte, „künftig keine Daten von Lehrkräften ohne deren Einwilligung an Dritte zur Herausgabe von Lehrerhandbüchern, Jahrbüchern oder ähnlichen Zwecken" weiterzugeben.

4. Wo die Mitarbeiterkontrolle ihre Grenzen hat

Nach der Freude über das Vertrauen, das seine schwerbehinderten Kollegen ihm durch die Wahl zum Vertrauensmann der Schwerbehinderten entgegenbrachten, kam für den Angestellten einer Universität bald Verdruss. Weil er nur halbtags beschäftigt war, konnte er die mit seiner neuen Aufgabe verbundene Mehrarbeit nicht in der normalen Arbeitszeit bewältigen und bat deshalb den Kanzler, diese um drei Stunden pro Woche zu verlängern. Dieser bewilligte zwei Stunden zusätzlich für zunächst ein halbes Jahr mit der Auflage, danach eine Aufstellung einzureichen, „welche Aufgaben angefallen sind (Anzahl und Namen der Fälle, Zeitdauer pro Fall)". Der Vertrauensmann gab sich mit zwei Stunden zufrieden und erstattete auch fristgerecht einen Bericht über seine Tätigkeit, allerdings ohne zu sagen, welche Schwerbehinderten sich an ihn gewandt hatten. Damit wollte sich die Universität aber nicht begnügen. Zwar bewilligte sie die zwei Überstunden für ein weiteres halbes Jahr, bestand aber gleichwohl darauf, wenigstens danach zu erfahren, mit welchen Schwerbehinderten der Vertrauensmann Kontakt hatte. Nun wollte es der Schwerbehindertenvertrauensmann genau wissen und fragte mich, was ich von dem Ansinnen der Universität hielte. Die Antwort fiel nicht schwer. Natürlich darf sich der Dienstherr einen Überblick darüber verschaffen, wie viel Zeit seine Mitarbeiter für welche Aufgaben einschließlich der Sonderfunktionen wie z. B. die Tätigkeit als Personalrat oder Schwerbehindertenvertreter aufwenden. Nur, alles hat seine Grenzen. Nach dem Schwerbehindertengesetz unterliegen die Vertrauensleute der Schwerbehinderten einer besonderen Verschwiegenheitspflicht über die Dinge, die ihnen wegen ihres Amtes bekannt geworden sind. Geschützt sind aber nicht nur die zwischen ihnen und den Betroffenen ausgetauschten Informationen, sondern bereits die Tatsache, dass jemand Kontakt mit dem Schwerbehindertenvertreter hatte. So erklärt sich auch die Regelung des Finanzministeriums in der sog. Dienstanschlussvorschrift, nach der bei Personalräten und den Vertrauensleuten der Schwerbehinderten die angerufene Telefonnummer bei Gesprächen in Ausübung ihrer Sonderaufgabe nicht gespeichert werden darf. Kurzum: Die Universität durfte zwar erfragen, in wie vielen Fällen der Schwerbehindertenvertrauensmann welche Zeit aufgewandt hat, es ging sie jedoch nichts an, wer sich an ihn in seiner Sonderfunktion gewandt hatte.

5. Vorstellungsgespräch coram publico?

Eine kleine Stadt im Nordschwarzwald lud einen Beamten, der sich bei ihr um eine Amtsleiterstelle beworben hatte, zum Vorstellungsgespräch ein. Der Kandidat staunte indes nicht schlecht, als er zum vereinbarten Termin in den Sitzungssaal gebeten wurde. Dort waren nämlich nicht nur die Mitglieder des städtischen Auswahlgremiums, sondern auch alle Mitbewerber zugegen. Die Stadt hielt es – aus welchen Gründen auch immer – für angebracht, dass sich jeder Bewerber in dieser Runde vorstellen und dabei Name, Anschrift, Alter, Familienstand und andere persönliche Verhältnisse angeben und die Gründe für seine Bewerbung schildern sollte. Dass diese Variante eines Vorstellungsgesprächs rechtens sein soll, konnte sich der Bewerber allerdings kaum vorstellen. Er schrieb mir:

„Persönliche Daten gelangten bei diesem Verfahren zur Kenntnis Dritter (Mitbewerber), die diese nun unbedenklich verwerten oder auch weitergeben können. Die Schwierigkeiten, die sich hieraus für einen der Bewerber ergeben können, mag ich mir gar nicht ausmalen."

