Landtag von Baden-Württemberg **Drucksache 13 / 520**
13. Wahlperiode **03. 12. 2001**

Mitteilung

des Landesbeauftragten für den Datenschutz

Zweiundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 3. Dezember 2001:

Anbei übersende ich Ihnen unseren 22. Tätigkeitsbericht, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2001 zu erstatten ist.

Schneider

Eingegangen: 03. 12. 2001 / Ausgegeben: 19. 12. 2001

Zweiundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

1. Teil: Zur Situation

2. Teil: Öffentliche Sicherheit und Justiz

3. Teil: Technik und Organisation

1. Teil: Zur Situation

1. Datenschutz in stürmischem Fahrwasser

Vor etwas mehr als 31 Jahren verabschiedete der Hessische Landtag das erste Datenschutzgesetz und gab damit den Startschuss für die moderne Datenschutzgesetzgebung in der Bundesrepublik Deutschland. Bis zum Jahr 1980 verfügten dann sowohl der Bund als auch alle Bundesländer der alten Bundesrepublik über Datenschutzgesetze. Einen weiteren, für die Fortentwicklung des Datenschutzes äußerst wichtigen Eckpunkt setzte im Jahr 1983 das Bundesverfassungsgericht. Nach heftigen Auseinandersetzungen über eine geplante Volkszählung stellte das höchste deutsche Gericht damals klar, dass der Datenschutz den Rang eines Grundrechts besitzt und „eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“ darstellt. In der Folgezeit bemühten sich die Gesetzgeber im Bund und in den Ländern, den vom Bundesverfassungsgericht festgestellten Anforderungen an den Schutz des Grundrechts auf Datenschutz gerecht zu werden. Unter anderem kam es bis Anfang der 90er Jahre zur Novellierung sowohl des Bundesdatenschutzgesetzes als auch der Landesdatenschutzgesetze. Keine Frage war auch, dass die neuen Bundesländer sofort nach der Wiedervereinigung als Reaktion auf die schlimmen Erfahrungen mit den berüchtigten Methoden der Stasi Datenschutzgesetze erließen und sogar in ihren Verfassungen ausdrücklich den Grundrechtscharakter des Datenschutzes bestätigten. Damit nicht genug, mit ihrer Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 gab die Europäische Gemeinschaft einen weiteren Anstoß zur Stärkung des Datenschutzes, diesmal sogar europaweit. Die Umsetzung dieser Richtlinie in das deutsche Datenschutzrecht ging freilich nicht ganz reibungslos vonstatten. Das zeigt sich allein schon daran, dass es bis auf zwei Bundesländer allen anderen, und vor allem auch dem Bund, nicht gelang, die gebotene Gesetzesanpassung fristgerecht abzuschließen. Aber immerhin, sie haben es schließlich doch geschafft.

Betrachtet man diesen hier nur skizzenhaft dargestellten äußeren Ablauf der Geschichte der Datenschutzgesetzgebung, könnte man meinen, dass der Datenschutz bei uns zu etwas ganz Selbstverständlichem geworden ist, dessen Notwendigkeit und Sinnhaftigkeit von niemandem in Frage gestellt wird. Wie aber gerade die Reaktionen auf die schrecklichen Ereignisse des 11. September 2001 in den USA zeigten, ist dem offensichtlich beileibe nicht so. Wie sonst lässt sich erklären, dass schon unmittelbar danach gleichsam als erste zu veranlassende Maßnahme im Kampf gegen den Terrorismus Berufene und Unberufene pauschal eine Lockerung des Datenschutzes forderten. „Wir haben uns offensichtlich zu viel Datenschutz gegönnt“, solche und ähnliche Äußerungen waren in allen Medien zu lesen und zu hören. Altbekannte platte Sprüche wie „Datenschutz darf nicht zum Täterschutz werden“ machten wieder einmal die Runde. Offenbar besonders überzeugend fand der ein oder andere in Talkshows und anderswo die Parole „Menschenschutz geht vor Datenschutz“ und bewies damit lediglich, dass er offensichtlich immer noch nicht begriffen hat, worum es beim Datenschutz geht. Personenbezogene Daten werden schließlich nicht um ihrer selbst, sondern um der Menschen willen geschützt, auf die sie sich beziehen. Datenschutz ist also Menschenschutz. Das zugegebenermaßen auf den ersten Blick für nicht mit der Materie Vertraute eingängige Wortspiel macht also in Wirklichkeit keinerlei Sinn. Für jemanden, der wie ich die Datenschutzdiskussion in den letzten 20 Jahren miterlebt und erlitten hat, war dies alles keine Überraschung. Zu keiner Zeit war der Datenschutz völlig unangefochten. Schon immer gab es mehr oder weniger stark ausgeprägte Vorbehalte. Datenschutz bedeutet schließlich in letzter Konsequenz Beschränkung der Informationsbeschaffung und -verwendung, und wer verzichtet darauf schon gerne. Nicht umsonst waren nahezu alle Gesetzesvorhaben und andere Maßnahmen, die eine Stärkung des Datenschutzes zum Ziel hatten, im politischen Raum heftig umstritten. Man möge sich nur an die Auseinandersetzung über den Datenschutz in den 80er-Jahren erinnern. Ohne die Auto-

rität des Bundesverfassungsgerichts und das von dort drohende Verdikt der Verfassungswidrigkeit hätte die Datenschutzgesetzgebung nicht den Stand erreichen können, den sie heute hat. Es kann deshalb nicht verwundern, dass in Krisensituationen und nach schlimmen Vorfällen in wenig schöner Regelmäßigkeit als erste Maßnahme der Datenschutz aufs Korn genommen und nach einer Erweiterung der staatlichen Einsatzbefugnisse und damit nach einer Einschränkung des Datenschutzes gerufen wird. Dies klingt für die Wähler einleuchtend, kostet meist wenig und zeigt, dass man bereit ist etwas zu tun. Freilich, so massiv wie nach dem 11. September 2001 ist der Datenschutz noch selten von einem breiten politischen Spektrum zum Buhmann gemacht und seine Daseinsberechtigung in Frage gestellt worden.

Erfreulicherweise hat sich nach dem Bekanntwerden der ersten Forderungskataloge und Wunschlisten gezeigt, dass diese Attacken auf eine wichtige Errungenschaft unseres freiheitlich-demokratischen Rechtsstaats keineswegs auf ungeteilten Beifall gestoßen sind. Was da Bundes- und Landespolitiker in gar nicht so edlem Wettstreit forderten und vorschlugen, ging dann doch zu Recht vielen zu weit. Anstatt zuerst einmal sorgfältig und zielgerichtet zu prüfen, was wirklich zur Terrorismusbekämpfung notwendig ist, musste man den Eindruck gewinnen, dass ohne Rücksicht auf das in unserer Verfassung verankerte Übermaßverbot sofort all das vorgeschlagen wurde, was technisch möglich erscheint. Mitunter segelten unter der Flagge Terrorismusbekämpfung auch Forderungen, die damit nun wirklich nichts mehr zu tun haben. Ein besonders signifikantes Beispiel dafür ist die im Entschließungsantrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drucksache 807/01) enthaltene Forderung nach Abschaffung des Richtervorbehalts bei der Anordnung einer Genom-Analyse von Tatspuren. Inzwischen scheint es aber so, dass sich die Hektik und Aufgeregtheiten der ersten Tage und Wochen nach dem 11. September 2001 allmählich legen. So sieht der vor kurzem von der Bundesregierung beschlossene Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus zwar immer noch Regelungen vor, die unter rechtsstaatlichen Aspekten nicht akzeptabel sind, aber immerhin enthält er schon einige Verbesserungen gegenüber dem ersten Entwurf des Bundesinnenministeriums. Bleibt zu hoffen, da weiß ich mich mit meinen Kollegen im Bund und in den Ländern einig, dass der Gesetzentwurf einer gründlichen parlamentarischen Beratung unterzogen wird und am Ende eine Fassung findet, die den Prinzipien Rechnung trägt, die unseren Rechtsstaat prägen. Geschieht dies, dann wäre dies ein wichtiger Schritt zur Stabilisierung des Datenschutzes in der Bundesrepublik.

2. Das Amt

Sensationen und sonstige spektakuläre Ereignisse sind auch in diesem Jahr nicht zu vermelden. Für mich steht nach wie vor der einzelne Bürger mit seinen Sorgen und Anliegen im Vordergrund. Seinen Klagen nachzugehen und seine Fragen zu beantworten, also die Funktion eines Ombudsmanns in Sachen Datenschutz wahrzunehmen, bildet deshalb immer noch einen Schwerpunkt der Aktivitäten meines Amts. Dabei ist festzustellen, dass der Landesbeauftragte für den Datenschutz wie eh und je für viele Bürger die Stelle ist, an die man sich in Sachen Datenschutz wendet, ganz gleich, ob es sich um Datenschutz im öffentlichen oder im nichtöffentlichen Bereich handelt. Dies ist aus meiner Sicht neben einer Reihe weiterer Gründe ein wichtiger Aspekt, der dafür spricht, die Datenschutzkontrolle in eine Hand zu legen. Der Trend in der Bundesrepublik Deutschland geht, nicht zuletzt von der EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 gefordert, ohnehin in diese Richtung. Ich bin überzeugt, dass auch Baden-Württemberg nicht umhin kommen wird, sich diesem Trend anzuschließen. Die Beschäftigung mit Bürgereingaben nimmt u. a. auch deshalb einen besonderen Stellenwert ein, weil ich dabei gewissermaßen aus erster Hand erfahre, wo den Bürger der Schuh drückt und wie Behörden mit ihm und seinen Daten umgehen. Wichtig ist bei dieser Arbeit, dass die beteiligten Behörden auch bereit sind, meinem Amt zügig die Auskünfte zu geben, die es benötigt, um dem Bürgeranliegen nachzugehen. Leider tat sich damit

die ein oder andere Behörde schwer, und zwar auch solche, von denen man ein solches Verhalten nun wirklich nicht erwarten konnte. So musste ich neben der Gemeinde Baindt und der Stadt Herbolzheim die Stadt Stuttgart und sogar auch die Rechtsanwaltskammer Stuttgart wegen einer Verletzung ihrer nach § 29 LDSG mir gegenüber bestehenden Unterstützungspflicht förmlich beanstanden. Das waren erfreulicherweise krasse Ausnahmen, in aller Regel konnte ich mich nicht über mangelnde Kooperationsbereitschaft beklagen.

Nicht alles lässt sich im schriftlichen Verfahren oder in Besprechungen erledigen, Besuche vor Ort sind nach wie vor unverzichtbar. Trotz des damit verbundenen Aufwands war es im vergangenen Jahr immerhin möglich, über 30 Kontroll- und Informationsbesuche bei den unterschiedlichsten Behörden und anderen öffentlichen Stellen durchzuführen.

Wie schon in den vergangenen Jahren nahm die Beteiligung am Erlass von Rechts- und Verwaltungsvorschriften und die Beratung von öffentlichen Stellen einen breiten Raum ein. Sei es bei der Erarbeitung des von der Landesregierung angestrebten Einheitlichen Personalverwaltungssystems des Landes, der weiteren Entwicklung der e-Bürgerdienste, dem Projekt „Schulverwaltung ans Netz“, bei Forschungsvorhaben, der Einrichtung von klinischen Tumordokumentationen oder bei zahlreichen anderen Projekten, überall bemühte sich mein Amt dem vielfältigen Beratungsbedarf gerecht zu werden. Last but not least beteiligten sich Mitarbeiter meines Amts an einer ganzen Reihe von Fortbildungs- und Informationsveranstaltungen und leisteten auf diese Weise wichtige Beiträge für einen mit Augenmaß praktizierten Datenschutz.

Allen diesen Aktivitäten, so notwendig und wünschenswert sie auch sind, setzt die geringe Personalausstattung meines Amtes Grenzen. Obwohl sich bei der Aussprache über meinen letzten Tätigkeitsbericht im Landtag alle Fraktionen einig waren, dass eine Personalverstärkung notwendig ist und selbst die Regierungskoalition in ihrer Koalitionsvereinbarung eine Stellenausweitung vorgesehen hatte, weist auch der Haushaltsplan-Entwurf 2002/2003 keine einzige neue Stelle auf. Dabei wäre schon ein zusätzlicher Mitarbeiter kaum mehr als der berühmte Tropfen auf den heißen Stein, so groß ist der Bedarf, wie nicht zuletzt auch der Vergleich mit der Personalausstattung meiner Kolleginnen und Kollegen in anderen vergleichbaren Bundesländern zeigt. Im Übrigen: Nicht nur dass die moderne Informations- und Kommunikationstechnik in steigendem Maße in der öffentlichen Verwaltung eingesetzt wird und damit der Beratungs- und Kontrollbedarf immer mehr zunimmt, auch die Maßnahmen zur Terrorismusbekämpfung erfordern ein aktives Mitwirken meines Amts. Wenn schon die Sicherheitsbehörden neue Datenverarbeitungsbefugnisse erhalten sollen und zum Beispiel im Rahmen der Rasterfahndung zahlreiche unverdächtige Personen in die Ermittlungen einbezogen werden, dann muss bei alledem jedenfalls eine Beratung und Kontrolle durch den Datenschutzbeauftragten möglich sein, die diese Bezeichnung auch verdient. Durchaus zu Recht verstärkt die Landesregierung aus diesem Anlass die Sicherheitsbehörden und stattet sie mit moderner Technik aus. Dem muss aber auf der anderen Seite auch eine zumindest personelle Verstärkung meines Amts folgen, das diese Maßnahmen ja schließlich kritisch zu begleiten hat.

3. Erste Erfahrungen mit dem geänderten Landesdatenschutzgesetz

Die durch europarechtliche Vorgaben veranlasste Novellierung des Landesdatenschutzgesetzes (LDSG) liegt jetzt gut ein Jahr zurück. Die ursprünglichen Befürchtungen, dass die vielen Änderungen im Gesetzestext in der behördlichen Praxis zu Anwendungsproblemen führen könnten, haben sich offenbar nicht bestätigt. Mir sind jedenfalls kaum Anfragen bekannt, in denen um eine Erläuterung der neuen Rechtslage gebeten worden wäre. Auch eine vom Städtetag Baden-Württemberg bei seinen Mitgliedern durchgeführte Umfrage erweckte nicht den Eindruck, dass man sich mit den neuen Regelungen sonderlich schwer tut. Dies kann kaum verwundern, da ja mit der Novelle weitgehend nur alter Wein in neue Schläuche gefüllt wurde – ein Umstand, den ich damals schon beklagt hatte.

3.1 Der behördliche Datenschutzbeauftragte

Eine nicht unbedeutende Änderung erfuhr das Landesdatenschutzgesetz allerdings dadurch, dass dort erstmals der behördliche Datenschutzbeauftragte verankert wurde. Auch wenn der Landtag die Bestellung eines Datenschutzbeauftragten nicht wie von mir gewünscht zur Pflicht gemacht hat, hat die Neuregelung wenigstens bewirkt, dass das Thema „Behördlicher Datenschutzbeauftragter“ seitdem ins Bewusstsein der Verantwortlichen gedrungen ist. Nach meinem Eindruck ist die Bereitschaft, den Datenschutz vor Ort zu stärken, deutlich gestiegen und hat auch schon Früchte getragen. Nicht zuletzt ist dies auch das Verdienst des Innenministeriums, das nicht nur mit gutem Beispiel vorangegangen ist und schnell einen eigenen Datenschutzbeauftragten bestellt hat, sondern engagiert bei staatlichen und kommunalen Behörden für die Bestellung behörtlicher Datenschutzbeauftragter geworben hat.

Einer Übersicht des Städtetags Baden-Württemberg vom September 2000 zufolge hatten zu diesem Zeitpunkt 26 v. H. der Mitglieder, die an der Umfrage teilgenommen hatten, bereits einen eigenen Datenschutzbeauftragten bestellt, 19 v. H. beabsichtigten dies und 55 v. H. hatten dies nicht vor. Seitdem soll die Zahl kommunaler Datenschutzbeauftragter deutlich zugenommen haben, wobei mir konkrete Zahlen nicht vorliegen. Allerdings fällt unangenehm auf, dass es gerade auch Stadtkreise, die eigentlich die personellen Kapazitäten hätten und bei denen dies allein auf Grund des Umfangs der verarbeiteten Daten am ehesten erforderlich wäre, bisher nicht für nötig empfunden haben, für einen wirksamen Datenschutz vor Ort zu sorgen. Und schlicht für unverständlich halte ich es, dass gerade die Landeshauptstadt Stuttgart, der im kommunalen Bereich eigentlich eine Vorreiterrolle zukommt, hier eher als negatives Vorbild angeführt werden muss. Ich habe mich vor kurzem in dieser Sache unmittelbar an die Oberbürgermeister der betroffenen Städte gewandt, um vielleicht doch noch einen Sinneswandel zu erreichen. Aber auch in der Landesverwaltung gibt es hartleibige Behörden, die partout nicht einsehen wollen, dass die Bestellung eines Datenschutzbeauftragten auch in ihrem ureigensten Interesse liegt. Herausragendes Beispiel dafür ist das Landesamt für Besoldung und Versorgung Baden-Württemberg, das doch wahrlich in erheblichem Umfang personenbezogene Daten von großer Sensibilität zu verarbeiten hat.

Insbesondere von kommunaler Seite bin ich wiederholt danach gefragt worden, worin denn nun eigentlich der Vorteil liege, wenn man einen eigenen Datenschutzbeauftragten bestellt. Ich habe mich dazu gegenüber dem Städtetag Baden-Württemberg wie folgt geäußert:

> „Es ist eigentlich eine alte, von den kommunalen Landesverbänden zu Recht oft hervorgehobene Erfahrungstatsache, dass Aufgaben am besten dort erledigt werden, wo sie konkret anfallen. Das gilt auch für die Sicherstellung des Datenschutzes. Angesichts der personellen Ausstattung meiner Dienststelle ist es schlichtweg nicht zu leisten, bei den über 8000 öffentlichen Stellen im Lande nach dem Rechten zu sehen. Eine Vor-Ort-Instanz, die diese wichtige Aufgabe übernehmen würde, würde nicht nur meine Arbeit erleichtern, sondern den Datenschutz insgesamt und damit einen wichtigen Gemeinwohlbelang stärken. In Heller und Pfennig lässt sich das allerdings nicht ausdrücken.
>
> Worum geht es konkret? Eine der Aufgaben des Datenschutzbeauftragten besteht darin, die Behördenmitarbeiter, die mit personenbezogenen Daten umgehen, über die insoweit maßgeblichen Datenschutzbestimmungen zu informieren. Häufig erfolgen Datenschutzverstöße aus Unkenntnis der Rechtslage. Durch Schulungsangebote kann der Datenschutzbeauftragte solche Defizite beseitigen oder zumindest verringern. Sache des Datenschutzbeauftragten ist es auch, die Führungsebene wie auch den einzelnen Mitarbeiter bei konkreten Fragestellungen zu beraten. Gerade bei der Inangriffnahme datenschutzrechtlich relevanter Projekte ist die Einbeziehung des Sachverstands einer Person, die mit den örtlichen Verhältnissen vertraut ist, von unschätzbarem Vorteil. So können Fehler von

vornherein vermieden werden, die bei nachträglichem Erkennen manchmal nur schwer zu reparieren sind und in der Öffentlichkeit für negative Schlagzeilen sorgen können. Die Einschaltung meiner Dienststelle ist mitunter zeitaufwendig und kann zu Verzögerungen bei der Umsetzung von Maßnahmen führen. Auch für den einzelnen Behördenmitarbeiter ist es einfacher, sich mit einem konkreten datenschutzrechtlichen Problem an einen ihm bekannten und leicht zu erreichenden kompetenten Kollegen zu wenden als an eine ihm eher unbekannte Kontrollinstanz. Er wird hierzu im Zweifel auch eher bereit sein, wodurch ebenfalls Fehler bei der Sachbehandlung vermieden werden können. Schließlich ist es Aufgabe des örtlichen Datenschutzbeauftragten, auf die Einhaltung der einschlägigen Datenschutzregelungen hinzuwirken. Er kann dies viel besser als eine zentrale Einrichtung des Landes, da er die handelnden Personen und die Verwaltungsabläufe kennt und, wenn es geboten ist, schnell reagieren kann.

Ein anderer Gesichtspunkt ist, dass das Landesdatenschutzgesetz die öffentlichen Stellen mehrfach verpflichtet, sich an meine Dienststelle zu wenden. So muss ihr beispielsweise der Einsatz und jede wesentliche Änderung automatisierter Verfahren mit einer umfangreichen Beschreibung gemeldet werden. Sind solche Verfahren mit besonderen Risiken verbunden, muss eine Vorabkontrolle stattfinden. Das Untersuchungsergebnis und die Begründung sind mir vorzulegen, bevor das Verfahren eingesetzt werden darf. Dies gilt beispielsweise auch für interne automatisierte Abrufverfahren. Hat die Gemeinde dagegen einen eigenen Datenschutzbeauftragten bestellt, kann die Maßnahme intern abgewickelt werden. Eine Beteiligung meiner Dienststelle ist nicht mehr notwendig. Dies trägt wesentlich zur Verwaltungsvereinfachung und zur Verfahrensbeschleunigung bei.

Zusammengefasst lässt sich aus meiner Sicht sagen, dass die Bestellung eines behördlichen Datenschutzbeauftragten der Forderung nach Dezentralisierung und Herabstufung von Aufgaben auf die kommunale Ebene Rechnung trägt. Sie bewirkt eine Verwaltungsvereinfachung und Verfahrensbeschleunigung, weil Meldepflichten entfallen und datenschutzrechtlich relevante Projekte schneller durchgeführt werden können. Darüber hinaus führt sie zu einer Verbesserung des Schutzes personenbezogener Daten der Bürger und fördert dadurch das Erscheinungsbild der Stadt in der Öffentlichkeit, indem diese zeigt, dass sie in dem sensiblen Bereich des Datenschutzes gewillt ist, ihrer Verantwortung gerecht zu werden.“

Noch gebe ich die Hoffnung nicht auf, dass auch diejenigen, die bisher noch Zurückhaltung üben, ihre Skepsis überwinden und sich für einen eigenen Datenschutzbeauftragten entscheiden.

3.2 Der Wegfall des Datenschutzregisters

Nach dem alten Landesdatenschutzgesetz hatte mein Amt ein Register der von den öffentlichen Stellen eingesetzten automatisierten Verfahren zu führen, das sog. Datenschutzregister. Dazu waren diese verpflichtet, mir eine Reihe von Angaben aus dem von ihnen zu führenden Verfahrensverzeichnis zu melden. Wen dies interessierte, der konnte das Datenschutzregister einsehen oder daraus Auskunft erhalten.

Ich habe dieses Datenschutzregister schon lange für überflüssig gehalten. Zum einen war es nie aktuell und vollständig, weil die meldepflichtigen Stellen insoweit nicht sehr zuverlässig waren. Zum anderen hatte sich in den letzten Jahren praktisch nie jemand dafür interessiert, was in dem Register steht. Als die Änderung des Landesdatenschutzgesetzes anstand, habe ich deshalb darauf gedrängt, dass das Datenschutzregister abgeschafft wird. Dies ist erfreulicherweise auch geschehen. Die neue Rechtslage sieht nun so aus:

Nach § 32 LDSG haben nur noch die öffentlichen Stellen Meldepflichten gegenüber meinem Amt, die keinen eigenen Datenschutzbeauftrag-

ten bestellt haben. Mitzuteilen sind dann der Einsatz und die wesentliche Veränderung automatisierter Verfahren sowie das Verfahrensverzeichnis nach § 11 Abs. 2 LDSG. Da mein Amt nicht mehr verpflichtet ist, die Meldungen in einem Register zu führen, andererseits aber jedermann Anspruch darauf hat zu erfahren, was in dem Verfahrensverzeichnis steht, wurde die Pflicht, diese Angaben verfügbar zu machen, auf die jeweilige öffentliche Stelle übertragen.

Diese sich klipp und klar aus dem Gesetzestext ergebende Änderung der Rechtslage ist bisher offensichtlich vielen öffentlichen Stellen verborgen geblieben. So musste ich z. B. ein Regionales Rechenzentrum, das umfangreiche „Meldungen zum Datenschutzregister nach § 32 LDSG (alt § 28 LDSG)“ übersandt hatte, auffordern, erst einmal zu prüfen, welche Gemeinden, für die es die Daten im Auftrag verarbeitet, einen eigenen Datenschutzbeauftragten bestellt haben und deshalb nicht meldepflichtig sind. Aber nicht nur das. Was mittlerweile mehr als ein Jahr nach In-Kraft-Treten des neuen Rechts nicht mehr hinzunehmen ist, ist der Umstand, dass die vorgelegten Verfahrensverzeichnisse durchweg nicht dem Gesetz entsprechen. Die Gesetzesnovelle vom Mai 2000 hat auch inhaltliche Änderungen für das Verfahrensverzeichnis gebracht, die anscheinend kaum zur Kenntnis genommen werden. Da ich zugunsten der öffentlichen Stellen annehme, dass sie sich nicht bewusst über das Gesetz hinwegsetzen wollen, bleibt eigentlich nur der Schluss, dass sie das Gesetz nicht gelesen haben. Dies zeigt in meinen Augen einmal mehr, dass dem Datenschutz in der Verwaltungspraxis nicht immer die gebührende Aufmerksamkeit geschenkt wird. Denn gerade das Verfahrensverzeichnis ist ein für die Behörden selbst wichtiges Instrument, um zum einen für sich transparent zu machen, welche Verfahren der Datenverarbeitung sie überhaupt einsetzen und welche Rahmenbedingungen hierfür bestehen. Zum anderen ist es Grundlage für die Erfüllung der Informationspflicht gegenüber interessierten Bürgern, aber auch für mögliche Kontrollen durch mein Amt. Hier besteht also noch erheblicher Nachholungs- und Nachbesserungsbedarf. Es ist zu hoffen, dass zunehmend behördliche Datenschutzbeauftragte bestellt werden, deren Aufgabe unter anderem auch das Führen des Verfahrensverzeichnisses ist und die diesem aus Sicht des Datenschutzes wichtigen Kontrollinstrument vermehrt Aufmerksamkeit widmen.

3.3 Die Beteiligung am Erlass von Rechts- und Verwaltungsvorschriften

Neu in das Landesdatenschutzgesetz aufgenommen wurde eine Bestimmung, wonach der Landesbeauftragte für den Datenschutz bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften zu beteiligen ist, wenn diese die Verarbeitung personenbezogener Daten betreffen (§ 31 Abs. 3 Satz 2 LDSG). Diese Vorschrift hat zu Missverständnissen geführt. Nimmt man sie nämlich wörtlich, würde dies bedeuten, dass alle Kommunen sowie sämtliche sonstigen Körperschaften und Anstalten des öffentlichen Rechts, die eine Rechtsverordnung, Satzung oder Verwaltungsvorschrift neu erlassen oder wesentlich ändern wollen, meine Dienststelle beteiligen müssten, soweit (auch) die Verarbeitung personenbezogener Daten betroffen ist. Da diese Voraussetzung bei den meisten derartigen Vorschriften gegeben ist, kann diese Interpretation wegen der damit verbundenen Folgen vom Landtag so nicht gewollt sein. Damit würden nämlich die Kapazität meiner Dienststelle hoffnungslos überfordert und die Stellen, die solche Regelungen erlassen wollen, ganz erheblich belastet werden. Sowohl im eigenen, wie aber auch in deren Interesse halte ich deshalb, übrigens entgegen der Auffassung des Innenministeriums, eine restriktive Auslegung des § 31 Abs. 3 Satz 2 LDSG für geboten und gehe davon aus, dass meine Dienststelle nur dann zwingend zu beteiligen ist, wenn es um die Ausarbeitung von Rechts- und Verwaltungsvorschriften durch die Landesregierung, einzelne Ministerien oder sonstige Behörden des Landes geht. Den anderen Behörden bleibt es selbstverständlich nach wie vor unbenommen, sich in solchen Fällen an mich zu wenden und sich beraten zu lassen.

2. Teil: Öffentliche Sicherheit und Justiz

1. Folgen des Terroranschlags

Nach den Terroranschlägen vom 11. September 2001 in New York und Washington kam die größte Verbrecherjagd der Kriminalgeschichte in Gang. Seither suchen in den Vereinigten Staaten und in Europa Tausende Polizisten nach den Attentätern. Schnell zeigte sich, dass eine Spur nach Deutschland führt. Ein Mann aus Ägypten, der die erste Maschine in das World Trade Center geflogen haben soll, hatte bis dahin unauffällig in Hamburg gelebt und an der dortigen Universität sein Diplom als Stadtplaner gemacht. Kaum war dies bekannt geworden, kamen aus dem politischen Raum zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit mit gravierenden Auswirkungen auf den Datenschutz. Der Bundesinnenminister forderte ganz pauschal eine generelle Einschränkung des Datenschutzes, andere sprachen gar davon, der Datenschutz müsse entrümpelt werden. Dass die Sicherheits- und Strafverfolgungsbehörden bereits über weitreichende Befugnisse zur Terrorismusbekämpfung verfügen, blieb unerwähnt. So ist beispielsweise die Rasterfahndung zur Strafverfolgung generell möglich, inzwischen in allen Bundesländern auch zur Gefahrenabwehr durch die Polizei. Die Ausländerämter und das Bundesamt für die Anerkennung ausländischer Flüchtlinge können bereits heute Erkenntnisse über terroristische Aktivitäten an Polizei und Verfassungsschutz übermitteln. An einer effektiven Zusammenarbeit mit dem Verfassungsschutz ist die Polizei jedenfalls durch die geltende Rechtslage nicht gehindert; umgekehrt gilt dasselbe. Vorgeschlagen wurde, was technisch machbar scheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist.

1.1 Die Rasterfahndung

Ende September 2001 übersandte das Innenministerium meinem Amt die Verfügungen, mit denen der Präsident des Landeskriminalamtes diverse Rasterfahndungen angeordnet hatte. Nach einer Besprechung überarbeiteten Landeskriminalamt und Innenministerium die Verfügungen. Durchgreifende Bedenken dagegen bestehen jetzt nicht mehr. § 40 des Polizeigesetzes räumt nämlich der Polizei eine recht großzügige Befugnis für Rasterfahndungen ein. Nach dieser Vorschrift kann die Polizei von öffentlichen und nichtöffentlichen Stellen die Übermittlung von Daten bestimmter, in automatisierten Dateien gespeicherter Personengruppen zum Zwecke des maschinellen Abgleichs mit anderen in automatisierten Dateien gespeicherten Datenbeständen verlangen, wenn dies zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Die Übermittlung ist dabei auf Namen, Anschrift, Tag und Ort der Geburt der betroffenen Personen sowie auf im Einzelfall festzulegende Merkmale zu beschränken. Mit der Rasterfahndung will die Polizei islamistischen Gewalttätern und so genannten Schläfern, mithin also Personen auf die Spur kommen, die sich dem hiesigen Lebensstil angepasst haben, um irgendwann als Terrorist aktiv zu werden. Um sie zu finden werden in einem ersten Schritt anhand der Melderegister Personen ermittelt, die aus bestimmten Staaten stammen; von 270 000 Personen ist die Rede. Deren Daten sollen mit Datenbeständen einer ganzen Reihe anderer Stellen, darunter beispielsweise von Universitäten und Hochschulen, abgeglichen werden. Am Ende, so die Idee, werden 10 bis 20 Personen übrig bleiben, die die Polizei dann näher unter die Lupe nehmen will. All dies und weitere Einzelheiten waren inzwischen in der Presse nachzulesen.

Ob die Rechnung aufgeht, weiß trotz des enormen Aufwands, mit dem die Polizei die Rasterfahndung betreibt, niemand. Diese Fahndungsmethode führte schon bei der Suche nach RAF-Terroristen kaum zu nennenswerten Erfolgen. Diesmal wird es wahrscheinlich nicht anders sein. Die Aussicht, mit einer Rasterfahndung einen wirklichen Treffer zu landen, ist nach den damaligen Erfahrungen schon gering genug. Sie nimmt umso mehr ab, je grobmaschiger das Raster ist, und allzu eng ist es bei den aktuellen Datenbankabgleichen nun wirklich nicht. Ganz gleich was am Ende heraus kommt: Meine Aufgabe sehe ich in der ak-

tuellen Situation vor allem darin, darauf zu achten, dass die Rasterfahndung nach den dafür vorgesehenen Regeln abläuft und dass dabei in die Datenschutzrechte der vielen, vielen Betroffenen nicht mehr als unerlässlich notwendig eingegriffen wird. Dazu gehört vor allem, dass nicht mehr Daten angeliefert werden, als vom Landeskriminalamt verlangt worden sind und dass zusätzliche Daten nur dann an das Landeskriminalamt gelangen, wenn sie sich von den in der jeweiligen Rasterfahndungsanordnung aufgezählten Angaben wirklich nur mit unverhältnismäßig großem Aufwand trennen lassen. Selbstverständlich wird sich unser ganz besonderes Augenmerk darauf richten, dass solche zusätzlichen Daten nicht verwendet und dass nach Abschluss der Rasterfahndung die übermittelten sowie die im Zusammenhang mit dem Abgleich angefallenen Daten ordnungsgemäß gelöscht werden.

1.2 Das Terrorismusbekämpfungsgesetz

Keine Frage: Der Datenschutz ist keine ein für allemal feststehende Größe. Er muss sich immer wieder bewähren und neuen Fragen stellen. Deshalb kann man sich in der gegenwärtigen, schwierigen Situation Forderungen nach Einschränkungen kaum verschließen, wenn deren Notwendigkeit nachgewiesen ist. Das setzt jedoch voraus, dass zuerst geprüft werden muss, was jetzt schon möglich ist und ob das auch praktiziert wird oder ob es Vollzugsdefizite bei der Anwendung der geltenden Regelungen über die Datenverarbeitung gibt. Davon ist im Entwurf eines Terrorismusbekämpfungsgesetzes, den die Bundesregierung vor kurzem dem Bundesrat zugeleitet hat, nicht die Rede. Er ist zwar gegenüber dem Referentenentwurf des Bundesinnenministeriums etwas moderater ausgefallen. Gleichwohl sieht er aber immer noch für Sicherheits- und Ausländerbehörden neue Befugnisse vor, die das Grundrecht auf Datenschutz ganz erheblich strapazieren. Kritikpunkte sind insbesondere:

– Das Bundeskriminalamt soll bei sämtlichen öffentlichen und nichtöffentlichen Stellen Daten zur Erfüllung seiner Aufgabe als Zentralstelle oder sonst zu Zwecken der Auswertung erheben dürfen. Damit würde die unterstützende Zentralstellenfunktion des Bundeskriminalamts ausgeweitet und ihm eine Grauzone für Ermittlungen im Vorfeld eines Tatverdachts eröffnet.

– Dem Bundesamt für Verfassungsschutz sollen umfangreiche Auskunftsansprüche gegenüber Banken, Post-, Telekommunikations- und Teledienstunternehmen eingeräumt werden. Wenn es nach dem Entwurf geht, müssen

  • Kreditinstitute, Finanzdienstleistungsinstitute und Finanzunternehmen über Konten, Konteninhaber und sonstige Berechtigte sowie weitere am Zahlungsverkehr Beteiligte und über Geldbewegungen und Geldanlagen Auskunft geben;

  • Personen und Unternehmen, die Postdienstleistungen erbringen, Namen, Anschriften, Postfächer und sonstige Umstände des Postverkehrs offen legen;

  • Telekommunikations- und Teledienstunternehmen Auskünfte über Verbindungs- und Nutzungsdaten geben, dem Verfassungsschutz also beispielsweise mitteilen, wer wann von wo aus mit welchem Handy mit wem telefoniert oder wer wem wann eine E-Mail geschickt hat;

  • Luftfahrtunternehmen Auskunft über Namen, Anschriften und zur Inanspruchnahme von Transportleistungen und sonstigen Umständen des Luftverkehrs geben.

  Mit diesen Auskunftspflichten, die ein Novum darstellen, gehen ganz gravierende Eingriffe in das Datenschutzrecht der Betroffenen einher, weil sie unabhängig davon Platz greifen sollen, ob sich die Betroffenen in irgendeiner Weise strafrechtlich verdächtig gemacht haben und weil die Betroffenen von solchen Auskünften praktisch nichts erfahren.

– Biometrische Merkmale sollen in Pässe und Personalausweise aufgenommen werden können. Unklar ist schon, was das für die Terrorismusbekämpfung bringen soll, zumal andere Länder wie Frankreich, Großbritannien und die USA gar keinen Personalausweis haben und auch jetzt nicht daran denken, einen solchen einzuführen. Zudem lässt der Gesetzentwurf offen, ob die biometrischen Merkmale in Referenzdateien gespeichert werden dürfen. Er sagt auch nichts dazu, welche Nutzungen der biometrischen Merkmale durch andere Stellen möglich und geplant sind.

– In einer Vielzahl von ausländerrechtlichen Bestimmungen wird in das Datenschutzrecht von Ausländern eingegriffen, ohne den Nachweis zu führen, dass dies im überwiegenden Allgemeininteresse unbedingt notwendig ist. Zu weit geht auf jeden Fall, dass Angaben über die Religionszugehörigkeit von Ausländern in staatlichen Informationssystemen erfasst werden sollen, obwohl unsere Verfassung dem Staat die Frage nach der Religionszugehörigkeit nur gestattet, wenn davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert. Inakzeptabel ist aber auch, dass sensible Angaben aus Asylanträgen ohne Schutzvorkehrungen an die Geheimdienste übermittelt werden können und selbst die Weiterübermittlung an den Geheimdienst des Heimatlandes möglich ist.

– Um dem Bundesamt für Verfassungsschutz die Arbeit zu erleichtern, sollen die bisher üblichen 5- und 10-jährigen Speicherfristen auf 10 bzw. 15 Jahre ausgedehnt werden.

2. Die Mitwirkung am Erlass von Rechts- und Verwaltungsvorschriften

Die Beratung der Ressorts bei der Erarbeitung von Rechts- und Verwaltungsvorschriften ist ein wichtiger Teil der Aufgaben, die das Landesdatenschutzgesetz meinem Amt zugewiesen hat. Damit wir dieser Aufgabe nachkommen können, ist es unerlässlich, dass wir möglichst frühzeitig von Regelungsabsichten und Entwürfen Kenntnis erhalten. Insbesondere mit dem Justizministerium gab es damit in der Vergangenheit immer wieder Probleme (vgl. 20. Tätigkeitsbericht, LT-Drs. 12/4600, S. 70 f.). Das setzte sich leider auch im Berichtsjahr fort. Neuerdings scheint sich jedoch ein Wandel anzubahnen, eine Entwicklung, die ich nur begrüßen kann.

Auch heuer hatten wir uns wieder mit einer Reihe von Regelungsvorhaben zu befassen, exemplarisch hiervon Folgende:

– Von dritter Seite und nicht vom Justizministerium ging uns der Referentenentwurf für eine Nachfolgeregelung zu § 12 des Gesetzes über Fernmeldeanlagen (FAG) zu. Diese Bestimmung tritt mit Ablauf des 31. Dez. 2001 außer Kraft. Sie räumt bisher den Strafverfolgungsbehörden die Befugnis ein, von Telekommunikationsunternehmen zur Verfolgung jedweder Straftat Auskunft über Telekommunikationsverbindungsdaten zu verlangen. Angesichts der Digitalisierung der Telekommunikation und der massenhaften Nutzung der neuen Medien werden immer mehr personenbezogene Daten elektronisch übertragen und gespeichert und können dadurch mit geringem Aufwand in großem Umfang ausgewertet werden. Anhand der Telekommunikationsverbindungsdaten kann man nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Allein durch die Verbindungsdaten können daher Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Damit ermöglicht § 12 FAG massive Eingriffe in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung selbst zur Verfolgung geringfügiger Straftaten. Zur Wahrung des Grundsatzes der Verhältnismäßigkeit ist deshalb eine Überarbeitung dieser Vorschrift längst überfällig. Wie die Befristung ihrer Geltungsdauer zeigt, sah dies bisher auch der Bundesgesetzgeber so. Der Gesetzentwurf der Bundesregierung, der aus datenschutzrechtlicher Sicht durchaus verbesserungsfähig gewesen wäre, war dem Bundesrat dann allerdings viel zu datenschutzfreundlich. Wenn es nach ihm geht, sollen die Telekommunika-

tionsunternehmen den Strafverfolgungsbehörden sogar über zurückliegende Aktivmeldungen von Mobiltelefonen selbst bei reinem Stand-by-Betrieb Auskünfte erteilen und eigens für Zwecke der Strafverfolgung Telekommunikationsverbindungsdaten aufzeichnen müssen. Zwischenzeitlich hat sich die Bundesregierung im Wesentlichen gegen die Vorschläge des Bundesrates ausgesprochen. Es bleibt daher zu hoffen, dass die vom Bundesrat vorgeschlagenen Verschärfungen nicht Gesetz werden.

– Mit dem Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung und anderer Gesetze sollen Bekanntmachungen in Insolvenzverfahren im Internet ermöglicht werden, damit die Kosten für die vorgeschriebenen Bekanntmachungen, die üblicherweise über die Tageszeitung erfolgen, bei den Gerichtskosten nicht so zu Buche schlagen. Dabei darf aber der Datenschutz nicht auf der Strecke bleiben. Anders als bei den herkömmlichen Bekanntmachungen in Printmedien lässt sich im Internet die Verbreitung der Informationen weder zeitlich noch räumlich begrenzen. Zudem können die Daten auf vielfältige Weise ausgewertet werden. Dies kann dazu führen, dass Dritte die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und über längere Zeit im Internet verfügbar halten. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit am Schuldenpranger stehen. Der Gesetzentwurf hat inzwischen Bundestag und Bundesrat passiert. Er sieht jetzt eine Ermächtigung für das Bundesministerium der Justiz vor, durch Rechtsverordnung Löschungsfristen zu bestimmen. Es soll auch sicherstellen, dass die Veröffentlichungen im Internet unversehrt, vollständig und aktuell bleiben, jederzeit ihrem Ursprung nach zugeordnet und nach dem Stand der Technik durch Dritte nicht kopiert werden können. Ein Entwurf der Verordnung liegt bereits vor. Damit zeichnet sich ein akzeptabler Kompromiss ab.

– Mit dem Referentenentwurf eines Gesetzes zur Änderung des Ordnungswidrigkeitenverfahrensrechts will das Bundesministerium der Justiz – um es mit den Worten des Entwurfs zu sagen – das Ordnungswidrigkeitengesetz an die mit dem Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) geschaffenen Regelungen zur Erteilung von Auskünften und Akteneinsicht aus Strafverfahren, zur sonstigen Verwendung von Daten für verfahrensübergreifende Zwecke sowie zur Verwendung personenbezogener Daten in Dateien anpassen. Wer weiß, dass dieses Ziel mithilfe zahlreicher Verweisungen erreicht werden soll, die zudem nur schwer lesbar und völlig unübersichtlich sind, kann sich leicht vorstellen, was da herauskommen kann. Deshalb liegt mir viel daran, dass auf Verweisungen so weit wie möglich verzichtet wird und die entsprechenden Regelungen dafür im Ordnungswidrigkeitengesetz ausformuliert werden.

– Die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) sind um eine Bestimmung zum Opferschutz ergänzt worden, ehe wir davon erfuhren. Sie soll eine besonders sensible Behandlung von Lichtbildern sicherstellen, die Opfer von Sexualstraftaten ganz oder teilweise unbekleidet zeigen. Der Anwendungsbereich dieser Bestimmung beschränkt sich jedoch auf Lichtbilder, die zu Beweiszwecken gefertigt wurden. Diese Bemühungen um den Opferschutz in allen Ehren. Aber warum blieb es bei diesem halben Schritt in die richtige Richtung? Für einen wirksamen Opferschutz darf es keine Rolle spielen, zu welchem Zweck die Lichtbilder angefertigt worden sind. Ich habe beim Justizministerium daher angeregt, sich für eine entsprechende Änderung der eingefügten Vorschrift einzusetzen. Ob das Justizministerium dem entspricht, weiß ich nicht.

– Das Justizministerium schien sich auch nicht für die Auffassung meines Amtes zu der Frage zu interessieren, ob es nötig ist, Beschuldigte wenigstens über die Einstellung des Ermittlungsverfahrens zu informieren, wenn sie bis dahin nichts von dem Ermittlungsverfahren mitbekommen haben. Eine entsprechende Umfrage des Bundesministeriums der Justiz hatte es lieber für sich behalten. Mit der Einleitung eines staatsanwaltschaftlichen Ermittlungsverfahrens gehen besonders sensible Datenspeicherungen einher. Deshalb muss der Beschuldigte die Möglichkeit haben, seine Aus-

kunfts-, Berichtigungs- und Sperrungsansprüche geltend zu machen. Dies setzt aber voraus, dass er weiß, dass gegen ihn ein Ermittlungsverfahren gelaufen ist. Deshalb habe ich eine entsprechende Änderung von § 170 StPO vorgeschlagen. Beim Justizministerium stießen wir auf taube Ohren. Das Bundesministerium der Justiz will prüfen.

– Kurz vor Ablauf der letzten Legislaturperiode verabschiedete der Landtag das Gesetz über die Unterbringung besonders rückfallgefährdeter Straftäter (Straftäter-Unterbringungsgesetz – StrUBG). Dieses, in der juristischen Literatur heiß diskutierte Gesetz ist das erste seiner Art in der Bundesrepublik und ermöglicht die Unterbringung von Strafgefangenen über das Ende ihrer Strafhaft hinaus. Nach § 4 dieses Gesetzes hat die zuständige Strafvollstreckungskammer in öffentlicher Verhandlung die für die Entscheidung wesentlichen Tatsachen mit den Verfahrensbeteiligten zu erörtern. In einer solchen Verhandlung können vielerlei Informationen über den Betroffenen bis hin zu Dingen aus dessen innerstem Lebensbereich zur Sprache kommen. Dies zeigt sich bereits daran, dass vor einer Anordnung der Unterbringung zwei voneinander unabhängige Sachverständige zu hören sind. Dabei wird das gesamte Verhalten des Betroffenen im Strafvollzug samt seinen familiären oder sonstigen Bindungen erörtert werden. Dass der Betroffene und die Personen, deren Lebensumstände hierbei angesprochen werden, ein berechtigtes Interesse daran haben, dass diese Umstände nicht vor der Öffentlichkeit ausgebreitet werden, liegt auf der Hand. Ich habe deshalb dafür plädiert, dass die Entscheidung über die Unterbringung in dem für Strafvollstreckungskammern üblichen nichtöffentlichen Beschlussverfahren ergeht oder zumindest die Vorschriften des Gerichtsverfassungsgesetzes über den Ausschluss der Öffentlichkeit uneingeschränkt anwendbar bleiben. Das Innenministerium konnte sich daraufhin gerade mal zu einem Hinweis in der Gesetzesbegründung durchringen, dass die im Gerichtsverfassungsgesetz vorgesehenen Möglichkeiten, die Öffentlichkeit im Einzelfall auszuschließen, unberührt bleiben. Hoffentlich ist der Hinweis nicht zu gut versteckt.