Deshalb wollte er von mir wissen, „ob diese Art von ‚Vorstellungsgespräch' datenschutzrechtlich unbedenklich bzw. überhaupt zulässig ist". Die Antwort lautete Nein, denn wer sich um eine Stelle bewirbt, hat einen Anspruch darauf, dass der Dienstherr in spe sein Persönlichkeitsrecht achtet. Der besondere Schutz von Personaldaten erstreckt sich nämlich dem Grunde nach auch auf das Bewerberauswahlverfahren. Das zeigt z. B. die Regelung des § 13 Abs. 4 Satz 1 des Landesbeamtengesetzes, wonach der Dienstherr persönliche Angaben von Bewerbern nur erfragen darf, soweit dies zur Begründung des Dienstverhältnisses erforderlich ist. Um einem Dienstherrn eine Auswahlentscheidung zu ermöglichen genügt es, wenn die Bewerber die Angaben über ihre persönlichen Verhältnisse, wie Familienstand, Kinderzahl, bisherige Arbeitgeber und die Beweggründe ihrer Bewerbung, allein dem für die Auswahl zuständigen Gremium machen. Die Anwesenheit der Mitbewerber ist dabei nicht notwendig und deshalb auch nicht gerechtfertigt. Anders mag die Rechtslage sein, wenn Auswahlverfahren eingesetzt werden, bei denen die in die engere Wahl gekommenen Bewerber in der Gruppe bestimmten Tests unterzogen und beurteilt werden. Soweit solche psychologischen Tests zulässig sind, was nur eingeschränkt der Fall ist, gelten sie heute als probates Hilfsmittel, um herauszufinden, wer von den Bewerbern den Erwartungen entspricht. In jedem Fall sind diese aber vorher darüber zu informieren, dass die Bewerberauslese in dieser Form praktiziert wird.

6. Ist die Schnüffelei des Vorgesetzten zulässig?

Mitarbeiter im öffentlichen Dienst konfrontieren mich immer wieder auch mit folgendem Aspekt der Mitarbeiterkontrolle: „Darf mein Vorgesetzter ohne mein Wissen auf meine im Computer gespeicherten Dateien zugreifen, um mich zu überwachen?" So oder ähnlich lautet meist die Frage. Sie lässt sich allerdings nicht mit einem klaren Ja oder Nein beantworten. Zunächst einmal ist zu fragen, ob der Bedienstete die EDV dienstlich oder privat nutzt. Grundsätzlich ist die gesamte Tätigkeit am Computer natürlich als dienstlich anzusehen. Nur in dem bei einer Behörde kaum vorkommenden Ausnahmefall, dass sie den Mitarbeitern erlaubt hat, Speicherplatz privat zu nutzen, muss dieser für Vorgesetzte und Kollegen tabu bleiben. Ansonsten gilt auch für den Zugriff von Vorgesetzten auf Dateien von Untergebenen der Grundsatz: Nur das Erforderliche! Je nachdem, ob und in welchem Umfang sie lesenden oder/und schreibenden Zugriff auf von diesen erstellte Dateien benötigen, sind ihre Zugriffsrechte auszugestalten. Ein Vorgesetzter könnte natürlich mit Hilfe des Systemverwalters unterschiedslos alle Dateien einsehen. Dies wäre freilich eine unzulässige Umgehung des Zugriffsrechtesystems. Eine bedeutende Ausnahme gibt es allerdings. Hat der Vorgesetzte tatsächliche Anhaltspunkte für einen Missbrauch der Computernutzung, kann er die nötigen Kontrollen vornehmen und dazu auf Dateien des Bediensteten mit Hilfe des Systemverwalters zugreifen. Diese Voraussetzungen wären z. B. dann gegeben, wenn ein Mitarbeiter unter Einsatz des dienstlichen Computers Straftaten oder in nicht unerheblichem Maß Dienstpflichtverletzungen begeht.