– Das Innenministerium verlängerte die Aussonderungsprüffristen für Erwachsene, die mutmaßlich oder tatsächlich ein „einfaches“ Sexualdelikt oder eine vergleichbare sexuell motivierte Straftat begangen haben, auf 10 Jahre und für Jugendliche auf 5 Jahre. Dem hätten wir nur zustimmen können, wenn die bis dahin üblichen drei- und fünfjährigen Aussonderungsprüffristen für „einfache“ Sexualdelikte zu Unzuträglichkeiten bei der Verfolgung von Sexualdelikten geführt hätten. Solche Umstände hat das Innenministerium indes nicht dargetan; dafür ist angesichts der ohnehin recht langen Aussonderungsprüffristen auch nichts ersichtlich. Für die allermeisten Sexualdelikte bis hin zu exhibitionistischen Handlungen ist nämlich bereits seit 1999 für Erwachsene und Jugendliche eine 20-jährige Aussonderungsprüffrist vorgesehen. Die Fristen beginnen zudem vor der Entlassung des Täters aus der Haft gar nicht zu laufen. Kommt während der offenen Frist ein anderes Delikt hinzu, bleiben alle Delikte gespeichert bis die längste Aussonderungsprüffrist abgelaufen ist. Deshalb sind in über der Hälfte aller Fälle mutmaßlich oder tatsächlich begangene Sexualdelikte in der Personenauskunftsdatei (PAD) der baden-württembergischen Polizei immer noch registriert, obwohl die für diese Delikte übliche Aussonderungsprüffrist längst abgelaufen ist. Selbst nach Ablauf der längsten Aussonderungsprüffrist erfolgt die Löschung nicht automatisch. Vielmehr kann die Polizei die Speicherung, wenn die Kenntnis der Daten zur Erfüllung ihrer Aufgaben weiterhin erforderlich ist, jeweils um drei Jahre verlängern. Dass bei diesen weit reichenden Möglichkeiten der Polizei, Daten von Personen in ihrer Personenauskunftsdatei zu speichern, wieder einmal das unsägliche Wortspiel vom Datenschutz und Täterschutz ins Feld geführt wurde, kann ich mir nur mit dem Fehlen von Argumenten erklären.

3. Die polizeiliche Videoüberwachung

Mitte November 2000 brachte die Landesregierung einen Entwurf zur Änderung des Polizeigesetzes und des Meldegesetzes in den Landtag ein. Kernpunkt dieses Gesetzentwurfs war die Ergänzung des Polizeigesetzes

um eine Regelung der polizeilichen Videoüberwachung. Bereits vier Wochen später hatte die vorgeschlagene Regelung den Landtag unverändert passiert und trat am 29. Dez. 2000 in Kraft. Seitdem können, um es mit den Worten des Polizeigesetzes zu sagen, der Polizeivollzugsdienst und die Ortspolizeibehörden zur Abwehr von Gefahren, durch die die öffentliche Sicherheit bedroht wird, oder zur Beseitigung von Störungen der öffentlichen Sicherheit die in § 26 Abs. 1 Nr. 2 des Polizeigesetzes genannten Orte, soweit sie öffentlich zugänglich sind, offen mittels Bildübertragung beobachten und Bildaufzeichnungen von Personen fertigen. Die Bildaufzeichnungen sind nach 48 Stunden zu löschen, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten länger benötigt werden. Damit waren die berechtigten Datenschutzbelange der Bürger leider wieder einmal zu kurz gekommen. Statt, was ausgereicht hätte, wenigstens den Aufzeichnungsknopf erst dann zu drücken, wenn sich vor den Objektiven der Überwachungskameras etwas Verdächtiges abspielt, darf die Polizei permanent sämtliche Videobilder für die Dauer von 48 Stunden aufzeichnen. So avancieren aber völlig unverdächtige Bürger und nicht die Personen, die Delikte der Straßenkriminalität im Schilde führen und denen die polizeiliche Videoüberwachung erklärtermaßen gilt, zu Hauptdarstellern auf den Videofilmen der Polizei. Mit der Verabschiedung der Ergänzung des Polizeigesetzes durch den Landtag war die Diskussion über das Für und Wider der polizeilichen Videoüberwachung praktisch beendet. Jetzt ging und geht es allein noch um die praktische Umsetzung der neuen Regelungen.

3.1 Die Verwaltungsvorschrift

Nicht alle Gesetze sind ohne weiteres praktikabel. Manche bedürfen näherer Erläuterungen durch Verwaltungsvorschriften ehe sie im Alltag zur Anwendung kommen. Gerade so liegen die Dinge bei den im Polizeigesetz geschaffenen Vorschriften zur polizeilichen Videoüberwachung. Wer sich die oben zitierten Regelungen in Erinnerung ruft, weiß warum: Kein Wort, geschweige denn eine gesetzliche Definition dazu, was eigentlich unter dem Begriff eines Kriminalitätsbrennpunkts zu verstehen ist. Nichts Näheres darüber, was es in der Praxis bedeutet, dass die Videoüberwachung offen erfolgen muss. Keine Vorschrift dazu, wer bei der Polizei eine Videoüberwachung anordnen kann. Und vor allem auch nichts Näheres zu den Anforderungen, die an die Begründung der Anordnung einer polizeilichen Videoüberwachung zu stellen sind. Festlegungen hierzu sind aber notwendig, damit die Polizei bei einer Videoüberwachung nicht stärker als unausweichlich in die Grundrechte der ins Visier zu nehmenden Personen eingreift und Grundrechte anderer Personen keinesfalls verletzt werden.

Diese Festlegungen traf das Innenministerium alsbald nach dem In-Kraft-Treten der Änderung des Polizeigesetzes in einer Verwaltungsvorschrift, der sog. Führungs- und Einsatzanordnung Videoüberwachung im öffentlichen Raum. Wenn auch nicht alle unsere Hinweise und Vorschläge, die ich dem Innenministerium dazu unterbreitet habe, darin ihren Niederschlag gefunden haben, so ist damit doch immerhin Folgendes klar:

- Als Kriminalitätsbrennpunkt kann nur ein öffentlich zugänglicher Ort in Frage kommen, an dem nach Auswertung lokaler Kriminalitätslagebilder ein erhöhtes Gefährdungspotential für die öffentliche Sicherheit besteht, weil sich dort erfahrungsgemäß Straftäter verbergen oder Personen Straftaten verabreden, vorbereiten oder begehen. Der Ort muss sich dabei in seiner Kriminalitätsbelastung deutlich von anderen Orten abheben. Wesentliche Grundlage für die Einstufung eines Ortes als Kriminalitätsbrennpunkt bilden die Straftaten, die typischerweise zur sog. Straßenkriminalität zählen.
- Die Anordnung einer Videoüberwachung durch den Polizeivollzugsdienst ist Sache des Leiters einer Landespolizeidirektion, der Wasserschutzpolizeidirektion, eines Polizeipräsidiums oder einer Polizeidirektion. Die Anordnung muss schriftlich erfolgen.
- In der Anordnung sind das Einsatzziel und die Gründe für die polizeiliche Videoüberwachung anzugeben. Allein statistische Angaben

reichen dabei nicht. Vielmehr sind die Gefahren für die öffentliche Sicherheit und die sie begründenden tatsächlichen Anhaltspunkte anhand spezieller örtlicher Lagebilder unter besonderer Berücksichtigung der Straßenkriminalität und anderer Straftaten, die das Sicherheitsgefühl der Bevölkerung besonders beeinträchtigen, konkret darzulegen. Dazu gehören notwendigerweise nähere Angaben sowohl über die bisherigen Geschehnisse an dem betreffenden Ort und deren Bedeutung für dessen Einstufung als Kriminalitätsbrennpunkt wie auch zu der Prognose, dass es an diesem Ort weiterhin zu solchen Straftaten kommen wird und weshalb die Videoüberwachung zur Bekämpfung dieser Straftaten notwendig ist.

– Die polizeiliche Videoüberwachung muss offen erfolgen. Wer einen kameraüberwachten Ort betritt, muss erkennen können, dass er einer polizeilichen Videoüberwachung ausgesetzt ist. Darauf ist durch Schilder hinzuweisen, die leicht verständlich und gut erkennbar sein müssen und in ausreichender Zahl anzubringen sind.

– Ordnet eine Polizeidienststelle die Videoüberwachung eines Kriminalitätsbrennpunktes an, muss sie in einer Dienstanweisung auch die technischen und organisatorischen Maßnahmen regeln, die einen datenschutzgerechten Umgang mit den aufgezeichneten Videobildern gewährleisten.

3.2 Die Realisierung

Während mancherorts Stadtverwaltung und Polizei unisono erklärt haben, dass es in ihren Mauern keinen Kriminalitätsbrennpunkt gibt, sprachen sich Stadtverwaltung und Polizei in Stuttgart und Mannheim von Anfang an für den Einsatz der polizeilichen Videoüberwachung aus. Inzwischen gesellte sich Heilbronn zu ihnen. In Mannheim läuft die polizeiliche Videoüberwachung bereits. In Stuttgart sind die Planungen für die Videoüberwachung des Rotebühlplatzes schon weit gediehen. Mit diesen beiden Vorhaben haben wir uns näher befasst.

3.2.1 Mannheim

„Die Polizei sieht alles“, „Mannheim macht den Vorreiter bei der Kameraüberwachung“, so lauteten schon im Sommer 2000 die Schlagzeilen in der Presse. Damals hatte der Gemeinderat der Stadt Mannheim der von der Stadtverwaltung in Absprache mit dem Polizeipräsidium Mannheim vorgeschlagenen Teilnahme an einem Pilotprojekt zur Videoüberwachung des Paradeplatzes, des Marktplatzes und des Bereichs um das Neckartor zugestimmt. Lokalpolitikern, Stadträten und sogar veritablen Innenministern führten Polizeipräsidium und Stadt Mannheim ihre Testanlage vor. Als wir fragten, nach welchen Kriterien die für die Videoüberwachung vorgesehenen Plätze ausgesucht worden sind, insbesondere welche Straftaten, die sich dort ereignet haben, der Auswahl zu Grunde liegen, und welche Technik zur Videoüberwachung eingesetzt wird, gaben sich Stadt und Polizeipräsidium wesentlich zugeknöpfter. Viel mehr als Statistiken und allgemeine Hinweise auf polizeiliche Erfahrungen sowie die Versicherung, die gebotenen technischen Datenschutzmaßnahmen seien getroffen, bekamen wir aus Mannheim nicht zu lesen. Weil sich trotz wiederholter, sich über ein Jahr hinziehender Nachfragen und eingehender Hinweise die Sache im schriftlichen Verfahren nicht klären ließ, schauten wir uns die Videoüberwachung in Mannheim vor Ort an. Wer gedacht hat, dass es dort eine aussagekräftige Anordnung für die Videoüberwachung gibt, die wenigstens den Anforderungen der bis dahin immerhin schon über ein halbes Jahr alten Führungs- und Einsatzanordnung des Innenministeriums entspricht, der sieht sich ebenso enttäuscht wie derjenige, der die Zusicherung, die notwendigen technischen Datenschutzmaßnahmen seien getroffen, für bare Münze genommen hat. Jetzt die Mängel der Reihe nach:

– Kriminalitätsbrennpunkte nicht belegt

Das Polizeipräsidium Mannheim überwacht seit 26. Juli 2001 den Paradeplatz, den Marktplatz und den Bereich des Neckartors in Mannheim mit Videokameras. 6 der 8 beschafften Videokameras waren im Zeitpunkt unseres Kontrollbesuchs in Betrieb. Die Videobilder laufen im Führungs- und Lagezentrum des Polizeipräsidiums auf Überwachungsmonitoren auf. Dort werden sie von Polizeibeamten live verfolgt und automatisiert aufgezeichnet. Die Videoüberwachung hat das Polizeipräsidium am 25. Juli 2001 schriftlich angeordnet. Die Anordnung lautet so:

„Gemäß § 21 Abs. 3 PolG-BW wird die offene Bildaufzeichnung für die Bereiche des
1. Markplatzes G 1,
2. Paradeplatzes O 1,
3. Neckartores
ab dem 26. Juli 2001 zunächst für die Dauer von 6 Monaten angeordnet. Gemäß § 21 Abs. 4 PolG-BW sind Bildaufzeichnungen nach Absatz 3 nach 48 Stunden zu löschen, sofern sie nicht im Einzelfall zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich sind.

Gründe:
Gemäß § 21 Abs. 3 PolG-BW kann der Polizeivollzugsdienst zur Beseitigung von Störungen der öffentlichen Sicherheit und Ordnung an Orten, an denen sich erfahrungsgemäß Straftäter verbergen oder Personen Straftaten verabreden, vorbereiten oder verüben (§ 26 Abs. 1 Nr. 2 PolG-BW), soweit sie öffentlich zugängliche Orte sind, mittels Bildübertragung beobachten und Bildaufzeichnungen von Personen fertigen.

Bei den o. g. Örtlichkeiten handelt es sich um Orte i. S. von § 26 Abs. 1 Nr. 2 PolG-BW. Sie sind als Kriminalitätsbrennpunkte bekannt und mittels statistischer Auswertung belegt (siehe hierzu Anlage 1).“

Diese Anordnung gibt keinen Aufschluss über die Gründe für die Videoüberwachung. Sie wiederholt lediglich den Gesetzestext, sagt aber kein Wort dazu, auf Grund welcher konkreten Vorkommnisse das Polizeipräsidium angenommen hat, dass es sich beim Marktplatz, beim Paradeplatz oder beim Neckartor um Kriminalitätsbrennpunkte handelt. Statt – was auch nach der oben erwähnten Führungs- und Einsatzanordnung des Innenministeriums geboten gewesen wäre – anhand spezieller örtlicher Lagebilder wenigstens konkret darzulegen, welche Delikte der Straßenkriminalität und welche anderen Straftaten, die das Sicherheitsgefühl der Bevölkerung besonders beeinträchtigen, sich auf dem Marktplatz und dem Paradeplatz sowie am Neckartor zugetragen haben und welche Bedeutung ihnen für die Einstufung dieser Plätze als Kriminalitätsbrennpunkte zukommt, begnügte sich das Polizeipräsidium mit einem dürren Verweis auf vier Statistiken. Auf statistische Angaben allein lässt sich aber eine Videoüberwachung schon deshalb nicht stützen, weil sich den nackten Zahlen nichts zu der hier maßgeblichen Frage entnehmen lässt, welcher Vorfall sich jeweils dahinter verbirgt und welche Bedeutung ihm für die Einstufung eines Ortes als Kriminalitätsbrennpunkt zukommt. Dass sich zwei Statistiken gar nicht auf die videoüberwachten Plätze beziehen, kommt hinzu. Ins Bild passt auch, dass das Polizeipräsidium unserer Wochen vorher schriftlich geäußerten Bitte, zum Kontrollbesuch exemplarisch die Akten und Unterlagen bereitzulegen, die den in den beiden anderen Statistiken für den Paradeplatz ausgeworfenen Zahlenangaben zu Grunde liegen, nicht entsprochen hatte. Deshalb konnten wir uns – in der Anordnung des Polizeipräsidiums vom 25. Juli 2001 stand

dazu ja nichts – kein Bild davon machen, welche Fälle überhaupt hinter diesen Zahlenangaben stehen.

Nach alledem leidet die Anordnung des Polizeipräsidiums Mannheim an einem gravierenden Mangel: Das Vorliegen der gesetzlichen Voraussetzungen, die § 21 Abs. 3 des Polizeigesetzes an den Einsatz einer polizeilichen Videoüberwachung stellt, ist nicht belegt. Will das Polizeipräsidium Mannheim die Videoüberwachung weiterführen, muss es deshalb zunächst seine Anordnung vom 25. Juli 2001 überarbeiten und dabei vor allem, so es welche gibt, die näheren Umstände für die Einstufung des Marktplatzes, des Paradeplatzes und des Bereichs um das Neckartor als Kriminalitätsbrennpunkte dartun. Dies ist keineswegs eine bloße Formalie.

Mit einer Videoüberwachung, wie sie das Polizeipräsidium Mannheim auf dem Paradeplatz, dem Marktplatz und im Bereich des Neckartors durchführt, gehen gravierende Eingriffe in das Persönlichkeitsrecht einer Vielzahl völlig unverdächtiger Personen einher, weil die Videokameras unterschiedslos alle Personen erfassen, die sich dort aufhalten. Die Videokameras liefern praktisch nämlich von jeder Stelle Bilder, auf denen sich die aufgenommenen Personen identifizieren lassen. Dabei wird nicht nur deren Anwesenheit an den besagten Orten in Mannheim registriert, sondern vor allem auch, wie sie sich dabei gegeben haben, mit wem sie sich dort aufgehalten haben und ob ihr Verhalten in ein bestimmtes Raster passt. Solche Eingriffe in ihr Persönlichkeitsrecht müssen sich die aufgezeichneten Personen nur gefallen lassen, wenn durch konkrete Tatsachen belegt ist, dass es sich bei den videoüberwachten Plätzen tatsächlich um Kriminalitätsbrennpunkte handelt.

– Fristgerechte Löschung nicht sichergestellt

Das Polizeipräsidium Mannheim speichert sämtliche Videobilder, die die Videokameras aufnehmen, in einem Computer. Nach § 21 Abs. 4 PolG muss das Polizeipräsidium diese Videobilder spätestens nach 48 Stunden löschen. Nur wenn die Bilder – was bisher nur ganz selten vorgekommen ist – im Einzelfall zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden, darf das Polizeipräsidium sie länger aufbewahren. Die termingerechte Löschung der Videobilder nach 48 Stunden ist indes nicht sichergestellt. Zwar verfügt das ca. 1,2 Mio. DM teure Videoüberwachungssystem über ein automatisches Löschprogramm, das sich so einstellen lässt, dass die Löschung der Bilder jeweils präzise nach 48 Stunden erfolgt. Dieses Löschprogramm hatte das Polizeipräsidium jedoch kurzerhand deaktiviert, weil das Videoüberwachungssystem insgesamt noch an manchen Kinderkrankheiten leidet und deshalb noch nicht stabil läuft. Im Gegenzug hatte das Polizeipräsidium zwar in seinem Computer den Speicherplatz für die Aufzeichnung der Videobilder begrenzt. Mit einer solchen Speicherplatzbegrenzung lässt sich aber nicht garantieren, dass die Videobilder – wie es das Polizeigesetz verlangt – jeweils spätestens nach 48 Stunden gelöscht werden. Videobilder brauchen nämlich je nach dem, was auf ihnen zu sehen ist, mehr oder weniger Speicherplatz. Deshalb muss das Polizeipräsidium so schnell wie möglich das Löschprogramm wieder aktivieren und bis dahin durch Stichproben sicherstellen, dass die Videobilder nicht länger als 48 Stunden gespeichert bleiben.

– Passwortschutz fehlt, automatische Protokollierung wirkungslos, Zugriffsbeschränkungen nicht vorhanden

Wer personenbezogene Daten mithilfe von Computern verarbeitet, muss technische und organisatorische Maßnahmen ergreifen, um eine datenschutzgerechte Verarbeitung sicherzu-

stellen. Zu den Standardmaßnahmen gehört, dass sich jeder Nutzer durch Eingabe einer individuellen Benutzerkennung und einem dazu gehörigen Passwort legitimieren muss, bevor er auf gespeicherte Daten zugreifen kann. Ferner zählen dazu eine effektive Protokollierung und maßgeschneiderte Zugriffsbefugnisse. Auf unsere Fragen hierzu bekamen wir aus Mannheim zu lesen, Passwortschutz, Protokollierung und Zugriffsbeschränkungen seien gewährleistet. Als wir dann beim Kontrollbesuch die Probe aufs Exempel machten, sah dies ganz anders aus:

- Das Videoüberwachungssystem bietet zwar die Möglichkeit, für jeden Benutzer eine individuelle Benutzerkennung und ein Passwort zu vergeben. Davon hatte das Polizeipräsidium jedoch keinen Gebrauch gemacht. Deshalb kann jeder, der Zutritt zu dem an das Videoüberwachungssystem angeschlossenen PC hat, auf die gespeicherten Videobilder zugreifen, sie am Bildschirm aufrufen und die Videobilder sogar auf Datenträger kopieren. Um diesen gravierenden Mangel abzustellen, muss das Polizeipräsidium den vorhandenen Passwortschutz endlich aktivieren.

- Das Videoüberwachungssystem verfügt über ein Spezialprogramm zur Speicherung und Auswertung von Videobildern, mit dessen Hilfe man sämtliche Zugriffe auf die gespeicherten Videobilder automatisch protokollieren kann. Die Protokolle geben dann Auskunft darüber, wer wann auf welche Videobilder zugegriffen hat und ob er womöglich Kopien gezogen hat. Dieses Spezialprogramm läuft in Mannheim jedoch aus mancherlei Gründen ins Leere. Zum einen kann man es auf ganz einfache Weise umgehen. Zum anderen lässt sich – selbst wenn man das Spezialprogramm nutzt – aus den Protokollen nicht nachvollziehen, wer wann auf die Videobilder zugegriffen hat, weil die Benutzer bei der Anmeldung am Videoüberwachungssystem keine individuelle, sondern eine einheitliche Kennung eingeben müssen. Um diesen erheblichen Mangel zu beheben, muss das Polizeipräsidium dafür sorgen, dass sich alle Benutzer mit individueller Kennung anmelden und dass es unmöglich ist, das Spezialprogramm mit seiner Protokollierung zu umgehen.

- Zum kleinen Einmaleins des Datenschutzes gehört inzwischen, dass jedem Mitarbeiter nur die Zugriffsrechte auf Programme und Daten eingeräumt werden dürfen, die er für die Erfüllung seiner dienstlichen Aufgaben tatsächlich benötigt. Von solch differenzierten Zugriffsberechtigungen war zwar in den Schreiben aus Mannheim die Rede, tatsächlich gab es sie jedoch nicht. Vielmehr hatte das Polizeipräsidium allen ca. 60 Polizeibeamten, die abwechselnd an dem Videoüberwachungssystem Dienst tun, unterschiedslos eine umfassende Zugriffsberechtigung eingeräumt, mit der sie nicht nur Videobilder in Sekundenschnelle heraussuchen, bearbeiten und auf Datenträger kopieren, sondern beispielsweise neue Software installieren oder vorhandene Software entfernen und sogar Protokolldaten löschen können. Um diesen schweren Mangel zu beheben, muss das Polizeipräsidium maßgeschneiderte Zugriffsberechtigungen vergeben, die dem jeweiligen Mitarbeiter lediglich diejenigen technischen Möglichkeiten an die Hand geben, die er für seine Aufgaben benötigt.

Die nichtssagende Anordnung des Polizeipräsidiums, den fehlenden Passwortschutz, die wirkungslose Protokollierung und die umfassenden Zugriffsberechtigungen habe ich vor kurzem gegenüber dem Innenministerium beanstandet. Das Innenministerium räumte die Mängel bei der Löschung, beim Passwortschutz, bei der Protokollierung und bei den Zugriffsberechtigungen ein.

Es hofft, dass sie sich mit der „ersten endgültigen Version“, die Ende November 2001 installiert werden soll, beheben lassen. Im Klartext heißt das: Das Polizeipräsidium Mannheim hat nach Abschluss der Testphase das Videoüberwachungssystem in Betrieb genommen, obwohl elementare technische Datenschutzmaßnahmen fehlten, und betreibt es mit dem Segen des Innenministeriums weiter. Bei der nichtssagenden Anordnung sprang es dem Polizeipräsidium unter Hinweis auf ein Urteil des Verwaltungsgerichts Karlsruhe vom 10. Oktober 2001 zur Seite, das zur Begründung des sowieso schon recht konturenlosen Begriffs des Kriminalitätsbrennpunktes polizeiliche Erfahrungen ausreichen lassen will und deshalb die Klage eines Mannheimer Bürgers gegen die Videoüberwachung abgewiesen hat. Zugleich räumte das Innenministerium jedoch ein, dass es „detaillierte Erhebungen“ über die Kriminalitätsbelastung der videoüberwachten Plätze (noch) nicht gibt; nähere Angaben hierzu würden die ersten sechs Monate der Videoüberwachung bringen. So aber beißt sich doch die Katze in den Schwanz. Dass das Innenministerium auch noch meinte, die inhaltsleere Anordnung des Polizeipräsidiums entspreche den Anforderungen, die nach seiner eigenen Führungs- und Einsatzanordnung vom 22. Februar 2001 an die Begründung der Anordnung einer Videoüberwachung zu stellen sind, verstehe wer will.

3.2.2 Stuttgart

Die für das Stuttgarter Stadtgebiet zuständige Landespolizeidirektion Stuttgart II beabsichtigt ab Januar 2002 den Rotebühlplatz mit fünf Videokameras zu überwachen. Der Rotebühlplatz liegt mitten in Stuttgart. Er erstreckt sich von der Königstraße bis zur Theodor-Heuss-Straße. Über diverse Abgänge kann man die unterirdisch gelegene Rotebühl-Passage und die Haltestellen mehrerer Stadt-/U-Bahn-Linien und der S-Bahn-Linien erreichen. Zwei Videokameras sollen oberirdisch, die drei anderen Kameras unterirdisch installiert werden. Diesem Vorhaben stimmte der Gemeinderat der Landeshauptstadt Stuttgart Ende April 2001 mit der Maßgabe zu, dass es sich um einen auf ein Jahr befristeten Versuch handelt und dass die Stadtverwaltung ihm danach über die Ergebnisse zu berichten hat.

Als wir in der Presse davon gelesen und bei der Landeshauptstadt danach gefragt hatten, was der Annahme zu Grunde liegt, dass es sich beim Rotebühlplatz um einen Kriminalitätsbrennpunkt handelt, verwies sie uns an die Landespolizeidirektion Stuttgart II. Diese legte ihre Karten gleich auf den Tisch; zugleich regte sie an, alles zu besprechen. Dies erwies sich auch als notwendig, weil in ihrer schriftlichen Antwort Fragen offen geblieben waren. Die Landespolizeidirektion erläuterte uns dann alle Einzelheiten und legte auf unsere Bitte die Akten und Unterlagen zu den Delikten aus dem Jahr 2000 vor, die sie in ihre Beurteilung einbezogen hatte. Sie griff unsere Vorschläge zur Verbesserung der Transparenz ihrer Vorgehensweise auf und erarbeitete ein aktuelles, 16 Seiten langes Kriminalitätslagebild für den Rotebühlplatz. Dieses Lagebild und den Entwurf einer mehrseitigen Anordnung für die Videoüberwachung übersandte die Landespolizeidirektion uns vor kurzem. Unser Fazit war, dass Anordnung und Lagebild den Anforderungen an die Darlegung der Voraussetzungen eines Kriminalitätsbrennpunktes Rechnung tragen und sich danach die Einstufung des Rotebühlplatzes als Kriminalitätsbrennpunkt nicht von der Hand weisen lässt. Bei diesem Stand muss es freilich nicht ein für allemal bleiben. Die Landespolizeidirektion muss deshalb die Entwicklung der Straßenkriminalität im Auge behalten und ihr Kriminalitätslagebild fortschreiben.

4. Die DNA-Analysen

„Abgeordnete fordern Gentests für alle Männer“, so lauteten im Frühjahr 2001 die Schlagzeilen in der Presse. Einige namhafte Sicherheits- und Rechtspolitiker hatten sich nach einem Sexualmord an einem 12-jährigen Mädchen dafür ausgesprochen, dass alle Männer rein vorsorglich einen genetischen Fingerabdruck abgeben und in einer DNA-Datei registriert werden sollen, um so künftig Gewaltverbrecher schneller fassen zu können. War den Protagonisten dieser Aktion denn gar nicht in den Sinn gekommen, dass die damit einhergehende massenhafte Datenerhebung auf Vorrat, die im Ergebnis die Hälfte der Bevölkerung als potentielle Straftäter behandelt, mit dem Grundgesetz nicht zu vereinbaren ist? Hatten sie nicht bedacht, dass zudem der erwartete Abschreckungseffekt äußerst fragwürdig ist? Nach einer heftigen Mediendebatte verschwand diese abstruse Idee ganz rasch wieder in der Versenkung. Schlimm genug, dass sie überhaupt aufgetaucht ist.

In der Alltagsarbeit der Ermittlungsbehörden hat die DNA-Analyse bereits eine enorme Karriere hinter sich. Sie kommt auf zwei Feldern zum Einsatz: zum einen bei der Aufklärung von Straftaten, zum andern zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren. Seit 1997 ist in der Strafprozessordnung geregelt, unter welchen Voraussetzungen Beschuldigte oder andere Personen in einem laufenden Ermittlungsverfahren zur Aufklärung einer Straftat eine Speichelprobe, eine Blutprobe oder sonstige Körperzellen zur Erstellung eines sog. genetischen Fingerabdrucks abgeben müssen. Von dieser neuen Ermittlungsbefugnis machen die Ermittlungsbehörden regen Gebrauch. Bisweilen setzen sie bei der Aufklärung einer Straftat sogar ihre letzte Hoffnung auf den genetischen Fingerabdruck und bitten halbe Ortschaften oder gar tausende von Personen zum Massenscreening. Seit September 1998 ist geregelt, unter welchen Voraussetzungen von Personen, die einer Straftat von erheblicher Bedeutung verdächtig sind, oder von Personen, die früher einmal wegen einer der im DNA-Identitätsfeststellungsgesetz aufgezählten Straftaten verurteilt worden sind und deswegen noch im Bundeszentralregister stehen, ein genetischer Fingerabdruck zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren erhoben und in die bundesweite DNA-Datei eingespeichert werden darf. In dieser Datei, die das Bundeskriminalamt im April 1998 eingerichtet hat und auf die auch die Polizeien der Länder zugreifen können, sind mittlerweile 135 000 Personen erfasst, 25 000 davon aus Baden-Württemberg; Tendenz rasch steigend. Im Berichtsjahr haben wir uns mit DNA-Analysen bei einem sog. Massenscreening und mit DNA-Analysen zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren von Personen befasst, die wegen einer Straftat von erheblicher Bedeutung verurteilt wurden und deshalb noch im Bundeszentralregister erfasst waren (Altfälle).

4.1 Die DNA-Analyse bei Altfällen

Um festzustellen, wie Staatsanwaltschaften und Polizei hierzulande in Altfällen bei der DNA-Analyse verfahren, sahen wir uns exemplarisch bei der Staatsanwaltschaft Stuttgart 40 Altfälle und bei der Staatsanwaltschaft Heidelberg 80 Altfälle näher an. Das Bundeszentralregister hatte auf Anfrage der Staatsanwaltschaft Stuttgart 20 000 und der Staatsanwaltschaft Heidelberg 4 000 Personen gemeldet, die in ihrem Sprengel wegen einer in § 2c des Identitätsfeststellungsgesetzes aufgeführten Straftaten verurteilt worden und deswegen noch im Zentralregister registriert waren. Die Staatsanwaltschaft Stuttgart hatte 2 500 Fälle abgearbeitet. In 1 400 Fällen davon hatte sie sich für die Durchführung einer DNA-Analyse entschieden und eine entsprechende richterliche Anordnung beantragt. Die übrigen 1 100 Fälle hatten sich erledigt, weil der Verurteilte verstorben oder unbekannt verzogen oder bereits in der DNA-Datei erfasst war oder weil die Staatsanwaltschaft das Vorliegen der gesetzlichen Voraussetzungen für eine DNA-Analyse verneint hatte. Die Staatsanwaltschaft Heidelberg hatte 3 000 Fälle abgearbeitet. In 800 Fällen hatte sie eine richterliche Anordnung für die Durchführung einer DNA-Analyse beantragt. Die übrigen 2 200 Fälle hatten sich aus den bei der Staatsanwaltschaft Stuttgart erwähnten Gründen erledigt. Hatte der Richter die beantragte Anordnung erlassen,

baten die Staatsanwaltschaften die Polizeidienststellen vor Ort, das DNA-Material zu erheben. In den allermeisten Fällen waren die Betroffenen mit der Abgabe einer Speichelprobe einverstanden, in den anderen Fällen veranlasste die Polizei entsprechend der richterlichen Anordnung die Entnahme einer Blutprobe. Weil das Landeskriminalamt eine Lawine von DNA-Analysen auf sich zurollen sah, welche die Kapazitäten seines Kriminaltechnischen Instituts gesprengt hätte, vergab es die molekulargenetischen Untersuchungen der Speichelproben an eine Firma aus dem Bayerischen.

Bei unseren Kontrollen zeigte sich, dass bei den DNA-Analysen bei den Staatsanwaltschaften und bei der Polizei längst nicht alles rund lief. Nicht in Ordnung war vor allem, wie die beiden Staatsanwaltschaften bei den DNA-Analysen per Formblatt nach Schema F verfuhren. Als wir das Justizministerium damit konfrontierten, reagierte es in der mittlerweile hinreichend bekannten Art. Wieder einmal lautete seine Devise: Keine Kontrollbefugnis des Datenschutzbeauftragten. Doch jetzt der Reihe nach:

4.1.1 Straftat von erheblicher Bedeutung und Negativprognose nicht belegt

Um sich bei dem Berg von Altfällen die Arbeit zu erleichtern, stellten die beiden Staatsanwaltschaften ihre Anträge auf Erlass einer richterlichen Anordnung für die Durchführung einer DNA-Analyse mithilfe eines Formblatts. In dieses Formblatt trugen sie die Personalien des Betroffenen ein und kreuzten an, dass die Entnahme einer Speichelprobe und im Falle der Weigerung die Entnahme einer Blutprobe angeordnet werden soll. Ferner vermerkten sie anhand der Auszüge aus dem Bundeszentralregister, wann der Betroffene wegen welcher Straftat durch welches Gericht zu welcher Strafe verurteilt worden war. Daraus ersichtliche Hinweise darauf, dass die Strafe zur Bewährung ausgesetzt und nach erfolgreichem Ablauf der Bewährungsfrist erlassen worden war, erwähnten die Staatsanwaltschaften in der Regel nicht. Bei der Negativprognose beschränkten sie sich fast durchweg darauf, eine oder mehrere der auf dem Formular vorgedruckten Alternativen „Wegen der Art der Tat“, „Wegen der Ausführung der Tat“, „Wegen der Persönlichkeit des Täters“ anzukreuzen; nähere Angaben dazu, worauf sich die Staatsanwaltschaften dabei stützten, fanden sich in den Formularen nicht.

Mit dieser schematischen Verfahrensweise machten es sich die beiden Staatsanwaltschaften viel zu leicht und trugen den Datenschutzrechten der Betroffenen nicht hinreichend Rechnung. Voraussetzung für eine DNA-Analyse ist, dass der Betroffene wegen einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verurteilt oder nur wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit nicht verurteilt worden ist und die entsprechende Verurteilung im Bundeszentralregister oder im Erziehungsregister noch nicht getilgt ist. Hinzu kommen muss, dass wegen der Art und der Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind, mithin sich also eine sog. Negativprognose stellen lässt. Die Anlasstat muss mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit in der Bevölkerung erheblich zu beeinträchtigen. Das Vorliegen eines der genannten Regelbeispiele entbindet dabei nicht in jedem Fall von einer einzelfallbezogenen Prüfung dieser Voraussetzungen. Gibt es etwa im Hinblick auf eine milde Strafe oder eine Strafaussetzung zur Bewährung Hinweise aus dem zu Grunde liegenden Strafverfahren auf das Vorliegen

einer von der Regel abweichenden Ausnahme, muss sich die Entscheidung, gleichwohl eine DNA-Analyse zu beantragen, damit im Einzelnen auseinander setzen. Die Negativprognose setzt von Verfassungs wegen voraus, dass zuvor eine zureichende Sachaufklärung, insbesondere durch Beiziehung der verfügbaren Straf- und Vollstreckungsakten, des Bewährungsheftes und zeitnaher Auskünfte aus dem Bundeszentralregister erfolgt ist. Dabei ist eine auf den Einzelfall bezogene Entscheidung erforderlich, die auf schlüssigen, verwertbaren und in der Entscheidung nachvollziehbar dokumentierten Tatsachen beruht und die Annahme der Wahrscheinlichkeit künftiger Straftaten von erheblicher Bedeutung belegt. Für die Annahme einer Wiederholungsgefahr bedarf es positiver, auf den Einzelfall bezogener Gründe, denen Aussagekraft für die Wahrscheinlichkeit einer künftigen Tatbegehung zukommt. Die bloße Bezugnahme auf den Gesetzeswortlaut oder die Wiedergabe des Gesetzestextes reicht nicht aus. Gerade darauf beschränkten sich aber die beiden Staatsanwaltschaften in aller Regel. Ihre Formblattanträge sahen beispielsweise so aus:

> „Der Betroffene wurde durch rechtskräftiges Urteil des Amtsgerichts ... vom ... 1990 zur Freiheitsstrafe von einem Jahr wegen eines Vergehens der sexuellen Nötigung verurteilt. Es wurden somit Straftaten von erheblicher Bedeutung begangen. ... Die molekulargenetische Untersuchung des Spurenmaterials ist zur Feststellung des DNA-Identifizierungsmusters zum Zweck der Identitätsfeststellung in künftigen Straftaten erforderlich, weil wegen der Art der Tat und der Persönlichkeit des Verurteilten Grund zu der Annahme besteht, dass gegen den Betroffenen künftig erneut Strafverfahren wegen einer vorgenannten Straftat zu führen sind."

Weil der Betroffene tatsächlich – was die Staatsanwaltschaft aber gar nicht erwähnte, obwohl es in dem ihr vorliegenden Bundeszentralregisterauszug stand – eine versuchte und keine vollendete sexuelle Nötigung begangen hatte und die Freiheitsstrafe zur Bewährung ausgesetzt und später erlassen worden war, hätte die Staatsanwaltschaft, anstatt bloß den Gesetzeswortlaut zu wiederholen, allen Anlass gehabt zu prüfen, ob es sich wirklich um eine Straftat von erheblicher Bedeutung gehandelt hat und nachvollziehbar dartun müssen, warum auch noch mehr als 10 Jahre nach der Verurteilung Grund zu der Annahme bestehen soll, dass gegen den Betroffenen künftig erneut ein Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sein wird.

Die unzureichende Vorgehensweise der beiden Staatsanwaltschaften beanstandete ich. Die Antwort des Justizministeriums war nur auf den ersten Blick überraschend. Es hätte sich leicht ins rechte Licht rücken und darauf verweisen können, dass es schon mit einem Erlass vom Oktober 1998 die Staatsanwaltschaften darauf hingewiesen hatte, dass bei DNA-Analysen in Altfällen jeder Einzelfall hinsichtlich der Wiederholungswahrscheinlichkeit extra zu behandeln ist und welche Kriterien dabei von Bedeutung sein können. Auch nichts von seinem Erlass vom Januar 2000, mit dem es die Staatsanwaltschaften an die Notwendigkeit einer Einzelfallprüfung erinnert und zugleich betont hatte, dass bei lange zurückliegenden Verurteilungen ohne erneute Straffälligkeit eine DNA-Analyse in der Regel nicht in Frage kommt. Und schließlich auch nichts davon, dass es die Staatsanwaltschaften im Februar 2001 darüber belehrt hatte, dass formelhafte Begründungen, die sich ohne Einzelfallabwägung mit der bloßen Wiedergabe des Gesetzeswortlauts begnügen, den mit einer DNA-Analyse einhergehenden Eingriff in das Grundrecht auf Datenschutz nicht rechtfertigen können und dass regelmäßig erhöhte Anforderungen an die Begründung einer Wiederholungsgefahr zu stellen sind, wenn die Strafe für die Anlasstat zur Bewährung ausgesetzt worden ist. Offen ließ das Justizministerium

auch, wie es sicherstellen will, dass sich die Staatsanwaltschaften wenigstens an seine Erlasse in Sachen DNA-Analysen halten, womit für die Datenschutzrechte der Betroffenen schon eine ganze Menge gewonnen wäre. Stattdessen schrieb das Justizministerium uns kurz und knapp: Strafprozessuale Maßnahmen der Staatsanwaltschaften, die wie DNA-Analysen einem Richtervorbehalt unterliegen, würden nach seiner Auffassung der Kontrolle meines Amtes auch dann nicht unterfallen, wenn wir – wie in den vorliegenden Fällen – die Datenverarbeitung der Staatsanwaltschaften prüfen. Dies deshalb nicht, weil wir mit der Datenschutzprüfung bei den Staatsanwaltschaften mittelbar auch die richterlich angeordnete Maßnahme überprüfen würden. Dem liegt eine Verquickung völlig unterschiedlicher Dinge zu Grunde. Die Datenverarbeitung durch Gerichte ist eine Sache, die der Staatsanwaltschaften eine ganz andere. Allein die Datenverarbeitung der beiden Staatsanwaltschaften, die nach § 2 i. V. mit § 28 des Landesdatenschutzgesetzes der Datenschutzkontrolle meines Amtes uneingeschränkt unterliegen, war Gegenstand unserer Kontrolle in Stuttgart und Heidelberg. Aber was hilft in solchen Fällen schon ein Hinweis auf die Rechtslage: Noli me tangere oder – für Nichtlateiner – Rühre mich nicht an, so heißt nun einmal die Devise der Justiz.

4.1.2 Verfahren bei der Untersuchungsstelle präzise regeln

DNA-Analysen dürfen nur durch öffentlich bestellte oder durch das Verpflichtungsgesetz verpflichtete Sachverständige oder durch Amtsträger durchgeführt werden, die der die Ermittlung führenden Behörde entweder nicht angehören oder aber von ihr sachlich und organisatorisch getrennt sein müssen. Bei der Untersuchung dürfen andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, nicht getroffen werden. Das übersandte Untersuchungsmaterial ist zu vernichten, sobald es für die molekulargenetische Untersuchung nicht mehr benötigt wird. Die beauftragten Sachverständigen müssen durch technische und organisatorische Maßnahmen gewährleisten, dass keine unzulässigen molekulargenetischen Untersuchungen durchgeführt werden und dass eine unbefugte Kenntnis Dritter von den Untersuchungsergebnissen ausgeschlossen ist.

Das Landeskriminalamt hatte die Mitarbeiter der Firma aus dem Bayerischen, die mit der molekulargenetischen Untersuchung der von der baden-württembergischen Polizei angelieferten Speichelproben zu tun haben, nach dem Verpflichtungsgesetz verpflichtet. Es hatte außerdem Regelungen erarbeitet, wie die Firma bei den DNA-Analysen zu verfahren hat. Präzisierungsbedürftig waren allerdings noch die Bestimmungen über die technischen und organisatorischen Maßnahmen, die unzulässige molekulargenetische Untersuchungen verhindern und eine Kenntnisnahme der Untersuchungsergebnisse durch unbefugte Dritte ausschließen. Statt sich beispielsweise auf den allgemeinen Hinweis zu beschränken, dass die Firma Maßnahmen zu treffen hat, die geeignet sind, Unbefugten den Zutritt zu den DNA-Analysen zu verwehren, hätte das Landeskriminalamt in der Vereinbarung regeln müssen, mithilfe welcher konkreten Schritte die Firma eine effektive Zutrittskontrolle gewährleistet. Nur wenn in der Vereinbarung bei der Zutrittskontrolle und bei den anderen gebotenen Datensicherungsmaßnahmen geregelt ist, welche konkreten Vorkehrungen jeweils von der Firma zu treffen sind, kann sich das Landeskriminalamt ein Bild davon machen, ob diese Maßnahmen einen korrekten Umgang mit den DNA-Analysen gewährleisten und ob die Firma diese Maßnahmen auch einhält.

4.1.3 Fehler bei den Untersuchungsaufträgen

Ordnet ein Richter eine DNA-Analyse an, muss er in der schriftlichen Anordnung den Sachverständigen bestimmen, der mit der molekulargenetischen Untersuchung beauftragt wird. Dem Sachverständigen ist das Untersuchungsmaterial ohne Mitteilung des Namens, der Anschrift und des Geburtstags und -monats des Betroffenen zu übergeben. So steht es ausdrücklich in der Strafprozessordnung. An diese klaren Vorgaben haben sich Polizeidienststellen bei der Übersendung der Speichelproben nicht immer gehalten. Bei unseren Kontrollen stießen wir auf Fälle, in denen die Polizei die Speichelprobe nicht dem in der richterlichen Anordnung genannten Sachverständigen, sondern einem anderen Sachverständigen übersandt oder das Anonymisierungsgebot nicht beachtet hatte:

– Das Landeskriminalamt gab nach dem Vertragsschluss mit der Firma aus dem Bayerischen Speichelproben dorthin zur molekulargenetischen Untersuchung auch dann weiter, wenn der Richter in seiner Anordnung das Kriminaltechnische Institut des Landeskriminalamts mit der DNA-Analyse beauftragt hatte.

– Eine Polizeidirektion trug auf dem Formular, mit dem die Polizeidienststellen die Speichelproben an die Firma aus dem Bayerischen anonym übersenden müssen, den Vor- und Familiennamen sowie das Geburtsdatum des Betroffenen ein und schwärzte diese Angaben dann so unzureichend, dass sie trotzdem noch zu lesen waren. In einem Untersuchungsauftrag einer anderen Polizeidirektion konnte die Firma schwarz auf weiß den Namen und das Geburtsdatum des Betroffenen lesen.

Das Innenministerium ließ uns auf meine Beanstandung wissen, es teile unsere Auffassung, dass sich das Landeskriminalamt nicht über die richterliche Bestimmung des Sachverständigen hinwegsetzen durfte. Das Landeskriminalamt habe die Polizeidienststellen nochmals an die strikte Einhaltung des Anonymisierungsgebots erinnert und für den Fall des Falles, dass dennoch nicht oder nicht ausreichend anonymisierte Untersuchungsaufträge in seinem Kriminaltechnischen Institut auflaufen, Vorsorge dafür getroffen, dass der Sachverständige den Untersuchungsauftrag nicht zu Gesicht bekommt.

4.2 Das Massen-Screening

Die DNA-Analyse hat sich bei der Aufklärung von Straftaten zu einem bedeutsamen Beweismittel entwickelt. Bei Beschuldigten und Verletzten einer Straftat dürfen DNA-Analysen zur Feststellung der Tatsache durchgeführt werden, ob aufgefundenes Spurenmaterial von ihnen stammt. Bei Dritten, also unverdächtigen Personen, sind solche Untersuchungen ebenfalls zulässig; dabei geht es in der Regel um die Frage, von wem Spurenmaterial stammt, das beim Beschuldigten oder beim Tatopfer gefunden worden war. Ohne Einwilligung dürfen diesen Personen nur auf Grund einer richterlichen Anordnung Blutproben oder sonstige Körperzellen für eine DNA-Analyse entnommen werden. Die DNA-Analyse wiederum darf nur durch einen Richter angeordnet werden. Wunderdinge darf man jedoch auch von der DNA-Analyse nicht erwarten. Wer meint, mit einem Treffer sei der Täter überführt, muss bedenken, dass man mit der DNA-Analyse lediglich eine statistische Aussage zur Belastungswahrscheinlichkeit treffen kann, die eine Würdigung aller weiteren Beweisumstände nicht überflüssig macht. Eine andere Frage ist, was überhaupt ins Reagenzglas der Untersuchungsstellen kommt. Wenn ein ausgefallenes Haar zur Identifizierung ausreicht, wie leicht ist es dann, dass der Verdacht auf eine falsche Person fallen oder ganz bewusst auf sie gelenkt werden kann. Das Spurenlegen ist ein ganz gewaltiges Problem, warnte erst vor kurzem ein DNA-Experte aus dem Bundeskriminalamt. Wenn allzu sehr auf die DNA-Spur gesetzt wird und beispielsweise die molekulargenetisch untersuchte Zi-

garettenkippe nicht diejenige ist, die der Täter am Tatort geraucht, sondern eine andere Person achtlos weggeworfen hat, kann dies für die Ermittlung fatale Folgen haben. Zu solchen DNA-Analysen, die dem Nachweis der Täterschuld dienen, kann man stehen wie man will. Der Gesetzgeber hat sie zugelassen; die Kautelen dafür sind in der Strafprozessordnung geregelt.