5. Abschnitt: Schule

1. Die datenschutzgerechte Schülerbefragung – für das Kultusministerium offenbar noch immer ein Buch mit sieben Siegeln

Es gibt einige Dinge im Alltag meines Amtes, bei denen man sich wie Sisyphus vorkommt und manchmal am liebsten die Flinte ins Korn werfen würde, das Thema Datenschutz und Forschung ist eines davon. „Umfragen bei Bürgern für Planungs- und Forschungszwecke beschäftigen mein Amt schon seit es existiert", so war im 15. Tätigkeitsbericht (Landtags-Drucksache 11/5000, S. 107) unter Hinweis auf vier frühere Tätigkeitsberichte zu lesen. Erneut machten wir damals darauf aufmerksam, auf was

bei Konzeption und Durchführung von Forschungsvorhaben zu achten ist, damit sie datenschutzgerecht sind. Der Erfolg? Offenbar gering, denn gleich im nächsten Tätigkeitsbericht mussten wir erneut über zwei datenschutzrechtlich verunglückte Forschungsprojekte berichten (Landtags-Drucksache 11/6900, S. 90). Auffällig ist, dass es sich relativ häufig um Befragungen in Schulen, oft im Auftrag der Kultusverwaltung, handelt. Was sich allerdings in diesem Jahr bei drei Schülerbefragungen abspielte, die das Kultusministerium zu verantworten hat, ist schon erstaunlich. Dazu muss man sich zunächst vor Augen halten, welche Anforderungen das Kultusministerium schon seit vielen Jahren an andere und sich selbst stellt, damit der Datenschutz bei Untersuchungen in der Schule gewährleistet ist:

Als 1984 eine Universität eine Schülerbefragung zur Untersuchung über „Möglichkeiten der Suchtprävention“ in Stuttgart durchführte, „vergaß“ es die Schüler und ihre Eltern vorher darüber zu informieren und deren Einwilligung zur Teilnahme einzuholen. Die Sache hatte ein parlamentarisches Nachspiel; auf eine Landtagsanfrage antwortete das Kultusministerium u. a.:

> „Es wird streng auf die Einhaltung der Bestimmungen über den Datenschutz geachtet. In der Genehmigung wird auf den Datenschutz hingewiesen und die Genehmigung in der Regel insbesondere mit folgenden Auflagen verbunden:
>
> 1. Der Untersuchende hat die Schüler und insbesondere ihre Erziehungsberechtigten auf die Freiwilligkeit der Teilnahmen hinzuweisen.
> 2. Vor Einholung der Zustimmung ist über Ziel und Durchführung des Projekts zu informieren.
> 3. Die Befragungen müssen in der Regel in anonymer Form durchgeführt werden. Sollten vom Zweck des Projekts her persönliche Daten unverzichtbar sein, muss sich die Information und Zustimmung auch hierauf beziehen.
> 4. Aus der Darstellung des Ergebnisses des Projekts dürfen keine Schlüsse auf konkrete Einzelpersonen möglich sein.“

Um den Bekanntheitsgrad seiner Vorgaben zur Beachtung des Datenschutzes bei Schülerbefragungen zu steigern, bestimmte das Kultusministerium dann im August 1985 in einer Verwaltungsvorschrift:

> „Erhebungen, insbesondere Umfragen und wissenschaftliche Untersuchungen in Schulen durch Personen oder Institutionen außerhalb der Schulverwaltung bedürfen der Genehmigung. Die Genehmigung kann erteilt werden, wenn der Erhebung ein erhebliches pädagogisch-wissenschaftliches Interesse anzuerkennen ist und sich die Belastung für Schüler, Schule und Lehrer in zumutbarem Rahmen hält. Sie ist mit den erforderlichen Auflagen zu verbinden, insbesondere hinsichtlich der Information, der Zustimmung und der Anonymität der zu Befragenden oder ihrer Eltern sowie des Datenschutzes. Personenbezogene Daten von Schülern dürfen nur mit Einwilligung der Eltern oder der volljährigen Schüler erhoben werden. Bei Erhebungen, die über den Bereich eines Oberschulamts hinaus stattfinden sollen, erteilt die Genehmigung das Kultusministerium, im Übrigen das zuständige Oberschulamt.“

Soweit die hehren Ziele und Vorgaben des Kultusministeriums. Doch, um mit den Worten Tucholskys zu sprechen, „was nützen die besten Worte, wenn sie über die Wirklichkeit hinwegtäuschen?“ Die sieht nämlich noch heute ganz anders aus:

1.1 Das Projekt „PISA“

Ziel eines Programms der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist es, den Mitgliedsstaaten vergleichende Daten über die Leistungsfähigkeit ihrer Bildungssysteme zur Verfügung zu stellen. Zu diesem Programm gehört eine internationale Schulleistungsstudie namens „Programme for International

Student Assessment“ (PISA), bei der verschiedene Schüler- und Elternbefragungen vorgesehen sind. Durchgeführt wird PISA im Auftrag der Kultusminister der Länder durch das Max-Planck-Institut für Bildungsforschung in Berlin (MPI). Die Feldarbeit und die Datenverarbeitung hat ein sog. Data Processing Center (DPC) in Hamburg übernommen. Auf die Studie und den ihr vorgeschalteten Feldtest machten mich zunächst Kollegen anderer Bundesländer aufmerksam. Diese hatten jeweils von den für Schulen zuständigen Ressorts Informationen und Unterlagen erhalten, die allerdings voneinander abwichen. Später erhielt auch ich vom Kultusministerium den Teil der für die im Feldtest geplanten Befragungen maßgebenden Unterlagen, den das Ministerium bis dato hatte. Bei der Durchsicht der Unterlagen zeigten sich dann rasch gravierende datenschutzrechtliche Mängel. Zudem wurden eine Reihe von Fragen und Problemen sichtbar, die teilweise bis heute ungeklärt sind. Im Wesentlichen war Folgendes zu kritisieren:

– Die angebliche Anonymität

  Sowohl in einem Informationsheft zu PISA als auch in zwei Entwürfen von Anschreiben an die Eltern behauptete das MPI, dass durch die Befragungen der Datenschutz nicht berührt sei. So ist z. B. in einem Elternanschreiben zu lesen: „Selbstverständlich sind alle Angaben anonym, eine Zuordnung zu Personen ist nicht möglich“. Im Informationsheft und im anderen Elternanschreiben hieß es sinngemäß, dass die Erhebung so anonymisiert durchgeführt wird, dass eine Zuordnung von Ergebnissen zu Personen ausgeschlossen ist. Auch hätten die Datenschutzbeauftragten der Länder Anlage und Durchführung der Studie geprüft und genehmigt.

  Die Worte „Anonymität“ oder „anonym“ üben auf Forschungseinrichtungen offenbar eine magische Anziehungskraft aus, denn es gibt kaum eine Befragung, bei der sie nicht auftauchen. Der Wirklichkeit entspricht dies freilich in den seltensten Fällen. Auch hier wäre es dem DPC leicht möglich gewesen, einzelne oder alle antwortenden Schüler zu identifizieren. Dazu hätte es sich lediglich eine Schülerliste besorgen müssen oder hätte durch leicht beschaffbare Informationen zusammen mit den Antworten auf verschiedene Fragen zur Person des Schülers dessen Identität feststellen können. Folglich hätte das MPI bei den Befragungen die datenschutzrechtlichen Vorschriften beachten müssen, die besagen, dass die Befragungen und die weitere Verarbeitung der Daten nur auf Grund wirksamer Einwilligung möglich waren.