Polizei und Staatsanwaltschaften schlagen indes zunehmend einen anderen Weg ein. Nicht mehr Schuld-, sondern Unschuldsbeweise sind gefragt. Sie fordern in Ermittlungsverfahren ganze Gruppen von Personen, von denen sie meinen, der Täter könnte sich unter ihnen befinden, auf, eine Speichelprobe für eine DNA-Analyse zum Abgleich mit einer Tatortspur abzugeben, ohne dass dafür eine richterliche Anordnung ergangen ist. Beispielsweise bat die Tübinger Polizei in einem Mordfall 4 000 Münchner Porsche-Fahrer um eine Speichel-/Blutprobe für eine DNA-Analyse. In Kehl richtete die Polizei im Zuge ihrer Ermittlungen zur Aufklärung der sog. Kehler Mordfälle eine entsprechende Bitte an 3 000 Männer. Gar 10 000 Speichelproben sammelte die Böblinger Polizei im Mordfall eines 11-jährigen Buben aus dem Schönbuch ein. Zur Aufklärung der Verbrechen haben die DNA-Analysen bisher nicht geführt. Die Massen-Screenings laufen mit Einverständnis der Betroffenen; sie unterschreiben vorformulierte Einverständniserklärungen, denen zufolge sie auf freiwilliger Basis die Speichelproben abgeben. Die allermeisten Personen kommen der Aufforderung der Polizei nach. Manche, weil sie meinen, dass der Polizei geholfen werden müsse, wenn in ihrem Ort oder im Nachbardorf ein solches Verbrechen verübt worden ist. Andere gehen nolens volens zur Speichelprobe und fragen sich, was hilft es eigentlich der Polizei, wenn sie weiß, wer alles nicht der Täter ist. Und – was heißt schon freiwillig, wenn von der Polizei mehr oder weniger unverhohlen die Einholung einer richterlichen Anordnung in den Raum gestellt wird oder wenn die zur Abgabe einer Speichelprobe aufgeforderten Männer vom Rathaus zu hören bekommen, dass mit dem Massentest endlich der Verdacht von der Gemeinde genommen werden soll, der Täter könnte einer von ihnen sein, oder wenn der Freund aus dem Fußballclub oder gar der eigene Vater sagt: Heute gehen wir zum Speicheltest. Dem kann man sich dann kaum entziehen, selbst wenn man das Bundesverfassungsgericht auf seiner Seite weiß, das schon 1996 betont hat, dass allein eine Verweigerung der Mitwirkung nicht als ein den Tatverdacht begründendes oder bestärkendes Indiz gewertet werden darf und damit dem Einwand, wer sich nicht der Untersuchung stelle, mache sich automatisch verdächtig, den Boden entzogen hat. Und schließlich: Werden mit einem Massen-Screening nicht zunächst einmal unbescholtene Bürger in die Nähe der aufzuklärenden Straftat gerückt? So empfanden es etwa Bürger aus dem Schönbuch, wie wir aus Eingaben wissen. Kurzum: Die Technik der DNA-Analyse, die mittlerweile einfach anzuwenden ist und genetische Fingerabdrücke praktisch am Fließband ermöglicht, hat den Kreis derer, die ins Visier der Fahnder geraten, ins beinahe Uferlose ausgeweitet. Dabei wird die klassische Unschuldsvermutung auf den Kopf gestellt. Es geht nach dem Motto: Ohne Verdacht ist jeder verdächtig, so lange zumindest, bis er den Behörden seine Unschuld nachgewiesen hat. Aus gutem Grund will es das Grundgesetz gerade andersherum.

Unser besonderes Augenmerk richtete sich bei Massen-Screenings darauf, dass die Betroffenen, bevor sie die Einwilligungserklärung unterschreiben, umfassend aufgeklärt werden. Dies war in der Vergangenheit nicht der Fall, wie in meinem 20. Tätigkeitsbericht (vgl. LT-Drs. 12/4600, S. 73 f.) und in meinem 21. Tätigkeitsbericht (vgl. LT-Drs. 12/5740, S. 56 f.) nachzulesen ist. Deshalb war uns an einer Überarbeitung der dazu verwendeten Formulare gelegen. Das Innenministerium nahm unser Angebot, bei der Neugestaltung mitzuwirken, dankend an und übersandte uns seinen mit dem Justizministerium abgestimmten Entwurf. Nicht alle unsere Vorschläge fanden ihren Niederschlag. Wichtig wäre uns gewesen, dass der Betroffene erfährt, welcher Sachverständige seine Speichelprobe molekulargenetisch untersucht und damit genauso gestellt wird, wie in den Fällen, in denen eine richter-

liche Anordnung ergeht, in der der Richter von Gesetzes wegen den mit der molekulargenetischen Untersuchung beauftragten Sachverständigen benennen muss. Dem trug das Innenministerium nicht Rechnung, weil es davon ausging, dass womöglich nach der Einholung der Einwilligung einmal ein Wechsel der Untersuchungsstelle notwendig werden könnte. Weil es zudem Fälle für denkbar hielt, in denen auf Grund der Ermittlungsergebnisse weitere Untersuchungen erforderlich sein könnten, will es sich mit dem Hinweis in den Formularen begnügen, dass das Untersuchungsmaterial unverzüglich vernichtet wird, „sobald es zu Vergleichszwecken im Zusammenhang mit dem Ermittlungsverfahren nicht mehr benötigt wird“. Damit kann sich doch derjenige, der eine Speichelprobe abgeben soll, kein Bild davon machen, wann diese vernichtet wird! Wenn jedoch schon nur ein solch unbestimmter Hinweis gegeben wird, läge es dann nicht nahe, die Betroffenen wenigstens über die Vernichtung zu unterrichten? Damit würde die Polizei deren Aufwand bei der Abgabe der Speichelprobe honorieren und ein Stück Bürgernähe praktizieren.

5. Die Datenschutzkontrolle bei den Gerichten

Kann die unabhängige Datenschutzkontrolle prüfen, ob Gerichte beim Einsatz der EDV die nach § 9 des Landesdatenschutzgesetzes gebotenen technischen und organisatorischen Maßnahmen getroffen haben? Das Justizministerium hatte zweimal sein Veto gegen eine solche Kontrolle eingelegt. Wer 1999 und 2000 meinen Tätigkeitsbericht gelesen hat, kennt die kontroversen Standpunkte des Justizministeriums und meines Amtes in dieser Frage und weiß, woran sich die Diskussion entzündet hatte (vgl. LT-Drs. 12/4600, S. 68 f., und 12/5740, S. 53 f.). Bei der Beratung meines letztjährigen Tätigkeitsberichts erklärte der Herr Justizminister im Ständigen Ausschuss des Landtags, sein Haus sei bereit in dieser Frage nach einer Linie zu suchen, die der meinem Amt im Landesdatenschutzgesetz eingeräumten Kontrollbefugnis Rechnung trägt. Das Angebot nahmen wir gerne an. Bei einer Besprechung erläuterten wir dem Justizministerium am Beispiel des Passwortschutzes, dass sich die beim Einsatz der EDV gebotenen technischen und organisatorischen Maßnahmen sehr wohl prüfen lassen, ohne dabei die richterliche Datenverarbeitung zu tangieren. Beim Passwortschutz geht es beispielsweise um die Frage, ob Passwörter überhaupt eingerichtet sind, ob sie so kurz und trivial sind, dass Unbefugte sie leicht erraten oder ausforschen können, ob sie einem automatischen Verfall unterliegen und ob sie verschlüsselt abgespeichert werden. All diese und weitere Fragen des Passwortschutzes lassen sich aber bei einer Datenschutzkontrolle klären, ohne auf die im EDV-System eines Gerichts von einem Richter gespeicherten Daten zuzugreifen oder sie auch nur zu Gesicht zu bekommen. Auf Bitten des Justizministeriums stellten wir eine Liste mit weiteren Beispielen zusammen, bei denen dies genauso ist. Mitte Juli 2001 ließ es uns wissen, es habe die Präsidenten der Oberlandesgerichte sowie des Verwaltungsgerichtshofs, des Landessozialgerichts und des Finanzgerichts Baden-Württemberg und wegen der grundsätzlichen Bedeutung der Angelegenheit darüber hinaus die Justizministerien der Länder und das Bundesjustizministerium um Stellungnahme gebeten. Seither haben wir vom Justizministerium nichts mehr gehört.

6. Fälle aus der Praxis

Jeden Tag wenden sich Bürger an mein Amt, weil sie nicht in Ordnung finden, wie Behörden mit den Datenschutzrechten umgegangen sind. Einige Beispiele hierzu:

6.1 Die Folgen einer Rechtsberatung

Ein Mitarbeiter eines freien Trägers der Wohlfahrtspflege, gegen den ein Ermittlungsverfahren wegen des Verdachts eines Verstoßes gegen das Rechtsberatungsgesetz in Gang gekommen war, wandte sich an uns. Ihm ging es nicht so sehr um sich selber, sondern vielmehr um die Frage, ob in diesem Zusammenhang womöglich Sozialdaten, die bekanntermaßen unter besonderem Schutz des Zehnten Buches des Sozialgesetzbuches stehen, geflossen sind. Um der Sache auf den Grund zu

gehen, mussten wir bei mehreren Stellen nachforschen: beim Verwaltungsgericht Stuttgart, wo – wie sich herausstellen sollte – alles angefangen hatte, bei der Staatsanwaltschaft Stuttgart, die das Ermittlungsverfahren führte, bei der Landespolizeidirektion Stuttgart II, die von der Staatsanwaltschaft mit den Ermittlungen beauftragt worden war, und bei der Rechtsanwaltskammer Stuttgart, die auch mit von der Partie war. Während die anderen Stellen unsere Fragen ohne viel Aufhebens zügig beantworteten, stellte sich die Rechtsanwaltskammer Stuttgart von Anfang an quer. Über drei Monate schrieben wir mit diversen Briefen gegen ihre Weigerungshaltung an. Zunächst hatte sie uns die Frage entgegengehalten, nach welcher Rechtsgrundlage sie eigentlich unserem Amt Auskunft geben müsse, und sich damit nicht gerade als profunder Kenner des Datenschutzrechts geoutet. Ein Blick ins Landesdatenschutzgesetz hätte genügt. Dort ist in § 29 nachzulesen, dass die Behörden und öffentlichen Stellen verpflichtet sind, mein Amt bei der Erfüllung seiner Aufgaben zu unterstützen und ihm im Rahmen seiner Kontrollbefugnis insbesondere Auskunft zu seinen Fragen und Einsicht in alle Unterlagen zu geben, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Statt nach unserem Hinweis darauf wenigstens jetzt unsere Fragen zum Sachverhalt zu beantworten, philosophierte die Rechtsanwaltskammer über den Datenschutz und stellte dabei Überlegungen an, die – gelinde gesagt – das geschriebene Recht konterkarieren. Weil wir die Hoffnung immer noch nicht aufgegeben hatten, gingen wir auf die Einlassungen der Rechtsanwaltskammer ein und baten abermals, unsere Fragen zu beantworten. Jedoch wiederum keine Antwort, sondern nur fadenscheinige Ausflüchte. Deshalb musste ich dieses gesetzwidrige Verhalten der Rechtsanwaltskammer beanstanden, weil wir – worauf aber jeder Bürger nach dem Landesdatenschutzgesetz Anspruch hat – ohne Stellungnahme die Eingabe nicht in angemessener Frist beantworten konnten. Zugleich bat ich das Justizministerium, das die Rechtsaufsicht über die Rechtsanwaltskammer führt, dafür zu sorgen, dass diese nun endlich unsere Fragen beantwortet. Das Justizministerium hatte daraufhin nichts Wichtigeres zu tun, als von uns die Eingabe anzufordern. Weil jeder Bürger, der sich an mein Amt wendet, Anspruch darauf hat, dass wir seine Eingabe vertraulich behandeln und weil das Justizministerium sie zur Beurteilung meiner Beanstandung in Wirklichkeit auch gar nicht brauchte, kamen wir seiner Bitte selbstverständlich nicht nach. Nachdem die Frist, die ich nach § 30 des Landesdatenschutzgesetzes in meiner Beanstandung für die Beantwortung unserer Fragen gesetzt hatte, um sage und schreibe sieben Wochen verstrichen war, schickte uns die Rechtsanwaltskammer endlich Unterlagen, aus denen wir das Notwendige ersehen konnten. Sozialdaten waren nicht geflossen. So hartnäckig wie sich ausgerechnet die Rechtsanwaltskammer, von der man eigentlich anderes erwartet hätte, ihrer gesetzlichen Unterstützungspflicht entzogen hat, das sucht schon seinesgleichen.

6.2 Begleiterscheinungen einer Bundesrichterwahl

Wer Richter am Bundesgerichtshof werden will, muss ein kompliziertes Verfahren durchlaufen. Er wird vom Bundesjustizminister gemeinsam mit dem Richterwahlausschuss berufen und vom Bundespräsident ernannt. Der Wahlausschuss setzt sich aus den 16 Justizministern der Länder und 16 Mitgliedern zusammen, die vom Bundestag berufen werden, ihm aber nicht angehören müssen. Vor der Berufung eines Richters gibt der Präsidialrat des Bundesgerichtshofs eine Stellungnahme über die Eignung der Bewerber ab. Diese ist für den Wahlausschuss nicht bindend. Der Wahlausschuss entscheidet in geheimer Abstimmung mit der Mehrheit der abgegebenen Stimmen. Seine Mitglieder sind zur Verschwiegenheit verpflichtet. Die Sitzungen des Wahlausschusses sind nichtöffentlich. Dieses Verfahren ist nach der Bundesrichterwahl vom 15. Februar 2001 ganz erheblich in die Kritik geraten; sogar von Kungelei war die Rede. Auslöser war die Wahl zweier Richter durch den Richterwahlausschuss gegen das Votum des Präsidialrats des Bundesgerichtshofs. Doch nicht darum geht es hier, sondern um ein grobes Foul bei der Richterwahl. Was war passiert?

In einer großen Tageszeitung stand zu lesen, wie sich der baden-württembergische Justizminister am Tag nach der Richterwahl dieser Zeitung gegenüber über die Wahl der beiden Richter echauffiert hatte. Weil der Zeitungsartikel den Eindruck vermittelte, der Herr Justizminister habe die Namen der beiden Richter und die Stellungnahme des Präsidialrats des Bundesgerichtshofs über deren Qualifikation in die Öffentlichkeit getragen, fragten wir beim Justizministerium nach. In seiner Antwort betonte das Ministerium, der Minister habe sich im Gespräch mit der Zeitung zu der grundsätzlichen Frage geäußert, ob Richter gegen das Votum des Präsidialrats des Bundesgerichtshofs zu Bundesrichtern gewählt werden sollen; er habe dabei weder den Namen der beiden Richter erwähnt noch sei es um deren Qualifikation gegangen. Die Namen der gewählten Kandidaten, die Umstände der Wahl und die Voten des Präsidialrats des Bundesgerichtshofs seien vielmehr schon unmittelbar nach der Richterwahl öffentlich bekannt gewesen. Weil sich das Justizministerium damit praktisch auf eine Verletzung der Vorschriften über die Vertraulichkeit der Beratung und Entscheidung des Richterwahlausschusses durch andere berufen hatte, was schon in Anbetracht der an der Richterwahl beteiligten Persönlichkeiten erklärungsbedürftig war, hakten wir nach. Das Justizministerium blieb bei seiner Darstellung.

Ebenso nicht zu klären war, wie es dazu kommen konnte, dass in der Ausgabe der Südwestpresse vom 17. Februar 2001 Zitate aus einem gemeinsamen, an den Herrn Justizminister persönlich adressierten Brief der Präsidenten der Oberlandesgerichte Karlsruhe und Stuttgart vom 16. Februar 2001 zu lesen waren. Diese enthielten Informationen über einen der beiden Richter, die weder die Präsidenten noch das Justizministerium nach den für sie geltenden Vorschriften zum Schutz der Personaldaten hätten an die Presse weitergeben dürfen. Sowohl die Verfasser des Briefes als auch das Justizministerium versicherten uns übereinstimmend, dass sie die Presse nicht informiert haben und auch nicht wissen, wie diese davon erfahren hat. Also muss es logischerweise der große Unbekannte gewesen sein, ein Phänomen, das in der Justiz in anderem Zusammenhang ja hin und wieder auftreten soll.

6.3 Fahrerlaubnis entzogen und doch nicht entzogen

Ein Stuttgarter sprach in meinem Amt vor und legte uns seinen Führerschein auf den Tisch. Er erzählte uns von einer Verkehrskontrolle mit Folgen und von einer netten Polizeibeamtin, die ihm geraten hatte, sich an uns zu wenden, damit es ihm bei der nächsten Verkehrskontrolle nicht wieder so ergehe wie geschehen. Der Stuttgarter war ein paar Tage zuvor in eine Verkehrskontrolle geraten. Er hatte den kontrollierenden Polizeibeamten auf deren Bitte seinen Führerschein ausgehändigt. Diese fragten über den Online-Anschluss der Polizei das Zentrale Verkehrsinformationssystem (ZEVIS) des Kraftfahrt-Bundesamtes ab. Damit nahm das Unheil seinen Lauf. Die Polizeibeamten hielten dem Stuttgarter vor, ihm sei laut ZEVIS die Fahrerlaubnis vorläufig entzogen und nahmen ihn mit auf das Revier. Alles Beteuern, dass die vorläufige Entziehung der Fahrerlaubnis längst aufgehoben sei, nutzte nichts. Erst nachdem er ein Schreiben herbeischaffen konnte, mit dem ihm im November 2000 die Staatsanwaltschaft nach der Aufhebung der vorläufigen Entziehung der Fahrerlaubnis seinen Führerschein zurückgeschickt und ihm – wie wenn sie es geahnt hätte – geraten hatte, das Schreiben immer mit sich zu führen, damit er es bei einer etwaigen Polizeikontrolle vorweisen könne, nahm die Sache eine Wendung. Die Polizei rief bei der Staatsanwaltschaft an; diese bestätigte die Aufhebung der vorläufigen Entziehung der Fahrerlaubnis; die Polizei ließ den Stuttgarter sogleich laufen.

Ein Blick in ZEVIS zeigte sofort, warum die Polizei so handeln musste wie geschehen. Der Stuttgarter war dort immer noch als jemand registriert, dem die Fahrerlaubnis durch ein Gericht vorläufig entzogen ist. Die Sache klärte sich rasch: Dem Stuttgarter war einst in der Tat wegen Nötigung im Straßenverkehr die Fahrerlaubnis vorläufig entzogen worden. In der Berufungsverhandlung war diese Maßnahme aber aufgeho-

ben worden. Darüber hatte die Staatsanwaltschaft das Kraftfahrt-Bundesamt Mitte Oktober 2000 informiert. Das Kraftfahrt-Bundesamt hatte – wie es uns schrieb – die Mitteilung auch erhalten und daraufhin den Eintrag über die vorläufige Entziehung der Fahrerlaubnis zwar im Verkehrszentralregister (VZR), nicht jedoch in ZEVIS gelöscht. Offenbar hatte der mit der Löschung befasste Mitarbeiter des Kraftfahrt-Bundesamtes nicht genau aufgepasst und übersehen, dass bei der Löschung der vorläufigen Entziehung der Fahrerlaubnis im VZR der entsprechende Eintrag im ZEVIS stehen geblieben war. Jetzt ist der Eintrag auch in ZEVIS gelöscht.

6.4 Die Teilnahme an einer Demonstration gegen Castor-Transporte

Die Eltern zweier junger Burschen wandten sich an uns, nachdem diese bei einer friedlichen Mahnwache gegen einen Castor-Transport von der Polizei wegen des Verdachts eines Vergehens gegen das Versammlungsgesetz festgenommen worden waren. Sie legten uns eingehend dar, weshalb von einem Vergehen gegen das Versammlungsgesetz keine Rede sein könne und baten uns, für die Löschung der über die beiden Burschen gespeicherten Daten zu sorgen. Als wir die Polizeidienststelle, die die beiden festgenommen hatte, damit konfrontierten, ließ sie uns wissen, ihre umfassende Recherche habe ergeben, dass sich die Geschehnisse weitestgehend so abgespielt haben, wie sie die Eltern uns geschildert hatten. Sie habe sich deshalb inzwischen bei den beiden Burschen und ihren Eltern für die Festnahme und die dabei getroffenen weiteren Maßnahmen entschuldigt. Ein mit der Materie nicht Vertrauter kann sich kaum vorstellen, wo das angebliche Vergehen gegen das Versammlungsgesetz überall Datenspuren hinterlassen hat und wo wir uns überall um die Löschung kümmern mussten:

- Natürlich gibt es eine Ermittlungsakte bei der Staatsanwaltschaft. Diese Akte bewahrt die Staatsanwaltschaft fünf Jahre lang auf; so sind die Vorschriften. Die Polizeidienststelle wird ihr Doppel der Ermittlungsakte – wie es sich gehört – nach einem Jahr in den Reißwolf schieben.
- Die Polizeidienststelle hatte die beiden Burschen erkennungsdienstlich behandelt, von ihnen also Lichtbilder und Fingerabdrücke gefertigt. Einen Satz Lichtbilder und Fingerabdruckblätter hatte sie entsprechend den dafür geltenden Richtlinien über das Landeskriminalamt an das Bundeskriminalamt weitergegeben, Mehrfertigungen hatte sie für sich behalten. Das Bundeskriminalamt hatte die beiden Burschen daraufhin in der erkennungsdienstlichen (ed-)Datei, die alle Polizeibeamten rund um die Uhr abfragen können, registriert. Die Lichtbilder und Fingerabdruckblätter sind inzwischen hier wie dort vernichtet, in der ed-Datei sind die Einträge gelöscht.
- Die Polizeidienststelle hatte über die vorgesetzte Landespolizeidirektion das Landeskriminalamt im Rahmen des sog. Informationsaustausches in Staatsschutzsachen über die Festnahme unterrichtet, weil sie in dem angeblichen Vergehen gegen das Versammlungsgesetz eine Straftat mit staatsfeindlicher Zielrichtung gesehen hatte. Die Polizeidienststelle und die Landespolizeidirektion haben die Meldungen inzwischen vernichtet.
- Das Landeskriminalamt hatte – wie dies üblich ist – die beiden Burschen aus Anlass der besagten Meldungen in der Arbeitsdatei PIOS Innere Sicherheit (APIS) erfasst. Diese APIS-Speicherung ist jetzt gelöscht. In den Meldungen hat das Landeskriminalamt ihre Daten gesperrt.
- Das Landeskriminalamt hatte Meldungen an das hiesige Landesamt für Verfassungsschutz, an das Landeskriminalamt in Hannover – die beiden Burschen wohnten in Niedersachsen – und an die Abteilung Staatsschutz des Bundeskriminalamts weitergegeben. Das Landesamt für Verfassungsschutz hat inzwischen auf der erhaltenen Meldung die Daten gegen eine weitere Nutzung gesperrt. Aus Niedersachsen wissen wir bereits, dass dort über sie nichts (mehr) gespeichert ist. Die Prüfung beim Bundeskriminalamt läuft noch.

6.5 Hausverbot für Männer – Wer darf unterrichtet werden?

Seit geraumer Zeit läuft das Modellprojekt „Rote Karte für häusliche Gewalt“. Eine ganze Reihe von Städten beteiligt sich daran. Ein Polizeibeamter aus der Praxis erklärte das Modellprojekt treffend so: Wenn die Polizei früher von Nachbarn gerufen wurde, hätten die Polizeibeamten an der Wohnungstür nur allzu oft erfahren, dass sich die Partner angeblich wieder versöhnt hätten; mit einem unguten Gefühl wären die Polizeibeamten oftmals wieder gegangen. Das hätte sich mit dem Modellprojekt geändert. Erkennt ein Polizeibeamter, dass eine Frau misshandelt worden war, greift er ein. Nicht selten fordert er den Mann auf, die Wohnung zu verlassen – und zwar sofort. Ist damit die Situation nicht bereinigt, erteilt die Stadtverwaltung dem Mann einen Platzverweis; er muss also für gewisse Zeit der Wohnung fernbleiben. Die zurückgebliebenen Frauen können in vielfacher Hinsicht Betreuung gebrauchen, sei es, dass ihnen jemand für Gespräche zur Verfügung steht, sie bei anfallenden Behördengängen begleitet, ihnen Termine bei Beratungsstellen verschafft oder ihnen sonst mit Rat und Tat zur Seite steht. Vielerorts haben sich neben den sowieso schon existierenden Beratungsstellen auch sog. Frauennotrufzentralen gegründet, in denen ehrenamtlich tätige Frauen sich dieser Aufgaben annehmen. Damit liegt die Frage auf dem Tisch: Darf die Polizei, die zu einem Fall häuslicher Gewalt gerufen wird, ohne Einwilligung der Frau oder gar über deren Kopf hinweg eine ehrenamtliche Mitarbeiterin der Frauennotrufzentrale oder die Mitarbeiterin einer Beratungsstelle in die Wohnung rufen oder muss die Polizei die Entscheidung darüber der Frau überlassen? Über diese Frage besteht vor Ort zwischen Stadt und Polizei nicht immer Klarheit, wie mir Polizeibeamte schrieben, die für das Entscheidungsvorrecht der Frau plädiert hatten. Damit lagen sie richtig. Die Frauennotrufzentralen und die Beratungsstellen nehmen keine polizeilichen Aufgaben wahr. Bei der Beratung der Frauen in der Frage, wie sie ihr Leben weiter gestalten und ob sie dazu die Hilfe der Frauennotrufzentrale oder einer Beratungsstelle in Anspruch nehmen wollen, geht es nicht um die Abwehr einer Gefahr im Sinne des Polizeirechts und damit nicht um eine polizeiliche Aufgabe. Die Gefahr ist nämlich mit der Ingewahrsamnahme und Entfernung des gewalttätigen Mannes aus der Wohnung beseitigt. Dies bedeutet freilich nicht, dass die Polizei Frauennotrufzentrale und Beratungsstelle in Fällen häuslicher Gewalt überhaupt nicht verständigen darf. Ausgeschlossen ist allein eine Unterrichtung ohne oder gar gegen den Willen der Frauen. Die Polizei kann sie durchaus auf Beratungsstellen und Frauennotrufzentralen hinweisen und deren Hilfsangebote erläutern. Sie kann ihnen auch die Inanspruchnahme dieser Hilfsangebote nahe legen und gegebenenfalls anbieten, der Frauennotrufzentrale oder einer Beratungsstelle Namen und Anschrift oder Telefonnummer weiterzugeben, um eine Kontaktaufnahme zu ermöglichen. Klar muss dabei aber immer sein: Der Frau muss die Entscheidung überlassen bleiben, ob sie das will oder nicht.

3. Teil: Technik und Organisation

1. Die Vorabkontrolle

Will eine öffentliche Stelle ein DV-Verfahren einsetzen, das mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann, so muss sie zuvor eine Vorabkontrolle durchführen. Das Verfahren darf erst dann zum Einsatz kommen, wenn sich dabei herausstellt, dass solche Risiken entweder gar nicht bestehen oder sie sich durch technische oder organisatorische Maßnahmen vermeiden lassen. Das Ergebnis der Vorabkontrolle sowie dessen Begründung sind schriftlich zu dokumentieren. Im vergangenen Jahr wurde mein Amt mehrfach gefragt, wie die Vorabkontrolle durchzuführen ist. Wir gaben dazu folgende Hinweise:

– In welchen Fällen ist eine Vorabkontrolle notwendig?

  In einer Reihe von Fällen schreibt das Landesdatenschutzgesetz eine Vorabkontrolle ausdrücklich vor. Notwendig ist sie etwa, wenn eine öffentliche Stelle mithilfe eines sog. automatisierten Abrufverfahrens online auf Daten zugreifen will, die in der Verantwortung einer anderen Stelle gespeichert werden. Eine Vorabkontrolle muss auch durchführen, wer beabsichtigt besonders sensible Daten zu verarbeiten. Das Landesdatenschutzgesetz zählt dazu Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben hervorgehen. Ferner ist immer dann eine Vorabkontrolle erforderlich, wenn eine öffentliche Stelle Chipkarten, Magnetkarten oder ähnliche mobile Datenträger an Bürger ausgeben will. Darüber hinaus können aber auch andere DV-Vorhaben besondere Gefahren für das Persönlichkeitsrecht mit sich bringen und damit eine Vorabkontrolle erfordern. Diese besonderen Gefahren, so erläutert es das Landesdatenschutzgesetz, können sich insbesondere auf Grund der Art oder der Zweckbestimmung der Verarbeitung ergeben. Zu den Vorhaben, die auf Grund ihrer Art eine Vorabkontrolle erfordern, gehört die Videoüberwachung. Die besondere Problematik dieser Technik besteht darin, dass damit vielfach Daten zahlreicher Personen erfasst und gespeichert werden, die gemessen am Zweck der Überwachungsanlage, etwa der Verfolgung von Straftaten, gar nicht benötigt werden.

– Wer führt die Vorabkontrolle durch?

  Die öffentliche Stelle, die den EDV-Einsatz plant, muss die Vorabkontrolle selbst durchführen und nicht nur deren Ergebnisse, sondern auch deren Begründung schriftlich festhalten. Sofern die Stelle einen behördlichen Datenschutzbeauftragten bestellt hat, muss sie ihm das Ergebnis der Vorabkontrolle zur Prüfung vorlegen, ansonsten meinem Amt.

– Welche Inhalte muss die Vorabkontrolle ansprechen?

  Generell lässt sich sagen, dass die Vorabkontrolle in jedem Fall diejenigen Angaben enthalten muss, die auch in das gemäß § 11 LDSG zu führende Verfahrensverzeichnis aufzunehmen sind. Außerdem muss die Vorabkontrolle die mit der eingesetzten Technik verbundenen Risiken benennen und beschreiben, welche technischen und organisatorischen Datenschutzmaßnahmen gemäß § 9 LDSG ergriffen werden sollen, um diese Risiken abzuwehren. Ferner ist darzustellen, welche Restrisiken verbleiben und wie diese zu bewerten sind.

Konkret hatte sich mein Amt mit vier Vorabkontrollen zu befassen. Dabei zeigte sich Folgendes:

1.1 Videoüberwachung im Labor und in der Universitätskasse

Eine Universität informierte mein Amt über ein Vorhaben, bei dem eine automatisch arbeitende Laboranlage aus einem anderen Raum heraus überwacht wird. Da sich täglich nur für kurze Zeit überhaupt Personen im überwachten Raum aufhalten, es sich dabei um einen eng begrenzten Personenkreis handelt, die in dem Raum dienstliche Aufgaben wahrnehmen, die Videoaufnahmen dem Schutz der Mitarbeiter bei eventuell auftretenden Störfällen in der Anlage dienen und die Videobilder nur an einem Kontrollmonitor angesehen, nicht aber aufgezeichnet werden können, hielten wir diesen Einsatz der Videoüberwachung für ausreichend begründet und angemessen realisiert.

Etwas anders sah es bei einem Projekt aus, bei dem die Kassenräume einer Universität videoüberwacht werden sollen. Im Unterschied zum Vorhaben der Laborüberwachung werden von den Kameras im Kassenraum viel mehr Personen erfasst. Außerdem werden die Videobilder regelmäßig aufgezeichnet. In zwei Punkten war die vorgelegte Konzeption zunächst unzulänglich:

Zum einen war vorgesehen, dass die Kassierer jederzeit sog. Verdachtsaufnahmen auslösen können. Wenn sich dabei eine Situation, die ein

Kassierer zunächst als problematisch einschätzte und daher aufzeichnen ließ, später als harmlos erweist, müssen diese Aufzeichnungen umgehend wieder gelöscht werden. Dies war nach dem vorgelegten Konzept nicht möglich. Es sah stattdessen vor, alle Verdachtsaufnahmen unter Beteiligung der Polizei auszuwerten und erst danach zu löschen.

Zum anderen stellte sich heraus, dass die Universität nicht darüber informiert war, wie die Passwortkonventionen am Videocomputer eingerichtet waren. Sie konnte daher nicht beurteilen, ob es für einen Unberechtigten leicht oder schwer ist, sich die gespeicherten Videodaten anzusehen. Zur Begründung führte die Universität an, dass sie ein Unternehmen mit der Systemverwaltung beauftragt habe und daher nicht über die von ihm gewählten Einstellungen Bescheid wisse. Damit ließ sie jedoch die Regeln der Auftragsdatenverarbeitung außer Acht, nach denen sie auch dann für die Einhaltung der notwendigen technischen und organisatorischen Maßnahmen verantwortlich bleibt, wenn sie eine externe Stelle mit einer Datenverarbeitungsaufgabe, hier der Computerbetreuung, betraut.

1.2 Chipkarteneinsatz an Hochschulen

Der Einsatz von Chipkarten stellt regelmäßig besondere Anforderungen an die Vorabkontrolle. Bei einer solchen Vorabkontrolle für ein Chipkartensystem sind die vorgesehene Nutzung, die eingesetzte Chipkartentechnik und die für den Datenschutz relevanten technischen und organisatorischen Maßnahmen zu beschreiben. Unter anderem ist dabei zu dokumentieren, welche Datenfelder die Karten enthalten, wofür sie genutzt werden, wie sichergestellt ist, dass nicht benötigte Felder leer bleiben und dass die beteiligten Stellen jeweils nur auf die für ihre Aufgaben erforderlichen Daten zugreifen können. Ferner muss sichergestellt sein, dass sich niemand unbefugt Informationen aus dem Datenverarbeitungssystem beschaffen kann. Außerdem muss auf Antrag des Karteninhabers – etwa bei Verlust der Chipkarte – deren Benutzung durch Dritte unterbunden werden können und die Möglichkeit bestehen, ihn alsbald mit neuer Zugangsidentifizierung zuzulassen. Nicht zuletzt ist darzulegen, dass sowohl die auf Chipkarten als auch die auf den Hintergrundsystemen gespeicherten Daten fristgerecht gelöscht werden.

Der von einer Universität zunächst vorgelegte Entwurf der Vorabkontrolle für einen Chipkarteneinsatz war nicht konkret genug und wurde den eingangs beschriebenen Anforderungen noch nicht gerecht. Es fehlten beispielsweise nähere Angaben über die verarbeiteten Datenarten, deren Speicherdauer und die zugriffsberechtigten Stellen. Zudem blieb offen, wie die einzelnen technischen Komponenten ausgestaltet sein sollen und welche technischen und organisatorischen Maßnahmen ergriffen werden sollen, um unbeabsichtigte Datenverluste und unberechtigte Verarbeitung der Daten zu verhindern.

In der auf unsere Veranlassung überarbeiteten Fassung der Vorabkontrolle waren diese Mängel dann weitgehend behoben. Positiv zu erwähnen waren insbesondere die verschlüsselte Kommunikation der einzelnen, am Datenfluss beteiligten Systeme, die Möglichkeit für anonyme Bezahlfunktionen, z. B. bei der Mensa, eine nichtpersonalisierte Karte zu erhalten sowie die organisatorischen Maßnahmen zur Abschottung zwischen Karten-ID und Namen der Karteninhaber.

Insgesamt deuten die ersten Erfahrungen darauf hin, dass die öffentlichen Stellen, trotz einiger Unzulänglichkeiten im Einzelnen, verantwortungsvoll und angemessen mit dem neuen Instrument der Vorabkontrolle umgehen.

2. e-Bürgerdienste – von der Theorie zur Praxis

Land und Kommunen rüsten gegenwärtig ihre EDV weiter auf, damit sie den Bürgern bis zum Jahr 2005 viele Dienstleistungen online anbieten können. Dabei geht es aber nicht nur um neue Technik in der Verwaltung. Soweit es bei der Inanspruchnahme einer solchen Dienstleistung auf die Identität des Bürgers ankommt, muss dieser mit Hilfe einer digitalen Signatur nachweisen, wer er ist. Um diese ausreichend fälschungssicher zu gestalten,

hat jeder, der ein elektronisches Dokument digital signieren will, dazu eine speziell dafür vorgesehene Chipkarte zu benutzen. Die Landesverwaltung lässt in einem ersten Schritt 1 000 solcher Chipkarten, die so genannte Baden-Württemberg-Card, herstellen und an Bürger und Mitarbeiter in den Behörden ausgeben, um die neu entwickelten e-Bürgerdienste unter diesen Bedingungen zu erproben.

Im Rahmen meiner Beratungstätigkeit habe ich auf folgende, für den Datenschutz relevante Aspekte hingewiesen:

2.1 Die Baden-Württemberg-Card

Was für den Bürger gilt, gilt auch für die Verwaltung. Will sie ihrem elektronischen Dokument Geltung verleihen, muss dieses ebenso wie die Anträge der Bürger digital signiert sein, damit der Bürger sicher sein kann, dass es tatsächlich von der Behörde stammt. Dazu muss man wissen, dass sich digitale Signaturen dahin gehend unterscheiden können, welche Angaben durch sie bestätigt werden sollen. Im Fall der Baden-Württemberg-Card sind dies nur Name und Vorname des Karteninhabers, auf seinen Wunsch auch die private Wohnanschrift. Konkret heißt das: Der Empfänger kann zwar zweifelsfrei sicher sein, dass eine Person mit dem aus der Signatur ersichtlichen Namen das Dokument unterzeichnet hat. Ob diese Person aber der als Absender bezeichneten Behörde überhaupt angehört und ob sie zur Unterschrift berechtigt ist oder es sich nur um den Hausmeister des Amtes handelt, lässt sich der Signatur nicht entnehmen. Aus diesem Grund ist die Baden-Württemberg-Card in ihrer gegenwärtigen Form zur Signierung amtlicher Mitteilungen an Privatpersonen kaum geeignet. Solange das so ist, sollten diese Karten, für deren Ausgabe der Nutzer dem mit der Herstellung beauftragten Unternehmen unter anderem seine Privatadresse und Personalausweisdaten nennen muss, nur auf freiwilliger Basis an die Bediensteten ausgegeben werden.

2.2 Das Internet-Portal

Das federführend vom Innenministerium konzipierte Internet-Portal für Bürgerdienste soll den Bürgern einen zentralen und komfortablen Zugang zur Nutzung verschiedener e-Bürgerdienste ermöglichen. Dabei soll es weit mehr bieten als nur Links auf kommunale und staatliche e-Bürgerdienste. Künftig sollen die Bürger vielmehr darin beispielsweise ihren Namen und den Wohnort, ihre Telefon- und Telefaxnummer, die E-Mail-Adresse und behördliche Akten- oder Buchungszeichen hinterlegen können. Stellen sie später über das Portal Anträge an Behörden, müssen sie diese Angaben nicht in jedes Antragsformular eingeben, sondern können die zuvor hinterlegten Daten übernehmen. Außerdem sollen die im Portal gespeicherten Bürgerdaten im Rahmen der sog. Personalisierung des Portals dazu verwendet werden, um einem Bürger nur die für ihn relevanten Informationen anzuzeigen. Statt sich aus allen 35 Landratsämtern das für ihn zuständige heraussuchen zu müssen, bekäme er dann von vornherein nur dieses angezeigt. Im Wege einer Ausschreibung sucht das Innenministerium gegenwärtig ein Unternehmen, das die technische Realisierung und den Betrieb des Internet-Portals übernehmen soll. Die Ausschreibungsunterlagen enthielten unter anderem auch Anforderungen an die datenschutzrechtliche Gestaltung des anzubietenden Systems. Positiv zu erwähnen sind dabei die Forderungen, dass die im Portal hinterlegten Bürgerdaten verschlüsselt zu speichern sind, der Zugriff darauf nur mit einem digitalen Zertifikat möglich sein soll, die zwischen Bürger und Portal ausgetauschten Daten verschlüsselt über das Internet zu übertragen sind und dass bei der Gestaltung des Systems generell das Prinzip der Datensparsamkeit zu berücksichtigen ist.

Auf eine Reihe datenschutzrelevanter Fragen gaben die Unterlagen des Innenministeriums jedoch noch keine befriedigende Antwort. Offen blieb, für welche Zwecke die Daten im Einzelnen gespeichert werden sollen, welche Stellen darauf zugreifen können, an welche Stellen personenbezogene Daten übermittelt werden, wie unberechtigte Zugriffe

auf diese Daten verhindert werden und last not least wann und durch wen die Daten wieder gelöscht werden. Zudem war nicht zu erkennen, ob sichergestellt ist, dass die Bürger über alle Nutzungen ihrer Daten unterrichtet werden. Weil die Sicherheitstechniken zum Teil nur ansatzweise beschrieben waren, bat ich das Innenministerium um nähere Informationen darüber, welche Mechanismen genutzt werden sollen, um zu verhindern, dass man sich gegenüber dem Portal unter fremdem Namen anmelden kann und wo der zur Entschlüsselung der Bürgerdaten benötigte Schlüssel gespeichert wird, wer darauf Zugriff hat und wie er vor unberechtigtem Zugriff geschützt ist. Das Innenministerium antwortete, es stelle sich die technische Umsetzung so vor, dass nicht die Verwaltung oder der Portalbetreiber, sondern nur der Bürger selbst auf die von ihm eingegebenen Daten zugreifen kann und er in jedem Einzelfall ausdrücklich der Übermittlung seiner Daten an eine Behörde oder eine andere dem Portal angeschlossenen Stelle zustimmen muss. Wenn es gelingt, diesen Anforderungen Rechnung zu tragen, ist aus datenschutzrechtlicher Sicht gegen das Projekt nichts einzuwenden. Noch ist aber nicht klar, wie diese Sicherheitsanforderungen mit den Vorstellungen über die möglichen Funktionen des Portals, wie etwa der Personalisierung, in Einklang gebracht werden können.

Bleibt zu hoffen, dass es dem vom Innenministerium zur fachlichen Begleitung des Projekts geplanten Lenkungsausschuss gelingt, einen datenschutzgerechten Weg zur Realisierung des Internet-Portals aufzuzeigen.

3. Internet

Auch in diesem Jahr hatten wieder zahlreiche Bürgereingaben und Beratungswünsche mit Fragen rund um das Internet zu tun. Wie groß die Bandbreite der davon berührten Fragestellungen war, mag die folgende Übersicht illustrieren:

3.1 Jeder Mitarbeiter ein Surfer?

Die Fähigkeit, mit Medien, insbesondere dem Internet, professionell umzugehen, gewinnt im heutigen Berufs- und Wirtschaftsleben zunehmend an Bedeutung. Verständlich ist daher das Anliegen des Staatsministeriums, dass auch die Landesbediensteten auf diesem Gebiet auf der Höhe der Zeit bleiben sollen. Damit möglichst viele Mitarbeiterinnen und Mitarbeiter eine solche Medienkompetenz erwerben können, wandte sich Herr Staatsminister Palmer Ende vergangenen Jahres an seine ministeriellen Kolleginnen und Kollegen und bat darum, jedem Mitarbeiter die Nutzung des Internets am Arbeitsplatz selbst dann zu ermöglichen, wenn dies für dienstliche Zwecke nicht notwendig ist. Der für Fragen ressortübergreifender IuK-Projekte zuständige Arbeitskreis Informationstechnik erkannte zu Recht, dass dieser Vorschlag erhebliche Auswirkungen auf die Sicherheit der EDV-Systeme des Landes sowie der darin gespeicherten Daten haben kann. Er sprach sich deshalb dafür aus, sorgfältig zu prüfen, welche Sicherheitsmaßnahmen getroffen werden müssen, wenn man diesen Vorschlag realisieren will. Was das damit beauftragte Unternehmen dann ein halbes Jahr später als Ergebnis vorlegte, war allerdings mehr als enttäuschend.

Anstatt eine Studie vorzulegen, die auf die vorgeschlagene Vollversorgung und den daraus resultierenden konkreten Nutzungsbedarf der Verwaltung Bezug nimmt und darauf zugeschnittene Lösungswege aufzeigt, lieferte das Unternehmen lediglich allgemeine Aussagen zur Sicherung eines Internet-Anschlusses, die weder aktuell noch neuartig, sondern teilweise sogar aus einer im Internet veröffentlichten Diplomarbeit kopiert waren. In einem Anfang Oktober 2001 geführten Gespräch sagte das Unternehmen zu, sein Gutachten nochmals gründlich zu überarbeiten. Bedauerlich bleibt, dass seit Erteilung dieses Auftrags viele Monate verstrichen sind, ohne dass man einer Lösung der gestellten Aufgabe näher gekommen ist.

3.2 Anonyme Veröffentlichung von News-Beiträgen?

Spricht man von der Nutzung des Internets, denken viele zunächst an E-Mail und WWW. Daneben bietet das Internet aber noch eine Reihe anderer Kommunikationsmöglichkeiten. Der mit einem großen schwarzen Brett vergleichbare News-Dienst beispielsweise ermöglicht es, an themenspezifischen Diskussionsforen teilzunehmen, dort die Beiträge anderer Nutzer zu lesen und selbst Beiträge dazu zu veröffentlichen. Ein Student, der Zugang zum News-Server seiner Universität hatte, störte sich daran, dass diese alle Nutzer dieses Servers verpflichtete, in ihren Beiträgen ihren Namen und ihre E-Mail-Adresse anzugeben. Unter Hinweis auf das im Teledienstedatenschutzgesetz vorgesehene Gebot, nach Möglichkeit eine anonyme oder zumindest pseudonyme Nutzung der angebotenen Dienste zu ermöglichen, verlangte er, eigene Beiträge auch ohne Nennung von Namen und E-Mail-Adresse veröffentlichen zu dürfen.

Auf diese Frage eine Antwort zu finden, erfordert eine Abwägung der unterschiedlichen Datenschutzinteressen der verschiedenen Beteiligten: Auf der einen Seite steht der Verfasser eines News-Beitrages, der diesen auch ohne Namensnennung veröffentlichen können will. Auf der anderen Seite, auch das zeigen uns Bürgereingaben, fühlen sich Menschen zunehmend als Opfer von Veröffentlichungen im Internet, in denen verunglimpfende Aussagen über sie getroffen werden. Diese Personen sind, wenn sie falsche oder unrechtmäßige Veröffentlichungen verfolgen wollen, darauf angewiesen, die Identität des Verfassers zu erfahren. Beiden Anliegen scheint mir am besten dadurch Rechnung getragen, dass die Verfasser der Beiträge dem Serverbetreiber ihre Identität offen legen müssen, sie aber nicht dazu verpflichtet werden, ihren Namen und ihre E-Mail-Adresse in jedem Beitrag zu veröffentlichen. Es genügt, wenn diejenigen, die sich durch eine Veröffentlichung in ihren Persönlichkeitsrechten beeinträchtigt sehen, im Einzelfall die Identität des Autors erfahren können. Leider war die Universität bislang nicht bereit, diesen Überlegungen zu folgen und fordert nach wie vor die Angabe von Name und E-Mail-Adresse in jedem Beitrag.

3.3 Web-Cam im Internet-Café

Sehen ist besser als hören und hören besser als schreiben. Von diesem Motto schien eine Universität geleitet, die nicht nur ein Internet-Café einrichtete, in dem die Studenten im Web surfen, E-Mails schreiben und mit Kommunikationspartnern in aller Welt chatten konnten, sie installierte dort auch zwei sog. Web-Cams, deren Aufnahmen sie mehrmals pro Minute über eine Web-Seite im Internet veröffentlichte. Damit sollte es den Chat-Kommunikationspartnern möglich sein, nicht nur schriftlich mit ihrem Partner zu kommunizieren, sondern ihrem „Gegenüber“ auch Live-Bilder von sich zu übermitteln. Die dafür vorgesehenen Kameras waren aber so angebracht, dass sie nicht nur einzelne, sondern gleich mehrere Nutzer des Internet-Cafés aufnahmen. Nur zu verständlich, dass jemand, der im Internet-Café lediglich seine E-Mails abrufen wollte, unangenehm berührt war, als er nach dem Besuch des Internet-Cafés von Bekannten darauf angesprochen wurde. Um dies künftig zu vermeiden, baten wir die Universität, die Kameras so anzubringen, dass sie nur die an einem PC stehende Person erfasst und dass diese Person frei darüber entscheiden kann, ob sie die Kamera einschalten will oder nicht. Anstatt diese datenschutzgerechte Lösung zu realisieren, zog es die Universität dann allerdings vor, die Web-Kameras ganz außer Betrieb zu nehmen.

3.4 Datenschutzgerechtes Web-Angebot: keine Selbstverständlichkeit

Um ein positives Umfeld für die Akzeptanz neuartiger elektronischer Dienste zu schaffen, hat der Bundesgesetzgeber bereits vor einigen Jahren unter anderem das Teledienstegesetz sowie das Teledienstedatenschutzgesetz verabschiedet. Eine maßgebliche Zielsetzung war dabei, dass bei der elektronischen Abwicklung von Vorgängen nicht mehr Daten erfasst werden sollen als dies geschieht, wenn man den gleichen

Vorgang auf herkömmliche Art und Weise tätigt. In der täglichen Praxis verlieren Internet-Inhaltsanbieter diese Ziele jedoch gelegentlich aus dem Blickfeld. Ein Beispiel hierfür ist das für jedermann kostenlos nutzbare Angebot des Vorschriftendienstes Baden-Württemberg (VD-BW) zum Abruf von Gesetzen und Verordnungen des Landes, das der Staatsanzeiger gemeinsam mit einem privaten Verlag im Internet anbietet.

Bekundet man beim erstmaligen Besuch der Homepage sein Interesse, den Vorschriftendienst zu nutzen, so erscheint eine mit „Anmeldung für den Bürgerdienst“ überschriebene Bildschirmmaske, die dem Nutzer Eingabefelder für Name, Vorname, Titel, Firma/Behörde, Postanschrift, E-Mail-Adresse präsentiert. Ferner enthält die Seite Eingabefelder für die Benutzerkennung und das Passwort, mit dem man künftig den Vorschriftendienst nutzen möchte. Letztere sind durch einen Hinweis als diejenigen gekennzeichnet, die auszufüllen sind. Dieser Aufbau der Maske und der Ablauf des Anmeldeverfahrens sind aus Sicht des Datenschutzes alles andere als glücklich. Manch ein Nutzer wird nämlich alle Felder ausfüllen und damit seine Identität offenbaren, obwohl dazu keine Notwendigkeit besteht.

Orientiert am Gebot der Datensparsamkeit wäre es sinnvoll, zunächst nur die Daten zu erfassen, die zur Nutzung des Dienstes erforderlich sind. Bietet der VD-BW darüber hinaus Zusatzdienstleistungen an, sollten die Nutzer darüber in einem zweiten Schritt informiert und ihnen insbesondere mitgeteilt werden, welche personenbezogenen Daten dafür erforderlich sind.

Da die Nutzer des VD-BW bislang nicht erfuhren, wofür die (freiwillig) eingegebenen Adressdaten verwendet und wie lange diese gespeichert werden, baten wir darum, die Nutzer auch darüber zu informieren.

Im Angebot des VD-BW wird die Javascript-Technik eingesetzt, die in einem Web-Angebot nicht nur mancherlei nützliche Aufgaben übernehmen, sondern auch dazu benutzt werden kann, den PC sowie das Surf-Verhalten des Nutzers auszuforschen. Um sich davor zu schützen, empfiehlt es sich, die Ausführung von Javascript sowie anderer so genannter aktiver Inhalte wie Java oder Active-X beim Surfen im Internet generell zu deaktivieren. Um dem Sicherheitsbedürfnis der Internet-Nutzer Rechnung zu tragen, sollte bei der Gestaltung der Web-Angebote auf die Verwendung dieser aktiven Inhalte möglichst verzichtet werden. Ist dies nicht möglich, sollten die Nutzer ausdrücklich auf die Verwendung dieser Techniken hingewiesen und ihnen erläutert werden, wozu die Technik jeweils benötigt wird. Dies ermöglicht es dem Nutzer, darüber zu entscheiden, ob er die Ausführung der aktiven Inhalte für den genannten Zweck zulassen will oder nicht.

Ähnliches gilt für die im Angebot des VD-BW ebenfalls verwendeten Cookies. Zwar können Cookies – im Unterschied zu aktiven Inhalten – nicht dazu benutzt werden, den Computer des Internet-Nutzers auszuspionieren. Denkbar ist jedoch, dass mit ihrer Hilfe Persönlichkeitsprofile erstellt werden, die Auskunft darüber geben, wofür sich der Computernutzer interessiert, während er im Internet surft. Die Verwendung von Cookies zählt zu den Techniken, die mit den Worten des Teledienstedatenschutzgesetzes gesprochen „eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten“. Konsequenz daraus ist, dass die Nutzer auch über die Verwendung von Cookies informiert werden müssen. Das geschah zwar, es war aber nicht sichergestellt, dass jeder Nutzer, der sich dort registriert, diese Information zuvor auch zur Kenntnis genommen hatte.

Der VD-BW will unseren Hinweisen bei der demnächst anstehenden grundlegenden Überarbeitung des Angebots Rechnung tragen.

3.5 Die Bibliothek und der Internet-PC

Bibliotheken sehen es als eine ihrer Aufgaben an, ihren Besuchern Wissen zu vermitteln. Deshalb ist es nur zu verständlich, dass sie diesen

immer öfter den Zugriff auf die vielfältigen Informationen, die das Internet bietet, ermöglichen. Zwar wird in der Regel bei der Benutzung dieser PC nicht der Nutzername erfasst; aber gleichwohl können datenschutzrechtliche Probleme auftreten. Dies ist jedenfalls dann der Fall, wenn ein Besucher erkennen kann, welche Informationen sein Vorgänger im Internet abgerufen und welche Suchanfragen er gestartet hat oder gar wie hoch dessen per Internet abgefragter Kontostand ist. Wer im Internet surft, hinterlässt dabei nämlich Spuren nicht nur auf den Rechnern (sog. WWW-Servern), von denen er Dokumente anfordert. Auch auf dem lokalen Rechner, mit dem er die abgerufenen Dokumente in Augenschein nimmt, werden bei jedem Abruf einer WWW-Seite eine Reihe von Informationen festgehalten, die es einem später mit diesem Rechner arbeitenden Nutzer festzustellen erlauben, welche WWW-Seiten durch den lokalen Rechner abgerufen wurden. Vor diesem möglichen Ausspähen besuchter WWW-Seiten durch spätere Nutzer muss die Bibliothek den Nutzer eines öffentlich zugänglichen Internet-PC schützen:

- Gängige Browser unterhalten auf dem lokalen Rechner einen schnellen Zwischenspeicher (den so genannten Cache), mit dessen Inhalt der Browser die Seiten generiert, die auf dem entsprechenden WWW-Server statisch gespeichert sind und seit dem letzten Abruf keine Änderung erfahren haben. Dieser Zwischenspeicher befindet sich in Form von Verzeichnissen und Dateien auf der Festplatte des lokalen Rechners. Diese müssen gegen Einsichtnahme späterer Nutzer geschützt werden. Da der Zugang für alle Nutzer des lokalen Rechners im Allgemeinen unter einer einheitlichen Benutzerkennung erfolgt, greift der nachfolgende Nutzer auf die gleichen Verzeichnisse und Dateien zu wie sein Vorgänger. Die üblicherweise in Betriebssystemen eingesetzten Mechanismen wie Schreib- und Leseschutz von Verzeichnissen und Dateien erweisen sich daher als wirkungslos. Es gibt folglich nur die Möglichkeit, entweder die Benutzeroberfläche so einzuschränken, dass der direkte Zugriff auf die Dateien nicht möglich ist, oder den lokalen Zwischenspeicher nach jeder Sitzung zu löschen.
- Wird nur der direkte Zugriff auf die Verzeichnisse und Dateien unterbunden und ermöglicht es der Browser, sich ein Inhaltsverzeichnis des Zwischenspeichers anzuschauen, so sollte der Zwischenspeicher bei jedem Start des Browserprogramms neu initialisiert werden.
- Die Löschung der entsprechenden Verzeichnisse und Dateien reicht dann nicht aus, wenn die Zugriffe auf WWW-Seiten in weiteren Dateien, einer so genannten „History-Tabelle“, aufgezeichnet werden. Auch diese Dateien sind dann nach einer Sitzung zu löschen.
- Der Einsatz eines mehreren Rechnern zugänglichen Zwischenspeichers auf einem dezidierten Server bleibt von diesen Maßnahmen dann unberührt, wenn keine Aufzeichnungen über den Zugriff auf den Zwischenspeicher der zu bedienenden Rechner angefertigt werden.
- Neben dem Zwischenspeicher auf der Festplatte kann ein Browser auch einen Zwischenspeicher im Hauptspeicher des lokalen Rechners unterhalten. Wenn der Browser die Erstellung eines Inhaltsverzeichnisses für diesen Zwischenspeicher unterstützt, muss der Nutzer ebenfalls vor einer möglichen Ausspähung geschützt werden. Dies kann dadurch erreicht werden, dass der Nutzer das Browserprogramm nach einer Sitzung beendet. Hierauf muss die Bibliothek in den Nutzungsbedingungen und durch deutlich erkennbare Hinweise aufmerksam machen.
- Bei den Browsern werden meist noch die zuletzt besuchten 10 bis 15 Internet-Adressen notiert. Diese Informationen sind im Regelfall für jeden späteren Nutzer über einen Mausklick einsehbar. Auch sie müssen deshalb gelöscht werden, wenn ein Nutzer seine Sitzung beendet.
- Als weiteres auf dem lokalen Rechner gespeichertes personenbezogenes Datum erweisen sich die auch in anderer Hinsicht nicht unpro-

blematischen und bereits oben angesprochenen „Cookies“. Durch Cookies können beispielsweise Einstellungen für den Zugriff auf WWW-Seiten festgehalten werden. Die Cookie-Attribute selbst werden häufig verschlüsselt abgespeichert, sodass der Nutzer nicht erkennen kann, welche Informationen durch das Cookie gespeichert werden. Insbesondere bei Angeboten, die eine Identifizierung der Nutzer erfordern, besteht die Gefahr, dass zur benutzerfreundlichen Gestaltung wiederholte Anmeldungen über in Cookies abgelegten Informationen abgewickelt werden. Beispielsweise kann auch festgehalten werden, dass beim Besuch eines bestimmten WWW-Servers durch einen über das Cookie identifizierten Nutzer die Seiten dynamisch entsprechend den durch das Cookie spezifizierten Interessenschwerpunkten erstellt werden. Diese Informationen sollten anderen Nutzern nicht zugänglich gemacht werden. Um das sicherzustellen, muss das Browserprogramm nach Ablauf der Sitzung beendet und die Datei, in der die Cookies gespeichert sind, gelöscht werden.

4. Verschlüsselung – ein Dauerthema

Wenn es gilt, schutzbedürftige Daten vor unberechtigtem Lesen zu schützen, kommt dem Einsatz von Verschlüsselungstechniken eine immer größere Bedeutung zu. Deshalb spielte das Thema Verschlüsselung bei Beratungen eine wichtige Rolle.

4.1 Verschlüsselung beim BK-Outsourcing

Der Betrieb von Bürokommunikationssystemen der Landesverwaltung durch ein privates Unternehmen (BK-Outsourcing) beschäftigt uns schon seit mehreren Jahren. Unbestritten gehört dazu eine wirkungsvolle Verschlüsselung, damit das Personal des Auftragnehmers trotz seiner zwangsläufig umfassenden Zugriffsberechtigungen keine schutzbedürftigen Daten lesen und erst recht nicht ändern kann. Weil die zunächst verwendete Verschlüsselungstechnik nicht erste Wahl war, setzte ich mich bereits letztes Jahr dafür ein, ein Produkt, das für die Verschlüsselung beim BK-Outsourcing besonders geeignet erschien, auf seine Praxistauglichkeit zu testen (vgl. 21. Tätigkeitsbericht, LT-Drs. 12/5740, S. 17). Nachdem ein vom federführenden Innenministerium beauftragtes Beratungsunternehmen die Eignung des Produkts bestätigt hatte, bat das Ministerium den Outsourcing-Auftragnehmer, zu ermitteln, welche Auswirkungen dessen Einsatz auf den täglichen Betrieb des Outsourcings hat. Auch dabei zeigte sich seine Tauglichkeit. Seine Feuertaufe muss es nun in der Kultusverwaltung bestehen. Damit können alle Dateien eines Nutzers auf dem Server ohne aufwändiges Zutun verschlüsselt werden. Weil die Entschlüsselung der Daten in jedem Fall erst auf dem lokalen PC stattfindet, sind die Daten auch noch während der Übertragung zwischen Server und Client geschützt.

Dieses Programm entfaltet seinen Schutz bei allen EDV-Anwendungen, bei denen der Nutzer Texte, Tabellen oder andere Dateien, die auf einem so genannten Ablageserver gespeichert sind, bearbeitet. Greift er dagegen auf Daten in einer Datenbank zu, die vielen Nutzern zur Verfügung steht, oder ruft er seine E-Mail aus einem von der Dienststelle betriebenen E-Mail-Server ab, bedarf es speziell darauf abgestimmter Konzepte, um auch dabei einen vergleichbaren Schutz zu erreichen.

4.2 Schutzmaßnahmen bei der Internet-Nutzung

Wer Computer mit dem Internet verbindet, geht damit zahlreiche Risiken ein. Notwendig sind daher Maßnahmen wie Firewalls, die Hackerangriffe abwehren. Weil trotz aller Sorgfalt Lücken in diesen Schutzmauern nicht auszuschließen sind, empfiehlt es sich, schutzbedürftige Daten zu verschlüsseln, damit ein Angreifer, der die Barrieren überwunden hat, zumindest keine Daten im Klartext lesen kann. Weil davon auch das Innenministerium ausgeht und eine flächendeckende Verschlüsselung für nötig hält, bat es das Unternehmen, das es mit der Erstellung einer „Konzeptstudie zur Realisierung einer sicheren Internet-Anbindung der Landesverwaltung“ beauftragt hatte, in dieser auch zu

prüfen, welche Rolle die Verschlüsselung der Daten spielen kann. Bedauerlicherweise maß die Studie gleichwohl dieser Frage keine große Bedeutung bei und stellte lediglich ganz allgemein dar, wozu eine Verschlüsselung zu gebrauchen ist.

Bei näherer Betrachtung hätte sich gezeigt, dass die Verschlüsselung zwar einen guten zusätzlichen Schutz bietet, dieser aber nicht gegen alle denkbaren Angriffe wirksam ist. Viele Hacker sind beim Angriff auf einen Computer darauf aus, die Kennung des Administrators zu knacken. Gelingt ihnen das, können sie auf alle gespeicherten Daten zugreifen. Sind diese jedoch so verschlüsselt, dass sie nur für die jeweiligen Bearbeiter lesbar sind, kann auch der Administrator und demzufolge ein Hacker diese Daten nicht im Klartext lesen. Gegenüber solchen Angriffen bietet die Verschlüsselung zusätzlichen Schutz. Demgegenüber ist die Verschlüsselung wirkungslos, wenn es dem Angreifer z. B. mittels eines Computervirus gelingt, einen Nutzer, der zum Zugriff auf die verschlüsselten Daten berechtigt ist, zur Ausführung eines Programmes zu bringen, das dann auf gespeicherte Daten zugreift und diese an den Angreifer sendet. Zudem kann die Verschlüsselung keinesfalls verhindern, dass schutzbedürftige Daten durch einen Angreifer geändert oder gelöscht werden.

4.3 Verschlüsselung beim elektronischen Dokumentenversand

Eine Arbeitsgruppe der Organisationsreferenten der Ministerien befasste sich geraume Zeit mit der Frage, in welchen Fällen Daten verschlüsselt zu übertragen sind und wann darauf verzichtet werden kann. Sie kam, was zu erwarten war, zum Ergebnis, dass personenbezogene oder andere schutzbedürftige Daten beim Versand über das Internet oder andere offene Netze zu verschlüsseln sind. Beim Versand von Daten über andere Übertragungswege gehen allerdings die Auffassung der Arbeitsgruppe und unsere um einiges auseinander:

– Verschlüsselung innerhalb eines lokalen Netzwerks

Bei der Datenübertragung in lokalen Netzwerken (LAN) sah die Arbeitsgruppe in der Regel keinen Grund zur Verschlüsselung. Wie bereits beim BK-Outsourcing aufgezeigt, kann aber im LAN ebenfalls eine Verschlüsselung erforderlich sein. Auch wenn ein lokales Netz über mehrere Standorte verteilt ist, die durch angemietete Telekommunikationsleitungen miteinander verbunden sind, sind Vertraulichkeit und Unverfälschtheit (Integrität) der im lokalen Netz übertragenen Daten ohne Verschlüsselung nicht ohne weiteres sichergestellt. Ein Verzicht auf Verschlüsselung im LAN als Regelfall kann daher allenfalls bei solchen Dienststellen in Frage kommen, die ihre Netzinfrastruktur und ihr BK-System selbst betreiben. Aber auch dann kann der Umgang mit besonders sensiblen personenbezogenen Daten die Verschlüsselung erfordern. Die Verschlüsselung ist beispielsweise geeignet zu verhindern, dass der Systemverwalter eines Landratsamts auf Daten des Gesundheitsamts oder einer psychologischen Beratungsstelle, die zum Landratsamt gehören, zugreifen kann.

– Verschlüsselung im Landesverwaltungsnetz

Auch bei dem von einem privaten Unternehmen betriebenen Landesverwaltungsnetz oder bei vergleichbaren Netzen sah die Arbeitsgruppe „nur für wenige Dateien“ die Notwendigkeit, sie zu verschlüsseln. Ein solcher grundsätzlicher Verzicht auf die Verschlüsselung wäre nur vertretbar, wenn auf andere Weise zuverlässig sichergestellt ist, dass die übertragenen Daten nicht unberechtigt gelesen werden können. Da das vom Betreiber des Landesverwaltungsnetzes selbst erarbeitete Datenschutz- und Sicherheitskonzept keine konkreten Aussagen über die ergriffenen Schutzmaßnahmen enthält (vgl. 21. Tätigkeitsbericht, LT-Drs. 12/5740, S. 18) und auch die weiteren, uns im Laufe des Jahres zur Verfügung gestellten Unterlagen in dieser Hinsicht Fragen offen ließen, kann man nicht ohne weiteres die Sicherheit des Netzes unterstellen.

Leider folgte der Landessystemausschuss weitgehend dem Vorschlag der Arbeitsgruppe. Es wird weitere Überzeugungsarbeit zu leisten sein.

5. Remote-Access-Technik – eine sinnvolle Nutzung des Internets

Mit dem durch die Liberalisierung des Telekommunikationsmarkts einhergehenden Ausbau der Telekommunikationsnetze erschließen sich auch für die Behörden und sonstigen öffentlichen Stellen im Lande völlig neue, kostengünstige Möglichkeiten, ihre Rechnernetze zu realisieren. Bisher mieteten sie für diesen Zweck in der Regel exklusiv Standleitungen an, die dann allerdings insbesondere in den Nachtstunden meist nicht optimal ausgelastet waren. Insbesondere gewinnt die Nutzung des Internets als Basis eines Behördennetzes beispielsweise auf kommunaler Ebene auf Grund der flächendeckenden Verfügbarkeit von Einwählknoten und der günstigen Kosten vermehrt an Bedeutung. Die Anbieter von Telekommunikationsausrüstung haben darauf reagiert und bieten seit längerem technische Lösungen zur Realisierung eines virtuellen privaten Netzwerks (VPN) an. Damit ist es möglich, ein in die Infrastruktur des Internets eingebettetes, abgeschlossenes privates Netzwerk aufzubauen. Derartige Lösungen sind freilich nur zulässig, wenn sichergestellt ist, dass Unberechtigte nicht auf Daten lesend oder gar schreibend zugreifen können und die an das Internet angeschlossenen Netze und Rechner ausreichend vor Angriffen aus dem Internet geschützt sind. Wenn öffentliche Stellen ihre Telekommunikationsnetze auf der Basis eines VPN realisieren wollen, müssen sie deshalb folgenden Anforderungen Rechnung tragen:

– Der Aufbau einer Verbindung muss über fälschungssichere Authentifizierungsmechanismen erfolgen. Dabei muss sich nicht nur der Initiator der Verbindung gegenüber dem Rechenzentrum, sondern umgekehrt auch dieses gegenüber demjenigen, der die Verbindung aufbauen will, zweifelsfrei identifizieren. Nur so kann dieser sicher sein, dass die beabsichtigte Verbindung tatsächlich auch zustande gekommen ist. Die normale Benutzerauthentifizierung von Betriebssystemen durch Benutzerkennung und Passwort reicht für diesen Zweck nicht aus. Vielmehr sind zertifikatsbasierte Lösungen durch Chip-Karten vorzuziehen.

– Alle Daten, die über eine Internet-VPN-Verbindung übertragen werden sollen, müssen hinreichend sicher verschlüsselt werden.

Wird, wie z. B. bei der Einrichtung von Telearbeitsplätzen, ein einzelner PC über ein VPN an ein Behördennetz angebunden, sind folgende flankierende Maßnahmen vorzusehen:

– Die Systemintegrität des PC muss sichergestellt sein. Das bedeutet, dass Betriebssysteme, die keine Trennung in Administratorenrolle und Benutzerrolle kennen und damit jedem Nutzer beliebige Zugriffsrechte beispielsweise auf Dateien und Systemkonfiguration einräumen, nicht eingesetzt werden dürfen. Wissentliche oder unwissentliche Änderungen an der Konfiguration der VPN-Software oder des Betriebssystems dürfen für normale Nutzer nicht möglich sein.

– Neben VPN-Verbindungen dürfen vom PC aus keine weiteren Verbindungen zum und vom Internet möglich sein. Eine Realisierung setzt daher den Einsatz einer sog. Personal Firewall auf dem einzelnen PC voraus, der nur die VPN-Verbindungen gestattet. Soll der PC auf das Internet zugreifen können, so darf der Zugriff nur über die VPN-Verbindung und über das Behördennetz erfolgen.

– Wenn die Netze größerer Organisationseinheiten miteinander verbunden werden, muss die Anbindung ohnehin über ein Firewall-System geschehen, wobei dann auch Maßnahmen gegen Denial-of-Service-Angriffe auf die die VPN-Verbindung herstellenden Netzknotenrechner ergriffen werden sollten. Beispielsweise muss es im Zusammenwirken mit dem Service-Provider möglich sein, kurzfristig die IP-Adresse und, sofern notwendig, den IP-Namen dieser Router zu ändern, um so derartigen Angriffen ihre Gefährlichkeit zu nehmen.

6. Internet-Wahlen – Idee mit Zukunft oder Büchse der Pandora?

Wohin man auch schaut – bei Bundestags-, Landtags- oder Kommunalwahlen – lässt die Wahlbeteiligung oft sehr zu wünschen übrig. Dies hat natürlich verschiedene Ursachen, eine davon ist gewiss die Bequemlichkeit mancher Wähler, die weder das Wahllokal aufsuchen noch das Verfahren der Briefwahl durchlaufen wollen. Ist dann noch am Wahltag schlechtes Wetter, bleiben manche, die eigentlich zur Wahl gehen wollten, daheim in der warmen Stube. Wäre es da nicht ein Segen, wenn der Wähler seine Stimme vom heimischen PC aus via Internet abgeben könnte? Derartige Ideen gibt es schon seit geraumer Zeit und im Rahmen eines Modellprojekts wurde an der Universität Osnabrück schon eine amtliche Wahl per Internet durchgeführt. Zwei Städte im Land wollten da nicht hintan stehen. Sie entschlossen sich, die Wahl ihrer Jugendgemeinderäte über das Internet durchzuführen in der Hoffnung, dadurch die Jugendlichen über ein ihnen vertrautes Medium zu erreichen und zur Stimmabgabe zu animieren. Weil die Gemeindeordnung nur regelt, dass ein Jugendgemeinderat eingerichtet werden kann, nicht aber wie dieser zustande kommt, gibt es dafür auch keine rechtlichen Hindernisse. In beiden Städten bestand aber Einigkeit darüber, dass die Wahl allgemein, frei, gleich und geheim sein sollte. Als wir jedoch die Konzeptionen näher unter die Lupe nahmen zeigte sich: Auch hier ist nicht alles Gold was glänzt. Die getroffenen technischen und organisatorischen Schutzvorkehrungen waren nicht so, dass eine 100%ige Garantie für allgemeine, freie, gleiche und geheime Internet-Wahlen gegeben war.

– Der Wahlserver

  Damit eine Stimme tatsächlich gewertet wird und nicht auf Abwege gerät, muss gewährleistet sein, dass der Wähler tatsächlich mit dem Wahlserver der Gemeinde in Verbindung tritt. Hierzu bedarf es des Einsatzes authentifizierender Mechanismen über so genannte Serverzertifikate, die den Wahlrechner gegenüber dem Wähler auf sichere Art und Weise eindeutig identifizieren. Andernfalls könnte sich ein übel meinender Zeitgenosse dazwischen schalten, sodass abgegebene Stimmen bei ihm auf- oder durchlaufen. Eine derartige Authentifizierung gab es bei beiden Wahlen nicht.

– Der Netzzugang

  Selbstverständlich dürfen Wähler bei der Stimmabgabe nicht behindert werden. Genau das war aber in einer Stadt der Fall, weil durch Defizite in der Konfiguration des Internet-Namensdienstes DNS die Wähler, die den Zugriff auf das Internet über einen von ihrem Provider betriebenen so genannten Proxy-Server vornahmen, keine Verbindung zu dem Wahlrechner der Gemeinde aufbauen konnten.

  Um einen ungehinderten Zugang zum Wahlserver zu gewährleisten, gilt es aber auch Folgendes zu bedenken:

  Das Verfahren muss so gestaltet sein, dass es unabhängig davon funktioniert, welchen Browser der Wähler verwendet.

  Darüber hinaus muss sichergestellt sein, dass niemand den Zugriff auf den Wahlserver einschränken oder verhindern kann, indem er den Rechner dermaßen in Anspruch nimmt, dass andere Teilnehmer nicht mehr auf dieses System zugreifen können. Es ist also die effiziente Abwehr dieser so genannten Denial-of-Service-Angriffe vonnöten.

– Die Anonymisierung

  Eine der beiden Städte verwendete zur Anonymisierung sog. Transaktionsnummern (TAN). Diese wurden von einem Trust-Center generiert und in verschlossenen Umschlägen an die Stadt geschickt. Diese wiederum sandte die Umschläge zusammen mit den übrigen Wahlunterlagen an die wahlberechtigten Jugendlichen. Bei der Stimmabgabe mussten die Wähler dann die TAN dem elektronischen Votum hinzufügen. Dieses Vorgehen hätte der Feststellung, wer welche Stimme abgegeben hat, Tür und Tor geöffnet. Die mit der Durchführung der Wahl betrauten Mitarbeiter der Stadt hätten dazu nur die Umschläge mit den TAN öffnen, die

TAN notieren, anschließend in einen anderen Umschlag stecken und aufschreiben müssen, welche TAN an welchen Wahlberechtigten geschickt worden war. Bei der Wahlhandlung hätten sie sich dann nur noch Zugang zu der Datei verschaffen müssen, in der die Stimmen gespeichert sind. So wäre die Anonymisierung ad absurdum geführt worden.

In der anderen Stadt wurde die Identifizierung des Wählers bei der Stimmabgabe nicht durch die Vergabe einer TAN, sondern mit einer Chipkarte vorgenommen. Zugleich wurde die Stimme mit dem öffentlichen Schlüssel eines asymmetrischen Verschlüsselungsverfahrens verschlüsselt und signiert zum Wahlrechner geschickt. Würden die verschlüsselten Stimmen zusammen mit der Signatur gespeichert werden, könnte derjenige, dem der private Schlüssel z. B. durch unvorsichtiges Verhalten des Wahlleiters oder seiner Mitarbeiter bekannt geworden ist, die Beziehung zwischen der Signatur, also dem Wähler, und seinem Votum herstellen. Mit dem Wahlgeheimnis wäre es aus und vorbei. Zudem muss technisch ausgeschlossen sein, dass der Wahlleiter, in dessen Besitz sich bis zur Auszählung der zu dem öffentlichen Schlüssel korrespondierende private Schlüssel befindet, Zugriff auf die Stimmzettel hat.

– Transparenz des Verfahrens

Bei manchen Wahlen kommt es auf eine oder einige wenige Stimmen an. Könnte bei einer Internet-Wahl jemand, z. B. ein Mitarbeiter der Gemeinde, der über das notwendige technische Know-how verfügt, oder ein Programmierer mit im Verfahren versteckten Einfallstoren Stimmen verändern oder hinzufügen oder das Wählerregister manipulieren, kann das weitreichende Folgen haben. Deshalb muss hier besonders genau geprüft werden, dass das Verfahren ordnungsgemäß arbeitet und Manipulationen durch Verschlüsselung und andere Sicherungsmaßnahmen so weit wie möglich ausgeschlossen sind.

Bei Internet-Wahlen kann die automatisierte Auszählung im Rechner naturgemäß nicht mit Argusaugen überwacht werden. Deshalb ist es unerlässlich, auch den Auszählungsvorgang transparent zu machen und sich vorher vom ordnungsgemäßen Funktionieren der Auszählung zu vergewissern. Bei beiden Wahlen war das nicht der Fall. Ob beispielsweise durch einen beabsichtigten oder unbeabsichtigten Softwarefehler Stimmen nicht gezählt oder Stimmzettel mehrfach gezählt wurden, war nicht auszuschließen. Auch war nicht erkennbar, ob die Datenbanken, in denen die Stimmzettel anonymisiert gespeichert waren, gegen Manipulationen effektiv geschützt waren.

Wer eine Wahl durchführt, kann bei alledem nicht einfach darauf vertrauen, das erworbene Verfahren werde schon ordnungsgemäß funktionieren und keine Schwachstellen aufweisen. Vielmehr ist hier eine besondere Prüfung des Verfahrens auf Korrektheit am Platz. Die Zertifizierung der für den Wahlprozess eingesetzten Software durch eine neutrale und vertrauenswürdige Institution halte ich dabei für unerlässlich.

Alles in allem: Würden diese Verfahren der Internet-Wahl auch bei Landtags- oder Kommunalwahlen angewandt, wären sie teils als noch nicht sicher genug einzustufen und müssten nachgebessert werden, teils müsste durch Zertifizierung nachgewiesen sein, dass die nötigen Schutzmaßnahmen gegen Angriffe und Manipulationen im Verfahren auch vorhanden sind.

7. Die Mängelliste – Ergebnisse unserer Kontrollbesuche

Auch in diesem Jahr stellten wir bei Kontrollen eine ganze Reihe technisch-organisatorischer Mängel fest. Die folgende, keineswegs vollständige Übersicht soll einen Eindruck davon vermitteln, wo bei der Realisierung eines angemessenen technisch-organisatorischen Datenschutzes der Schuh drückt:

7.1 Verfahrensverzeichnis

Jede öffentliche Stelle, die automatisiert personenbezogene Daten verarbeitet, muss ein Verfahrensverzeichnis führen und darin eine Reihe datenschutzrelevanter Angaben über die von ihr eingesetzten EDV-Verfahren eintragen. Näheres hierzu ist unseren Hinweisen zum Verfahrensverzeichnis zu entnehmen, die im Internet unter *www.baden-wuerttemberg.datenschutz.de* abgerufen werden können. Eine solche schriftliche Dokumentation ist allein schon deswegen notwendig, damit die Stelle selbst den Überblick darüber behält, was sie mithilfe der EDV eigentlich tut und welche Daten sie auf welche Weise verarbeitet.

Drei Krankenhäuser führten nur unzulängliche Verfahrensverzeichnisse. Teils waren notwendige Angaben überhaupt nicht enthalten. Teils waren die Angaben zu allgemein und als Datenart beispielsweise nur medizinische Daten genannt.

Ein Bürgermeisteramt speicherte die Seriennummern für Passanträge mit einem Tabellenkalkulationsprogramm und erfasste dabei auch die Namen der Antragsteller. Es benutzte diese Datei wie eine Datenbank und gewährte mehreren Mitarbeitern Zugriff auf diesen Datenbestand. Auch solche Dateien müssen aber in das Verfahrensverzeichnis aufgenommen werden, wenn darin personenbezogene Daten dauerhaft gespeichert werden.

7.2 Zugriffsschutz

Werden personenbezogene Daten elektronisch gespeichert, sind diese gegen unberechtigte Nutzung zu schützen. Dazu gehört, dass

- sich alle Computernutzer mithilfe einer individuellen Anmeldung und einem geheimen Passwort gegenüber dem Computer als zugriffsberechtigte Nutzer ausweisen. Was dabei im Einzelnen zu beachten ist, ist unseren „Hinweisen zum Umgang mit Passwörtern“ zu entnehmen, die im Internet unter *www.baden-wuerttemberg.datenschutz.de* abrufbar sind,
- durch individuelle Zugriffsberechtigungen sichergestellt ist, dass jeder Computernutzer nur auf die Daten zugreifen kann, die er benötigt,
- Bildschirmschoner eingerichtet werden, die den Bildschirm automatisch nach einigen Minuten ohne Eingaben abdunkeln und mit einer Sperre versehen, die nur durch ein Passwort aufgehoben werden kann.

Leider war diesen altbekannten Anforderungen nicht durchweg Rechnung getragen:

- Passwortschutz unzulänglich

  In zwei Behörden waren weder Mindestlänge noch ein automatischer Verfall der Passwörter sichergestellt. Es gab auch keine Anmeldesperre nach mehreren Anmeldefehlversuchen und bei einem Passwortwechsel konnten frühere Passwörter wieder verwendet werden.

  In einem Krankenhaus verfielen einige der verwendeten Passwörter nicht automatisch nach einer gewissen Zeit. Ferner fehlte auch hier eine Anmeldesperre nach mehreren Fehlversuchen. Zudem war nicht sichergestellt, dass die Nutzer ihr vom Systemverwalter zugeteiltes Passwort bei der ersten Anmeldung durch ein eigenes ersetzen.

  Eine Beratungsstelle betrieb einen PC ganz ohne Passwortschutz und speicherte darauf Schreiben mit Informationen über Klienten und Vermerke über Beratungsgespräche. An einem weiteren PC garantierte der Passwortmechanismus weder eine Mindestlänge noch war die Anzahl der Anmeldefehlversuche beschränkt. Unzureichend war ferner, dass nach der Anmeldung jeder Nutzer auf alle im PC gespeicherten Daten zugreifen konnte, obwohl dies dienstlich nicht notwendig war. Alle diese Mängel wogen besonders schwer, da die PC vom Flur der Beratungsstelle aus frei zugänglich waren und die Bildschirmschoner nicht einmal einen Passwortschutz aufwiesen.

In einem Krankenhaus übernahmen jeweils zwei Ärzte für 24 Stunden die Funktion „Arzt vom Dienst“ und nutzten während dieser Zeit eine Benutzerkennung mit besonders umfangreichen Berechtigungen. Beim Schichtwechsel nannten sie den Nachfolgern jeweils das von ihnen gewählte Passwort. Dabei könnte leicht bekannt werden, wie der eine oder andere sein Passwort jeweils bildet. Ein Missbrauch der Kennung wäre nicht ausgeschlossen.

– Bildschirmschoner nicht datenschutzgerecht genutzt

Eine Stadt und ein Krankenhaus hatten zwar Bildschirmschoner eingerichtet, diese aber nicht mit einem Passwortschutz versehen.

Ein anderes Krankenhaus überließ es den Mitarbeitern, ob an ihren PC ein passwortgeschützter Bildschirmschoner zum Einsatz kam oder nicht.

Ein weiteres Krankenhaus hatte nur an einem Teil der von ihm eingesetzten PC passwortgeschützte Bildschirmschoner eingerichtet. Und selbst dort war der Schutz nur sehr gering: An mehreren Arbeitsplätzen bestand dieses Passwort nur aus einem Buchstaben. Über einem Monitor der Pforte war das Passwort auf einem Zettel notiert. Außerdem hätten die Mitarbeiter den Bildschirmschoner und dessen Passwortschutz jederzeit deaktivieren können.

7.3 Nur erforderliche Software installieren

Viele Computerprogramme können auch zur Verarbeitung personenbezogener Daten genutzt werden. Um ein mögliches Missbrauchsrisiko von vornherein so gering wie möglich zu halten, dürfen diese Programme nur dort installiert und zur Nutzung bereitgestellt werden, wo dies zur Erfüllung dienstlicher Aufgaben benötigt wird.

Zwei Behörden nahmen es damit offenbar nicht so genau: Die eine hatte an jedem Arbeitsplatz ein Datenbanksystem installiert, mit dem die Nutzer eigene Datenbanken hätten aufbauen und betreiben können. Aber längst nicht jeder Behördenmitarbeiter benötigt derart leistungsfähige Werkzeuge. Bei der anderen Dienststelle räumte eine stichprobenweise befragte Mitarbeiterin ein, Software nutzen zu können, die sie dienstlich nicht benötigt.

7.4 Dateifreigaben im Netz

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.

Bei zwei Kontrollen mussten wir feststellen, dass die Mitarbeiter von diesen Möglichkeiten Gebrauch gemacht hatten, ohne dass dies den für die EDV-Sicherheit Verantwortlichen bekannt war.

Problematisch war dabei, dass jeder Nutzer der vernetzten PC alle auf der lokalen Festplatte seines PC gespeicherten Daten zum Zugriff über Netz freigeben konnte. Eine spezielle Dienstanweisung oder sonstige organisatorische Vorgaben zum Umgang mit dieser Möglichkeit gab es in beiden Fällen nicht. Zudem war der Passwortschutz, der unberechtigte Zugriffe auf freigegebene Daten verhindern sollte, unzulänglich. Die Anzahl der möglichen Anmeldefehlversuche war nämlich nicht beschränkt.

7.5 Diskettenlaufwerke

Ein frei zugängliches Diskettenlaufwerk birgt stets das Risiko, dass Computerviren oder andere unerwünschte Programme oder Daten auf den PC gelangen sowie dass umgekehrt personenbezogene Daten vom PC abgezogen und Dritten, für die sie nicht bestimmt sind, zugänglich werden. Außerdem kann der Computer, sofern dies nicht über weitere Einstellungen verhindert wird, über das Diskettenlaufwerk mit einem

fremden Betriebssystem gestartet und mit dessen Hilfe vorhandene Zugriffsbeschränkungen möglicherweise umgangen werden. Um all das zu verhindern, sollten Diskettenlaufwerke, die nicht regelmäßig für dienstliche Zwecke benutzt werden, verriegelt oder deaktiviert werden.

Dies wird nicht überall beherzigt: Obwohl die Mitarbeiter zweier Dienststellen in der Regel nicht mit Disketten an ihrem PC arbeiten mussten, konnte jeder die Diskettenlaufwerke seines PC nutzen.

7.6 Computerreparatur

Wer einen Computer oder eine Festplatte, auf dem personenbezogene Daten gespeichert sind, zur Reparatur gibt, muss besonders sorgfältig vorgehen. Ein Landratsamt, das es daran hatte fehlen lassen, sah sich plötzlich damit konfrontiert, dass eine von ihm früher genutzte Festplatte, auf der noch ca. 900 Schreiben der Führerscheinstelle gespeichert waren, auf einem Flohmarkt auftauchte. Dabei stellten wir unter anderem fest:

– Daten zu lange gespeichert

  Als die Festplatte ausgewechselt wurde, waren darauf bis zu 5 Jahre alte Schreiben gespeichert. Da die gespeicherten Briefe in erster Linie der Abwicklung der Korrespondenz dienten, hätte auch eine Speicherdauer von drei Monaten ausgereicht.

– Keine Datenschutzvereinbarung bei Reparaturauftrag

  Obwohl das Landratsamt bereits vermutete, dass der Defekt des PC mit der Festplatte zu tun hatte, traf es im Auftrag keine spezielle Vereinbarung über den Umgang mit den auf der Festplatte gespeicherten personenbezogenen Daten.

7.7 Fernwartung

Wird ein Unternehmen mit Fernwartungsarbeiten betraut, erfordert dies einen schriftlichen Auftrag. Da dabei eine fremde Stelle Zugriff auf das DV-System erhält, sind die notwendigen Datenschutzmaßnahmen präzise festzulegen. Woran dabei aus Sicht des Datenschutzes zu denken ist, ist unserer Orientierungshilfe zur Fernwartung zu entnehmen, die im Internet-Angebot meiner Dienststelle unter *www.baden-wuerttemberg.datenschutz.de* abgerufen werden kann.

Vier Aufträge, die diesen Anforderungen nicht gerecht wurden, hatte ein Krankenhaus und nicht weniger als sieben solcher Aufträge hatte eine Stadtverwaltung abgeschlossen. Letztere hatte zudem die zum Verbindungsaufbau erforderlichen Passwörter im Klartext in einer Tabelle notiert. Leicht hätten sie dadurch Unberechtigten bekannt werden können.

Bei einem weiteren Krankenhaus und zwei Behörden war nicht nur das Fehlen jeglicher schriftlicher Vereinbarungen zu bemängeln, dort hätte der Auftragnehmer sogar jederzeit auch ohne Mitwirkung oder vorherige Information des Krankenhauses auf dessen Computer zugreifen können.

Ein Krankenhaus gestattete seinem Auftragnehmer die Einschaltung von Unterauftragnehmern, allerdings ohne sich vorzubehalten, Subunternehmen, die es nicht als ausreichend zuverlässig ansieht, vom Online-Zugriff auf seine Computer auszuschließen. Ferner hätte der Auftragnehmer vertraglich verpflichtet werden müssen, seinerseits die Subunternehmer vertraglich zur Einhaltung der gleichen Datenschutzregelungen zu verpflichten, die er zu beachten hat.

7.8 Internet-Anschluss

Der Anschluss eines Computernetzwerks an das Internet bringt vielfältige Risiken für den Datenschutz mit sich. Einen Überblick darüber sowie über mögliche Gegenmaßnahmen gibt unser Merkblatt zu Internet und Datenschutz, das im Internet unter *www.baden-*

wuerttemberg.datenschutz.de zum Abruf bereitsteht. Erfreulich war, dass alle Stellen ihr lokales Netzwerk durch eine Firewall vor den im Internet lauernden Gefahren abgesichert hatten. Bei der Art und Weise, wie diese geplant und realisiert wurde, gab es jedoch eine Reihe von Unzulänglichkeiten:

– Keine redundante Auslegung sicherheitsrelevanter Funktionen

  Während es zu einer sicherheitsorientierten Vorgehensweise bei der Realisierung von Firewalls gehört, sicherheitskritische Bestandteile der Firewall mehrfach und in technisch unterschiedlicher Ausführung zu realisieren (Prinzip von Redundanz und Diversifikation), hatten eine Stadtverwaltung und zwei Krankenhäuser diese jeweils nur in einfacher Ausführung realisiert.

– Zu viele Kommunikationsmöglichkeiten gestattet

  Bei der Konfiguration einer Firewall ist stets nach dem Grundsatz vorzugehen, dass nur die unbedingt notwendigen Kommunikationsmöglichkeiten zugelassen werden. Ein Krankenhaus hatte jedoch mehrere Kommunikationsmöglichkeiten gestattet, die niemand dienstlich benötigte. Für die Durchführung von Systemarbeiten war ferner der Verbindungsaufbau mit einem einzelnen Computer notwendig: Das Krankenhaus hatte aber den Verbindungsaufbau zu beliebigen Computern im Internet gestattet.

– Verbindungen an der Firewall vorbei zugelassen

  Ein Krankenhaus ließ es zu, dass eine Systemverwalterin von ihrem vernetzten internen Arbeitsplatz-PC unter Umgehung der Firewall ungeschützt auf das Internet zugreifen konnte.

– Unzureichender Schutz vor Gefahren, die von aktiven Web-Inhalten ausgehen

  Drei Krankenhäuser und eine Stadtverwaltung hatten keine ausreichenden technischen und organisatorischen Maßnahmen ergriffen, um sich vor unerwünschten Wirkungen der beim Surfen anzutreffenden aktiven Inhalte wie z. B. Java, JavaScript, Active-X-Controls zu schützen.

– Konzeptionelle Mängel

  Ein Krankenhaus hatte die für die Einrichtung einer Firewall unerlässliche schriftliche Konzeption nur lückenhaft erstellt: Weder war ihr zu entnehmen, wozu es den Internet-Anschluss benötigt, noch war genannt, welche Risiken die geplante Nutzung mit sich bringt und wie diese vermieden werden sollen. Auch die von einer Stadt vorgelegte Konzeption schwieg sich zu den Punkten Kommunikationsbedarf und Risiken aus. Außerdem hieß es darin, sie sei lediglich als „erster Konfigurationsvorschlag“ anzusehen. Ein anderes Krankenhaus erreichte nicht einmal dieses Niveau: Es musste einräumen, dass es seinen Internet-Anschluss ganz ohne schriftliche Konzeption realisiert hatte.

7.9 Einwahlverbindungen

Wer seine Computer mit dem öffentlichen Telekommunikationsnetz verbindet und beispielsweise für die Fernwartung die Einwahl per ISDN oder Modem auf diese Computer gestattet, öffnet damit eine Tür, durch die unter Umständen auch ungebetene Gäste auf den Computer gelangen können. Notwendig ist daher, sich genau zu überlegen, wie die Einwahlmöglichkeiten gestaltet werden, und für jede Konfigurationsoption zu prüfen, ob diese für die angestrebte Nutzung notwendig ist. Daran ließ es ein Krankenhaus mangeln, das für die Einwahlverbindungen nicht nur das tatsächlich benötigte Kommunikationsprotokoll, also quasi die Sprache, mit der sich die Computer miteinander verständigen, sondern gleich noch zwei weitere zugelassen hatte.

7.10 Sicherheitsrelevante Einstellungen der Netzknoten-Computer nicht bekannt

Verbindet man ein lokales Netzwerk mit dem Landesverwaltungsnetz oder dem Kommunalen Verwaltungsnetz, so eröffnet dies weitreichende Möglichkeiten zum Datenaustausch mit anderen, an diese Netze angeschlossenen Stellen. Inwieweit diese Möglichkeiten tatsächlich bestehen, hängt unter anderem von den Einstellungen der zur Netzkoppelung verwendeten Netzknoten-Computer (Router) ab. Mitunter ist den Dienststellen gar nicht bekannt, wie diese Netzknoten-Computer konfiguriert sind und welche Daten sie passieren lassen und welche nicht. Ohne dieses Wissen lässt sich aber nicht beurteilen, ob und, wenn ja, welche Sicherheitsrisiken sich aus diesem Anschluss für ihr internes Netz ergeben. Zwei Justizbehörden verfügten nicht über diese Informationen.

7.11 Drucker im Serverraum

Wer über ein modernes lokales Netzwerk verfügt, speichert in der Regel alle selbst erstellten Schreiben, die in Datenbanken erfassten Datensätze sowie sonstige Daten zentral auf speziell dafür eingerichteten Servern. Das macht es nötig, diese Server besonders zu schützen. Dazu gehört, dass Server in einem Raum aufgestellt sein sollten, der nicht noch anderen Zwecken dient.

Das ließ ein Krankenhaus außer Acht, das in einem Raum neben einem Buchhaltungsserver noch mehrere Drucker betrieb und allen Mitarbeitern der Buchhaltung gestattete, diesen Raum zu betreten. Wie zur Demonstration, wie problematisch dies ist, lag zum Zeitpunkt unseres Kontrollbesuchs auf dem Server auch noch ein Sicherungsband, das man mühelos hätte mitnehmen können.