– Die unwirksame Einwilligung

  Wer jemandes Einverständnis einholen will, um dessen persönliche Daten verwenden zu dürfen, muss ihn auf den Zweck der Verarbeitung, die Empfänger einer vorgesehenen Weitergabe der Daten sowie auf die möglichen Folgen der Verweigerung der Einwilligung hinweisen. In den Elternanschreiben des MPI suchte man danach weitgehend vergebens. Die Freiwilligkeit der Teilnahme an der Befragung und dass durch die Nichtteilnahme keinerlei Nachteile entstehen, wollte es überhaupt nicht erwähnen. In der Information der Eltern über den Inhalt des Schülerfragebogens erfuhren die Eltern zwar, dass ihre Kinder nach Lesegewohnheiten, Freizeitinteressen, soziodemografischem Hintergrund und den Merkmalen des Unterrichts und des Schullebens gefragt würden. Dass jedoch noch wesentlich sensiblere Fragen nach dem häuslichen Umfeld und Verhaltensmustern, wie z. B. Straftaten und Gewalttätigkeiten der Kinder sowie physischer und psychischer Druck aus dem Elternhaus, gestellt werden, wollte das MPI den Eltern verschweigen.

– Auf welcher Grundlage agiert das DPC?

  Bis heute weiß ich nicht, ob das MPI mit dem DPC schriftliche Vereinbarungen über die Datenverarbeitung getroffen hat und welchen Inhalt sie haben.

Dass das MPI gleichwohl an mehreren Stellen behauptete, die Konzeption der Studie sei von den Datenschutzbeauftragten der Länder geprüft und für in Ordnung befunden worden, ist an Unverfrorenheit wohl kaum zu überbieten. In keinem Land war zum damaligen Zeitpunkt eine abschließende Prüfung, geschweige denn eine Unbedenklichkeitsbescheinigung oder gar Genehmigung erfolgt.

In dieser Situation wäre es nun Sache des Kultusministeriums gewesen, die datenschutzrechtlichen Mängel festzustellen, das MPI zur Nachbesserung aufzufordern und ihm getreu seiner Verwaltungsvorschrift die nötigen Auflagen zu erteilen. Das Kultusministerium schlug dagegen einen anderen Weg ein. Es leitete kurzerhand mir die Unterlagen mit der Bitte um kurzfristige Prüfung zu. Auf diese Bitte ging ich nur deshalb ein, damit der Datenschutz der Schülerinnen und Schüler und ihrer Eltern beim Feldtest nicht völlig unter die Räder gerät und weil das Kultusministerium für die knapp bemessene Zeit keine Schuld trug. In der Folge gelang es dann doch noch, die meisten datenschutzrechtlichen Mängel des PISA-Feldtests wesentlich zu entschärfen oder auszumerzen.

Auch meine Kolleginnen und Kollegen sorgten dafür, dass der Feldtest in ihren Ländern einigermaßen datenschutzgerecht ablaufen konnte, was das MPI einige zusätzliche Zeit und Mühe gekostet haben dürfte. Diesen Schlamassel hätte es vermeiden können, wenn es frühzeitig die Kultusressorts und die Datenschutzbeauftragten in die Konzeption eingebunden hätte. Dies hat das MPI offenbar inzwischen erkannt, denn es will jetzt die relevanten Unterlagen der PISA-Hauptuntersuchung mit den Datenschutzbeauftragten besprechen.

1.2 Die Studie „Civic Education“

Unmittelbar nachdem mein Amt dem Kultusministerium die datenschutzrechtlichen Mängel der PISA-Studie aufgezeigt und auf Abhilfe gedrängt hatte, erfuhren wir – wieder nicht vom Kultusministerium, sondern von einem Kollegen –, dass das Kultusministerium über die Teilnahme unseres Landes an einer anderen internationalen Studie zu befinden hat. Dabei ging es um die Studie der International Association for the Evaluation of Achievement (IEA) zur politischen Bildung der Schüler. Für diese Studie zeichnet ebenfalls das MPI verantwortlich. Deren Bestandteil ist eine umfangreiche Befragung von Schülern und Lehrern. Schon auf Grund der ersten spärlichen Unterlagen, die meinem Amt zur Verfügung standen, war zu sehen, dass Konzeption und Durchführung der Studie im Wesentlichen unter den gleichen datenschutzrechtlichen Mängeln litt wie das PISA-Projekt. Wir machten deshalb das Kultusministerium umgehend darauf aufmerksam und baten es, die vollständigen Unterlagen über die Durchführung der Studie zu übersenden und mitzuteilen, welche datenschutzrechtlichen Auflagen es dem MPI erteilt hat. Daraufhin besann sich das Kultusministerium der Vogel-Strauß-Politik und ging so vor: Das Schreiben meines Amtes legte es auf die Seite und steckte den Kopf in den Sand. Anstatt sich über das Persönlichkeitsrecht der Lehrer und Schüler Gedanken zu machen, beeilte es sich lieber, die Durchführung der Studie knapp zwei Wochen später mit folgenden Auflagen zu genehmigen:

„Die Genehmigung an den Haupt- und Realschulen ist an folgende Voraussetzungen gebunden:

– Die Mitwirkung der Schulen oder Beteiligten ist freiwillig, die Zustimmung der Erziehungsberechtigten ist einzuholen.

– Die Anonymität der Mitwirkenden muss gewährleistet sein, es dürfen keine Rückschlüsse auf die beteiligten Personen möglich sein.“

Dass das MPI diese Plattitüden nicht zum Anlass nahm, die Datenschutzdefizite zu beseitigen, versteht sich von selbst.

Erst als wir nach weiteren vier Wochen an unsere Anfrage erinnerten, bequemte sich das Kultusministerium zwei Wochen später zu einer

Antwort und teilte lapidar mit, wann und mit welchen Auflagen es die Durchführung der Studie genehmigt habe und dass nach seiner Auffassung keine datenschutzrechtlichen Bedenken gegen den Fragebogen bestünden. Beigefügt war ein Teil der maßgeblichen Unterlagen, wesentliche Komponenten behielt es lieber für sich. Erst auf erneutes Drängen übersandte es dann doch noch die fehlenden Unterlagen.

Um es kurz zu machen: Weil das Kultusministerium in Kenntnis der gravierenden datenschutzrechtlichen Mängel die Durchführung der Studie genehmigte, hat das MPI von allen teilnehmenden Lehrern und Schülern infolge deren unwirksam erteilter Einwilligungen rechtswidrig Daten erhoben. Es blieb mir gar nichts anderes übrig, als dieses Vorgehen des Kultusministeriums förmlich zu beanstanden. Zudem beanstandete ich, dass das Ministerium seiner Auskunfts- und Unterstützungspflicht nicht nachgekommen ist.

1.3 Das Projekt „Faustlos“

Im Auftrag des Kultusministeriums führt eine Universitätsklinik das Forschungsprojekt „Faustlos“ zur Gewaltprävention an Schulen durch. Dazu wurden in einer ersten Stufe an 20 Grundschulen Schüler und ihre Eltern befragt. Nach der ursprünglichen Konzeption dieser Erhebung sollten die Eltern im Fragebogen ihren Vornamen, den ersten und letzten Buchstaben des Nachnamens, das Geschlecht, das Geburtsdatum und die Schule des Kindes angeben. Zudem sollten sie Angaben über Alter und den ausgeübten Beruf machen sowie ihre Anschrift angeben, wenn sie über die Ergebnisse des Projekts informiert werden wollten. Im Vorblatt des Fragebogens hieß es: „Bei der Datenauswertung werden alle Namen gelöscht, so dass Ihre Anonymität gewahrt bleibt. Die Adressen werden nach Versendung der Ergebnisse vernichtet.“ Eine Information der Eltern darüber, welche Auswertungen vorgesehen sind, wo und wie lange die Daten in welcher Form gespeichert werden und – hinsichtlich der Befragung der Kinder – welche Angaben von diesen erfragt werden sollen, gab es nicht. Auch hier fehlte jeder Hinweis darauf, dass die Teilnahme an der Befragung freiwillig ist und eine Verweigerung der Einwilligung zu keinerlei Nachteilen führt.