7.12 Löschung unvollständig und ohne Konzept

Öffentliche Stellen dürfen personenbezogene Daten nicht ewig speichern, sondern stets nur so lange, wie dies zur Erledigung ihrer Aufgaben erforderlich ist. Unumgänglich ist daher, dass jede Stelle für sich festlegt, wie lange sie die einzelnen Datenarten benötigt und wann sie zu löschen sind. Doch eine solche Festlegung fehlt häufig.

7.13 Dienstanweisung

Jede Stelle, die personenbezogene Daten verarbeitet, muss die zum Datenschutz erforderlichen Verhaltensregeln für die Mitarbeiter in einer Dienstanweisung zum Datenschutz festlegen. Dies geschieht nicht immer mit der notwendigen Sorgfalt:

Ein Krankenhaus besaß nur eine unvollständige Dienstanweisung und bei einer Stadtverwaltung existierte sie nur als Entwurf. Ein Landratsamt hatte überhaupt keine erlassen und meinte dazu, die im Landesdatenschutzgesetz verankerte Pflicht zum Ergreifen der erforderlichen Schutzmaßnahmen verpflichte ja unmittelbar jeden Mitarbeiter, das jeweils Notwendige zu tun. Weiteres sei überflüssig.

4. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheitswesen

1. Dauerpatient Krankenhaus

Wer sich als Patient zur Behandlung ins Krankenhaus begibt, erwartet meist nicht nur, dass er nach den Regeln der ärztlichen Kunst versorgt, sondern hofft auch, dass ihm Verständnis für seine persönlichen Sorgen und Nöte entgegengebracht wird. Dass aber auch die Krankenhäuser Probleme haben, mit den an sie gestellten vielfältigen, oft nur schwer miteinander zu verein-

barenden Anforderungen zurecht zu kommen, wird meist nicht gesehen. Als Landesdatenschutzbeauftragter komme ich häufig mit Krankenhausleitungen, aber auch mit Krankenhausärzten ins Gespräch und höre ihre Klagen. Von daher habe ich ein gewisses Verständnis dafür, dass auch in Sachen Datenschutz nicht immer alles so optimal läuft, wie man es sich wünschen würde. Bei allem Verständnis kommt man aber gleichwohl nicht an der Tatsache vorbei, dass die Art und Weise, wie ein Krankenhaus mit Patientendaten umzugehen hat, gesetzlich vorgeschrieben ist. In diesem Spannungsverhältnis, einerseits den Klinikbetrieb mit den zur Verfügung stehenden Ressourcen möglichst effizient und reibungslos zu gestalten, andererseits aber (auch) die Datenschutzbestimmungen und vor allem die ärztliche Schweigepflicht zu beachten, gilt es, möglichst einen tragfähigen Ausgleich zu finden. Das Bestreben meines Amtes ist und war es bisher, Augenmaß zu wahren und, soweit rechtlich vertretbar, praktikable Lösungen zu suchen und zu akzeptieren. Aus ihrer Verantwortung für die Einhaltung der vom Gesetzgeber aus wohlüberlegten Gründen getroffenen Regelungen über den Umgang mit Patientendaten kann ich dabei allerdings die Krankenhäuser nicht entlassen. So gibt es nach wie vor Mängel, die in unseren Tätigkeitsberichten schon mehrfach gerügt worden waren und die von daher eigentlich nicht mehr vorkommen dürften. Dies ist vor allem dann ärgerlich, wenn es sich um Mängel handelt, die ohne großen technischen und finanziellen Aufwand beseitigt werden könnten. Hierzu gehört, ich mag es schon fast nicht mehr schreiben, das unsinnige Abfragen überflüssiger persönlicher Daten bei der Krankenhausaufnahme. Völlig unbeeindruckt von meiner mehrfachen Beanstandung dieser Praxis in der Vergangenheit wird munter drauflos gefragt. Dafür, dass solche Informationen über die Lebensumstände des Einzelnen ein höchstpersönliches Gut sind, mit dem sorgsam umgegangen werden muss, fehlt offenbar das Gespür. Mitunter, vor allem dann, wenn ich einen Kontrollbesuch meines Amtes angekündigt habe, fällt schließlich doch noch der Groschen. So in einem Kreiskrankenhaus, das schnell noch einen älteren Tätigkeitsbericht zurate gezogen und versucht hatte, vor dem Besuch wenigstens die gröbsten Mängel zu beseitigen. Als wir uns dann vor Ort informierten, zeigte sich, dass sich die Änderungen bei den betroffenen Mitarbeitern und Mitarbeiterinnen noch gar nicht herumgesprochen hatten. Die waren bass erstaunt, dass sie auf bestimmte Funktionen plötzlich nicht mehr zugreifen konnten. Während dessen mussten wir in einem anderen von uns besuchten Kreiskrankenhaus den Eindruck gewinnen, dass dort die datenschutzrechtliche Diskussion um die Datenerhebung bei der Aufnahme offenbar völlig spurlos vorbeigegangen ist. Die Mängelliste war ebenso vollständig wie die Bereitschaft groß war, sofort in Aktion zu treten und alles nach unseren Vorstellungen umzugestalten.

Von den insgesamt drei Kontrollbesuchen in Krankenhäusern ist Folgendes erwähnenswert:

1.1 Die Auftragsdatenverarbeitung

In unserem letzten Tätigkeitsbericht (21. Tätigkeitsbericht 2000, LT-Drs. 12/5740, S. 23 ff.) bin ich ausführlich auf die sich aus der Änderung des § 48 Abs. 2 des Landeskrankenhausgesetzes (LKHG) ergebenden Konsequenzen eingegangen. Die Verarbeitung von Patientendaten außerhalb des Krankenhauses ist gesetzlich nur noch durch Rechenzentren zugelassen. In der Praxis üblich ist es aber, dass Krankenhäuser beispielsweise ihre ausgesonderten Akten und sonstige Datenträger durch private Firmen entsorgen lassen. Eines der kontrollierten Krankenhäuser lässt Arztbriefe von einem privaten Schreibbüro schreiben. Was immer wieder, so auch bei den diesjährigen Kontrollbesuchen, festgestellt wird, ist, dass die für eine solche Praxis erforderlichen vertraglichen Grundlagen fehlen. Will nämlich ein Krankenhaus Teile seiner Datenverarbeitung von einem Dritten erledigen lassen, muss es mit diesem einen Vertrag schließen. In diesem muss sich der Auftragnehmer verpflichten, einen Datenschutzstandard zu gewährleisten, wie er beim Krankenhaus vorausgesetzt wird. Es darf dabei aber nicht bei allgemeinen Verpflichtungen bleiben. Das Krankenhaus hat vielmehr darauf zu achten, dass konkret festgelegt wird, was der Auftragnehmer an einzelnen technischen und organisatorischen Maßnahmen ergreifen

muss. Hinzu kommt, dass der Patient über die beabsichtigte Verarbeitung seiner Daten außerhalb des Krankenhauses informiert und gefragt werden muss, ob er damit einverstanden ist. Das Krankenhaus, das Gesundheitsdaten eines Patienten aus der Hand gibt, ohne dass es diesen hierzu um Erlaubnis gebeten und ohne dass es dem Auftragnehmer vorgeschrieben hat, wie er mit den Daten umzugehen hat, handelt unverantwortlich. Ich habe diese Missstände beanstandet und die kontrollierten Krankenhäuser aufgefordert, noch ausstehende Verträge umgehend abzuschließen. Ebenfalls aufgefordert habe ich sie, in den Fällen, in denen die Patienteneinwilligung erforderlich ist, eine ordnungsgemäße Patienteninformation sowie ein Einwilligungsformular zu erarbeiten. Beides wurde zugesagt.

1.2 Die Archivierung der Patientendokumentation

Noch ist die Digitalisierung der Datenverarbeitung in den Krankenhäusern nicht so weit fortgeschritten, dass auf herkömmliche Archive verzichtet werden kann. Dort sammeln sich im Laufe der Zeit Akten in solchen Mengen an, dass die Aufnahmekapazität an ihre Grenzen stößt. Im Archiv eines der kontrollierten Krankenhäuser waren etwa 320 000 Akten gelagert. Was dies konkret bedeutet, erschloss sich erst, als wir das Archiv besichtigten. Die Akten waren zum Teil in Kisten gestopft, die im Gang zwischen den Schieberegalen aufgereiht waren. Akten lagen auf den Schränken, im Zwischenraum zwischen den Schränken und der Wand, sogar am Boden des zum Außenbereich gelegenen Fensters, und zwar so, dass jeder, der draußen am Fenster vorbeiging, die Beschriftung auf den Akten, etwa den Patientennamen, ohne Mühe lesen konnte. Wie in diesem Chaos eine bestimmte Akte überhaupt noch aufzufinden war, blieb ein Geheimnis der dort tätigen Registraturkraft. Eine der Ursachen für diese Zustände war, wie sich herausstellte, dass das Krankenhaus seit seiner Gründung keine einzige Akte ausgesondert und vernichtet hatte. Es gab auch keine entsprechende Konzeption, wie mit Altakten zu verfahren sei, insbesondere für welchen Zeitraum sie aufbewahrt werden sollten. Dies verstößt gegen Datenschutzrecht, da nach § 9 Abs. 2 des Landesdatenschutzgesetzes (LDSG) organisatorische Regelungen getroffen werden müssen, die die Beachtung der datenschutzrechtlichen Erfordernisse gewährleisten sollen. Nach § 23 LDSG sind personenbezogene Daten dann zu löschen, wenn sie für die weitere Aufgabenerfüllung nicht mehr erforderlich sind. Sind sie zwar nicht mehr erforderlich, können sie aus bestimmten Gründen aber gleichwohl nicht gelöscht werden, sind sie nach § 24 LDSG zu sperren. Ob nun, was ich für richtig halte, für die Frage der fachlichen Erforderlichkeit einer Speicherung medizinischer Daten die 10-Jahres-Frist der ärztlichen Berufsordnung gilt oder ob eine längere Aufbewahrung mit Sperrung der Daten vonnöten ist, darüber kann diskutiert werden. Dass sich allerdings keines der kontrollierten Krankenhäuser zu dieser Frage Gedanken gemacht und eine Sperr- und Löschkonzeption erarbeitet hatte und die Patientendaten deshalb zum Teil über Jahrzehnte ohne erkennbaren Zweck gespeichert wurden, stellt eine Verletzung wesentlicher datenschutzrechtlicher Organisationspflichten dar. Dass es in keinem der kontrollierten Krankenhäuser eine schriftliche Registraturordnung mit klaren Handlungsanleitungen für das Personal über den Umgang mit den Patientendokumentationen gab, kommt hinzu und sei nur am Rande erwähnt.

Die Krankenhäuser haben diese Kritik akzeptiert und angekündigt, unverzüglich Abhilfe zu schaffen.

1.3 Vernichtung von Akten der Verwaltung

Die medizinische Patientendokumentation ist nach der ärztlichen Berufsordnung mindestens zehn Jahre lang aufzubewahren. Bei einem der kontrollierten Krankenhäuser wurde festgestellt, dass es auch die über den Patienten geführte Verwaltungsakte erst nach zehn Jahren vernichtet. Dies ist nicht richtig.

Zu den datenschutzrechtlichen Pflichten des Krankenhauses gehört es, personenbezogene Daten, die für die weitere Aufgabenerfüllung nicht

mehr erforderlich sind, zu vernichten. Die Verwaltungsakten enthalten die Patientendaten, die zur verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses, insbesondere zur Leistungsabrechnung, erforderlich sind. Diese Aufgabe ist spätestens dann erfüllt, wenn der Patient entlassen ist und der Sozialleistungsträger die Kosten erstattet hat. Nach einem Urteil des Bundessozialgerichts vom 17. Juni 1999 (Das Krankenhaus 2000, S. 39) verjähren Zahlungsansprüche eines Krankenhauses innerhalb von vier Jahren. Dieser Zeitraum kann auch als Anhaltspunkt für die Frage dienen, wie lange die Verwaltungsakten vorgehalten werden dürfen. Die Verwaltungsakten müssen deshalb spätestens sechs Jahre nach Ablauf des Kalenderjahrs, in dem die letzten abrechnungsfähigen Leistungen erbracht worden sind, ausgesondert und vernichtet werden. In dieser Frist ist auch ein ausreichend bemessener Zeitraum berücksichtigt, in dem eventuelle Rückfragen geklärt werden können. Das Krankenhaus hat dem zugestimmt.

1.4 Die Übersendung von Arztberichten

In einem der kontrollierten Krankenhäuser ging es bei der Versendung von Arztberichten recht unbürokratisch zu. Immer dann, wenn ein niedergelassener Arzt einen solchen Bericht anforderte, erhielt er ihn auch – wenn sich auf dem Anforderungsschreiben nur sein Arztstempel befand. Danach, ob er zur Anforderung tatsächlich auch berechtigt sei, wurde nicht gefragt. Nach § 46 Abs. 1 LKHG darf das Krankenhaus einem anderen Arzt Patientendaten ohne Einwilligung des Patienten aber nur dann übermitteln, wenn der Arzt den Patienten im Anschluss an die stationäre Behandlung ambulant weiterbehandelt. Vor einer Datenübermittlung hat sich das Krankenhaus hiervon stets zu überzeugen. Andernfalls muss es den anfordernden Arzt auffordern nachzuweisen, dass er zum Empfang der Daten berechtigt ist, etwa indem er eine Erklärung des Patienten darüber vorlegt, dass das Krankenhaus insoweit von der Schweigepflicht entbunden ist.

Bei dem Besuch zeigte sich außerdem, dass die Arztberichte regelmäßig per Telefax versendet wurden. Auch wenn der Faxversand von Dokumenten heute im Allgemeinen gang und gäbe ist, sollten Schriftstücke mit sensitiven Inhalten, wie dies gerade bei Arztberichten der Fall ist, grundsätzlich nur in besonders begründeten Ausnahmefällen in dieser Form übermittelt werden. Der Faxversand weist gegenüber dem herkömmlichen Versand per Brief besondere Risiken auf. So besteht die Gefahr, dass wegen einer nicht korrekten Eingabe der Zielrufnummer die Daten in falsche Hände gelangen. In der Regel weiß der Absender auch nicht, wo das Empfangsgerät steht und wer alles zu diesem Zugang hat. Nicht zu vernachlässigen ist schließlich auch die Abhörgefahr. Diese besteht zwar auch bei Telefongesprächen, ohne dass gefordert würde, vertrauliche Daten nicht mehr per Telefon auszutauschen. Im Unterschied zum Telefongespräch enthält allerdings ein per Fax versendeter Arztbericht sensitive Daten in konzentrierter Form, was es einem potenziellen Mitleser wesentlich leichter macht, an solche Daten heranzukommen. Ich habe das Krankenhaus deshalb aufgefordert, medizinische Unterlagen künftig nur noch ausnahmsweise per Fax zu versenden und in diesen Fällen Vorkehrungen zu treffen, die verhindern, dass Unbefugte von den Daten Kenntnis erlangen können. Das Krankenhaus hat mitgeteilt, es werde dies berücksichtigen.

1.5 Das Postverteilerzimmer

In einem der kontrollierten Krankenhäuser ist die Verteilung der Post so organisiert, dass in einem eigens dafür vorgesehenen Raum für jeden Arzt ein eigenes Postfach eingerichtet ist. Die Fächer waren zum Besuchszeitpunkt teils offen, teils verschließbar. Die Post wird jeweils in die Fächer einsortiert und kann dann vom Empfänger abgeholt werden. Gleichzeitig wird in dem Raum die vom Schreibdienst kommende Post in offenen Körben gesammelt, von einem Postfahrer abgeholt und zu den einzelnen Einheiten transportiert. Die zurückgehende Post wird vom Fahrer ebenfalls in offenen Körben transportiert und im Postraum abgestellt. Der Raum ist zwar verschlossen, Schlüssel haben aber neben

den einzelnen Postfachinhabern der Postfahrer, Bedienstete der Poststelle und das Reinigungspersonal. Ich habe diese Organisation als nicht datenschutzgerecht kritisiert.

Die zum Teil offenen Postfächer ermöglichen es, dass Personen, die sich, wenn auch durchaus zu Recht, im Postraum aufhalten, ungestört auf nicht für sie bestimmte Dokumente zugreifen und sich so unbefugt Kenntnisse über Patienten verschaffen können. Da diese Daten der ärztlichen Schweigepflicht unterliegen, kann die mangelhafte Organisation dazu führen, dass diese verletzt wird. Dies kann das zwischen Arzt und Patient bestehende Vertrauensverhältnis nachteilig beeinflussen. Dabei kommt es nicht darauf an, dass es in der Regel Ärzte sind, die Zugang zu dem Raum haben. Denn grundsätzlich besteht die Schweigepflicht auch unter Berufskollegen. Zum anderen hat auch nichtärztliches Personal Zugangsmöglichkeiten. Meiner Forderung, alle Postfächer verschließbar zu machen, will das Krankenhaus nachkommen.

Weiter habe ich gefordert, Patientenunterlagen nur noch in abschließbaren Behältnissen zu sammeln und auf dem Gelände des Krankenhauses zu transportieren. Auch dadurch reduziert sich die Gefahr, dass sich Unbefugte Kenntnis von den Inhalten der Schreiben verschaffen oder dass Post während des Transports verloren geht. Auch hierzu hat sich das Krankenhaus bereit erklärt.

1.6 Moloch Krankenhausinformationssystem

Die elektronische Datenverarbeitung hält in immer mehr Bereichen des Krankenhauses Einzug: Spielte sie anfangs nur bei der Buchhaltung und der Abrechnung der erbrachten Leistungen eine Rolle, so wird die EDV immer häufiger auch genutzt, um die medizinische Patientendokumentation zu führen. Unbestreitbar hat dies Vorteile sowohl für den Patienten als auch für das ärztliche und das Pflegepersonal. Nicht übersehen werden darf dabei aber, dass die schnelle, leichte und vollständige Verfügbarkeit der Patientendaten auch Risiken hinsichtlich des Datenschutzes mit sich bringt. Denn mehr und mehr Untersuchungsergebnisse, Therapiepläne und ärztliche Diagnosen werden elektronisch erfasst. Dabei erhalten nicht nur Ärzte Zugriff auf die in einem solchen Krankenhausinformationssystem gespeicherten Daten, sondern auch Pflegepersonal, Mitarbeiter der Verwaltung bis hin zu Mitarbeitern des Controllings, die ermitteln wollen, welche Selbstkosten dem Krankenhaus für seine Dienstleistungen entstehen und ob diese noch wirtschaftlich angeboten werden können. Wie die Praxis auch jetzt wieder bei den Kontrollbesuchen gezeigt hat, wird in den Krankenhäusern zu wenig darauf geachtet, wer alles auf welche Daten zugreifen kann. Auch innerhalb des Krankenhauses gelten nämlich die ärztliche Schweigepflicht und der datenschutzrechtliche Erforderlichkeitsgrundsatz. Dies bedeutet, dass nur die Personen innerhalb des Krankenhauses die – vor allem – medizinischen Daten über den Patienten zu Gesicht bekommen dürfen, die diese Daten für Behandlungszwecke brauchen. Der datenschutzgerechte Einsatz eines Krankenhausinformationssystems ist daher nicht möglich, ohne zuvor festzulegen, wer darin welche Daten lesen und bearbeiten darf. Diese Entscheidungen müssen dann in individuelle Zugriffsberechtigungen umgesetzt werden.

Leider geht jedoch nicht jedes Krankenhaus so vor.

Ein besonders schlechtes Beispiel gab in der Hinsicht das Kreiskrankenhaus Leonberg. Dort hatten mehr als 500 Mitarbeiterinnen und Mitarbeiter Zugriff auf die im Krankenhausinformationssystem gespeicherten Daten. Neben Ärzten, Chefarztsekretariaten, Pflegekräften, Funktionsdienst (wie z. B. der Krankenhaushygiene), Verwaltung, Controlling gehörte dazu auch die Finanzbuchhaltung.

Hinzu kam Folgendes: Das Kreiskrankenhaus Leonberg betreibt sein Krankenhausinformationssystem nicht selbst, sondern lässt dies gemeinsam mit den Kreiskrankenhäusern in Böblingen und Herrenberg von dem in Böblingen angesiedelten zentralen Krankenhausrechenzentrum erledigen. Dies machte es technisch möglich, dass einige Mitarbei-

ter Patientendaten sogar Krankenhaus übergreifend lesen oder ändern konnten. Weit gefehlt war aber die Annahme, dass das Krankenhaus Leonberg für alle diese Organisationseinheiten und Benutzergruppen festgelegt hätte, auf welche Patientendaten sie jeweils zugreifen dürfen und welche für sie tabu sind. Lediglich für den Pflegedienst hatte es eine solche Konzeption erarbeitet. Anhand welcher Kriterien die tatsächlich eingerichteten Zugriffsberechtigungen der übrigen Mitarbeiterinnen und Mitarbeiter zustande kamen, ließ sich nicht mehr im Einzelnen nachvollziehen. Zwar waren für den Bereich des gesamten Krankenhausrechenzentrums über 1 200 so genannte Zugriffsprofile hinterlegt, in denen jeweils eine ganze Reihe einzelner Zugriffsberechtigungen zusammengefasst sind. Aber schon unser Versuch, herauszufinden, welche dieser 1200 Profile tatsächlich auch Nutzern zugeordnet sind und welche nur Karteileichen darstellen, war zum Scheitern verurteilt. Auch als wir stichprobenweise nachfragten, warum bestimmte Nutzer und Nutzergruppen des Krankenhausinformationssystems auf zahlreiche Datenarten zugreifen konnten, erhielten wir keine befriedigende Antwort. Unumwunden räumte das Krankenhaus allerdings ein, dass es ursprünglich vielen Mitarbeitern sehr umfassende Zugriffsmöglichkeiten gewährte und diese erst nach und nach beschränkt hat. Dass es dabei auf halbem Weg stehen blieb, zeigte sich an einigen Feststellungen, die angesichts der Schwierigkeiten, überhaupt einen Überblick über die eingerichteten Berechtigungen zu erhalten, nur exemplarischer Natur sein können:

Vor unserem Kontrollbesuch konnten elf Mitarbeiter des Kreiskrankenhauses Leonberg, darunter mehrere Controller, alle im Krankenhausinformationssystem gespeicherten Daten lesen und ändern sowie die Systemkonfiguration beliebig ändern. In einem ersten Schritt reduzierte das Krankenhaus die Zahl dieser Berechtigungen von 11 auf 5. Bezogen auf den gesamten Bereich des Krankenhausrechenzentrums verfügten dann aber immer noch 20 Mitarbeiter, darunter 14 EDV-Mitarbeiter und 3 Controller, über das umfassende Profil.

Für das gesamte, vom Krankenhausrechenzentrum Böblingen betreute Informationssystem gab es ferner:

- 20 Mitarbeiter, die innerhalb der medizinischen Dokumentation alle Daten lesen und ändern und darüber hinaus auch die Systemkonfiguration ändern konnten,
- 20 Mitarbeiter, die innerhalb der Patientenverwaltung und Leistungsabrechnung alle Daten lesen und ändern sowie darüber hinaus auch die Systemkonfiguration ändern konnten,
- 30 Mitarbeiter, davon 17 aus dem ärztlichen Dienst des Kreiskrankenhauses Böblingen, die über ein Profil verfügten, das nur vorübergehend mit der Einführung einer neuen Softwareversion sinnvoll ist und es ermöglicht, alle in der neuen Version erstmals enthaltenen Funktionen zu nutzen.

Diese Benutzerkennungen erlaubten zudem nicht nur den Zugriff auf Daten eines Krankenhauses, sondern aller vom Krankenhausrechenzentrum betreuten Krankenhäuser.

Mit der Gewährung solch umfassender und vielfach mit Systemverwalter-Privilegien ausgestatteter Berechtigungen verfuhren die vom Krankenhausrechenzentrum Böblingen betreuten Kreiskrankenhäuser zu großzügig. Nicht erforderlich war beispielsweise, den Controllern allumfassenden Zugriffsmöglichkeiten zu gewähren. Das Recht, Patientendaten zu ändern, benötigen sie ebenso wenig wie die Möglichkeit, in die Konfiguration des gesamten Krankenhausinformationssystems einzugreifen. Aber selbst bei den lesenden Zugriffsmöglichkeiten stellt sich die Frage, ob Controller durchweg auf alle Patientendaten zugreifen können müssen. Viele vom Controlling durchzuführende Aufgaben sollten sich auch mit aggregierten Daten erledigen lassen, die keinen Rückschluss auf einzelne Patienten zulassen. Das Recht zum Zugriff auf Daten einzelner identifizierbarer Patienten sollte die Ausnahme bleiben. Nicht erforderlich war auch, 17 Nutzern des ärztlichen Diens-

tes des Kreiskrankenhauses Böblingen Sonderberechtigungen einzuräumen, die nur im Zusammenhang mit der Einführung neuer Softwareversionen sinnvoll sind. Generell war festzustellen, dass zu viele Mitarbeiter über umfassende Zugriffsberechtigungen verfügten.

Die Mängel im Zusammenhang mit der Gewährung von Zugriffsberechtigungen im Bereich der Kreiskrankenhäuser des Landkreises Böblingen waren insgesamt so gravierend, dass ich sie beanstanden musste. Der für die Krankenhäuser des Kreises zuständige Landrat sagte daraufhin Abhilfe zu. Die ausstehenden Festlegungen über die den einzelnen Organisationseinheiten zu gewährenden Zugriffsberechtigungen sollen getroffen und die tatsächlich am System eingerichteten Zugriffsmöglichkeiten dementsprechend konfiguriert werden. Darüber hinaus soll künftig ein Hilfsprogramm zur systematischen Erstellung von Zugriffsprofilen eingesetzt werden.

Wenn es sich hierbei auch um einen besonders gravierenden Fall handelte, so ist dies doch leider beileibe kein Einzelfall. Auch bei der Kontrolle eines anderen Krankenhausinformationssystems stießen wir auf ähnlich gelagerte Probleme.

Dass es aber auch anders geht, bewies das Psychiatrische Zentrum Nordbaden in Wiesloch: Es hatte vor der Einführung seines Krankenhausinformationssystems mit allen Organisationseinheiten Vorgespräche geführt und dabei erörtert, wer welche Zugriffsberechtigungen benötigt. Das Ergebnis dieser Erörterungen wurde in einer Zugriffsberechtigungstabelle eingetragen und diese zur Einrichtung der Berechtigungen im anschließend installierten Krankenhausinformationssystem herangezogen.

1.7 Die elektronische Patientenakte

Die Aufbewahrung der Patientenakten eines Krankenhauses erfordert große Lagerräume. Nur zu verständlich ist daher, dass immer wieder der Wunsch nach elektronischen Patientenakten aufkommt, die die Papierakten möglichst vollständig ersetzen sollen und deren digitale Aufbewahrung nur einen Bruchteil der Stellfläche des Aktenarchivs benötigt. Das Psychiatrische Zentrum Nordbaden in Wiesloch gehört zu den wenigen Einrichtungen, die bereits solche elektronischen Patientenakten verwenden. Wichtig ist, dass dabei stets nachgeprüft werden kann, wer welche Einträge in einer solchen Akte vorgenommen hat und dass nachträgliche Änderungen verhindert werden oder zumindest nicht unerkannt durchgeführt werden können. Das vom Psychiatrischen Zentrum eingesetzte EDV-Programm bietet die Möglichkeit, einzelne Einträge in einem speziellen Arbeitsschritt als endgültig zu markieren und damit spätere unerkannte Änderungen durch Ärzte oder Pflegekräfte zu verhindern. Offen blieb jedoch, ob Systemverwalter auch die als endgültig markierten Einträge der elektronischen Patientenakten unerkannt ändern können. Zwar muss die elektronische Akte selbst bei einer solchen Möglichkeit nicht zwangsläufig unsicherer sein als die klassische Aktenführung, bei der mit einigem Aufwand ebenfalls nachträgliche Manipulationen an Akten möglich sind. Gleichwohl baten wir darum, im Rahmen der Weiterentwicklung der elektronischen Aktenführung zu prüfen, ob die darin vorgenommenen Einträge nicht durch die Verwendung digitaler Signaturen, wie sie etwa beim elektronischen Grundbuch genutzt werden, noch besser vor unerkannten Änderungen geschützt werden können.

2. Die Gesundheitsämter

Mit Beschwerden darüber, dass ein Gesundheitsamt gegen den Datenschutz verstoßen habe, hat sich meine Dienststelle verhältnismäßig selten zu befassen. Ich werte dies als ein Zeichen dafür, dass sich die Amtsärzte ihrer ärztlichen Verantwortung auch hinsichtlich der Geheimhaltung dessen, was sie in Ausübung ihrer Tätigkeit über den Patienten erfahren, bewusst sind. Gleichwohl kommt es auch im Gesundheitsamt hin und wieder zu Fehlverhalten. So etwa in folgendem Fall:

2.1 Das Tauglichkeitsgutachten

Eine Straßenverkehrsbehörde hatte einen Bürger aufgefordert, ein amtsärztliches Gutachten über seine Eignung zum Führen von Kraftfahrzeugen vorzulegen. Mit Einverständnis des Bürgers übersandte die Behörde dem Gesundheitsamt zu diesem Zweck die Führerscheinakte. Im Anschreiben bat sie darum, das Gutachten zusammen mit der Führerscheinakte wieder direkt an die Behörde zurückzusenden. Dieser Wunsch war dem Gesundheitsamt Befehl. Es schickte das Gutachten direkt zu. Damit aber hatten beide, das Gesundheitsamt wie auch die Straßenverkehrsbehörde, gegen Datenschutzrecht verstoßen. Sie hätten Folgendes beachten müssen:

Will eine Behörde Daten über einen Bürger erheben, muss sie sich grundsätzlich zunächst an diesen selbst wenden. Bei Dritten dürfen Daten ohne Zustimmung des Betroffenen nur unter engen Voraussetzungen angefordert werden. Unzulässig ist eine solche Erhebung jedenfalls dann, wenn es nach Lage der Dinge nicht erforderlich ist, sich an den Dritten zu wenden. So war es hier. Die Straßenverkehrsbehörde hätte, statt das Gesundheitsamt zu bitten, ihr das Gutachten unmittelbar zu übermitteln, ebenso gut den betroffenen Bürger hierzu auffordern können. Dies wäre auch der richtige Weg gewesen. Es war ja nicht so, dass die Behörde auf das Gutachten zur Erfüllung ihrer Aufgabe angewiesen gewesen wäre. Denn ein positives Gutachten vorzulegen, ist ausschließlich im Interesse des Betroffenen, weil er hiermit die bei ihm vermutete Nichteignung zum Führen von Kraftfahrzeugen widerlegen kann. Kann er den entsprechenden Nachweis nicht führen, darf die Behörde nach der Fahrerlaubnis-Verordnung auf seine Nichteignung schließen. In der Fahrerlaubnis-Verordnung steht deshalb auch ausdrücklich, dass die Beibringung eines Gutachtens (nur) durch den Betroffenen zu erfolgen hat. Und das Verkehrsministerium hat hierzu in einem Erlass von 1992 klargestellt, dass medizinisch-psychologische Gutachten ausschließlich dem Betroffenen zugesandt werden müssen. Es ist dann dessen Entscheidung überlassen, wie er mit dem Gutachten weiter verfahren will.

Dies alles hat die Straßenverkehrsbehörde bei ihrer Aufforderung an das Gesundheitsamt, ihr das Gutachten unmittelbar zu übersenden, nicht bedacht. Den Datenschutzverstoß habe ich beanstandet. Mir wurde daraufhin geantwortet, es habe sich hier um einen Ausnahmefall gehandelt. Generell werde entsprechend den gesetzlichen Vorgaben verfahren.

Beanstandet habe ich aber auch das Gesundheitsamt. Denn dieses hätte das Gutachten nicht so ohne weiteres der Straßenverkehrsbehörde zuleiten dürfen. Immerhin geht es dabei um Daten, die der ärztlichen Schweigepflicht unterliegen. Das Gesundheitsdienstgesetz bestimmt für die Weitergabe solcher Daten einen engen Rahmen. Dieser wurde hier klar überschritten. Medizinisch-psychologische Begutachtungen in Fahrerlaubnisangelegenheiten sind beim Gesundheitsamt sicher keine Seltenheit. Es kann somit angenommen werden, dass die maßgeblichen Bestimmungen der Fahrerlaubnis-Verordnung sowie der einschlägige Erlass des Verkehrsministeriums hierzu bekannt waren. Aber selbst wenn dies nicht der Fall gewesen sein sollte, hätte vom Amtsarzt erwartet werden müssen, dass er sich sorgfältig danach erkundigt, ob er dazu berechtigt ist, bevor er solche sensitiven Daten aus der Hand gibt. Das Gesundheitsamt hat sein Fehlverhalten auch ohne Umschweife eingeräumt, den Fehler bedauert und intern nochmals ausdrücklich auf die maßgeblichen Vorschriften hingewiesen. Das Sozialministerium ist dem beigetreten und hat den Einzelfallcharakter betont. Ich kann nur hoffen, dass das tatsächlich so ist.

2.2 Der Notdienst

Mit dem In-Kraft-Treten des Infektionsschutzgesetzes am 1. Januar 2001, das das bisherige Bundes-Seuchengesetze abgelöst hat, sahen sich die Gesundheitsämter vor neue Herausforderungen gestellt. Das neue Gesetz verpflichtet die meldepflichtigen Personen, dem Gesund-

heitsamt spätestens innerhalb von 24 Stunden mitzuteilen, wenn sie von einer meldepflichtigen Krankheit oder von nachgewiesenen Krankheitserregern Kenntnis erhalten haben. Das Gesundheitsamt hat dann umgehend zu entscheiden, wie in der Sache weiter verfahren werden soll. Die Umsetzung dieser gesetzlichen Verpflichtung in die Praxis führte datenschutzrechtlich zu zwei Fragen: Dürfen die Meldungen generell per Telefax übermittelt werden und wie lässt sich dem Problem begegnen, dass der Amtsarzt an Wochenenden und Feiertagen regelmäßig nicht im Gesundheitsamt anwesend ist?

Dazu ist zu sagen:

Grundsätzlich ist der Versand von Gesundheitsdaten wegen der damit verbundenen besonderen Risiken sehr kritisch zu bewerten. Gleichwohl wird anders die Forderung des Gesetzes, die zuständigen Stellen zeitnahe über potenzielle Gefahren zu informieren, kaum zu erfüllen sein. Ich habe mich deshalb nicht gegen den generellen Einsatz des Telefax für solche Eilmeldungen ausgesprochen.

Klar ist dabei, dass es Sache der Gesundheitsämter ist, dafür zu sorgen, dass die Warnmeldungen sehr schnell beim Amtsarzt ankommen. Einen Bereitschaftsdienst mit Präsenzpflicht des Amtsarztes an Wochenenden und Feiertagen zu organisieren, sind jedoch nicht alle Gesundheitsämter ohne weiteres in der Lage. Nachdem mehrere andere Lösungsansätze (auch) aus datenschutzrechtlichen Erwägungen nicht weiter verfolgt wurden, präsentierte ein Gesundheitsamt den Vorschlag, ein Mobiltelefon einzusetzen, das in der Lage ist, Telefaxe zu empfangen. Ich habe diesen Vorschlag letztendlich akzeptiert, wohl wissend um die damit verbundene Problematik. Denn ist schon die reguläre Kommunikation per Telefax aus Sicht des Datenschutzes nicht unbedenklich, so gilt dies erst recht dann, wenn hierzu mobile Empfangsgeräte verwendet werden. Dies bringt zusätzliche weitere Risiken mit sich. So ist vor allem der Kreis derjenigen, die potenziell auf die empfangenen Daten zugreifen können, deutlich größer. Werden Telefaxe stationär in einem Raum des Gesundheitsamts empfangen, lässt sich verhältnismäßig einfach und sicher regeln, wer Zugang zu den eingegangenen Meldungen hat. Schwieriger ist es dagegen, Zugriffe durch Unbefugte auszuschließen, wenn die Daten von einem mobilen Gerät im privaten Bereich empfangen werden. Unbefugt in diesem Sinne wären etwa Familienangehörige des Amtsarztes, Personen, die sich in seiner unmittelbaren Nähe aufhalten, aber auch solche Personen, die in den Besitz des Handys gelangen, sei es durch Diebstahl oder weil der Amtsarzt es verloren hat. Der Einsatz eines Fax-Handys ist deshalb allenfalls dann verantwortbar, wenn eine Reihe von technischen und organisatorischen Sicherheitsvorkehrungen getroffen werden. So muss beispielsweise sichergestellt sein, dass bei einer Aktivierung der Rufumleitung vom Telefaxgerät des Gesundheitsamts auf das Fax-Handy die Zielrufnummer nicht verwechselt und das Telefax an die falsche Adresse weitergeleitet wird. Beim Amtsarzt muss sichergestellt sein, dass keine Unbefugten auf eingehende Meldungen zugreifen können. Um dies zu verhindern, muss vorgesehen werden, dass Kommunikationsvorgänge jeweils nur nach Eingabe einer persönlichen Kennung möglich sind, insbesondere eingehende Meldungen nur nach Eingabe des Passworts abgerufen werden können. Dieser Passwortschutz darf nicht vom Amtsarzt aufgehoben werden können. Der Amtsarzt muss dabei schriftlich auf die Einhaltung gewisser Sicherheitsstandards verpflichtet werden, etwa dass er das Gerät keinem Dritten zugänglich machen darf.

Mittlerweile haben sich etliche Gesundheitsämter für die mobile Telefaxlösung entschieden. Aus ihren Zuschriften ergibt sich allerdings, dass sie den von mir genannten Voraussetzungen qualitativ höchst unterschiedlich nachkommen wollen. Ich beabsichtige deshalb, zu gegebener Zeit die datenschutzrechtlichen Anforderungen zu konkretisieren.

3. Die Ärztekammer

Die Angehörigen freier Berufe, wie etwa Ärzte, müssen kraft Gesetzes Mitglied in ihrer jeweiligen Berufsvertretung sein. Diese als Kammern bezeichneten Berufsvertretungen haben unter anderem die Aufgabe, darüber zu wachen, dass ihre Mitglieder ihre Berufspflichten erfüllen. Wird dagegen verstoßen, kann die Kammer berufsgerichtliche Maßnahmen treffen. Werden im Zusammenhang hiermit personenbezogene Daten der Mitglieder verarbeitet, kommt es mitunter auch zu Konflikten über Art und Ausmaß der datenschutzrechtlichen Befugnisse. Im Berichtszeitraum hatte ich mich mit zwei Fällen zu befassen.

3.1 Ärztekammer und Gesundheitsamt – die einheitliche Staatsverwaltung

Bei einem neu gegründeten Unternehmen aus dem Wellness-Bereich war der Verdacht aufgekommen, dort würde unberechtigt Heilkunde ausgeübt. Auf Veranlassung eines Gesundheitsamts überprüfte dies der Wirtschaftskontrolldienst an Ort und Stelle. Die Kontrolle bestätigte den Verdacht nicht. Allerdings ergab sich, dass das Unternehmen und eine in demselben Gebäude untergebrachte Arztpraxis ein gemeinsames Wartezimmer betrieben. Da das Gesundheitsamt vermutete, der Arzt könne damit gegen seine standesrechtlichen Pflichten verstoßen haben, wandte es sich an die zuständige Bezirksärztekammer und berichtete ihr von den Beobachtungen. Die Bezirksärztekammer bat das Gesundheitsamt daraufhin, ihr weitere Unterlagen zur Verfügung zu stellen, was auch geschah.

Vom betroffenen Arzt, gegen den die Bezirksärztekammer Ermittlungen eingeleitet hatte, um Rat gefragt, ob das alles zulässig sei, musste ich mich im Weiteren mit den reichlich merkwürdigen Rechtsauffassungen der beteiligten Akteure auseinander setzen. So teilte der Amtsarzt mit, nach seinen ihm „im Amtsarztkurs vermittelten juristischen Kenntnissen (könne) es nicht sein, dass eine Behörde es einfach auf sich beruhen lässt, wenn sie Kenntnis über rechtswidrige Dinge erhält, auch wenn sie nicht primär dafür zuständig ist“. Entweder hatte der Amtsarzt da etwas falsch verstanden oder die für den Amtsarztkurs Verantwortlichen sollten sich Gedanken über die Qualität ihrer Fortbildung machen. Es ist schon sehr bedenklich, wenn einem Amtsarzt schon das diffuse Gefühl eines rechtswidrigen Verhaltens offenbar als Begründung dafür ausreicht, personenbezogene Daten an Außenstehende zu übermitteln. Noch mehr erstaunte aber der nachfolgende Rechtfertigungsversuch der Bezirksärztekammer Südwürttemberg. Diese meinte nämlich, das Gesundheitsamt habe sie über den Vorgang „unter dem Blickwinkel der Einheit der Staatsverwaltung“ völlig zu Recht informiert. Der „Blickwinkel der Einheit der Staatsverwaltung“ als Rechtfertigungsgrund für eine Datenverarbeitung war mir bisher nun wirklich völlig neu. Darauf hingewiesen, dass diese Auffassung die Entwicklung des Datenschutzrechts der letzten Jahrzehnte außer Acht lässt, legte die Bezirksärztekammer nach und versuchte, argumentativ zu retten, was zu retten ist. Überzeugt hat mich das dennoch nicht. So wurde geltend gemacht, der Verstoß gegen standesrechtliche Pflichten (der hier im Zeitpunkt der erstmaligen Unterrichtung durch das Gesundheitsamt ja noch keineswegs feststand) stelle „einen erheblichen Nachteil für das Gemeinwohl dar, weil das Rechtsstaatsprinzip des Artikels 19 Abs. 4 GG erheblich betroffen“ sei. Bei allem Verständnis für die Bedeutung des Standesrechts scheint mir diese Auffassung etwas weit gehend. Kurz und gut, ich habe das Gesundheitsamt darauf hingewiesen, dass es falsch gehandelt hat. Eine Datenübermittlung wäre hier nur zulässig gewesen, wenn die Voraussetzungen des § 16 Abs. 1 LDSG erfüllt gewesen wären. Neben der Erforderlichkeit zur Aufgabenerfüllung hätte danach (zusätzlich) eine der in § 15 Abs. 1 bis 4 LDSG genannten Voraussetzungen vorliegen müssen. Dies war aber nicht der Fall. Insbesondere ging es hier nicht um die Abwehr erheblicher Nachteile für das Gemeinwohl. Fraglich ist schon, ob allein das gemeinsame Nutzen eines Wartezimmers durch einen Arzt und ein gewerbliches Unternehmen ein Nachteil für das Gemeinwohl sein kann. Nicht jedes Standesinteresse ist zwangsläufig auch ein Gemeinwohlinteresse. Und selbst

wenn dies so wäre, würde die Übermittlungsbefugnis an der anerkanntermaßen hohen Schwelle der Erheblichkeit des Nachteils scheitern. Dies alles hätte das Gesundheitsamt bei einer verantwortungsbewussten Prüfung der Zulässigkeit der Übermittlung erkennen können und müssen. Dann hätte es sich letztlich auch nicht durch die unzutreffenden Rechtsauskünfte der Bezirksärztekammer, die zurechtzurücken mich einige Mühe gekostet hat, ins Bockshorn jagen lassen.

3.2 Die voreilige Aktenvernichtung

Auch in einem anderen Fall gab die Bezirksärztekammer Südwürttemberg Anlass zur Kritik. Wieder hatte sich ein Arzt an uns gewandt und Folgendes vorgetragen:

Vor Jahren habe die Bezirksärztekammer im Zusammenhang mit einem berufsgerichtlichen Verfahren Akten über ihn angelegt. Er habe im Februar 1999 beim Kammeranwalt Einsicht in diese Akte beantragt. Dies sei ihm mit dem Hinweis verweigert worden, nach der Berufsgerichtsordnung sei eine Akteneinsicht nur durch einen Rechtsanwalt möglich. Deshalb habe er gleich einen Rechtsanwalt bevollmächtigt. Dieser habe dann im April 1999 schriftlich und unter Hinweis auf ein zuvor geführtes Telefonat mit dem Kammeranwalt um Akteneinsicht ersucht. Mit Erstaunen und Verärgerung habe er aber zur Kenntnis nehmen müssen, dass die Bezirksärztekammer die Akte mittlerweile vernichtet habe.

Die Bezirksärztekammer hat das Vorbringen bestätigt. Als Begründung trug sie vor, Akten des Kammeranwalts würden routinemäßig nach fünf Jahren vernichtet. Diese Frist sei bedauerlicherweise gerade zwischen dem Auskunftsbegehren des Arztes und dem Schreiben seines Rechtsanwalts abgelaufen. Ich meine, so kann das nicht gehen!

Es ist ja lobenswert, dass die Bezirksärztekammer Löschungsfristen für ihre Akten bestimmt hat. Damit handelt sie völlig im Sinne des Datenschutzes. Denn auch das unnötig lange Vorhalten personenbezogener Daten ohne sachlichen Grund verletzt das informationelle Selbstbestimmungsrecht des Einzelnen. Allerdings erkennt das Gesetz auch an, dass es Situationen geben kann, in denen zwar die Behörde Daten nicht mehr braucht, sie aber gleichwohl nicht gelöscht werden dürfen, weil der Betroffene ein schutzwürdiges Interesse an der weiteren Aufbewahrung hat. So steht es in § 23 Abs. 4 Nr. 1 LDSG und so war es hier.

Durch sein Ersuchen auf Akteneinsicht hatte der Arzt gegenüber der Bezirksärztekammer deutlich gemacht, dass er den Akteninhalt aus seiner Sicht für bedeutsam hielt. Er hat sich danach in einem durchaus noch als angemessen anzusehenden Zeitraum an einen Rechtsanwalt gewandt. Wie sich aus dessen Schreiben, mit dem um Akteneinsicht gebeten wurde, ergab, hatte er sich kurz vor dem Schreiben in dieser Sache bereits bei dem Kammeranwalt gemeldet. Zu diesem Zeitpunkt existierte die Akte wohl noch; jedenfalls wurde der Rechtsanwalt offensichtlich nicht darauf hingewiesen, dass sie bereits vernichtet worden sei. Denn andernfalls hätte er wohl kaum noch ein schriftliches Einsichtsersuchen an die Kammer gerichtet. Folglich muss die Akte in dem (kurzen) Zeitraum zwischen dem Telefonat und der schriftlichen Antragstellung vernichtet worden sein. Zu diesem Zeitpunkt war der Bezirksärztekammer aber klar, dass der Betroffene immer noch an der Akteneinsicht interessiert war. Wenn sie, obwohl sie dies wusste, gleichwohl die Akte vernichtet hat, hat sie sich damit über ihre datenschutzrechtliche Pflicht zur weiteren Aufbewahrung hinweggesetzt. Dies kann auch nicht damit gerechtfertigt werden, dass die Akte routinemäßig vernichtet worden sei. Denn es hätte jedenfalls am Kammeranwalt gelegen, dafür Sorge zu tragen, dass die Akte aus dieser Routine herausgenommen wird. Trotz meiner Bemühungen konnte ich die Bezirksärztekammer Südwürttemberg nicht davon überzeugen, dass sie falsch gehandelt hat.