Mit der „Anonymität“ war es natürlich nicht weit her. Bei den Eltern, die ihre Adresse angegeben hatten, um über die Ergebnisse der Untersuchung informiert zu werden, konnte von einer Verarbeitung anonymisierter Daten von vornherein nicht die Rede sein. Aber auch bei den übrigen Fragebogen ließen sich mit bereits vorhandenem Zusatzwissen oder mit relativ geringer Mühe in einzelnen Fällen durchaus die antwortenden Eltern aus der Kombination ihrer Antworten auf die genannten Fragen identifizieren. Auf unsere Frage nach den datenschutzrechtlichen Auflagen, wie sie die Verwaltungsvorschrift des Kultusministeriums vorsieht, erhielten wir nur eine „Fehlanzeige“. Das Ministerium meinte nur entschuldigend, es sei „selbstverständlich davon ausgegangen, dass die bei wissenschaftlichen Untersuchungen erforderlichen datenschutzrechtlichen Bestimmungen eingehalten werden“. Von einer Beanstandung dieser missglückten Schülerbefragung habe ich nur deshalb abgesehen, weil die Universitätsklinik die datenschutzrechtlichen Mängel ohne viel Federlesens beseitigte und die bereits erhobenen persönlichen Angaben dann tatsächlich weitgehend anonymisierte.

2. Der kostenlose Schülerausweis als Köder

Seit geraumer Zeit sorgt für Furore, dass Unternehmen, die sich auf das Fotografieren von Schülern spezialisiert haben, an Schulen herantreten und ihnen folgendes Geschäft vorschlagen: Wenn sie die Schüler fotografieren und ihnen später ein sog. „Fotopackage“, bestehend aus vier Portrait-, vier Pass- und 16 Kleinfotos sowie einem Klassenfoto zum Kauf anbieten dürften, bekäme die Schule für die Schüler kostenlos digitale Schülerausweise aus Plastik im Scheckkartenformat. Einem solchen Angebot können manche Schulleiter nicht widerstehen und gehen auf den Handel ein. Dazu geben sie der Firma zunächst die Namen und Geburts-

daten der Schüler, ohne allerdings vorher diese oder ihre Eltern um Erlaubnis gefragt oder wenigstens informiert zu haben. Wenn dann der „Schulfotograf“ kommt, die Schüler fotografiert und hinterher die Fotos zum Kauf angeboten werden, sind Beschwerden der Eltern vorprogrammiert. Aus der Sicht des Datenschutzes ist die Sache klar: Die Schule darf die Schüler nur fotografieren lassen und deren Namen und Geburtsdatum an die Firma weitergeben, wenn diese oder ihre Eltern schriftlich ihr Einverständnis erklärt haben. Weil nämlich das Ausstellen von Schülerausweisen zwar dem Schulverhältnis immanent ist, aber nicht unmittelbar zum Erziehungs- und Bildungsauftrag der Schule gehört, steht es dem einzelnen Schüler frei, ob er überhaupt einen Schülerausweis haben und sich zu diesem Zweck in der Schule fotografieren lassen will. Ein Recht der Schule, Schülerdaten ohne Einwilligung an Dritte für kommerzielle Zwecke weiterzugeben, gibt es schon gar nicht. Darüber bestand mit dem Kultusministerium schon 1996 Einvernehmen. Nur behielt es diese Erkenntnis damals für sich, so dass sich immer wieder Schulen wegen des Köders „kostenloser Schülerausweis“ zu Datenschutzverstößen verleiten ließen. Deshalb musste ich wohl oder übel einen solchen Fall, der von mehreren Eltern an mich herangetragen wurde, gegenüber dem Kultusministerium beanstanden. Dieses teilte mit, es habe die Beanstandung zum Anlass genommen, die Schulen darüber zu unterrichten, dass Schülerfotos nur mit Einwilligung der Schüler bzw. deren Eltern angefertigt werden dürfen und von der Weitergabe personenbezogener Daten an gewerbliche Fotounternehmen abzusehen ist.