4. Die Beratungsstelle

Immer wieder wenden sich Mitarbeiter psychosozialer Beratungsstellen an mein Amt, um Rat zu Fragen des Datenschutzes und der beruflichen Schweigepflicht einzuholen. Dies war für mich Anlass, einer solchen Stelle auch einmal einen Besuch abzustatten. Die Wahl fiel auf eine Suchtberatungsstelle, die hauptsächlich Alkoholkranke betreut. Um es vorweg zu sagen: Besonders gravierende Mängel konnten nicht festgestellt werden. Deutlich war das Bemühen festzustellen, peinlich genau darauf zu achten, dass nichts, was im Rahmen der Beratungstätigkeit über die Klienten erfahren wird, nach außen dringt. Die Bedeutung der Schweigepflicht war den Mitarbeiterinnen und Mitarbeitern insoweit offensichtlich bewusst und sie wurde und wird auch ernst genommen. Was zu kritisieren war, waren eher Nachlässigkeiten im inneren Betriebsablauf, die ihre Ursache mitunter auch in der beengten räumlichen Situation und in einer nicht gerade üppigen Finanzausstattung der Beratungsstelle hatten. So wurde Folgendes festgestellt:

– Klienten der Beratungsstelle werden zunächst in ein Wartezimmer geleitet, wo sie, wenn die Reihe an sie kommt, von der Therapeutin oder dem Therapeuten abgeholt werden. Üblich war es, die Betreffenden namentlich aufzurufen. Ich meine, das muss nicht sein. Der Aufruf führt dazu, dass alle anderen anwesenden Besucher erfahren, wie die Person, die sie bisher nur optisch wahrnehmen konnten, heißt. Ihnen wird damit ohne Not eine Information über den Klienten der Beratungsstelle vermittelt, die, soweit jemand ein Interesse daran hat, Grundlage für weitere Nachforschungen sein kann. So könnte etwa mittels des Namens aus einem Telefonbuch die Adresse herausgefunden und ein – unerwünschter – Kontakt hergestellt werden. Ich habe die Beratungsstelle deshalb aufgefordert, hier nach anderen Wegen zu suchen. Sie hat mitgeteilt, künftig würde der Therapeut oder die Therapeutin im Wartezimmer den eigenen Namen nennen und der Klient, der sich angesprochen fühle, könne dann mitkommen. Ich halte das für eine gute Lösung.

– Im Gespräch mit den Mitarbeitern ergab sich, dass Fälle bei den regelmäßigen Teambesprechungen, aber auch bei den Supervisionen namensbezogen behandelt werden. Dabei ist zu bedenken, dass die Therapeuten Berufsgruppen angehören, denen nach § 203 Abs. 1 des Strafgesetzbuches besondere Geheimhaltungspflichten obliegen. Und diese Schweigepflicht gilt grundsätzlich auch unter Berufskollegen. Regelmäßig dürfte es zwar so sein, dass jedenfalls bei rein internen Teambesprechungen die Teilnehmer wissen, um welchen Klienten es geht, auch wenn der Name nicht genannt wird. Dies liegt daran, dass die Beratungsstelle verhältnismäßig klein ist, die Mitarbeiter sich gegenseitig vertreten und von daher die Klienten im Allgemeinen allen bekannt sein werden. Dies muss aber nicht immer so sein. Da Fallbesprechungen, in denen es um Sachverhalte, nicht um Namen geht, generell anonym stattfinden können, ohne an Qualität einzubüßen, sollte es auch so gehandhabt werden. In jedem Fall gilt dies aber bei Supervisionen. Hieran nehmen nämlich regelmäßig eine externe Psychologin, aber auch die bei der Beratungsstelle beschäftigte Präventionsfachkraft, die ansonsten keine Klientenberatungsfunktion wahrnimmt, teil. Nicht nur, dass die Namen der Klienten auch hier nichts zur Sache tun. Jeder, der Namen nennt und damit Außenstehenden gegenüber den Fall persönlich zuordenbar macht, muss sich vielmehr darüber im Klaren sein, dass er damit gegen seine Schweigepflicht verstößt und das Vertrauen seines Klienten missbraucht.

  Die Beratungsstelle hat mitgeteilt, sie werde ihre Mitarbeiter hierüber informieren. Ich hoffe, dass dies in der Praxis auch beachtet wird.

– Über die Beratungen werden Aufzeichnungen geführt. Diese werden in Akten abgelegt. Die Akten der laufenden Fälle werden in einem im Flur der Beratungsstelle aufgestellten abschließbaren, im Allgemeinen aber (während der Dienstzeiten) nicht abgeschlossenen Schrank aufbewahrt. Prinzipiell kann also tagsüber jeder jederzeit auf die Akten zugreifen. Auf dem Weg zum Wartezimmer kommen auch Klienten an dem Schrank vorbei.

Ich habe das als nicht datenschutzgerecht kritisiert. Eine datenschutzgerechte Organisation verlangt vielmehr, dass personenbezogene Daten, besonders wenn sie so sensibel sind wie die in einer Suchtberatungsstelle erhobenen und gespeicherten Daten, wirksam gegen den Zugriff Unberechtigter gesichert werden. Dem Grunde nach ist unberechtigt in diesem Sinne auch der Kollege, der den Klienten aktuell nicht betreut. Ihm darf es nicht ermöglicht werden, ohne sachlichen Grund persönliche Daten von Klienten zur Kenntnis nehmen zu können, die nicht seine Klienten sind und die ihm diese Daten deshalb auch nicht anvertraut haben. Insofern wäre es konsequent, die Akten so aufzubewahren, dass jeweils nur der zuständige Therapeut darauf zugreifen kann. Geschieht dies nicht, ist jeder Mitarbeiter permanent in Gefahr, seine Schweigepflicht zu verletzen. Solche Situationen zu vermeiden, gehört im Übrigen auch zu den arbeitsvertraglichen Pflichten des Arbeitgebers.

Die Beratungsstelle hat mitgeteilt, eine dezentrale Aktenaufbewahrung sei nicht möglich, da dies die Beratungstätigkeit in nicht zu rechtfertigender Weise beeinträchtigen würde. Dies hänge damit zusammen, dass sich die therapeutischen Berater und Beraterinnen grundsätzlich untereinander vertreten würden und von daher jederzeit die Möglichkeit haben müssten, auf alle Akten zuzugreifen. Man sei meinen Bedenken aber insoweit nachgekommen, als man den Aktenschrank künftig auch tagsüber abschließen werde. Zu dem Schlüssel hätten nur die Therapeuten Zugang.

Ich meine, auch bei einer zentralen Aktenhaltung muss es möglich sein, die Akten nach den jeweiligen Therapeuten getrennt aufzubewahren und ihnen grundsätzlich die alleinige Verfügungsgewalt über ihre Akten zu ermöglichen. Damit ist nicht zwangsläufig ausgeschlossen, dass es im Vertretungsfall ermöglicht werden kann, dem Vertreter einzelne Akten zugänglich zu machen. Ich werde mich in dieser Frage nochmals an die Beratungsstelle wenden.

– Akten, die nicht mehr aktuell benötigt werden, verwahrt die Beratungsstelle in einem Altarchiv im Keller des Gebäudes, in dem sie untergebracht ist. Dort lagerten zum Zeitpunkt der Kontrolle Akten, die schon mehr als 50 Jahre alt waren. Dies verstößt gegen Datenschutzrecht.

  Akten sind zu vernichten, wenn sie zur Aufgabenerfüllung nicht mehr benötigt werden. Als generellen Anhalt dafür, wann dies in der psychosozialen Beratung der Fall sein kann, kann auf die zehnjährige Aufbewahrungsfrist nach der ärztlichen Berufsordnung abgestellt werden. Ist die Beratung abgeschlossen und ist der Klient auch nach zehn Jahren nicht mehr erschienen, spricht viel dafür, dass sich die Angelegenheit erledigt hat. Dann gibt es auch keinen Grund mehr, die Akten noch länger aufzubewahren. In begründeten Ausnahmefällen kann allerdings auch eine längere Aufbewahrung gerechtfertigt sein. In diesen Fällen sollte allerdings eine schriftliche Begründung hierzu zusammen mit der Angabe über das voraussichtliche Ende der Speicherung zu der Akte genommen werden.

  Die Beratungsstelle hat dies akzeptiert und mitgeteilt, die nicht mehr benötigten Akten würde sie zeitnah aussondern und vernichten.

5. Das Landeskrebsregister – Wie geht es weiter?

In unserem 14. Tätigkeitsbericht 1993 (LT-Drs. 11/2900, S. 81) war noch Folgendes zu lesen: „Kaum ein Thema beschäftigte mich während meiner nahezu 14-jährigen Amtszeit so häufig wie das Krebsregister – nachzulesen in sieben der dreizehn Tätigkeitsberichte“. Seitdem ist relative Ruhe eingekehrt. Zurückzuführen ist dies vor allem darauf, dass der Gesetzgeber aktiv geworden und unter maßgeblicher Beteiligung meines Amtes ein Landeskrebsregistergesetz erlassen hatte. Dies war im Jahr 1994. Wurde damals noch der Datenschutz – wie ich meine, zu Unrecht – als größtes Hindernis auf dem Weg zu einer flächendeckenden Erfassung aller Krebsdaten bezeichnet, plagen das Krebsregister heute ganz andere Sorgen. Liest man den (neuesten) Jahresbericht 2000, dann steht dort, dass die Vollzähligkeit der Erfassung von entscheidender Bedeutung für die Aussagekraft des Registers sei. Die Vollzähligkeit der Erfassung sei von der Kooperationsbereit-

schaft der Ärzte und Krankenhäuser abhängig – und damit ist es offenbar nicht besonders weit her! So betrug beispielsweise die Meldequote im Stadtkreis Mannheim mit seinem Universitätsklinikum für das Jahr 1997 gerade mal 40 v. H., also weniger als die Hälfte! Hier muss die Frage erlaubt sein, welchen Sinn es macht, sensible Gesundheitsdaten in nicht unbeträchtlicher Zahl im Land umherzuschicken, wenn der Zweck des Ganzen, nämlich verlässliche Daten zur Krebsinzidenz und -prävalenz zu erhalten, wegen mangelnder Mitarbeit einzelner potenzieller Datenlieferanten nicht erreicht werden kann. Dabei sind es keineswegs nur die Krankenhäuser, die sich mit Meldungen zurückhalten. Auch die Gesundheitsämter sind in dieser Frage keine Musterknaben und übermitteln dem Krebsregister die Leichenschauscheine nicht so vollständig, wie dies nach dem Landeskrebsregistergesetz vorgesehen ist. Hier wäre es Aufgabe des Sozialministeriums, ein klärendes Wort zu sprechen!

Besonders ärgerlich ist es in diesem Zusammenhang, wenn ich vor allem von einem Tumorzentrum ständig wieder gefragt werde, ob es aus datenschutzrechtlicher Sicht nicht doch akzeptiert werden könne, dass die Regionalen Rechenzentren ihm und auch den anderen Tumorzentren sowie den Onkologischen Schwerpunkten zur Ermittlung des Überlebensstatus ehemaliger Krebspatienten routinemäßig die Sterbedaten aller in einem Jahrgang Verstorbenen übermitteln. Meine Meinung dazu habe ich schon im 21.Tätigkeitsbericht 2000 (LT-Drs. 12/5740, S. 33 f.) geäußert. Diese Einrichtungen täten besser daran, die vorhandenen Möglichkeiten zu nutzen und dazu ihre Meldetätigkeit gegenüber dem Krebsregister zu intensivieren, als ständig nach neuen Methoden der Datengewinnung zu suchen. Denn dem Krebsregister wurde durch eine Änderung des Landeskrebsregistergesetzes gerade die Möglichkeit eingeräumt, den Einrichtungen die für ihre Arbeit nötigen Daten zur Verfügung zu stellen. Von daher ist es nicht zu viel verlangt, wenn diese ihrerseits etwas zum Gelingen des Krebsregisters beitragen.

6. Die Entschlüsselung des menschlichen Genoms

Anfang des Jahres konnte man in der Presse lesen, dass es Forschern gelungen sei, das menschliche Genom, also die Erbsubstanz, zu entschlüsseln. Damit ist man dem Ziel, die Funktion einzelner Gene aufzuklären, wieder einen Schritt näher gekommen. Angesichts der enormen Chancen, die dies vor allem für die Diagnose und Behandlung bislang noch unheilbarer schwerer Krankheiten mit sich bringt, fällt es schwer, Wasser in den Wein zu schütten und darauf hinzuweisen, dass diese Entwicklung für den Einzelnen auch Nachteile mit sich bringen kann. Eine Konsequenz ist nämlich, dass damit jeder Mensch als Forschungsobjekt taugt. Beispiele aus anderen Ländern (z. B. Island, Estland und Königreich Tonga) zeigen, dass Wirtschaftsunternehmen großes Interesse daran haben, Zugang zu Gendatenbanken zu erhalten. Schon daran lässt sich die enorme wirtschaftliche Bedeutung solcher genetischen Daten erahnen. Eine weitere Konsequenz ist, dass Arbeitgeber oder Versicherungen versucht sein könnten, die erblich bedingten Risikofaktoren als Auswahlkriterium heranzuziehen. Studien in den USA haben ergeben, dass bereits Hunderte von Menschen entweder ihre Arbeit oder ihren Versicherungsschutz auf Grund der Ergebnisse von Genom-Analysen verloren haben. Diese und weitere Bedenken hatten die Datenschutzbeauftragten des Bundes und der Länder dazu bewogen, auf ihrer 60. Konferenz am 12. und 13. Oktober 2000 eine Entschließung zu datenschutzrechtlichen Konsequenzen aus der Entschlüsselung des menschlichen Genoms zu fassen (Anhang 11 zum 21. Tätigkeitsbericht 2000, LT-Drs. 12/5740). Die damals erhobene Forderung nach einer gesetzlichen Regelung wurde jetzt auf der 62. Datenschutzkonferenz am 24. bis 26. Oktober 2001 durch eine weitere Entschließung (s. Anhang 15) konkretisiert. Dabei wurden konkrete Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen gemacht, an deren Erarbeitung auch mein Amt beteiligt war. Die Vorschläge sind als Anregung für anstehende Gesetzesinitiativen gedacht und stellen gleichzeitig einen Beitrag zur gesellschaftspolitischen Diskussion dar. Kernanliegen sind danach unter anderem

– eine Stärkung des Selbstbestimmungsrechts des Einzelnen dadurch, dass genetische Untersuchungen, auch zu Forschungszwecken, grundsätzlich nur mit Einwilligung durchgeführt werden dürfen;

– die Gewährleistung von Qualität und Sicherheit genetischer Tests durch Zulassungs- und Arztvorbehalt;

– die Verhinderung heimlicher Gentests;

– ein grundsätzliches Verbot, im Arbeitsleben und im Rahmen von Versicherungsverhältnissen Gentests oder hieraus gewonnene Erkenntnisse zu fordern und entgegenzunehmen;

– eine externe Datentreuhänderschaft, wenn Proben und genetische Daten als Voraussetzung für die Aufnahme in eine Proben- oder Gendatenbank pseudonymisiert werden sollen.

Daneben steht die Forderung an den Gesetzgeber, die Durchführung von Gentests unter Strafe zu stellen, wenn sie ohne ausdrückliche gesetzliche Ermächtigung oder ohne wirksame Einwilligung durchgeführt werden.

2. Abschnitt: Die gesetzliche Krankenversicherung

Auch wer sonst dem Thema Datenschutz desinteressiert bis kritisch gegenübersteht, reagiert meist äußerst empfindlich, wenn er etwa von seiner Krankenkasse aufgefordert wird, Angaben über seine finanziellen oder gesundheitlichen Verhältnisse zu machen. Solche sensiblen Daten behält man lieber für sich und gibt sie nicht gerne aus der Hand. Die Vorstellung, dass Mitarbeiter der Krankenkasse, mit denen man womöglich bekannt ist, Einblick in die eigenen Lebensumstände erhalten, wird meist als unerträglich empfunden. Das von Kritikern des Datenschutzes häufig vorgetragene, klassische Argument, wer sich nichts hat zu Schulden kommen lassen, der hat auch nichts zu verbergen, findet man in diesem Bereich selten. Dieser Empfindlichkeit steht andererseits die Tendenz gegenüber, mithilfe immer neuer Datensammlungen das Problem der ständig steigenden Kosten des Gesundheitswesens in den Griff zu bekommen. So hatte ich mich auch in diesem Jahr wieder mit etlichen Gesetzgebungsvorhaben zur gesetzlichen Krankenversicherung zu befassen.

1. Das Transparenzgesetz – Datenschutz bis zum Sankt-Nimmerleins-Tag?

Manchmal kann man die Bedeutung, die der Gesetzgeber einzelnen Problemen zumisst, danach beurteilen, wie schnell er tätig wird, um sie zu lösen. Ein gutes Beispiel hierzu liefern zwei Gesetzentwürfe, mit denen ich mich im Berichtszeitraum auseinander setzen musste.

Seit Monaten geistert der Entwurf eines „Gesetzes zur Verbesserung der Datentransparenz und des Datenschutzes in der gesetzlichen Krankenversicherung“, kurz: Transparenzgesetz, durch die Lande. Nun kann es derjenige, der sich einmal die Mühe gemacht hat, das Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – lesen oder gar verstehen zu wollen, nur vorbehaltlos begrüßen, wenn versucht wird, zu mehr Transparenz zu kommen. Aber, um es vorwegzusagen, daraus wird wohl so bald nichts. Um was es geht, ist schnell erklärt:

Unter großen Geburtswehen war vor etwa zwei Jahren die GKV-Gesundheitsreform 2000 in Kraft getreten. Gegenstand der GKV-Reform war ursprünglich auch der datenschutzrechtliche Teil des SGB V. Leider sind jedoch die noch in der Entwurfsfassung enthaltenen Regelungen zur Verbesserung des Sozialdatenschutzes nicht in das Gesetz übernommen worden. Dies sollte mit dem genannten Transparenzgesetz nachgeholt werden. Kernpunkt des Gesetzes soll dabei sein, dass die Leistungsträger, also die gesetzlichen Krankenkassen, künftig ausnahmslos alle Abrechnungsdaten nur noch unter einem Pseudonym sollen speichern dürfen. Derzeit ist es so, dass nur die Abrechnungsunterlagen der Vertragsärzte ohne Personenbezug an die Krankenkassen gelangen. Alle anderen Leistungserbringer, also beispielsweise die Krankenhäuser, rechnen dagegen versichertenbezogen ab und die Krankenkassen speichern diese Daten versichertenbezogen.

Das dem Transparenzgesetz zu Grunde liegende Konzept sieht die Schaffung neuer Strukturen vor. So sollen zentrale Datenannahme- und weiterleitungsstellen entstehen. Deren Aufgabe soll es sein, die Abrechnungsunterlagen entgegenzunehmen, auf ihre formale Richtigkeit zu prüfen und an die zuständige Krankenkasse weiterzuleiten. Diese darf die Daten selbst

nicht auf Dauer speichern, sondern muss sie nach sachlicher Prüfung an eine Vertrauensstelle weiterleiten. Die Vertrauensstelle ersetzt die Identifikationsmerkmale durch ein Pseudonym und gibt die so veränderten Daten, die dann keinen unmittelbaren Personenbezug mehr aufweisen, an die Krankenkasse zurück. Diese kann dann mithilfe dieser – für sie anonymen – Daten zur weiteren Erfüllung ihrer Aufgaben Fallkonten bilden. Nur in besonders begründeten, im Gesetz geregelten Einzelfällen kann die Krankenkasse über die Vertrauensstelle wieder den Personenbezug herstellen (lassen).

Die Umsetzung dieses Konzepts, das von allen Datenschutzbeauftragten einhellig begrüßt und gefordert wurde, würde zu einem deutlichen Mehr an Datenschutz in der gesetzlichen Krankenversicherung führen. Nach langem Hin und Her und der Diskussion etlicher Varianten scheint sich die Bundesregierung nun dazu entschlossen zu haben, den Gesetzentwurf wieder auf Eis zu legen. Wann es weitergehen soll, ist ungewiss. Aus Sicht des Datenschutzes kann dies nur bedauert werden.

Dass es, wenn nicht der Datenschutz, sondern wirtschaftliche Interessen im Vordergrund stehen, auch anders geht, zeigt ein Gesetzgebungsvorhaben, das zeitlich nach dem Transparenzgesetz in Angriff genommen worden ist und demnächst wohl auch abgeschlossen sein wird. Es geht um ein Gesetz zur Reform des Risikostrukturausgleichs in der gesetzlichen Krankenversicherung. Der Risikostrukturausgleich soll zu einer solidarischen Verteilung der Risikobelastung innerhalb der gesetzlichen Krankenversicherung beitragen. Wettbewerbsvorteile, die dadurch entstehen, dass einzelne Krankenkassen nur günstige Risiken versichern, sollen ausgeschlossen werden. Der Risikostrukturausgleich soll weiterentwickelt werden. Um dies zu erreichen, ist u. a. vorgesehen, für bestimmte chronische Krankheiten strukturierte Behandlungsprogramme einzuführen, an denen Versicherte freiwillig teilnehmen können. Es sollen Versichertengruppen anhand direkter Morbiditätsindikatoren gebildet werden. Deren sachgerechte Abgrenzung soll durch eine wissenschaftliche Untersuchung ermittelt werden. Schließlich soll ein Risikopool geschaffen werden, der von allen Krankenkassen gemeinsam finanziert wird. Hieraus sollen finanzielle Belastungen einzelner Krankenkassen, die aus aufwändigen Leistungsfällen herrühren, ausgeglichen werden.

Alle diese Maßnahmen sind mit dem Entstehen neuer, bisher nicht vorhandener versichertenbezogener Datensammlungen bei den Krankenkassen verbunden. Dies steht in klarem Widerspruch zum Anliegen des Transparenzgesetzes. Meine gemeinsam mit dem Bundesbeauftragten für den Datenschutz und den anderen Landesbeauftragten für den Datenschutz vorgebrachten, mit Alternativvorschlägen verbundenen Bedenken hiergegen wurden leider nicht berücksichtigt. Das Gesetz wird wohl bald in Kraft treten und den Sozialdatenschutz erneut ein Stück weit zurückdrängen.

2. Die Arzneimittelchipkarte

Im August 2001 machten Presseberichte die Runde, wonach das Bundesgesundheitsministerium als Konsequenz aus der sog. Lipobay-Affäre die Einführung eines Arzneimittel-Passes plane. Gedacht war an eine Chipkarte, auf der lückenlos alle von den behandelnden Ärzten verschriebenen Medikamente zu speichern seien. Damit sollte eine gleichzeitige Verschreibung von Medikamenten, die auf Grund ihrer Wechselwirkungen zu gesundheitlichen Problemen führen können, vermieden und eine größere Transparenz bei der Arzneimittelverordnung erreicht werden. Die Verwendung der Karte sollte bei jedem Arztbesuch und bei jeder Rezepteinlösung in der Apotheke Pflicht sein.

Mittlerweile scheint diese Idee aber schon wieder überholt zu sein. Nicht, dass man sich angesichts der nicht nur von Datenschutzbeauftragten vorgetragenen erheblichen Bedenken gegen eine solche Form der Datenhaltung und Datenverarbeitung eines Besseren besonnen hätte. Nein, die Bundesgesundheitsministerin sattelte noch einen drauf. Nach jüngsten ministeriellen Äußerungen sollen nun nicht nur verordnete Medikamente auf einer Chipkarte gespeichert werden. Gedacht ist vielmehr an einen umfassenden Gesundheitspass auf der Basis der Krankenversichertenkarte. Auf dieser sollen

neben Medikamenten auch Angaben über chronische Krankheiten, Allergien, Operationen, Röntgenuntersuchungen und wer weiß was noch alles gespeichert werden. Dem Bürger soll damit zugemutet werden, sein vollständiges Gesundheitsprofil ständig mit sich herumzutragen. Der vielfach beschworene „gläserne Patient“ scheint damit in greifbare Nähe gerückt zu sein. Formal soll die Verwendung zwar freigestellt werden. Allerdings ist offenbar daran gedacht, die „Freiwilligkeit“ dadurch zu befördern, dass bei Nichtverwendung höhere Zuzahlungen bei Medikamenten drohen. Auch gegen diesen nicht ganz zu Unrecht als neuen Luftballon am Gesundheitshimmel bezeichneten Versuch, Gesundheitsdaten leichter verfügbar zu machen, hat sich eine breite Front von Kritikern gebildet. Es bleibt – vor allem auch im Interesse der Patienten daran, das Wissen um ihre gesundheitlichen Verhältnisse für sich behalten zu können – zu hoffen, dass auch dieser Luftballon zum Platzen gebracht wird.

Unabhängig davon, wozu diese Vorstellungen letztlich führen, haben es die Datenschutzbeauftragten des Bundes und der Länder für wichtig gehalten, sich schon bei Bekanntwerden der Pläne für einen Medikamentenpass erneut mit der Problematik des Einsatzes von Chipkarten im Gesundheitswesen zu befassen. Sie haben nochmals betont, dass in jedem Fall die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung einer wie auch immer gearteten Karte gewährleistet sein muss. Dabei steckt der Teufel allerdings im Detail. Denn es ist nicht allein damit getan, dem Patienten die Karte in die Hand zu drücken und es ihm zu überlassen, ob er sie einsetzen will oder nicht. Diese Alternative des Alles oder Nichts wird der Problematik nicht gerecht. Eine wirkliche Freiwilligkeit ist nur dann gewährleistet, wenn der Karteninhaber auch von Fall zu Fall darüber entscheiden kann,

– welche Daten in die Karte aufgenommen werden,

– welche Daten im Einzelfall zugänglich gemacht werden und

– welche Daten wieder gelöscht werden.

Diese Freiheit des Einzelnen, ganz individuell und von Fall zu Fall über die Preisgabe seiner Gesundheitsdaten entscheiden zu können, muss durch die technische Ausgestaltung der Chipkarte gewährleistet werden. Hier bedarf es sicher noch etlicher Anstrengungen.

Die auf der 62. Datenschutzkonferenz des Bundes und der Länder vom 24. bis 26. Oktober 2001 gefasste und im Anhang 14 wiedergegebene Entschließung zur Medikamentenchipkarte stellt die wesentlichen Eckpunkte dar, die aus Sicht des Datenschutzes bei der Einführung solcher neuen Medien zu beachten sind. Es bleibt zu hoffen, dass die für das Gesundheitswesen Verantwortlichen die darin geäußerten Bedenken ernst nehmen, die Bedeutung der Vertraulichkeit der sensiblen Gesundheitsdaten würdigen und sie verantwortungsbewusst in ihre Überlegungen mit einbeziehen.

3. Einzelfälle

Von allen Zweigen der Sozialversicherung ist die gesetzliche Krankenversicherung derjenige, bei dem das Netz datenschutzrechtlicher Regelungen am dichtesten geknüpft ist. Dies hat einerseits den Vorteil, dass verhältnismäßig klar ist, wie Sozialdaten verarbeitet werden dürfen und wie nicht. Andererseits kann der oder die einzelne Beschäftigte eines Leistungserbringers oder Leistungsträgers leicht den Überblick verlieren und sich in diesem Normengeflecht verheddern. Mitunter wird aber auch aus – vermeintlichen – Sachzwängen heraus versucht, das enge Korsett zu sprengen, indem einzelne Vorschriften über ihre Grenzen hinaus ausgelegt oder schlicht missachtet werden. Hierzu folgende Beispiele:

3.1 Die Kassenärztliche Vereinigung und die Löschpflicht

Rechnet ein Vertragsarzt Leistungen ab, die er im Rahmen der gesetzlichen Krankenversicherung erbracht hat, schickt er seine Abrechnungsunterlagen nicht unmittelbar an die Krankenkasse, sondern an die Kassenärztliche Vereinigung. Deren Aufgabe ist es, die Abrechnung zu prüfen und sie unter Weglassen des Patientennamens an die Kranken-

kasse weiterzuleiten. Im Zusammenhang mit der Eingabe eines Arztes fand ich nun heraus, dass die Kassenärztliche Vereinigung Südbaden die Abrechnungsdaten nicht nach Ablauf der im Gesetz vorgegebenen Frist löscht, sondern sie weiter speichert. Als Grund gibt sie an, dass sie die Daten für die Prüfung ärztlichen Leistungsverhaltens benötige. Dies sei äußerst langwierig. Honorarstreitigkeiten würden oft Jahre dauern. Allerdings würden die Daten nach Ablauf der Löschungsfrist „pseudonymisiert", indem neben der Versichertennummer an Stelle der Identifizierungsdaten nur noch die ersten drei Buchstaben des Namens sowie Geburtsmonat und -jahr gespeichert würden.

Zunächst musste ich die Kassenärztliche Vereinigung davon überzeugen, dass sie die Abrechnungsdaten tatsächlich nach zwei Jahren zu löschen hatte. Diese Verpflichtung hatte sie nämlich in Abrede gestellt. § 304 Abs. 1 Satz 1 Nr. 2 SGB V bestimmt, dass Daten „nach § 295 Abs. 2" spätestens nach zwei Jahren zu löschen sind. Daten nach § 295 Abs. 2 SGB V sind die für die vertragsärztliche Versorgung erforderlichen Angaben über die abgerechneten Leistungen. Es sind also genau die Daten, die der Arzt der Kassenärztlichen Vereinigung zu Abrechnungszwecken überlässt. § 304 Abs. 1 Satz 1 Nr. 2 SGB V enthält keinen Anhalt dafür, dass die Kassenärztliche Vereinigung von der zweijährigen Löschungsfrist ausgenommen werden soll.

Schwieriger war es, der Kassenärztlichen Vereinigung klarzumachen, dass auch die von ihr ins Spiel gebrachte Pseudonymisierung nichts an ihrer Pflicht ändert, die Abrechnungsdaten nach zwei Jahren zu löschen. Denn durch die Pseudonymisierung wird weder der Personenbezug vollständig beseitigt noch wird die Personenbeziehbarkeit wenigstens so weit erschwert, dass von einer faktischen Anonymität auszugehen ist. Der Grad der Pseudonymisierung ist so schwach, dass sich der einzelne Patient ohne allzu große Mühe wieder identifizieren lässt, zumal die Kassenärztliche Vereinigung selbst die Informationen besitzt, die dazu benötigt werden. Angesichts dessen, dass sie nach wie vor meint, diese Daten für die Erfüllung ihrer Aufgaben personenbezogen zu brauchen, ist es auch nur konsequent, wenn sie von einer unumkehrbaren Anonymisierung absieht. Zwar hat die Kassenärztliche Vereinigung nachträglich ein intelligenteres Verschlüsselungsverfahren vorgeschlagen, das die Reidentifizierung bestimmten innerorganisatorischen Schutzmechanismen unterwirft. An dem grundsätzlichen Problem, dass die Daten dadurch nicht ihren Personenbezug verlieren und deshalb nach dem Gesetz spätestens nach Ablauf von zwei Jahren gelöscht werden müssen, ändert dies jedoch nichts.

Ärgerlich an der ganzen Angelegenheit ist nicht in erster Linie, dass hier unterschiedliche Auffassungen darüber bestehen, was die Kassenärztliche Vereinigung darf und was sie nicht darf. Ärgerlich ist vielmehr der Umstand, dass sich die Sache jetzt schon mehr als ein Jahr hinzieht und immer noch zu keinem greifbaren Ergebnis geführt hat. Allein seit Januar dieses Jahres musste die Kassenärztliche Vereinigung fünfmal aufgefordert werden, sich endlich zu äußern. In der Zwischenzeit verarbeitet sie die Versichertendaten weiterhin unter permanentem Verstoß gegen geltendes Recht. Ich werde weiter am Ball bleiben und darauf bestehen, dass die Rechte der Versicherten beachtet werden.

3.2 Gut gemeint, falsch gehandelt

Besonders unangenehm sind die Situationen, in denen man aus heiterem Himmel mit persönlichen Daten konfrontiert wird, die man eigentlich an ganz anderer Stelle vermutet hatte. So ging es einem Bürger, der vor dem Sozialgericht einen Prozess gegen eine Berufsgenossenschaft führte. In einem Schriftsatz berief sich die Berufsgenossenschaft plötzlich auf ein Gutachten, das der Medizinische Dienst der Krankenversicherung (MDK) im Auftrag der Krankenkasse über den Bürger erstattet hatte. Er wandte sich an mich und bat darum, die Sache aufzuklären. Was war geschehen?

Der Bürger hatte in einem persönlichen Gespräch mit dem Kundenberater seiner Krankenkasse beklagt, dass die Berufsgenossenschaft Leis-

tungen verweigere, die ihm seiner Meinung nach wegen eines Berufsunfalls zustünden. Der Berater, in der Meinung, dem Kunden damit einen Gefallen zu tun, schickte daraufhin das besagte MDK-Gutachten, das er in den Akten gefunden hatte, einfach an die Berufsgenossenschaft, wohlgemerkt ohne den Betroffenen vorher zu fragen, geschweige denn um Erlaubnis zu bitten. Die Berufsgenossenschaft verwendete das Gutachten gegen den Betroffenen.

Es ist durchaus lobenswert, wenn sich die Mitarbeiter der Krankenkassen für die Belange der Versicherten einsetzen. Die Fürsorge darf allerdings nicht so weit gehen, dass über den Kopf des Betroffenen hinweg unberechtigt Daten weitergegeben werden. So war es aber hier.

Das in den Akten der Krankenkasse abgeheftete medizinische Gutachten enthielt sensible Gesundheitsdaten. Da sie von einem Arzt erhoben worden waren, unterliegen sie einem besonderen Geheimnisschutz. § 76 Abs. 1 SGB X berechtigt deshalb die Krankenkasse, der diese Daten zugänglich gemacht wurden, zu einer Weitergabe nur unter denselben Bedingungen, unter denen der Arzt die Daten hätte weitergeben dürfen. Die ärztliche Schweigepflicht wird damit praktisch verlängert. Ausnahmen gelten nach § 76 Abs. 2 Nr. 1 SGB X allerdings dann, wenn es um Daten in einem medizinischen Gutachten geht, das im Auftrag eines Sozialversicherungsträgers erstattet worden ist. Dieses Gutachten darf auf Antrag auch einem anderen Sozialversicherungsträger übermittelt werden, wenn dieser es zur Erfüllung seiner Aufgaben benötigt. Etwas anderes gilt nur dann, wenn der Betroffene der Übermittlung widersprochen hat. Auf dieses Widerspruchsrecht ist er hinzuweisen.

Dass die Krankenkasse hier das MDK-Gutachten, wenn auch in guter Absicht, weitergegeben hat, ohne den Betroffenen vorher nochmals dazu zu befragen und ihm die Möglichkeit zum Widerspruch einzuräumen, habe ich gegenüber der Krankenkasse beanstandet. Sie hat diese Beanstandung akzeptiert und das Vorkommnis zum Anlass genommen, die Mitarbeiterinnen und Mitarbeiter nochmals darüber zu informieren, was in solchen Fällen zu beachten ist.

3.3 Krankenkasse auf der Hut

Man kann sich manchmal nur darüber wundern, wie gedankenlos oder vorschnell eine Behörde einer anderen Daten von Bürgern abverlangt. Besonders forsch ging das Staatliche Gewerbeaufsichtsamt (GAA) Göppingen vor. Einer seiner Mitarbeiter schickte kurzerhand folgendes Telefax an eine Krankenkasse:

> „Firma ... Leipzig. Das GAA GP bittet um Mitteilung über sämtliche Namen, Adresse u. Geburtsdatum derer, die von der ... bei Ihnen gemeldet sind.
>
> MfG“

Das GAA hielt es weder für nötig, der Krankenkasse mitzuteilen, wozu es die Daten benötigte, noch auf Grund welcher Rechtsgrundlage diese berechtigt sein sollte, dem Auskunftsersuchen zu entsprechen. Die Mitarbeiterin der Krankenkasse konnte ein solches Ersuchen freilich nicht beeindrucken und fragte den hauseigenen Datenschutzbeauftragten, ob sie die Mitgliederdaten herausgeben dürfe. Weil bei diesem spärlichen Auskunftsersuchen natürlich auch er keine Befugnis zur Datenweitergabe sah, fragte er beim GAA nach. Der dortige Sachbearbeiter bequemte sich allerdings nur zu der wenig aufschlussreichen Auskunft, er bearbeite den größten Fall Deutschlands, die Leitung des betreffenden Unternehmens stehe mit einem Bein im Gefängnis und die Mitarbeiter des Unternehmens müssten alle als Zeugen gehört werden. Auf die weitere Frage, warum er denn dazu die Geburtsdaten der Beschäftigten wissen müsse, erklärte er, auf die Angaben zum Geburtstag könne er auch verzichten, die seien nicht so wichtig. Der Datenschutzbeauftragte ließ sich jedoch nicht ins Bockshorn jagen und verweigerte die Auskunft endgültig, nachdem er sich bei meinem Amt rückversichert hatte, dass die Weitergabe der gewünschten Sozialdaten bei dieser Sachlage rechtswidrig wäre.

Als wir das GAA baten, sich zu dem Vorgang zu äußern, zeigte es sich zunächst wenig kooperativ und verweigerte die Antworten auf die Fragen meines Amts. Erst als wir deutlich auf die Auskunfts- und Mitwirkungspflicht des GAA hinwiesen, gab es eine Stellungnahme ab. Diese stellte dann auch unter Beweis, dass das GAA nicht einmal das kleine Einmaleins des Datenschutzes beherrscht. Abgesehen davon, dass es die Daten gar nicht benötigte, wusste es weder auf Grund welcher Rechtsgrundlage es selbst Daten erheben darf noch dass Daten grundsätzlich beim Betroffenen zu erheben sind. Zudem war ihm nicht klar, dass die Auskunft ersuchende Stelle in dem Fall, in dem ausnahmsweise die Erhebung von Daten bei einer anderen Stelle erforderlich ist, ihr Ersuchen so substantiiert darlegen muss, dass diese feststellen kann, ob sie die Daten herausgeben darf oder nicht. Eine förmliche Beanstandung des Vorgehens des GAA war die einzig mögliche Konsequenz.

Dieser Fall zeigt einmal mehr, wie wichtig es für die Behörden ist, eigene Datenschutzbeauftragte zu haben, welche die Mitarbeiter in datenschutzrechtlichen Fragen ad hoc konsultieren können.

3. Abschnitt: Die Jugendämter

1. Aus der Kontrollpraxis

Einer der Schwerpunkte der Kontrolltätigkeit meiner Dienststelle lag in diesem Jahr bei den Jugendämtern. Dazu besuchten Mitarbeiter meines Amtes die Landratsämter Tübingen, Schwarzwald-Baar-Kreis, Lörrach, Reutlingen und Freudenstadt sowie die Stadt Freiburg i. Br. Dabei ging es vor allem um die Frage, wie sich der Informationsfluss innerhalb ihrer Jugendämter abspielt und wie diese sicherstellen, dass der Datenschutz ihrer Klienten auch dann gewahrt bleibt, wenn sie sich zur Erfüllung ihrer Aufgaben sog. freier Träger bedienen.

1.1 Das Jugendamt – eine Informationseinheit?

Ein elementarer Grundsatz des Datenschutzes lautet: Auch innerhalb einer Behörde soll jeder nur die personenbezogenen Daten erhalten, die er zur Erfüllung seiner Aufgaben benötigt. Das Gleiche gilt selbstverständlich auch für die einzelnen Sachgebiete in den Jugendämtern. Wir stellten daher die Praxis der genannten Jugendämter auf den Prüfstand und gingen der Frage nach, welche Informationen der Soziale Dienst an die sog. Wirtschaftliche Jugendhilfe weitergibt.

Dazu muss man Folgendes wissen:

Der Soziale Dienst, Allgemeiner Sozialdienst oder auch Bezirkssozialarbeit genannt, ist das zentrale Sachgebiet der Jugendämter. Es soll Rat und Hilfe geben oder vermitteln, das schwierige Wächteramt zum Wohle des Kindes wahrnehmen, über konkrete Maßnahmen der Jugendhilfe entscheiden sowie in Verfahren der Vormundschafts- und Familiengerichte mitwirken, um nur einige Aufgaben zu nennen. Der Soziale Dienst hat seine Wurzeln in der Familienfürsorge, einer Institution in den Großstädten der 20er-Jahre. Diese Fürsorge wurde vornehmlich als aufsuchende Sozialarbeit und somit im Außendienst tätig. Auch heute noch können Beratung und Hilfestellung in Sprechstunden des Amtes, auf der Straße – z. B. als sog. Streetwork – oder in der Wohnung der Klienten erbracht werden. Nicht zuletzt auf Grund der hohen Verantwortung, die gerade diese Mitarbeiter tragen, sind solche sog. Kernaufgaben Fachkräften zu übertragen, also vor allem Sozialarbeitern, Sozialpädagogen, Erziehern und Psychologen. Sie entscheiden, ob und welche spezielle Hilfemaßnahme im Einzelfall notwendig und geeignet ist. Die Wirtschaftliche Jugendhilfe kümmert sich dagegen, vereinfacht formuliert, im Wesentlichen um die finanzielle Abwicklung der gewährten Hilfeleistungen. Für den größten Teil der Hilfeleistungen nach dem Kinder- und Jugendhilfegesetz (SGB VIII) kommt es auf eine vorhergehende Prüfung von Einkommen und Vermögen der Betroffenen aber nicht an. Dauer und Umfang der Hilfeleistung richten sich

nämlich nicht nach der finanziellen Leistungsfähigkeit der Betroffenen, sondern nach dem festgestellten erzieherischen oder pädagogischen Defizit. Der Nachrang sozialer Leistungen wird dann dadurch hergestellt, dass etwaige Ersatzpflichtige nachträglich zu den Kosten der Hilfemaßnahme herangezogen werden. Diese Heranziehung erfolgt durch die Wirtschaftliche Jugendhilfe.

Zu unserer Überraschung stellten wir fest, dass Sozialer Dienst und Wirtschaftliche Jugendhilfe trotz unterschiedlicher Aufgaben nahezu einen identischen Wissensstand über die persönlichen Verhältnisse der Personen aufwiesen, mit denen es die beiden Sachgebiete zu tun hatten. Wesentliche Ursache dafür war die Art und Weise, wie der Soziale Dienst die Wirtschaftliche Jugendhilfe in die Durchführung der Hilfemaßnahmen einbezog. So leitete er dieser von ihm erstellte Vorlagen und Berichte zu, die in epischer Breite über alle Details der Leistungsfälle informierten. Dabei wurde das gesamte Umfeld des zu betreuenden Kindes geschildert und vielfach auch Umstände dargestellt, die Jahre zurücklagen. Unter anderem trafen wir Berichte an, in denen über die problematische Kindheit einer Mutter ebenso informiert wurde wie über Alkoholprobleme eines ehemaligen Ehegatten, über schwere Erkrankungen eines Ehepaars und noch vieles andere an sensiblen Angaben mehr.

Aber damit nicht genug:

Der Gesetzgeber hält die Jugendämter dazu an, als Grundlage für die Ausgestaltung der Hilfe mit den Personensorgeberechtigten und dem Kind oder dem Jugendlichen in regelmäßigen Abständen einen sog. Hilfeplan zu erarbeiten. Dieser Plan soll Feststellungen über den erzieherischen Bedarf, die zu gewährende Art der Hilfe sowie die notwendigen Leistungen enthalten. Aus den von uns eingesehenen Hilfeplänen war z. B. zu ersehen, dass ein Sorgeberechtigter Kontakte zu Personen aus verrufenen Gegenden hatte, dass der Partner eines Elternteils erfolgloser Teilnehmer an mehreren Therapien war, und welche hygienischen Verhältnisse und Waschgewohnheiten in einer Familie herrschten. Alle diese Hilfepläne landeten komplett auch bei der Wirtschaftlichen Jugendhilfe.

Einmal abgesehen von der Frage, ob alle diese Angaben überhaupt in einen Hilfeplan gehören, wie ihn das Jugendhilfegesetz vorsieht: Ist es wirklich notwendig, dass diese vor sensiblen Informationen überbordenden Unterlagen, Berichte und Hilfepläne komplett der Wirtschaftlichen Jugendhilfe zur Verfügung gestellt werden? Die Frage stellen heißt, sie verneinen. Ich empfahl deshalb den Jugendämtern folgendes Vorgehen:

Die Wirtschaftliche Jugendhilfe sollte dem Sozialen Dienst generell vorgeben, welche Informationen sie für die Abwicklung eines Leistungsfalles benötigt. Daraufhin kann ihm dieser die erforderlichen Angaben zur Verfügung stellen. So wie bisher dessen Berichte und Hilfepläne komplett der Wirtschaftlichen Jugendhilfe weiterzugeben, muss der Vergangenheit angehören.

Die Reaktionen der Jugendämter auf meine Forderung, den Informationsfluss im Jugendamt zu reduzieren, waren zurückhaltend. Immerhin, man will das bisherige Vorgehen einer Überprüfung unterziehen. Da und dort wurde auch schon signalisiert, dass eine Umgestaltung beabsichtigt sei.

1.2 Die Inanspruchnahme von Trägern der freien Jugendhilfe

Die örtlichen Träger der öffentlichen Jugendhilfe, mithin die Landkreise und die kreisfreien Städte, bedienen sich zur Bewältigung ihrer vielgestaltigen Aufgaben oft und gerne der Hilfe sog. freier Träger. Dabei handelt es sich nicht um einen abgeschlossenen Kreis von Verbänden und Organisationen, sondern sowohl um gemeinnützige Einrichtungen als auch privat-gewerbliche Träger.

Die kontrollierten Jugendämter übertrugen Aufgaben wie z. B. die komplette Ausführung der Inobhutnahme und Notunterbringung von Kin-

dern und Jugendlichen, die Durchführung des betreuten Umgangs sowie verschiedene ambulante Hilfeleistungen auf freie Träger. Außerdem sollten freie Träger Jugendhilfestationen einrichten und darin nahezu alle Jugendhilfeleistungen vor Ort selbst erbringen.

Aus der Sicht des Datenschutzes ist die Einschaltung freier Träger in die Aufgaben der öffentlichen Jugendhilfe aber nicht unproblematisch. Sie sind auf Grund ihrer Autonomie nämlich keine Adressaten der Bestimmungen über den Sozialdatenschutz. Für sie gelten unmittelbar lediglich die Bestimmungen des allgemeinen Datenschutzrechts, wie das Bundesdatenschutzgesetz und für kirchliche Einrichtungen das jeweilige kirchliche Datenschutzrecht. Zwischen dem Sozialdatenschutz einerseits und dem allgemeinen Datenschutzrecht andererseits besteht aber ein qualitativer Unterschied.

Der Gesetzgeber beugte im Sozialgesetzbuch jedoch vor und verpflichtete die Jugendämter sicherzustellen, dass der Sozialdatenschutz auch bei den freien Trägern gewährleistet bleibt. Dazu gehört als Mindestvoraussetzung, dass die freien Träger vertraglich verpflichtet werden, die für das Jugendamt maßgebenden Bestimmungen zu beachten.

Bei den von uns eingesehenen Vereinbarungen mit den freien Trägern dachten die Vertragsparteien aber regelmäßig nicht an diese Sicherstellungsverpflichtung. Datenschutzrechtliche Regelungen waren zum Teil in den getroffenen Kontrakten nicht einmal erwähnt. In einigen wenigen Fällen lagen sogar überhaupt keine schriftlichen Vereinbarungen vor.

Jeweils davon auszugehen, dass die Mitarbeiter der freien Träger schon um die Sensibilität der von ihnen verarbeiteten Daten wissen, erscheint mir zu blauäugig. Ich forderte deshalb die Jugendämter auf, mit den freien Trägern entsprechende Vereinbarungen abzuschließen. Darin sind zumindest die maßgebenden datenschutzrechtlichen Vorschriften anzusprechen und die notwendigen Datenschutzvorkehrungen zu bezeichnen. Bereits geschlossene Vereinbarungen sind im Interesse der Klienten der Jugendämter insoweit zu ergänzen. Das soll jetzt geschehen.

2. Das viel gefragte Jugendamt

Die Jugendämter sehen sich vielen Auskunftswünschen von ganz unterschiedlicher Seite ausgesetzt. Sie zu beantworten, ist oft alles andere als einfach. Dazu einige Beispiele aus unserer Kontroll- und Beratungspraxis:

2.1 Die Auskunft über die eigenen Daten und die berechtigten Geheimhaltungsinteressen Dritter – ein Balanceakt

Jeder hat Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Diese hat jedoch u. a. dann zu unterbleiben, wenn die Daten wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen. So bestimmt es § 83 des Zehnten Buchs des Sozialgesetzbuchs (SGB X). Wie die Auskunft gegeben wird, entscheidet das Jugendamt, sie kann, muss aber nicht, auch durch Akteneinsicht gewährt werden. So einfach sich das liest, die Praktizierung macht hin und wieder Probleme.

– Gar nicht so selten wurde ich gefragt, wie bei Hinweisen aus der Nachbarschaft auf eine mögliche Gefährdung des Wohles eines Kindes zu verfahren ist. Nachvollziehbar ist, dass eine Familie, der das Jugendamt daraufhin einen Hausbesuch abstattet, gerne wissen will, wer der Informant war, um gegebenenfalls Strafanzeige erstatten zu können. Dies insbesondere dann, wenn der Besuch ergab, dass kein Anlass zum Einschreiten des Jugendamts besteht. Grundsätzlich umfasst der Auskunftsanspruch auch die Herkunft der Informationen und damit auch die Namen von Informanten. Nur, in solchen Fällen hat die Auskunftserteilung in der Regel schon deshalb zu unterbleiben, weil die Jugendämter bei der Erfüllung ihrer Aufgabe auf die Mithilfe der Bürger angewiesen sind. Oft erhalten sie nur durch Hinweise von Privatpersonen Kenntnis von Sachverhalten, die im Inte-

resse der Kinder ein Einschreiten notwendig machen. Müssten diese damit rechnen, dass ihre Identität später preisgegeben wird, würden sie es sich sicher mehr als einmal überlegen, ob sie solche Hinweise geben. Denunzianten erhalten freilich keinen Freibrief. Macht jemand bewusst wahrheitswidrige Angaben, steht deshalb der Auskunftserteilung nichts im Wege.

– Pflegeeltern verlangten von einem Jugendamt zum einen mehr Informationen über die Vorgeschichte des Pflegekindes, zum anderen Einblick in die Akten, die ausschließlich die Tätigkeit der Pflegeeltern betrafen. Das Jugendamt kam beidem nicht nach. Soweit es um weitere Auskünfte zur besonderen Problemlage des Pflegekindes und seiner Herkunftsfamilie ging, lag es dabei völlig richtig. Zu weitgehend war die Ablehnung des Auskunftsbegehrens der Pflegeeltern über die zu ihrer Person gespeicherten Daten. Die vom Jugendamt geführte Akte enthielt z. B. eine Fülle von Gesprächsnotizen über Unterredungen mit den Pflegeeltern selbst. Warum das Jugendamt dann nicht wenigstens diese herausrücken wollte, war nicht einzusehen. Meiner Aufforderung, die Blockade zu lockern und den Pflegeeltern wenigstens einige weitere Unterlagen bekannt zu geben, kam das Jugendamt dann allerdings schnell nach.

– Verständlich, dass eine Frau, für die in den 60er-Jahren das Jugendamt als Pflegerin bestellt worden war, jetzt wissen wollte, weshalb es damals zu der Pflegschaft gekommen war. Das Jugendhilfegesetz räumt ehemaligen Pfleglingen dieses Recht ausdrücklich ein. Allerdings, auch dieser Anspruch muss zurücktreten, wenn berechtigte Interessen Dritter dem entgegenstehen. Selbst wenn es solche Geheimhaltungsinteressen Dritter gibt, eine Totalverweigerung ist in aller Regel aber nicht gerechtfertigt. In solchen Fällen bleibt es deshalb den Jugendämtern nicht erspart, zu differenzieren und die in ihren Unterlagen enthaltenen Informationen daraufhin zu überprüfen, inwieweit eine Bekanntgabe möglich ist.

2.2 Auskünfte an Dritte

Weil die Jugendämter über viele personenbezogene Daten verfügen, sind sie sowohl für andere Behörden als auch für Privatpersonen begehrte Informationsquellen.

– Darf eine als Amtsvormund bestellte Mitarbeiterin des Jugendamts der Familienkasse beim Arbeitsamt Auskunft über das Kind und seine Mutter geben, wenn die Kasse gegen die Mutter ein strafrechtliches Ermittlungsverfahren wegen des Verdachts eines zu Unrecht erlangten Steuervorteils in Form von Kindergeld durchführt? Vor diese Frage sah sich ein Jugendamt gestellt und bat mich um Rat. Wer weiß, dass für das Jugendamt in aller Regel das Sozialgeheimnis gilt, das trotz aller Bestrebungen der Politik, es zurückzudrängen, nach wie vor eine Datenweitergabe für Zwecke der Strafverfolgung nur unter eingeschränkten Voraussetzungen zulässt, wird von der Antwort vielleicht überrascht sein. Die Mitarbeiterin wird nicht umhin können, die gewünschten Angaben zu machen. Denn das Sozialgeheimnis gilt nicht für den Amtsvormund. Er übt ein privates Amt aus und ist deshalb, was den Umgang mit personenbezogenen Daten betrifft, einem privaten Vormund gleichgestellt. Im Strafverfahren ist er deshalb als Zeuge in gleicher Weise zur Aussage verpflichtet wie dieser.

– Nicht nachgeben durfte dagegen ein Jugendamt dem Wunsch einer Studentin der Hochschule für Polizei nach Einsicht in dort geführte Akten der Jugendgerichtshilfe. Die Studentin war dem Phänomen der jugendlichen Intensivtäter auf der Spur und wollte darüber eine Diplomarbeit schreiben. In diesem Fall war das Sozialgeheimnis zu beachten. Die dafür maßgebenden Regelungen ermöglichen eine Datenweitergabe ohne Einwilligung der Betroffenen aber nur, soweit sie erforderlich ist für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich. Von einer Forschung in diesem Bereich konnte bei der Diplomarbeit über jugendliche Intensivtäter aber nun wirklich keine Rede sein.

– Schon sehr verärgert wandte sich ein Vater an mich, der vom Jugendamt Anschrift und Aufenthalt seiner 16-jährigen Tochter erfahren wollte. Er wollte dies wissen, so begründete er jedenfalls seinen Antrag, um an Stelle der Tochter den Unterhalt für deren Kind beim Kindsvater geltend machen zu können. Dies entsprach aber offensichtlich nicht dem Wunsch der Tochter, der das Vormundschaftsgericht das Recht eingeräumt hatte, selbst zu entscheiden, ob und wann sie mit ihrem Vater Umgang haben will. Daran hatte sich das Jugendamt zu halten.

3. Die Akte des Beistands und der Bundesrechnungshof

Aufgeschreckt durch die Ankündigung des Bundesrechnungshofs, er wolle die Aktivitäten seines Jugendamts als Unterhaltsvorschusskasse überprüfen und dazu auch Einblick in dort geführte Akten über sog. Beistandschaften nehmen, bat mich ein Landratsamt um Rat, wie es sich dazu verhalten sollte. Es sah wohl ein, dass es dem Rechnungshof die Einsicht in die Akten der Unterhaltsvorschusskasse nicht verwehren kann, denn der Bund trägt schließlich ein Drittel der für die Leistungen der Unterhaltsvorschusskasse an Kinder, die nur bei einem Elternteil wohnen und vom anderen Elternteil keinen ausreichenden Unterhalt erhalten, notwendigen Mittel. Demzufolge ist der Bund auch daran interessiert, dass das Jugendamt seiner Aufgabe, zahlungsunwillige Unterhaltspflichtige zu einer Begleichung ihrer Unterhaltsschuld zu veranlassen, korrekt nachkommt. Nicht einsehen wollte das Landratsamt allerdings, dass der Bundesrechnungshof dazu auch Einblick in Akten aus dem Bereich der Beistandschaften nehmen wollte, und das zu Recht:

Auf den ersten Blick erschien die Forderung des Bundesrechnungshofes einleuchtend. Nicht selten überträgt nämlich die Unterhaltsvorschusskasse den an sich von ihr geltend zu machenden, übergegangenen Unterhaltsanspruch gegen den unterhaltspflichtigen Elternteil treuhänderisch auf das unterhaltsberechtigte Kind. Das kann durchaus Sinn machen, da dann nur ein Unterhaltsrechtsstreit geführt werden muss. Vollends liegt diese Lösung nahe, wenn der Elternteil, bei dem das Kind wohnt und dem das Sorgerecht zusteht, beim Jugendamt für die Geltendmachung der Unterhaltsforderung des Kindes eine Beistandschaft beantragt hat. Diese Konstellation führt dann dazu, dass es Aufgabe des zum Beistand bestellten Mitarbeiters des Jugendamts ist, sowohl die originäre Unterhaltsforderung des Kindes als auch die an sich von der Unterhaltsvorschusskasse geltend zu machende übergegangene Unterhaltsforderung einzuziehen. Kein Wunder also, dass der Bundesrechnungshof sich in solchen Fällen für die Aktivitäten des Beistands interessiert, denn davon hängt schließlich ab, wie viel Geld in die auch vom Bund gespeiste Unterhaltsvorschusskasse zurückfließt. Gleichwohl, so kann es nicht gehen. Der Beistand übt ein privates Amt aus. Macht er Unterhaltsansprüche gegen den unterhaltspflichtigen Elternteil geltend, erfüllt er nur die Aufgabe eines gesetzlichen Vertreters des Kindes und wird nicht gleichzeitig für die Unterhaltsvorschusskasse tätig. Hätte sich der sorgeberechtigte Elternteil nämlich nicht der Dienste des Beistands bedient, wäre der Unterhaltsanspruch von ihm selbst geltend zu machen. Es ist aber geradezu unvorstellbar, dass ihn der Bundesrechnungshof zu Hause aufsucht und dort in seine Unterlagen Einblick nimmt. Beantragt der sorgeberechtigte Elternteil eine Beistandschaft für das Kind, kann dies angesichts der gleichen Interessenlage aber nicht anders sein. Die Vorlage der Beistandschaftsakten im Rahmen einer Überprüfung der Unterhaltsvorschusskasse durch den Bundesrechnungshof kommt somit nicht in Betracht.

4. Abschnitt: Die Sozialämter

1. Unzulässige Datenweitergabe beim Programm „Arbeit statt Sozialhilfe“ – eine mühsame Wahrheitsfindung

Wer Arbeit sucht, aber z. B. wegen seines Alters oder einer Behinderung keine findet, dem muss das Sozialamt bei Bedürftigkeit Hilfe zum Lebensunterhalt gewähren, soweit etwaige Leistungen des Arbeitsamts nicht ausreichen. Diesen Zustand wollen beide Seiten gewöhnlich so schnell wie

möglich beenden: das Sozialamt, um die Kosten der Sozialhilfe zu sparen und der Hilfeempfänger, um nicht ständig um die Hilfe bitten und betteln zu müssen. Um hier Erfolge zu erzielen, fehlt es nicht an Modellen und Programmen, die Sozialhilfeempfänger wieder in Lohn und Brot zu setzen. So verweist auch die Stadt Stuttgart stolz darauf, mit ihrem Programm „Arbeit statt Sozialhilfe“ im bundesweiten Vergleich mit an der Spitze zu liegen. Mit dem Datenschutz nahm sie es dabei allerdings nicht so genau, wie mir eine Bürgerin mitteilte, die zeitweise auf Sozialhilfe angewiesen war. Ihre rhetorische Frage, sie dürfe doch annehmen, dass auch arbeitslosen Bürgern die gleichen Datenschutzrechte wie allen Bürgern zustehen, konnte ich – wenn auch erst 10 Monate später – nicht nur mit ja beantworten, sondern ihr auch mitteilen, dass die Stadt Stuttgart inzwischen daraus auch die nötigen Konsequenzen ziehen will. Doch der Reihe nach.

Besagte Dame teilte mir Mitte September 2000 mit, das Stuttgarter Arbeitsamt besitze Listen mit Angaben über Sozialhilfeempfänger, die ganz offensichtlich vom Sozialamt der Stadt Stuttgart stammten. Damit nicht genug habe das Arbeitsamt diese Sozialdaten an ein Unternehmen, das in dessen Auftrag die Betroffenen umfassend berät und unterstützt, weitergegeben. Zur Weiterleitung ihrer Daten an das Arbeitsamt oder gar an Dritte habe sie aber ihre Zustimmung nicht erteilt und sie wäre auch nicht damit einverstanden gewesen, wenn sie davon gewusst hätte.

Wir machten uns also auf den Weg, den Sachverhalt zu eruieren, doch es sollte ein beschwerlicher werden. Auf unsere Bitte um Stellungnahme reagierte nämlich die Stadt zunächst nicht. Dann teilte sie mit, „ihres Wissens“ seien im Rahmen des Programms „Arbeit statt Sozialhilfe“ gar keine Sozialdaten weitergegeben worden, sie prüfe aber noch, ob dies außerhalb des Projekts geschehen sei. Als wir später an die Angelegenheit erinnerten, ließ uns die Stadt wissen, dass die Datenübermittlung vom Sozialamt an das Arbeitsamt auf einen Datenabgleich mit der Arbeitsverwaltung zurückgehe. Das Sozialamt dürfe nämlich überprüfen, ob Sozialhilfeempfänger Leistungen des Arbeitsamts beziehen oder bezogen haben, und dazu bestimmte Daten an sog. Auskunftsstellen zum Abgleich übermitteln. In diesem Fall sei der Abgleich aber unmittelbar mit dem Arbeitsamt erfolgt. Diese Erklärung war so unglaubwürdig, dass nur ein Kontrollbesuch vor Ort Licht in das Dunkel bringen konnte. Dabei entpuppte sich der Hinweis der Stadt auf einen angeblichen Datenabgleich zwischen Sozial- und Arbeitsamt prompt als Ablenkungsmanöver; er fand gar nicht statt. Vielmehr hatte das Sozialamt dem Arbeitsamt im Juni 2000 eine Liste übergeben, in der ca. 1 000 Sozialhilfeempfänger im Alter zwischen 25 und 54 Jahren aufgeführt waren, die zugleich Leistungen der Arbeitsverwaltung bezogen. Dabei war der Stadt klar, dass das Arbeitsamt für die Daten nur Durchgangsstation sein sollte, denn Empfänger war am Ende das bereits erwähnte Unternehmen, das mit den Sozialhilfeempfängern Kontakt aufnehmen und sie bei der Suche nach einem Arbeitsplatz beraten und unterstützen sollte.

Die falsche Auskunft der Stadt habe ich im Dezember 2000 förmlich beanstandet. Es versteht sich von selbst, dass Angaben, die mir Behörden auf Grund ihrer im Landesdatenschutzgesetz verankerten Auskunfts- und Unterstützungspflicht geben, auch stimmen müssen. Meine Kontrollaufgabe kann ich natürlich nur dann erfüllen, wenn ich mich darauf verlassen kann, dass die Antworten der öffentlichen Stellen auf Fragen meines Amts zutreffend sind. Zugleich stellte ich der Stadt konkrete Fragen zur Aufklärung des Geschehenen. Nachdem die Stadt die Angelegenheit schon bis dahin sehr zögerlich betrieb, übte sie sich jetzt erst einmal in Stillschweigen. Auf unsere erneute Erinnerung Ende Januar 2001 teilte mir die Stadt mit, der Vorgang befinde sich „im Mitzeichnungsverfahren“ und die Stellungnahme würde uns umgehend zugeleitet, sobald die angeschriebenen Referate mitgezeichnet haben. Ob dazu in diesem Fall Anlass bestand, kann man mit Fug und Recht bezweifeln, denn die Rechtslage ist eindeutig. Die Übermittlung von Daten von Sozialhilfeempfängern an das Arbeitsamt mit dem Zweck, diese Daten von dort an ein privates Unternehmen weiterzugeben, bedarf der Einwilligung der Hilfesuchenden, die dabei umfassend über den Zweck der Datenweitergabe und die Folgen der Verweigerung der Einwilligung aufzuklären sind. Die beteiligten Referate der Stadt taten sich offenbar schwer, diese von der Zentralen Datenschutzstelle aufgezeigte Rechtslage

zu akzeptieren, denn wieder einen Monat später schrieb uns der Oberbürgermeister, wider Erwarten verzögere sich die Stellungnahme und er bitte noch um etwas Geduld. Die war jedoch erschöpft, nachdem wieder ein Monat verstrichen war, in dem die Stadt nichts von sich hören ließ. So musste ich mich im März 2001 erneut an den Oberbürgermeister wenden und ihn dringend bitten, für die Erledigung der Sache durch seine Verwaltung Sorge zu tragen. Anfang April 2001 war es dann endlich so weit. Die Stadt Stuttgart bekannte sich zu dem Sachverhalt und räumte ein, dass die Datenweitergabe an das Arbeitsamt rechtswidrig war. Warum nicht gleich so?

2. Datenabgleiche – wie viele noch?

Keine Frage – Sozialämter müssen dem Erschleichen von Sozialhilfeleistungen wirksam entgegentreten können. Ob dabei die Kontrolle durch automatisierte Datenabgleiche allerdings der Weisheit letzter Schluss ist, muss mehr denn je bezweifelt werden, wenn man sich vor Augen hält, was der Sozialminister des Landes zu Beginn des Jahres verlauten ließ. Danach ergab sich nämlich infolge der computergestützten Abgleiche mit Datensammlungen von Sozialversicherungsträgern bei rund 400 000 erfassten Fällen eine Missbrauchsquote von nur 0,46 %. Der Minister wolle sich deshalb „vor allem vor die Menschen stellen, die auf Sozialhilfe angewiesen sind“, hieß es in der Pressemitteilung. Er sprach von „wenigen schwarzen Schafen“ und „klaren Fakten, die Spekulationen über einen weit verbreiteten Sozialleistungsbetrug widerlegen“. Gleichwohl hat der Bund eine neue Ermächtigung zum Datenabgleich, nämlich mit dem Bundesamt für Finanzen, geschaffen und einen Entwurf zur Änderung der sog. Sozialhilfedatenabgleichsverordnung vorgelegt. Das gab mir Veranlassung, dem Sozialministerium im Sommer dieses Jahres diesen Brief zu schreiben:

„Sehr geehrte Damen und Herren,

für die Übersendung des o.a. Referentenentwurfs bedanke ich mich. Änderungs- und Ergänzungsvorschläge habe ich dazu nicht. Jedoch gibt mir der VO-Entwurf Anlass zu folgenden Anmerkungen:

Mit dieser Verordnung soll nunmehr auch ein automatisierter Abgleich mit dem Datenbestand des Bundesamts für Finanzen ermöglicht werden. Meine grundsätzliche Haltung zu automatisierten Datenabgleichen in der Sozialhilfe ist dem Sozialministerium bekannt. Ich darf dazu auf die Ausführungen zu dieser Frage in meinem 19. Tätigkeitsbericht (LT-Drs. 12/3480, S. 12) verweisen. Die Ergebnisse der bisher durchgeführten Abgleiche bestätigen mich in dieser Beurteilung. Wie u. a. auch der Pressemitteilung des Sozialministeriums vom 30. Januar 2001 zu entnehmen ist, waren diese ausgesprochen dürftig. Sie beschränkten sich im Wesentlichen auf die Feststellung von nicht angegebenen sog. geringfügigen Beschäftigungen. Nach der Änderung der für solche Beschäftigungsverhältnisse maßgebenden Rechtsgrundlagen ist ihre Zahl erheblich zurückgegangen, sodass schon aus diesem Grunde die ohnehin geringe Zahl von Missbrauchsfällen noch weiter zurückgehen wird.

Anstatt sich die Frage zu stellen, ob es angesichts der Ergebnisse der bisherigen Datenabgleiche und des sonstigen höchst umfangreichen Instrumentariums zur Missbrauchsbekämpfung in der Sozialhilfe überhaupt noch vertreten werden kann, solche Datenabgleiche durchzuführen und damit alle Sozialhilfeempfänger als potenzielle Sozialhilfebetrüger zu behandeln, soll mit dem Verordnungsentwurf die Möglichkeit, Datenabgleiche vorzunehmen, sogar noch erweitert und damit die mit den Abgleichen verbundenen Eingriffe in das Grundrecht auf Datenschutz der Sozialhilfeempfänger noch verstärkt werden. Es ist mir angesichts der gegenwärtig im Sommerloch in der Politik erhobenen populären Forderung, mehr Druck auf die Sozialhilfeempfänger auszuüben, sehr wohl bewusst, dass meine Empfehlung, von Datenabgleichen abzusehen und schon gar nicht die Abgleichsmöglichkeiten zu erweitern, wenig Gehör finden mag. Von der Sache her gerechtfertigt ist sie aber allemal. Ich hoffe deshalb, dass sich wenigstens die Sozialhilfeträger in Baden-Württemberg wie bisher in dieser Frage zurückhalten und sich genau überlegen, ob es sich angesichts der geringen Erfolgs-

aussichten der Abgleiche wirklich lohnt, das Persönlichkeitsrecht der Sozialhilfeempfänger hintan zu stellen und den damit verbundenen bürokratischen Aufwand auf sich zu nehmen.

Mit freundlichen Grüßen“

Dem ist nichts hinzuzufügen.

3. Der Hausbesuch

Ein anderes Mittel, Sozialhilfemissbrauch auf die Spur zu kommen, ist der Einsatz von hin und wieder auch als Sozialdetektive bezeichneten Außendienstmitarbeitern. Ihre Aufgabe ist es, vor Ort zu ermitteln, ob die Angaben des Hilfeempfängers zutreffen und die Voraussetzungen für die Gewährung von Hilfeleistungen tatsächlich vorliegen. Dabei können sie sich auch die Wohnung eines Hilfeempfängers anschauen und müssen sich vorher nicht einmal anmelden, wenn das Sozialamt Anhaltspunkte dafür hat, dass dieser unrichtige Angaben gemacht hat. Freilich, Einlass muss er dem Sozialdetektiv auf Grund des insoweit nicht eingeschränkten Grundrechts der Unverletzlichkeit der Wohnung nicht gewähren und darauf ist er hinzuweisen. Welche Grenzen hat der Sozialdetektiv aber zu beachten, wenn ihm das Anschauen der Wohnung gestattet wurde? Anlass dieser Frage nachzugehen bot folgender Fall:

Eine Hilfeempfängerin hatte gegenüber dem Sozialamt angegeben, sie lebe von ihrem Ehemann getrennt und führe mit ihm keine Wohn- und Wirtschaftsgemeinschaft. Weil das Sozialamt anders lautende Hinweise bekommen hatte, schickte es zwei Mitarbeiter vorbei, die den Verdacht erhärten und Fakten für die Einstellung der Sozialhilfe liefern sollten. Nachdem die Frau die beiden eingelassen hatte, nahmen diese die Wohnung gründlich unter die Lupe und führten über ihre Feststellungen peinlich genau Protokoll. Darin war u. a. zu lesen, dass im Badezimmer auf einer Ablage links oberhalb des Waschbeckens in Reih und Glied verschiedene, exakt bezeichnete Herrentoilettenartikel platziert waren und dass sich in der rechten Abteilung des Spiegelschranks Rasierpinsel, angebrochene Rasierseife und eine Seifenschale befanden. Dem Protokoll war weiter zu entnehmen, dass auf einer Kleiderstange diverse Herrenbekleidung wie z. B. Lederjacken, Stoffjacken, Sakkos, Seidenblousons, Stoffhosen, Oberhemden hingen. Aufgeführt war schließlich auch, dass im Schlafzimmer zwar ein komplett bezogenes Doppelbett, aber weder ausreichend Damen- noch Herrenunterwäsche anzutreffen war und dass der Garderobenschrank Herrenwildlederschuhe und Herrensandalen verschiedener Farbe beherbergte. Mit diesen aufschlussreichen Erkenntnissen wollten sich beide Mitarbeiter des Sozialamts aber immer noch nicht begnügen. Sie nahmen sich auch die Schmutzwäsche in Wäschebox und Waschmaschinentrommel vor, um noch mehr Herrenbekleidung zu finden. Das ging dann doch entschieden zu weit. Zwar gelangten die Mitarbeiter des Sozialamts unwiderlegt jeweils mit dem Einverständnis der Hilfeempfängerin zu diesen Erkenntnissen, aber auch dann gilt es den Grundsatz der Verhältnismäßigkeit zu beachten. Zum einen kümmerten sich die beiden damit unvermeidbar auch um die Schmutzwäsche der Hilfeempfängerin und ihrer Kinder und zum andern hatten sie längst ausreichende Feststellungen getroffen. Erfreulicherweise teilte das Sozialamt ohne Umschweife meine Bedenken gegen dieses Vorgehen und folgte auch meinem Vorschlag, künftig den Amtsleiter oder von ihm besonders ermächtigte Mitarbeiter über die Durchführung von Wohnungsbesichtigungen entscheiden zu lassen.

5. Teil: Sonstige Bereiche

1. Abschnitt: Kommunalwesen

1. Kommunalabgaben

Nach dem Kommunalabgabengesetz können die Gemeinden und Landkreise für die Benutzung ihrer öffentlichen Einrichtungen Benutzungsgebühren erheben. Hierzu gehören auch die Müllgebühren, die den Stadt- und Landkreisen zustehen. Zur Erhebung einer Hundesteuer sind die Gemeinden sogar verpflichtet. Da auch bei der Erhebung von Kommunalabgaben personenbezogene Daten eine Rolle spielen, gibt es in diesem Bereich immer wieder Datenschutzprobleme, wie die folgenden Beispiele zeigen:

1.1 Der Kampfhund und die Hundesteuer

Die sog. Kampfhunde gerieten in letzter Zeit durch verschiedene schlimme Vorfälle ins Blickfeld der Öffentlichkeit. Im Mittelpunkt der öffentlichen Diskussion stand dabei die Frage, welche polizeilichen Maßnahmen notwendig sind, um die Menschen, insbesondere Kinder, vor einzelnen Exemplaren dieser Hunde zu schützen. Aber auch ihre Besteuerung warf Probleme auf. Die Gemeinden sind – wie einleitend bereits erwähnt – nach dem Kommunalabgabengesetz verpflichtet, das Halten von Hunden zu besteuern. Die Einzelheiten, insbesondere die Höhe der Hundesteuer, kann jede Gemeinde in ihrer Satzung selbst festlegen. Zahlreiche Gemeinden führten nun für Kampfhunde eine Strafsteuer ein. Die Halter mussten plötzlich für ihren Liebling das Mehrfache der normalen Hundesteuer entrichten. Das löste natürlich bei den betroffenen Hundehaltern Empörung aus. Diese wurde auch nicht dadurch gemildert, dass die Kommunen als eigentliches Motiv für das Anziehen der Steuerschraube die Abschreckung von (potenziellen) Kampfhundehaltern nannten. Doch die Kampfhundeproblematik war dadurch noch nicht erschöpft: Mir wurde bekannt, dass eine Reihe von Gemeinden von allen Hundehaltern verlangen, dass sie für Zwecke der Hundesteuer die Rasse ihres Hundes angeben, unabhängig davon, ob für den Hund der erhöhte Steuersatz gilt oder nicht. Auch das vom Gemeindetag Baden-Württemberg empfohlene Muster für eine Hundesteuersatzung sieht die Angabe der Hunderasse bei allen Hunden vor. So kann es nicht gehen. Die Gemeinden dürfen die Hundehalter nur zur Erteilung der Auskünfte verpflichten, die sie zur Besteuerung benötigen. Deshalb dürfen sie nur nach den Rassen fragen, für die explizit ein erhöhter Steuersatz vorgesehen ist. Kommt es dagegen auf eine andere Eigenschaft an, also beispielsweise darauf, ob es sich um einen Kampfhund im Sinne der Kampfhundeverordnung des Landes handelt, müssen sie sich darauf beschränken, die Angaben zu erfragen, die für die Feststellung dieser Eigenschaft notwendig sind.

1.2 Grundsteuerdaten für die Müllbeseitigung?

Der Landkreis Böblingen tut sich offensichtlich schwer, wenn es um die datenschutzgerechte Beschaffung von Informationen für die Müllbeseitigung und -gebührenerhebung geht. Schon im Jahr 1999 musste ich ihn darauf hinweisen, dass die Datenerhebung, so wie er sie betrieben hatte, nicht geht (20. Tätigkeitsbericht, LT-Drs. 12/4600, S. 98). Heuer sollte sich dies leider wiederholen.

Anlass dafür war die von ihm geplante Umstellung seines Müllgebührensystems. Ihm schwebte vor, neue Mülltonnen einzuführen und künftig die Grundstückseigentümer zur Kasse zu bitten. Der Haken an der Sache: Die Eigentümer von Grund und Boden im Kreisgebiet waren dem Landkreis und seinem Abfallwirtschaftsbetrieb nicht bekannt, weil das bisherige Gebührensystem mit Banderole oder Gebührenmarke auch ohne diese Angaben funktionierte. Doch der Abfallwirtschaftsbetrieb erinnerte sich daran, dass die Gemeinden von den Grundstücksbesitzern Grundsteuern erheben und deshalb diese Daten im Rechenzentrum der Kommunalen Datenverarbeitung Region Stuttgart speichern

lassen. Flugs ließ er sämtliche Gemeinden des Landkreises Böblingen eine Einverständniserklärung unterschreiben. Auf Grund dieses Persilscheins lieferte das Rechenzentrum dem Abfallwirtschaftsbetrieb auf dessen Anforderung bereitwillig nicht nur die Namen und Anschriften der Grundstückseigentümer sowie die Lage (Straße und Hausnummer, Flurstücksnummer) der Grundstücke, sondern auch zahlreiche weitere Grundstücksdaten. So erfuhr er unter anderem, ob und wie die Grundstücke bebaut sind, ob es sich z. B. um ein Mietwohngrundstück, ein gemischt genutztes Grundstück, ein Geschäftsgrundstück oder ein Grundstück handelt, das mit einem Ein- oder Zweifamilienhaus bebaut ist. Damit nicht genug: Frei Haus geliefert bekam der Abfallwirtschaftsbetrieb auch die Adressen derjenigen, denen die Grundsteuerbescheide zugestellt werden dürfen. Für diesen waren das natürlich willkommene Informationen. Er benutzte sie, um sich gezielt an die Eigentümer zu wenden. Auf der Strecke blieb bei diesem Vorgehen allerdings das Steuergeheimnis. Der Landkreis hätte bedenken müssen, dass die von den Gemeinden für die Erhebung der Grundsteuer gespeicherten Daten dem Steuergeheimnis unterliegen und deshalb nur dann an andere Behörden weitergegeben werden dürfen, wenn dies die Abgabenordnung zulässt. Für die vom Abfallwirtschaftsbetrieb geforderte Datenübermittlung durch die Gemeinden kommt aber lediglich § 31 Abs. 3 der Abgabenordnung als Rechtsgrundlage in Betracht. Diese Bestimmung lässt jedoch nur eine Weitergabe von Namen und Adressen von Grundstückseigentümern zu. Die Datenanforderung und -weitergabe war aber auch noch aus einem weiteren Grund unzulässig. Auch Name und Anschrift der Grundstückseigentümer dürfen die Gemeinden nach § 31 Abs. 3 der Abgabenordnung an andere Behörden nur weitergeben, wenn diese sie zur Erfüllung ihrer Aufgaben tatsächlich auch benötigen. Das war aber im Zeitpunkt der Datenanlieferung noch unklar. Denn bis dahin hatte der Kreistag das neue Gebührensystem noch gar nicht in der Abfallwirtschaftssatzung verankert, sondern nur eine entsprechende Satzungsänderung angekündigt.

Wäre der Landkreis korrekt vorgegangen, hätte er zunächst einmal die Änderung der Abfallwirtschaftssatzung abwarten müssen. Sodann hätte er sich von den Gemeinden die Namen und Anschriften der Eigentümer der Grundstücke, auf denen Müll anfallen kann, geben lassen können. Die weiteren für die Erhebung der Müllgebühren benötigten Daten hätte sich der Abfallwirtschaftsbetrieb unmittelbar bei den betroffenen Grundstückseigentümern, die darüber auskunftspflichtig sind, besorgen müssen. Ich habe das Vorgehen des Landkreises, dem bisher jedes Unrechtsbewusstsein abgeht, beanstandet. Dagegen habe ich von einer Beanstandung der rechtswidrigen Datenübermittlung durch die Gemeinden ausnahmsweise abgesehen, weil diese sich ebenso wie das Rechenzentrum offensichtlich auf die Autorität und Rechtskenntnis der Verantwortlichen des Landkreises verlassen und nicht damit gerechnet hatten, dass sie ihnen eine Verletzung des Steuergeheimnisses zumuten würden.

2. Das Bürgerbüro

Nach längerer Pause stattete mein Amt wieder einmal einem kommunalen Bürgerbüro einen Kontrollbesuch ab. Meine Mitarbeiter wollten natürlich nicht nur sehen, ob und auf welche Weise das vor wenigen Jahren im Heilbronner Rathaus eingerichtete „Zentrale Bürgeramt“ den Einwohnern ihre Behördengänge erleichtert und ihnen dabei die berühmt-berüchtigte Ämterrallye erspart. Ihr Hauptaugenmerk galt verständlicherweise dem Datenschutz. Denn die Konzentration verschiedenartigster Verwaltungsaufgaben in einem Großraumbüro und die Allzuständigkeit der Mitarbeiter birgt naturgemäß größere Gefahren für den Datenschutz als die herkömmliche Aufgabenerledigung durch Spezialisten in Einzelbüros. Dem muss durch geeignete Schutzvorkehrungen begegnet werden. So muss die Vertraulichkeit des gesprochenen Worts durch eine entsprechende räumliche Ausgestaltung sichergestellt werden. Geeignete Maßnahmen dafür können sein: genügende Abstände zwischen Warte- und Beratungsbereich sowie zwischen den einzelnen Beratungsplätzen, Sichtschutz durch Stellwände, große

Pflanzen usw. Ferner sollte den Bürgern angeboten werden, ihre Anliegen auf Wunsch in einem separaten Raum des Bürgerbüros oder beim jeweiligen Fachamt vorzubringen. Das gilt insbesondere für besonders sensible Bereiche wie Sozial- oder Steuerangelegenheiten, falls diese Aufgaben überhaupt einem Bürgerbüro übertragen werden.

Diese aus datenschutzrechtlicher Sicht bei der Gestaltung und beim Betrieb von Bürgerbüros oder Bürgerämtern zu beachtenden Kriterien erfüllt das Zentrale Bürgeramt der Stadt Heilbronn in nahezu vorbildlicher Weise. Trotzdem fanden meine Mitarbeiter bei ihrem Kontrollbesuch noch ein paar Haare in der Suppe:

– Die Stadt bietet den Besuchern des Bürgeramts zwar an, ihr Anliegen in einem separaten Beratungsraum oder beim Fachamt vorzutragen. Diesen schriftlichen Hinweis sieht der Bürger aber erst, wenn er bereits seinem Berater gegenüber sitzt. Mancher wird sich scheuen, in dieser Situation von dem datenschutzfreundlichen Angebot Gebrauch zu machen. Im Rahmen meines Kontrollberichts empfahl ich deshalb der Stadt, die Besucher zusätzlich an der Infothek im Eingangsbereich entsprechend aufzuklären. Die Stadt reagierte erfreulicherweise prompt und brachte den zusätzlichen Hinweis an.

– Alle Mitarbeiter des Bürgeramts können über ihr elektronisches Einwohnerinformationssystem auf das städtische Melderegister zugreifen. Das gilt auch für solche Daten von weggezogenen und verstorbenen Einwohnern, die nach dem Meldegesetz nach Ablauf von fünf Jahren gesondert aufbewahrt sowie durch technische und organisatorische Maßnahmen besonders gesichert werden müssen. Die Meldeverordnung schreibt vor, dass nur Personen, die hierzu besonders ermächtigt sind, diese Daten verarbeiten oder sonst nutzen dürfen. Ich empfahl deshalb der Stadt, den Zugriff auf die gesondert aufzubewahrenden Daten auf ein oder zwei Mitarbeiter des Bürgeramts zu beschränken. Die Stadt griff auch diese Anregung auf und reduzierte die Zahl der Ermächtigungen erheblich.

– In Heilbronn nehmen sowohl das Amt für Familie, Jugend und Senioren als auch das Bürgeramt Anträge auf Befreiung von der Rundfunkgebührenpflicht aus sozialen Gründen entgegen. Das Bürgeramt bearbeitet die bei ihm eingereichten Anträge selbst. Gegen diese bürgerfreundliche Verfahrensweise wäre eigentlich nichts einzuwenden gewesen, wenn diese Anträge und die Bescheide nicht doppelt, d. h. im Bürgeramt und im Fachamt aufbewahrt worden wären. Eine solche Doppelspeicherung ist sachlich nicht geboten und deshalb zu unterlassen. Künftig bewahrt die Stadt diese Unterlagen nur noch im Fachamt auf.

– Die Heilbronner können beim Bürgeramt Führungszeugnisse zur Vorlage bei einer Behörde beantragen. Dazu gibt das Amt die persönlichen Daten der Bürger in das elektronische Einwohnerinformationssystem ein. Zur Zeit des Kontrollbesuchs war es Mitarbeitern des Ausländeramts technisch möglich, über das Einwohnerinformationssystem die am selben Tag beim Bürgeramt gestellten Anträge zur Kenntnis zu nehmen. Die Stadt Heilbronn kam meiner Bitte, diese datenschutzrechtlich bedenkliche technische Lücke zu schließen, unverzüglich nach.

3. Moderne IuK-Technik und die Gemeinde

Wie bei anderen Behörden ist auch bei fast allen Gemeinden Schmalhans Küchenmeister; Sparen heißt die Devise. Auf der Suche nach Möglichkeiten, ihre Ausgaben zu senken, erhoffen sich viele, durch vermehrten Einsatz der IuK-Technik Geld einzusparen. Dabei darf allerdings der Datenschutz nicht aus dem Blickfeld geraten.

3.1 Durch CUPARLA mehr Rechte für Gemeinderat?

Über den wesentlichen Inhalt der Verhandlungen des Gemeinderats ist eine Niederschrift zu fertigen, so steht es in der Gemeindeordnung. Das ist auch gut so, denn auch Gemeinderäte können sich nicht alles merken und zudem gibt es nach jeder Wahl neue Mitglieder in diesem Gremium, die natürlich wissen müssen, was und aus welchen Gründen der Gemeinderat in diesem oder jenem Fall bisher besprochen und festgelegt hat. In

derselben Vorschrift heißt es aber auch, dass Mehrfertigungen von Niederschriften über nichtöffentliche Sitzungen nicht ausgehändigt werden und Gemeinderäte Protokolle über nichtöffentliche Sitzungen nur dann einsehen dürfen, wenn sie diese im Einzelfall für ihre Arbeit benötigen. Mit dieser Bestimmung kam eine Große Kreisstadt in Konflikt, als sie das von der Datenzentrale angebotene Verfahren CUPARLA (Computerunterstützung der Parlamentsarbeit) einführte, um den ehrenamtlich tätigen Mitgliedern des Gemeinderats ihre Arbeit zu erleichtern. Dazu stellte sie ihnen mit dem Verfahren konfigurierte Notebooks zur Verfügung. Über eine ISDN-Wählverbindung konnten sie von Zu Hause und unterwegs u. a. auf Sitzungsvorlagen und Protokolle zugreifen, ohne sich jedes Mal zur Stadtverwaltung bemühen zu müssen. Damit hatte die Stadt ihren Gemeinderäten aber einen unbeschränkten Zugriff auf sämtliche Protokolle aller nichtöffentlichen Gemeinderatssitzungen eingeräumt und ihnen dadurch de facto eine Mehrfertigung dieser Protokolle übermittelt. Als ich die Stadt auf diese Rechtslage hinwies, gerierte sie sich zunächst als ungläubiger Thomas und konsultierte das Regierungspräsidium. Erst als dieses der Stadt genau dasselbe sagte, kam sie meiner Bitte, den Zugriff auf Protokolle nichtöffentlicher Sitzungen zu sperren, nach.

3.2 Gemeinderatsprotokoll im Internet

Eine kleine Gemeinde in Oberschwaben veröffentlichte einen Bericht über eine öffentliche Gemeinderatssitzung, der einige Äußerungen über verschiedene Personen enthielt, nicht nur in ihrem Amtsblatt, sondern stellte ihn auch gleich ins Internet ein. Unter anderem ging es um eine Angelegenheit, die auf Grund einer Veröffentlichung in einer Tageszeitung Ortsgespräch war. Einer der Betroffenen wollte von mir wissen, ob die Gemeinde dazu berechtigt war. Ihm konnte ich Folgendes sagen:

Es ist aus der Sicht des Datenschutzes nichts daran auszusetzen, dass die Gemeinde den Bericht über die Gemeinderatssitzung in ihrem Amtsblatt veröffentlichte, denn die Gemeindeordnung verpflichtet den Bürgermeister, die Einwohner über die allgemein bedeutsamen Angelegenheiten der Gemeinde zu unterrichten. Dadurch soll das Interesse der Einwohner am kommunalpolitischen Geschehen geweckt werden. Hier war es auch gerechtfertigt, die Namen von Betroffenen wiederzugeben, weil die Angelegenheit zuvor schon unter Angabe von Namen in der Presse breit getreten worden war. Unzulässig war es jedoch, den Bericht auch in das Internet einzustellen. Es macht nämlich – worauf ich schon wiederholt hingewiesen habe – einen gewaltigen Unterschied, ob eine Gemeinde ihre Einwohner durch lokale, auflagenbegrenzte schriftliche Veröffentlichungen unterrichtet oder ob sie personenbezogene Informationen über das Internet weltweit an einen unbeschränkten Personenkreis verbreitet. Eine solche globale Information steht in krassem Gegensatz zum lokalen Aufgaben- und Wirkungskreis der Gemeinde. Die Masse der Internet-Nutzer außerhalb des lokalen Raumes und ohne Beziehung zur Kommune hat kein berechtigtes Interesse an solchen Informationen.

Zur datenschutzrechtlichen Fehleinschätzung der Gemeinde kam aber noch etwas hinzu. Auf die Bitte meines Amtes, sich zu dem Vorgang zu äußern und konkret zu sagen, über welches Medium (Mitteilungsblatt/Internet) die Gemeinde den Bericht über die Gemeinderatssitzung veröffentlicht habe, antwortete sie nämlich lapidar mit „im Amtsblatt“. Diese Antwort war zwar nicht falsch, aber unvollständig. Die Gemeinde wollte mir die Verbreitung der Erklärung über das Internet verschweigen, doch die war längst publik geworden. Zur Rede gestellt, wollte sich der Bürgermeister damit herausreden, die Gemeinde habe mit der Pflege ihrer Homepage einen Studenten betraut, der auch jenen Beitrag in das Internet eingestellt habe. Ich musste den Bürgermeister darüber aufklären, dass die Gemeinde als Inhaberin der fraglichen Domäne und der Bürgermeister als verantwortliche Person registriert waren und er deshalb selbst für den Inhalt der Internet-Seite seiner Gemeinde verantwortlich ist.

Die rechtswidrige Internet-Veröffentlichung und den Verstoß gegen die Auskunfts- und Unterstützungspflicht der Behörden habe ich förmlich beanstandet. Zu guter Letzt lenkte der Bürgermeister dann doch noch ein und versprach, sich künftig persönlich um die Internet-Beiträge seiner Gemeinde zu kümmern und die datenschutzrechtlichen Regelungen zu beachten.

4. Kontrollmitteilungen über Marktbeschicker

Sozialleistungsmissbrauch ist kein Kavaliersdelikt. Deshalb ist es eine wichtige Aufgabe der Sozialleistungsträger, den unberechtigten Bezug von Sozialleistungen zu verhindern und Verdachtsfällen nachzugehen. Allerdings müssen sie dabei beachten, dass ihnen andere Behörden nicht ohne weiteres die Informationen zur Verfügung stellen können, die aus der Sicht des einzelnen Leistungsträgers dabei möglicherweise hilfreich sein könnten. Anlass, mich mit dieser Frage auseinander zu setzen, gaben mir Hinweise von Gemeinden auf ein Rundschreiben eines Arbeitsamts, in dem dieses Gemeinden und Städte bat, ihm jeweils Listen mit den Namen aller Personen, die bei dort veranstalteten Märkten als Marktbeschicker auftreten, zukommen zu lassen. Das Arbeitsamt hoffte, auf diese Weise schwarzen Schafen auf die Schliche zu kommen, die Arbeitslosengeld oder -hilfe beziehen und ihr Konto nebenher durch den Warenverkauf auf Märkten aufbessern. Eine Rechtsgrundlage für solche Kontrollmitteilungen der Städte und Gemeinden gibt es jedoch nicht. Deshalb empfahl ich, dem Ansinnen des Arbeitsamts nicht Rechnung zu tragen.

Das bedeutet jedoch nicht etwa, dass die Marktbeschickerdaten für die Arbeitsämter in jedem Fall tabu sind. Hat ein Arbeitsamt Anhaltspunkte dafür, dass sich ein Leistungsempfänger als Marktbeschicker betätigt und seinen Mitteilungspflichten gegenüber dem Arbeitsamt nicht korrekt nachkommt, kann es darüber sehr wohl von Städten und Gemeinden, bei denen er möglicherweise als Marktbeschicker aufgetreten ist, eine Auskunft erhalten. Dazu genügt es allerdings nicht, auch darauf habe ich eine Gemeinde hingewiesen, dass das Arbeitsamt der Gemeinde ohne nähere Angaben eine Namensliste schickt und um entsprechende Mitteilung bittet. Dazu muss es in seinem Auskunftsersuchen schon auf die Existenz solcher Anhaltspunkte hinweisen.

5. Kein Spaß – versteckte Kamera im Stadttheater

Ähnlich verdutzt wie die Leute, die in Fernsehsendungen wie z. B. „Verstehen Sie Spaß?“ unfreiwillig Hauptdarsteller von heimlichen Filmaufnahmen werden, muss wohl ein Mitarbeiter der städtischen Bühnen in Freiburg gewesen sein. Dieser Mitarbeiter, so war in einem Zeitungsbericht zu lesen, habe im Freiburger Stadttheater eine versteckt angebrachte Videokamera entdeckt. Peu à peu sei herausgekommen, dass dies keineswegs die einzige Kamera sei und die Überwachung schon vor Jahren begonnen habe. Die Aufnahmen sollten angeblich Diebe überführen, doch seien sie auch geeignet gewesen, Mitarbeiter zu kontrollieren, denn die Fluchtwege, die beobachtet worden seien, benutzten nach Angaben des Personalrats hie und da auch Mitarbeiter, um das Haus unauffällig zu verlassen oder zu betreten.