3. Wenn Schüler aus dem Nähkästchen plaudern

Kindermund tut Wahrheit kund, so sagt der Volksmund. Manchen Eltern ist es freilich gar nicht recht, wenn ihre Sprösslinge Wahres an unpassender Stelle ausplaudern. Ein Ort, an dem dies bisweilen geschieht, ist die Schule. Weil die Schülerinnen und Schüler im familiären Umfeld verwurzelt sind, tragen sie dieses natürlich auch in die Schule hinein und offenbaren den Lehrern, oft ausgelöst durch das Thema von Aufsätzen oder durch bestimmte Hausaufgaben, Informationen über Eltern, Angehörige und die häusliche Umgebung. Manchmal fragen Lehrer ihre Schüler auch gezielt nach bestimmten familiären Verhältnissen. So gut ich das immer wieder an mich herangetragene Unbehagen der Eltern darüber nachempfinden kann, mit dem Datenschutz ist das Problem in aller Regel nicht zu lösen. Auch für den Lehrer gilt natürlich der Grundsatz „Nur das Erforderliche“. Er darf seine Schüler folglich nur nach dem fragen, was er benötigt, um seinen Erziehungs- und Bildungsauftrag erfüllen zu können. Dieser beschränkt sich jedoch nicht auf die reine Vermittlung von Wissen und Fähigkeiten. Vielmehr sollte zwischen Lehrer und Schülern ein Vertrauensverhältnis bestehen, in dem der Lehrer erzieherisch wirken kann. Dabei muss er die gesamte Persönlichkeit der Schüler berücksichtigen, um sie sachgerecht beurteilen und anleiten zu können. Soweit sich Fragen der Lehrkräfte in diesem erzieherischen Bereich bewegen, ist der Datenschutz außen vor. Auf einem anderen Blatt steht, ob bestimmte Fragen oder Aufsatzthemen pädagogisch immer sinnvoll sind.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
am 25./26. März 1999

Modernisierung des Datenschutzes jetzt – umfassende Novellierung des BDSG nicht aufschieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein „Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbindung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Anhang 2

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 7./8. Oktober 1999

Zum Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25. August 1999

Gesundheitsreform 2000

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes „Gesundheitsreform 2000“:

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiter reichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach

dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

Die zur Begründung besonders angeführten Punkte „Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern“ vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so dass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Anhang 4

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 7./8. Oktober 1999

Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten“ verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anhang 5

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 7./8. Oktober 1999

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 9./10. März 1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16. August 1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17. September 1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 17. Juni 1999

Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

Bei der Einführung der Befugnis zum „Großen Lauschangriff“ hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weit reichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Artikel 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz und hebt zugleich die politische Kontrollfunktion der Parlamente gegenüber der Exekutive hervor. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine Grundrecht sichernde Bedeutung. Jetzt ist jedoch bekannt geworden, dass einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnisse gewährleistet.

Wird durch eine solche Kontrolle deutlich, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

Anhang 7

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 7./8. Oktober 1999

DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozeßordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis – also ohne richterliche Anordnung – erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigt.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen – abweichend von den gesetzlich vorgesehenen Verfahren – systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Regelung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung in künftigen Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Anhang 8

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 7./8. Oktober 1999

Täter-Opfer-Ausgleich und Datenschutz

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28. Mai 1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs“ nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich“ Beteiligten muss gesetzlich geschützt werden.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 16. August 1999

Angemessener Datenschutz auch für Untersuchungsgefangene

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.

Diese Regelung muss das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, lässt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

– Entgegen dem Vorschlag des Bundesrats, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z. B. Fluchtgefahr) nur im Einzelfall auf Grund richterlicher Anordnung erfolgen dürfen.

  Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt anstelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelner Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.

– Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen wie vom Bundesrat befürwortet.

– Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z. B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

– Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

Anhang 10

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 7./8. Oktober 1999

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil auf Grund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31. Dezember 1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozeßordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

Anhang 11

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 7./8. Oktober 1999

Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anhang 12

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. März 1999

Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFO-POL '98)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFO-POL '98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

Anhang 13

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. März 1999

Entschließung zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur so lange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Anhang 14

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. März 1999

Transparente Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number – PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.