Als ich mich der Sache annahm und die Stadt um Stellungnahme bat, räumte diese ein, dass insgesamt drei Videokameras während ca. 4 Wochen im Jahr 1998 und das ganze Jahr 2000 über die Fluchtwege und die Haustechnik versteckt im Visier hatten. Die Aufzeichnungen seien jeweils nach 24 Stunden automatisch gelöscht worden. Die Stadt habe aber die angebrachten Kameras inzwischen entfernt. Sie versicherte, die Maßnahmen hätten sich nicht gegen das Personal gerichtet. Vielmehr seien allein die Sicherheit des Gebäudes und der Schutz der Mitarbeiter vor Diebstählen und Ähnlichem bezweckt gewesen. Zur Rechtsgrundlage ihres Vorgehens wollte sich die Stadt lieber nicht äußern. In diesem Punkt half ich der Stadt auf die Sprünge. Bei heimlichen Videoaufnahmen handelt es sich mit den Worten des Landesdatenschutzgesetzes gesprochen um eine Erhebung personenbezogener Daten beim Betroffenen ohne seine Kenntnis. Sie ist nur zulässig, wenn eine Rechtsvorschrift sie ausdrücklich vorsieht oder zwingend voraussetzt oder die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung

erforderlich macht und keine Anhaltspunkte dafür vorliegen, dass ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Diese Voraussetzungen lagen aber nicht vor. Selbst wenn, was wegen der vagen Angaben der Stadt nicht abschließend zu klären war, eine Videoüberwachung im Grundsatz in Betracht gekommen wäre, hätten es in jedem Fall die schutzwürdigen Interessen der von der Maßnahme betroffenen Personen verlangt, dass sie offen und nicht heimlich vorgenommen wird. Mit andern Worten: Im Theater hätten deutlich sichtbare Hinweise auf die Kameras und ihre Funktion vorhanden sein müssen.

6. Bürgeranliegen

Bei der großen Zahl von Gemeinden und deren Aufgabenvielfalt überrascht es nicht, dass mancher Bürger auch datenschutzrechtliche Probleme mit seiner Gemeinde hat. Die Betroffenen wenden sich häufig Hilfe suchend an mich, wie die folgenden Fälle beispielhaft zeigen:

6.1 Die Jahrgangsfeier

Eine Bürgerin wandte sich empört an mich. Sie hatte eine Einladung zu einer Jahrgangsfeier erhalten und von den in der Einladung genannten Organisatoren nicht erfahren, von wem die Adressdaten stammen. Sie vermutete als Quelle das Einwohnermeldeamt ihrer Wohngemeinde, weil die Adresse auch ihren sonst nicht verwendeten zweiten Vornamen enthielt. Mit dieser Vermutung lag sie in der Tat richtig, wie meine Recherchen bei der Großen Kreisstadt ergaben. Deren Einwohnermeldeamt berief sich auf das Meldegesetz des Landes, das den Einwohnermeldeämtern erlaubt, bestimmte im Melderegister gespeicherte Daten, u. a. Namen, Anschriften und Geburtstage, zum Zwecke der Versendung von Einladungen zu Jahrgangsfeiern und ähnlichen Veranstaltungen zu nutzen. Hatte das Einwohnermeldeamt demnach rechtmäßig gehandelt? Mitnichten! Es hätte die Melderegisterdaten nur dazu verwenden dürfen, vom Veranstalter zur Verfügung gestellte Einladungsschreiben zu adressieren und zu versenden. Diese sog. Adressmittlung trägt einerseits dem Anliegen der Veranstalter, mit den Betroffenen Kontakt aufnehmen zu können, Rechnung. Andererseits verhindert dieses datenschutzfreundliche Verfahren, dass die Adressen dem Veranstalter bekannt werden, obwohl der eine oder die andere Jahrgangsangehörige das vielleicht gar nicht will. Dass das Meldegesetz die Herausgabe der Adressdaten in solchen Fällen nicht erlaubt, hatte das Einwohnermeldeamt nicht beachtet. Offenbar war sein Personal aus Kapazitätsgründen nicht in der Lage, die Einladungen selbst zu adressieren und zu verschicken. Deshalb hatte es einem bei einem anderen Amt der Stadt beschäftigten Mitorganisator der Jahrgangsfeier kurzerhand eine Adressenliste der Jahrgangsangehörigen ausgehändigt. Dieser hatte dann die Einladungen adressiert und verschickt. So nicht, musste ich der Stadt mitteilen und der Beschwerdeführerin Recht geben.

6.2 Die Vollstreckungshilfe

Forderungen beizutreiben ist ganz gewiss kein leichtes Geschäft. Das entbindet jedoch nicht von der Verpflichtung, die dafür maßgebenden Regelungen zu beachten. Darauf musste ich eine kleinere Stadt hinweisen. Sie hatte eine Nachbargemeinde gebeten, ihr bei der Einziehung einer vollstreckbaren Gebührenforderung Vollstreckungshilfe zu leisten. Dies, obwohl die Nachbargemeinde gar keinen Vollstreckungsbeamten bestellt hatte und deshalb überhaupt nicht in der Lage war, Pfändungen vorzunehmen. Die Nachbargemeinde hatte sich dann auch darauf beschränkt, dem Schuldner einen Außendienstmitarbeiter ins Haus zu schicken und ihn, übrigens ohne Erfolg, um Begleichung der Gebührenforderung zu bitten. So hätte die Stadt nicht vorgehen dürfen. Die mit dem Versand eines Vollstreckungshilfeersuchens verbundene Übermittlung personenbezogener Daten des Schuldners ist nämlich nur dann gerechtfertigt, wenn die ersuchte Behörde in der Lage ist, Vollstreckungsmaßnahmen vorzunehmen und damit die erbetene Vollstreckungshilfe auch zu leisten. Die Stadt hätte sich deshalb vor dem Versand ihres Vollstreckungshilfeersuchens vergewissern müssen, ob

die Nachbargemeinde einen Vollstreckungsbeamten bestellt hat. Falls ihr dieses Vorgehen zu umständlich erschienen wäre, hätte sie an die Nachbargemeinde auch ein allgemein gehaltenes Schreiben richten und diesem ein verschlossenes Kuvert mit den personenbezogenen Daten des Schuldners beifügen können. In diesem Fall hätte die Stadt die ersuchte Gemeinde bitten müssen, den Umschlag ungeöffnet zurückzugeben, falls sie keinen Vollstreckungsbeamten hat. Bei beiden Alternativen hätte die ersuchte Gemeinde weder die Personalien des Betroffenen noch Höhe, Art usw. der Forderung erfahren.

6.3 Weitergabe von Bürgereingaben

Wie ich leider immer wieder feststellen muss, fehlt es Behörden allzu oft an der erforderlichen Sensibilität, wenn es um die vertrauliche Behandlung von Bürgereingaben geht. So kommt es immer wieder vor, dass Ämter die Schreiben von Bürgern, mit denen sich diese beschwerdeführend an sie gewandt haben, vollständig, also mit Namensnennung und Anschrift, als Kopie an andere Stellen oder Personen weitergeben, um sie über den Inhalt der Eingaben zu informieren oder ihnen Gelegenheit zu einer Stellungnahme zu geben. Für die Behörden ist es natürlich einfach und bequem, die Eingaben kurzerhand zu kopieren und dann komplett an andere weiterzugeben. Denn dadurch sparen sie sich den Zeitaufwand, den Inhalt der Schreiben in eigenen Worten wiederzugeben.

Offenbar sind sie sich dabei gar nicht darüber im Klaren, dass schon die Eingabe eines Bürgers ein personenbezogenes Datum des Bürgers ist und deshalb nur dann weitergegeben werden darf, wenn eine Rechtsvorschrift dies erlaubt oder der Bürger damit einverstanden ist. Außerdem übersehen viele Behörden, dass der Name des Bürgers oftmals gar nichts zur Sache tut und der Sachverhalt, um den es an sich geht, auch beurteilt werden kann, ohne den Namen des Beschwerdeführers zu kennen. In diesen Fällen ist es deshalb völlig ausreichend, wenn die Behörden andere Stellen oder Personen über den Inhalt einer Beschwerde informieren, ohne den Namen und die Anschrift des Bürgers zu nennen. Dazu einige Beispiele, in denen dies nicht beachtet wurde und die Bürger dadurch in unangenehme Situationen gerieten:

– Die Beschwerde bei der Kommunalaufsicht

  Ein Bürger bat ein Regierungspräsidium, im Wege der Kommunalaufsicht einen Sachverhalt zu überprüfen, der sich in seiner Wohnortgemeinde zugetragen hatte. Diese Angelegenheit hatte mit dem Bürger selbst nichts zu tun. Das Regierungspräsidium gab die Eingabe des Bürgers daraufhin vollständig als Kopie an die betreffende Gemeinde weiter, damit sich diese dazu äußern konnte. Dass das Regierungspräsidium der Gemeinde Gelegenheit zu einer Stellungnahme gab, ist ja sicher nicht zu beanstanden. Aber hätte sich das Regierungspräsidium dabei nicht darauf beschränken können, das Bürgermeisteramt über den Inhalt der Eingabe zu unterrichten, ohne den Namen des Bürgers zu offenbaren?

– Die Lärmbeschwerde

  Ein anderer Bürger beschwerte sich beim Ordnungsamt einer Großen Kreisstadt über Lärmbelästigungen, die von den Gaststätten in seiner Nachbarschaft herrührten. Das Ordnungsamt setzte daraufhin die betreffenden Gaststättenbetreiber über die Beschwerde in Kenntnis, indem es ihnen kurzerhand eine Kopie des Beschwerdeschreibens übersandte. Dies war so nicht zulässig. Das Ordnungsamt hätte die Gaststättenbetreiber bei der gegebenen Sachlage zwar in allgemeiner Form über den Inhalt der Beschwerde informieren können; dabei hätte es jedoch nicht den Namen und die Anschrift des beschwerdeführenden Bürgers preisgeben dürfen.

– Die veröffentlichten Briefe

In diesem Fall veröffentlichte eine Gemeinde mehrere Schreiben von Bürgern, mit denen sich diese in einer bestimmten Angelegenheit an den Bürgermeister oder an den Gemeinderat gewandt hatten, auszugsweise im städtischen Mitteilungsblatt, und zwar mit Absenderangabe. Dies ging jedoch entschieden zu weit! Denn es war keinesfalls notwendig, durch die Namensangaben öffentlich bekannt zu geben, welcher Bürger sich mit welchen Einwendungen und Argumenten an die Stadtverwaltung gewandt hatte. Für den mit der Veröffentlichung verfolgten Zweck hätte es genügt, den Inhalt der Briefe ohne Namensnennung wiederzugeben.

6.4 Der verräterische PC in der Bücherei

Ein Benutzer einer Stadtbibliothek staunte nicht schlecht, als er einen dort aufgestellten Recherche-PC bediente. Zum einen konnte er auf dem Bildschirm zur Kenntnis nehmen, welches Buch oder andere Medium der Benutzer XY zur Zeit entliehen hatte. Aber das war noch nicht alles: Neugierig geworden, welche Geheimnisse der schlaue PC sonst noch preisgeben würde, gab er seinen eigenen Namen ein. Und siehe da, er bekam schwarz auf weiß bestätigt, dass ganz besonders bei ihm auf die unbeschädigte Rückgabe entliehener Bücher zu achten sei. Nun ist es zwar aus datenschutzrechtlicher Sicht nicht von Nachteil, wenn die Betroffenen wissen, was über sie bibliotheksintern gespeichert ist. Dennoch musste ich, vom Benutzer darauf aufmerksam gemacht, der Sache auf den Grund gehen, schon wegen der geschilderten Einsichtsmöglichkeit in die Leserkonten Dritter. Die bei der Stadt angeforderte Stellungnahme ergab, dass die Möglichkeit, sich anzeigen zu lassen, wer was entliehen hatte, offenbar ihre Ursache in einem einmaligen technischen Fehler hatte, der dann kurzfristig behoben wurde.

Damit war die Sache allerdings noch nicht erledigt. Der im PC gespeicherte bibliotheksinterne Vermerk hatte nämlich gezeigt, dass das eingesetzte EDV-Verfahren über ein sog. Freitextfeld verfügte, in das die Mitarbeiter der Bibliothek beliebige Hinweise und Vermerke eintragen konnten. Aus der Sicht des Datenschutzes sind solche Datenfelder höchst problematisch, weil eine Kontrolle darüber, ob die Eintragungen in solchen Feldern tatsächlich auch notwendig und damit zulässig sind, kaum möglich ist. Solche Freitextfelder sollten deshalb möglichst nicht vorgesehen werden. Kann auf sie aus triftigen Gründen nicht verzichtet werden, müssen den Mitarbeitern konkrete Vorgaben dazu gemacht werden, was sie in das Feld eintragen dürfen. Auf einen Verzicht wollte sich die Stadt nicht einlassen, aber wenigstens will sie jetzt dem Bibliothekspersonal dafür Standardtexte vorgeben.

2. Abschnitt: Das Personalwesen

1. Personalamt zu Unrecht informiert

Immer wieder muss ich feststellen, dass der Datenfluss innerhalb einer Behörde keine Grenzen kennt und Daten intern „einfach so“ weitergegeben werden. So manche Behörde ist sich nämlich offenbar nicht darüber im Klaren, dass auch die Datenweitergabe von einem Amt an ein anderes nur zulässig ist, wenn es eine Rechtsgrundlage dafür gibt. Ein typisches Beispiel ist folgender Fall, in dem sich ein Mitarbeiter einer Stadt über seinen Dienstherrn beschwerte. Was war geschehen?

Der Mitarbeiter, der auch dienstlich Kraftfahrzeuge zu führen hat, war in seiner Freizeit mit mehr als 0,5 Promille am Steuer erwischt worden. Deshalb verhängte die Bußgeldstelle, genau wie es das Gesetz vorsieht, ein Bußgeld und ein Fahrverbot von einem Monat gegen ihn. Um sich Unannehmlichkeiten am Arbeitsplatz von vornherein zu ersparen, machte der Bedienstete von der neu geschaffenen Möglichkeit Gebrauch, selbst den Zeitpunkt des Wirksamwerdens des Fahrverbots zu bestimmen und gab seinen Führerschein während seines Urlaubs in amtliche Verwahrung. Als er danach wieder zur Arbeit erschien, hielt ihm sein Vorgesetzter vor, er habe

ihn pflichtwidrig nicht über das Fahrverbot unterrichtet. Wie sich herausstellte, hatte die städtische Bußgeldstelle das Personalamt über den Fehltritt des Mitarbeiters und das verhängte Fahrverbot informiert, weil dort bekannt war, dass es sich bei dem Delinquenten um einen Kollegen handelte. Das Personalamt wiederum setzte dessen unmittelbaren Vorgesetzten in Kenntnis. Nach den Gründen ihres Vorgehens gefragt, blieb mir die Stadt die Antwort auf die Frage nach der Rechtsgrundlage schuldig. Sie teilte mir lediglich mit, weil der Mitarbeiter ein Dienstfahrzeug führe und auch andere Mitarbeiter befördere, sei es unabdingbar gewesen, dessen Vorgesetzten via Personalamt über das Fahrverbot zu unterrichten, damit dieser feststellen kann, ob der Mitarbeiter die im Straßenverkehr erforderliche Fahreignung besitzt.

Mit dieser Begründung ließ sich diese interne Datenweitergabe freilich nicht rechtfertigen. Hätte die Bußgeldstelle einen Blick in die einschlägigen Rechtsvorschriften geworfen, hätte sie festgestellt, dass die Datenweitergabe an das Personalamt nur in Betracht gekommen wäre, wenn die Entscheidung der Bußgeldstelle Grundlage für eine arbeitsrechtliche Maßnahme hätte sein können. Das war aber unter keinen Umständen der Fall. Zudem war es nicht Aufgabe des Personalamts, die Einhaltung des Fahrverbots zu überwachen, und erst recht nicht darüber zu befinden, ob der Mitarbeiter die erforderliche Fahreignung besitzt.

Nach meiner Beanstandung will die Stadt künftig die Rechtslage beachten.

2. Personalratspost in falschen Händen

Dass Telefaxe manchmal nicht beim Empfänger, sondern ganz woanders ankommen, weil der Absender sein Telefaxgerät nicht sorgfältig genug bedient hat, ist leider eine altbekannte Erscheinung. Eine ganz andere Variante, wie Telefaxe auf Abwege geraten können, spielte sich bei einer Großen Kreisstadt ab. Eine Mitarbeiterin wollte an einem Wochenende von Zuhause aus dem Personalrat ein Schreiben zufaxen. Zuvor waren die beiden übereingekommen, das Telefax an den Fax-Anschluss der Stadtkämmerei zu senden, weil der Personalrat über kein eigenes Telefaxgerät verfügt. Adressiert war das Fax so:

An den Personalrat der Stadt ...
z. H. Herrn Vorsitzenden ...

In dem Schreiben erhob die Mitarbeiterin schwere Vorwürfe gegen den Leiter der Personalabteilung und ihre unmittelbare Vorgesetzte.

Nun hätte man vermuten können, das Telefax schlummere dort bis zum nächsten Montag, wo es der Personalratsvorsitzende dann hätte in Empfang nehmen können, doch es kam ganz anders. Ein Bürgermeister, dessen Arbeitseifer ihn auch an diesem Wochenende arbeiten ließ, sah das Telefax, nahm es an sich und leitete es umgehend dem Leiter der Personalabteilung zu. Erst einige Tage später und nur auf Nachforschungen hin erhielt auch der Adressat, der Personalratsvorsitzende, eine Kopie des Telefaxes. Dass die Stadt damit einen groben Datenschutzverstoß begangen hatte, bedarf wohl keiner näheren Begründung. Zwar ist der Personalrat formal betrachtet Teil der Dienststelle, also des Bürgermeisteramts. Unbestritten nimmt er jedoch seine Aufgaben unabhängig und eigenverantwortlich wahr und steht dem Behördenleiter dabei gleichberechtigt gegenüber. Den Beschäftigten ist es gestattet, sich ohne Wissen oder Beteiligung des Dienstherrn mit Anregungen und Beschwerden unmittelbar an den Personalrat zu wenden. Auch erstreckt sich das Direktions- und Organisationsrecht des Dienstherrn nicht auf die für den Personalrat bestimmte Post. Deshalb darf er von deren Inhalt keine Kenntnis nehmen.

Als ob der Datenschutzverstoß nicht schon schlimm genug gewesen wäre: Hanebüchen war, wie sich die Stadt aus der Affäre ziehen wollte. Sie meinte, der Bürgermeister habe das Telefax, ohne es durchzulesen (!), allein auf Grund des Absenders dem Leiter der Personalabteilung übergeben, weil er gewusst habe, dass zwischen der Mitarbeiterin und der Personalabteilung in arbeitsrechtlichen Fragen reger Schriftverkehr geführt wird. Wäre es tatsächlich so gewesen, würden sich folgende Fragen stellen:

– Warum hat der Bürgermeister zwar den Absender, nicht aber den direkt darunter aufgeführten Adressaten gelesen?

– Woher wusste der Bürgermeister, wenn er das Telefax gar nicht gelesen hatte, dass es einen „arbeitsrechtlichen“ Inhalt hatte?

– Warum hatte die Mitarbeiterin ihr Telefax, wenn es denn für die Personalabteilung bestimmt gewesen wäre, dann nicht auch an das für diesen Bereich eingerichtete Telefaxgerät, sondern an eines in einem ganz anderen Dezernat geschickt?

Um die Stadt nicht noch mehr in die Bredouille zu bringen, habe ich ihr diese Fragen gar nicht mehr gestellt, sondern sie aufgefordert, künftig die Rechtsstellung und die Unabhängigkeit des Personalrats zu achten und es zu unterlassen, sich der für ihn bestimmten Post zu bemächtigen.

3. Kein Datenschutz bei Personalknappheit?

Nicht auszurotten ist offenbar ein vor etlichen Jahren von einem Formularverlag herausgegebener Personalbogen, der heute immer noch landauf, landab kursiert. Auch in diesem Jahr feierte er wieder fröhliche Urständ, wie wir durch die Eingabe eines Stellenbewerbers erfuhren. Aus welchen Gründen dieser datenschutzrechtlich inakzeptabel ist, haben wir wiederholt kund getan (vgl. 13. Tätigkeitsbericht 1992, LT-Drs. 11/1060, S. 117; 14. Tätigkeitsbericht 1993, LT-Drs. 11/2900, S. 105). Gleichwohl verwendet eine Einrichtung, in der sich die Stadt Stuttgart und zahlreiche Städte und Gemeinden aus deren Umland zur Kulturförderung zusammengeschlossen haben, eben jenen völlig überholten Personalbogen. Dass es immer noch öffentliche Stellen gibt, die diesen Personalbogen verwenden, ist schon schlimm genug. Deprimierend war in diesem Fall aber auch, wie der Geschäftsführer der Einrichtung reagierte, nachdem wir ihn mit der Rechtslage bekannt gemacht hatten. Unter anderem schrieb er uns Folgendes:

> „Dennoch erlaube ich mir vorzubringen, dass ich es als nicht sonderlich fruchtbar empfinde, wenn ich im Nachhinein auf Interpellation eines nicht zum Zuge gekommenen Bewerbers mich dermaßen ausgiebig mit dieser Angelegenheit beschäftigten soll. Um es genau zu sagen: Ich bin dazu als ehrenamtlicher Geschäftsführer bei sonstiger personeller Ausstattung mit einer zu 50 % -beschäftigten Alleinsekretärin nicht bereit.
> ...
> Zur Sache selbst ist zu sagen, dass wir um die Ausfüllung eines Personalbogens lediglich **gebeten** haben. Etliche Bewerberinnen haben diesen nicht zurückgeschickt, ohne dass dies nachteilige Folgen für die jeweilige Bewerbung gehabt hätte.“

Diese Sätze sprechen aus sich heraus Bände und bedürfen keiner Kommentierung. Eines ist allerdings klar: Der Umstand, dass eine öffentliche Stelle – aus welchen Gründen auch immer – über zu wenig Personal verfügt, kann kein Rechtfertigungsgrund dafür sein, die Datenschutzrechte des Bürgers zu ignorieren und links liegen zu lassen. Warum der Geschäftsführer einen Personalbogen verwendete, obwohl er die darin erfragten Angaben offenbar überhaupt nicht benötigte, wird sein Geheimnis bleiben. Den Vorstand der Einrichtung habe ich gebeten dafür zu sorgen, dass künftig dort nur noch ein datenschutzgerechter Personalbogen verwendet wird, ähnlich dem, wie er in der Landesverwaltung schon seit 1990 verbindlich eingeführt ist.

4. Der Mitarbeiter fehlt – was dann?

In den meisten Behörden gehört es heute zum Standard, dass die Mitarbeiter über eine persönliche E-Mail-Adresse verfügen. Auf diese Weise können sie vom Bürger oder von Kollegen schnell und direkt Nachrichten entgegennehmen und bei Bedarf rasch reagieren. Die meisten haben heutzutage regelmäßig auch eine sog. Sprachbox (Anrufbeantworter), so dass es möglich ist, einem Mitarbeiter eine mündliche Nachricht zukommen zu lassen, auch wenn dieser gerade nicht anwesend ist. Der Nachteil dieser direkten Kommunikation liegt natürlich darin, dass Vorgesetzte und Kollegen nicht ohne weiteres erfahren, ob ein Mitarbeiter Nachrichten erhalten hat und ggf. welchen Inhalt sie haben. Dies nehmen die Behördenchefs, wenn sie persönliche E-Mail-Adressen und Sprachboxen einrichten lassen, meist klaglos

in Kauf, wenn der Mitarbeiter anwesend oder nur kurzfristig abwesend ist. Anders verhält es sich, wenn er länger, z. B. wegen Urlaub, Fortbildung oder Krankheit, fehlt. In diesem Fall herrscht vielfach Unklarheit oder Streit darüber, ob und ggf. in welchem Umfang Vorgesetzte oder Kollegen auf das E-Mail-Postfach und die Sprachbox eines Mitarbeiters zugreifen oder einfach eine Anrufumleitung an den Vertreter aktivieren dürfen. Die Antwort auf diese Frage ist in der Tat komplex und nicht ganz einfach. Es gilt Folgendes zu unterscheiden:

Weil es noch immer kein spezielles Arbeitnehmerdatenschutzgesetz des Bundes gibt, ist die Frage vor allem nach den Vorschriften des Landesbeamtengesetzes (LBG) und des Landesdatenschutzgesetzes (LDSG) zu beantworten. Diese besagen dazu aber nur, dass der Arbeitgeber Daten seiner Mitarbeiter speichern und nutzen darf, soweit dies zur Durchführung des Dienst- oder Arbeitsverhältnisses erforderlich ist; spezielle Regelungen dazu, was in diesem Sinne erforderlich ist, fehlen. Deshalb ist für die Beantwortung der Frage, ob und in welchem Umfang Verbindungsdaten oder der Inhalt der Telefon- oder E-Mail-Kommunikation der Mitarbeiter einem Vorgesetzten oder Kollegen bekannt werden dürfen, eine Gesamtwürdigung der Interessen des Dienstherrn, der Mitarbeiter und des an der Telekommunikation beteiligten Dritten vorzunehmen, soweit keine speziellen Vorschriften des Telekommunikationsrechts einschlägig sind. Bei dieser Abwägung ist auf der Seite des Dienstherrn dessen Recht und Pflicht zu berücksichtigen, die sachgerechte Aufgabenerledigung auch für den Fall der Abwesenheit eines Mitarbeiters sicherzustellen. Dieser hat ein legitimes Interesse daran, dass seine Telekommunikation keiner unverhältnismäßigen Verhaltens- und Leistungskontrolle unterworfen ist und auch eine Inhaltskontrolle nicht über das zumutbare Maß hinausgeht. Auf der Seite des mit dem Mitarbeiter in Kontakt tretenden Dritten ist dessen Interesse zu berücksichtigen, bestimmte Informationen nur diesem Mitarbeiter zukommen zu lassen. Konkret bedeutet das für einzelne Konstellationen Folgendes:

4.1 Angehörige besonderer Berufsgruppen und Bedienstete mit besonderer Vertrauensstellung

Das Abhören der Sprachbox durch den Vertreter, die Anrufumleitung an diesen, die Weiterleitung von E-Mails an ihn oder der Zugriff auf das elektronische Postfach durch den Vertreter ist von vornherein bei solchen Bediensteten unzulässig, die Träger von Berufsgeheimnissen sind oder eine besondere Vertrauensstellung einnehmen. Da diese einer besonderen, auch behördenintern wirkenden Schweigepflicht unterliegen, dürfen Vorgesetzte und Kollegen nicht einmal wissen, dass eine bestimmte Person Kontakt mit ihnen hat oder wünscht. Zu diesem Personenkreis zählen nach § 203 Abs. 1 des Strafgesetzbuchs insbesondere Ärzte und Angehörige anderer Heilberufe, Psychologen sowie Ehe-/Erziehungs-/Jugend- oder Suchtberater. Dasselbe gilt für Mitarbeiter mit einer besonderen Vertrauensstellung wie z. B. Personalräte.

4.2 Anrufumleitung und Abhören der Sprachbox

– Rechtslage bei privater Mitbenutzung

Soweit es den Mitarbeitern ausdrücklich oder durch Duldung gestattet ist, private Telefongespräche zu führen, wäre die Anrufumleitung an den Vertreter und das Abhören der Sprachbox durch diesen von vornherein unzulässig. Insoweit ist der Dienstherr nämlich nach § 85 Abs. 2 des Telekommunikationsgesetzes (TKG) Anbieter eines Telekommunikationsdienstes und unterliegt den Vorschriften dieses Gesetzes und der Telekommunikations-Datenschutzverordnung (TDSV) und damit dem Fernmeldegeheimnis. Nach § 85 Abs. 3 TKG ist es dem Anbieter eines Telekommunikationsdienstes jedoch untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.

– Rechtslage bei nicht zugelassener privater Mitbenutzung

Soweit die private Mitbenutzung des Telefonanschlusses durch die Mitarbeiter nicht erlaubt ist und auch nicht wissentlich geduldet wird, finden die Vorschriften des Telekommunikationsrechts keine Anwendung. Deshalb kann die Frage, ob der Vertreter berechtigt ist, beim Telefonapparat des abwesenden Kollegen die Anrufweiterleitung zu aktivieren oder die Sprachbox abzuhören, nur auf Grund der bereits angesprochenen Abwägung beantwortet werden. Zu berücksichtigen ist dabei zunächst, dass sich nach der Rechtsprechung des Bundesverfassungsgerichts ein Arbeitnehmer auch dann auf sein „Recht am eigenen Wort“ berufen kann, wenn er Dienstgespräche führt. Zudem ist wesentlich, dass auch der Anrufer diesen Schutz des Rechts am eigenen Wort genießt. Dieser Schutz des gesprochenen Wortes gilt zwar nicht uneingeschränkt, für einen Eingriff ist jedoch ein überwiegendes schutzwürdiges Interesse des Arbeitgebers erforderlich. Ein berechtigtes Interesse des Arbeitgebers kann darin bestehen sicherzustellen, dass für einen abwesenden Mitarbeiter bestimmte Telefonate während dessen Abwesenheit bearbeitet werden. Die zu treffende Abwägung fällt nach meiner Beurteilung aber zu Gunsten der Vertraulichkeit des gesprochenen Wortes, also zu Gunsten der Grundrechte des Anrufers und des angerufenen Mitarbeiters aus, und zwar aus folgenden Gründen:

Soweit es um eine geplante Abwesenheit des Bediensteten geht (Urlaub, Kur, Dienstreise etc.), besteht schon deshalb kein Grund, in die Rechte des Anrufers und des angerufenen Bediensteten einzugreifen, weil durch eine Ansage auf der Mailbox dem Anrufer mitgeteilt werden kann, dass der betreffende Bedienstete abwesend ist, wie lange dies der Fall ist und an wen sich der Betreffende ggf. wenden kann.

Bei ungeplanter Abwesenheit des Mitarbeiters (z. B. Krankheit) scheidet diese Möglichkeit aus. Gleichwohl halte ich die „Kundenfreundlichkeit“ des Arbeitgebers nicht für ein so überwiegendes schutzwürdiges Interesse, dass es den dargelegten Grundrechtseingriff rechtfertigen könnte. Wer die Durchwahlnummer eines Mitarbeiters wählt, muss nämlich stets damit rechnen, dass dieser – aus welchen Gründen auch immer – abwesend ist. Je nach Wichtigkeit und/oder Dringlichkeit der Angelegenheit kann sich der Anrufer in diesem Fall jederzeit an die Telefonzentrale wenden, um entweder mit dem Stellvertreter des betreffenden Mitarbeiters verbunden zu werden oder in Erfahrung zu bringen, wie lange dessen Abwesenheit voraussichtlich dauern wird.

Hinzu kommt Folgendes: Der Vorgesetzte oder der Stellvertreter des abwesenden Mitarbeiters dürfte ohnehin nicht ohne weiteres die Möglichkeit haben, dessen ankommende Anrufe auf seinen Apparat umzuleiten oder seine Sprachbox abzuhören. Eine Telefonanlage darf nämlich nicht so konfiguriert sein, dass jeder ohne Eingabe einer sog. persönlichen Identifikationsnummer (PIN) die Anrufumleitung initiieren kann. Die PIN der Mitarbeiter müssten also irgendwo verschlossen und besonders geschützt deponiert sein mit der Folge, dass nur besonders ermächtigte Mitarbeiter im Fall krankheitsbedingter Abwesenheit eines Kollegen die Anrufumleitung aktivieren oder den Zugang zur Sprachbox ermöglichen können.

4.3 E-Mail-Verkehr

Für die Weiterleitung von E-Mails an den Vertreter oder dessen Zugriff auf das elektronische Postfach des abwesenden Kollegen gilt genau dasselbe wie für die Anrufumleitung bzw. den Zugang zur Sprachbox. Zwar ist bei einer E-Mail nicht das Recht des gesprochenen Worts betroffen, doch steht der E-Mail-Verkehr der telefonischen Kommunikation näher als dem Wechseln von Briefen. E-Mails sind in der Regel dadurch gekennzeichnet, dass sie spontan und wenig förmlich formuliert werden und oft schnelle Reaktionen auf Äußerungen des Adressaten darstellen. Deshalb sollten sie den gleichen Schutz genießen wie Telefonate.

Bei geplanter Abwesenheit eines Mitarbeiters ist dies schon deshalb unproblematisch, weil dem Absender der E-Mail durch den Abwesenheitsassistenten (Auto-Reply-Funktion) automatisch die Dauer der Abwesenheit und die E-Mail-Adresse des zentralen Posteingangs oder des Vertreters mitgeteilt werden können. Im Übrigen muss auch der E-Mail-Absender damit rechnen, dass der Adressat abwesend ist. Will er eine E-Mail versenden, die wichtig und/oder dringlich ist, muss er diese entweder an den zentralen Posteingang der Dienststelle richten oder sich vergewissern, dass der betreffende Mitarbeiter die E-Mail auch zur Kenntnis nehmen kann.

5. Das Lehrerkollegium und die Leistungsstufe

Um die starren Besoldungsregelungen für beamtete Staatsdiener aufzuweichen und besondere Leistungen honorieren zu können, schufen im Jahr 1998 sowohl der Bund als auch die Länder die rechtlichen Voraussetzungen dafür, dass Beamten der Besoldungsordnung A sog. Leistungsstufen gewährt werden können. Danach kann die Besoldung eines Beamten, der „dauerhaft herausragende Gesamtleistungen erbringt“, so erhöht werden, wie wenn er bereits die nächsthöhere Besoldungsstufe erreicht hätte. Nachdem die Landesregierung die Beamten des Landes zunächst nicht in den Genuss von Leistungsstufen kommen lassen wollte, können auch sie seit Januar 2000 diese Segnung erhalten. Allerdings hat die Sache noch einen entscheidenden Haken: Gibt es in einer Behörde mehrere Beamte, die herausragende Leistungen erbringen, erhalten nicht etwa alle eine Leistungsstufe, sondern maximal 10 % der in Frage kommenden Beamten, die das Endgrundgehalt noch nicht erreicht haben. Deshalb müssen die Vorgesetzten häufig eine Auswahl treffen. Besonders im Schulbereich äußerte sich deswegen Unmut über die neue Regelung, zumal nach der ersten Runde der Leistungsstufengewährung im Jahr 2000 nicht transparent war, wer auf Grund welcher Kriterien in den Genuss der Vergünstigung gekommen war. In der zweiten Runde in diesem Jahr wurde deshalb der Wunsch laut, die Schulleiter sollten doch dem Lehrerkollegium die Namen derjenigen, die eine Leistungsstufe erhalten haben, bekannt geben, was aber in der Regel unter Hinweis auf den Datenschutz abgelehnt wurde. Auf entsprechende Nachfragen konnte ich diese Beurteilung nur bestätigen. Gäbe ein Schulleiter bekannt, wem er eine Leistungsstufe zugesprochen hat, wäre dies in der Terminologie des Datenschutzrechts ausgedrückt eine Weitergabe eines Personalaktendatums an Dritte i. S. von § 113 und § 113d des Landesbeamtengesetzes. Ohne Zustimmung des Bediensteten dürfen Personalaktendaten aber nur unter engen Voraussetzungen weitergegeben werden, die hier eindeutig nicht vorliegen. Seit April dieses Jahres teilt das Kultusministerium diese datenschutzrechtliche Bewertung, während es zuvor die Leistungsstufenempfänger im eigenen Haus in einem internen Rundschreiben veröffentlicht haben soll.

6. Die dünnhäutige Beihilfestelle

Weil die Beamten bekanntlich nicht der gesetzlichen Krankenversicherung angehören, müssen sie sämtliche Kosten für ärztliche Behandlung, Krankenhausaufenthalt und Arznei- und Hilfsmittel zunächst selbst bezahlen. Je nach Familienstand bekommen sie aber einen unterschiedlich hohen Teil der Kosten vom Dienstherrn zurückerstattet. Die Landesbeamten erhalten die Beihilfe vom Landesamt für Besoldung und Versorgung (LBV) in Fellbach. Bei der Festsetzung einer Beihilfe bleibt es nicht aus, dass es zu Meinungsverschiedenheiten zwischen Antragsteller und Beihilfestelle über die Beihilfefähigkeit einer Behandlung oder eines Arznei- oder Hilfsmittels kommt. So war es auch bei einer Grundschullehrerin, der das LBV eine Beihilfe von ca. 350 DM verweigerte. Da half alles Lamentieren und Bitten um eine großzügige Handhabung nichts; auch im Widerspruchsverfahren blieb das LBV bei seiner Ablehnung. Für diese Entscheidung zeigte die Lehrerin allerdings wenig Verständnis und schrieb abschließend an das LBV:

„Sie werden nicht glauben, dass ich im Ernst mit einer anderen Entscheidung gerechnet habe. Genauso wenig überrascht mich, dass Sie im Grunde auf meine eigentlichen Argumente (Kleinlichkeit, Freiwillig-

keit, ...) gar nicht eingegangen sind. Auch dass Sie es wegen ca. 350 DM auf eine Klage ankommen lassen, traue ich Ihnen zu. Nur, dafür sind mir doch meine Nerven zu schade.

Meine Konsequenzen sehen anders aus:

1. Ich war, wie Beurteilung und Elternreaktionen belegen, eine engagierte Lehrerin. Sie haben dazu beigetragen, dass meine Motivation ins Unermessliche steigt.

2. Ich werde für dieses Land und diesen Staat fortan ‚freiwillig' keinen Finger mehr rühren."

Zudem fügte sie ihrem Schreiben einen kritischen Aufsatz eines Professors über bürokratische Belastungen mittelständischer Unternehmen bei, in dem es heißt:

„Inzwischen aber dient der Bürger weithin der Verwaltung und hat sich die Bürokratie zu einem unsere Freiheit immer stärker einengenden Krebsgeschwür unserer Freiheit entwickelt."

Auf dieses Schreiben reagierte das LBV äußerst dünnhäutig. Es schickte eine Kopie des Briefes an das Oberschulamt Stuttgart mit der Bitte, das Verhalten der Lehrerin in dienstrechtlicher Hinsicht zu überprüfen. Dabei vergaß es nicht, ausdrücklich darauf hinzuweisen, dass „die Beihilfeangelegenheit der Beamtin korrekt bearbeitet wurde", wobei aus der ebenfalls angegebenen Personalnummer ohnehin ersichtlich war, dass es sich um eine Beihilfeangelegenheit handelte. Das Oberschulamt ließ sich das nicht zweimal sagen und forderte die Lehrerin unter Hinweis darauf, dass das LBV ihr Schreiben „dem Oberschulamt zur Aufnahme in ihre Personalakte" übersandt habe, zur Stellungnahme auf. Unter welchen dienstrechtlichen Gesichtspunkten es die Angelegenheit prüfen will, wollte das Oberschulamt der Lehrerin allerdings zu diesem Zeitpunkt nicht sagen. Deshalb gab die Lehrerin auch keine Stellungnahme ab, sondern machte das Oberschulamt lediglich darauf aufmerksam, dass sie die Übersendung des Schreibens durch das LBV für unrechtmäßig halte. Daraufhin fühlte sich das Oberschulamt wenigstens bemüßigt, der Lehrerin mitzuteilen, ihr Schreiben würde der Pflicht eines Beamten, durch sein Verhalten innerhalb und außerhalb des Dienstes der Achtung und dem Vertrauen gerecht zu werden, die sein Beruf erfordert, nicht gerecht und es sehe einen dienstrechtlichen Bezug in ihrer Äußerung „ ... für dieses Land und diesen Staat fortan ‚freiwillig' keinen Finger mehr (zu) rühren".

Um es kurz zu machen: Die Lehrerin gab die gewünschte Stellungnahme nicht ab und bat mich, die Angelegenheit zu überprüfen. Dabei kam ich zu folgendem Ergebnis:

Das LBV und das Oberschulamt haben die Sache viel zu hoch aufgehängt. Eine Dienstpflichtverletzung der Lehrerin hätte dann vorgelegen, wenn ihr Schreiben verletzende Äußerungen und/oder die Ankündigung, ihren Dienst künftig nicht mehr pflichtgemäß ausüben zu wollen, enthielte. Von beidem konnte weder das LBV noch das Oberschulamt auf Grund des in Rede stehenden Schreibens ausgehen. Allein darin, dass ein Beamter missbilligende Wertungen oder zugespitzte Kritik am Vorgehen von Vorgesetzten oder Behörden seines Dienstherrn vorträgt, liegt nämlich noch keine Verletzung der Dienstpflicht eines Beamten. Eine solche ist dann anzunehmen, wenn die Äußerungen ehrverletzenden Charakter haben, den ich aber im Schreiben der Lehrerin nun wirklich nicht erkennen kann. Auch in der Ankündigung der Petentin, sie werde „ ... für dieses Land und diesen Staat fortan ‚freiwillig' keinen Finger mehr rühren", liegt keine Dienstpflichtverletzung. Zwar kann ein Dienst nach Vorschrift dann pflichtwidrig sein, wenn er dazu bestimmt ist, staatliche Funktionen lahm zu legen oder als Bummelstreik anzusehen wäre. Das Oberschulamt meint zwar, eine Lehrkraft sei auch verpflichtet, freiwillige Leistungen zu erbringen, doch hier irrt es grundlegend. Wie sich bereits aus dem Wort freiwillig ergibt, handelt es sich dabei um Leistungen, zu denen der Beamte gerade nicht verpflichtet ist. Zur vollen Hingabe an das Amt gehört nur die Bewältigung des zugewiesenen Arbeitspensums eines Beamten, wozu er – soweit erforderlich – in engem Rahmen auch Überstunden zu machen hat. Tätigkeiten, die nicht zu Erfüllung der

Aufgaben auf einem bestimmten Dienstposten gehören, muss der Beamte auch nicht erbringen. Vor diesem Hintergrund war der Aktionismus des LBV und des Oberschulamts fehl am Platz. In jedem Fall unzulässig war, dass das LBV dem Oberschulamt mitteilte, dass sich die Angelegenheit im Rahmen eines Beihilfeverfahrens abgespielt hatte. Dies hat das LBV im Gegensatz zum Oberschulamt am Ende auch eingesehen.

7. Der Stellenplan de luxe

Seit jeher sind die Städte und Gemeinden verpflichtet, jährlich einen Stellenplan aufzustellen, der vom Gemeinderat als Bestandteil von Haushaltsplan und Haushaltssatzung beschlossen werden muss. In ihm bestimmt die Gemeinde die Stellen ihrer Beamten und der nicht nur vorübergehend beschäftigten Angestellten und Arbeiter, die für die Erfüllung der Aufgaben im betreffenden Jahr erforderlich sind. Zudem kann die Gemeinde einen Organisationsplan aufstellen, der auch die Bewertung der Stellen enthalten kann. Mit diesen Angaben wollte sich der Gemeinderat einer Großen Kreisstadt jedoch auf einmal nicht mehr zufrieden geben. Er forderte von der Gemeindeverwaltung einen „Organisationsstellenplan“, in dem bei der jeweiligen Stelle auch der Name der Stelleninhaberin oder des Stelleninhabers aufgeführt sein sollte. So hätte zumindest jedes Gemeinderatsmitglied nachlesen können, wer wo in welchem Umfang beschäftigt ist und wie der Betreffende besoldet oder eingruppiert ist. Der Personalrat, dem dieses Ansinnen entschieden zu weit ging, bat mich um Schützenhilfe. Die konnte ich ihm auch gewähren, denn die Gemeindeverwaltung darf dem Wunsch des Gemeinderats nicht entsprechen. Klar ist, dass der Gemeinderat Anspruch auf alle Informationen hat, die er als Grundlage für von ihm zu treffende Entscheidungen oder ein Tätigwerden im Rahmen seiner Zuständigkeit benötigt. Eine komplette personenbezogene Stellenübersicht gehört dazu aber nicht. Für die Beratung und Beschlussfassung über die Haushaltssatzung ist nämlich nur von Belang, in welchen Bereichen welche Stellen vorhanden sind oder ausgewiesen werden sollen. Um im Einzelfall Personalentscheidungen zu treffen, benötigt der Gemeinderat ebenfalls keine Auflistung sämtlicher städtischer Bediensteter. Personenbezogene Stellenübersichten benötigt man dagegen bei der Personalplanung und Personalwirtschaft. Dafür ist jedoch nicht der Gemeinderat, sondern nur der Bürgermeister zuständig.

3. Abschnitt: Ausländerwesen

1. Die Regelanfrage bei der Einbürgerung

Ein Diplomingenieur aus Stuttgart schrieb uns, er habe vor kurzem seine langjährige griechische Lebensgefährtin geheiratet. Weil seine Frau in Deutschland geboren und aufgewachsen sei, hätten sie sich nach der Hochzeit entschlossen, ihre Einbürgerung zu beantragen. Den Antragsformularen, die sie dafür von der Ausländerbehörde ausgehändigt bekommen hätten, sei ein Hinweisblatt beigelegen, in dem er zu seinem Erstaunen habe lesen müssen, dass seine Frau im Einbürgerungsverfahren einer sicherheitsmäßigen Überprüfung durch den Verfassungsschutz unterzogen werde.

Damit kam die vorläufige allgemeine Verwaltungsvorschrift des Innenministeriums zum Staatsangehörigkeitsrecht auf den Prüfstand. Darin hatte das Innenministerium Ende 1999 die Einbürgerungsbehörden angewiesen, dass sie bei allen Ausländern, die sich einbürgern lassen wollen und älter als 16 Jahre sind, eine Sicherheitsüberprüfung unter Einbeziehung des Verfassungsschutzes vorzunehmen haben. Aus dem Behördendeutsch übersetzt heißt das, dass die Einbürgerungsbehörden gehalten sind, unterschiedslos über jeden Ausländer, der sich einbürgern lassen will, beim Landesamt für Verfassungsschutz anzufragen, ob es dort Erkenntnisse über ihn gibt. Hätte das Innenministerium mein Amt beim Erlass der Verwaltungsvorschrift – wozu es nach den Vorschriftenrichtlinien der Landesregierung verpflichtet gewesen wäre – beteiligt, hätte ich es darauf hingewiesen, dass diese Regelanfrage zu weit geht. Die Rechtslage sieht nämlich so aus:

Nach § 85 des Ausländergesetzes hat ein Ausländer, der seit acht Jahren rechtmäßig seinen gewöhnlichen Aufenthalt in Deutschland hat, bei Vorlie-

gen der weiteren Voraussetzungen dieser Vorschrift Anspruch darauf, eingebürgert zu werden, wenn er sich gegenüber der Einbürgerungsbehörde ausdrücklich zur freiheitlichen demokratischen Grundordnung bekennt und eine entsprechende Loyalitätserklärung abgibt. Ein Einbürgerungsanspruch besteht allerdings nicht, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass der Einbürgerungsbewerber Bestrebungen gegen die freiheitliche demokratische Grundordnung verfolgt oder verfolgt hat. Allein der Umstand, dass dieser Ausschlussgrund im Ausländergesetz steht, rechtfertigt jedoch noch lange nicht, über jeden Einbürgerungsbewerber eine Anfrage an den Verfassungsschutz zu stellen. Behörden dürfen bekanntlich Auskünfte über jemanden bei anderen Stellen nur einholen, wenn ihnen eine Rechtsvorschrift dies erlaubt. Eine Regelung, die es den Einbürgerungsbehörden gestattet, mir nichts, dir nichts über Einbürgerungsbewerber bei anderen Behörden Erkundigungen einzuziehen, kennt unser Landesdatenschutzgesetz jedoch nicht. Es lässt in solchen Fällen eine Anfrage vielmehr nur zu, wenn im Einzelfall Angaben des Einbürgerungsbewerbers geprüft werden müssen, weil tatsächliche Anhaltspunkte für deren inhaltliche Unrichtigkeit bestehen. Derartige Zweifel an der Aufrichtigkeit der Loyalitätserklärung drängen sich jedoch höchstens dann auf, wenn die Einbürgerungsbehörde Grund zu der Annahme hat, dass der Einbürgerungsbewerber sich bereits extremistisch betätigt hat oder dies zu tun vorhat und darüber im Einbürgerungsverfahren unzutreffende Angaben gemacht hat. Auch vermag – wie aber das Innenministerium zu meinen scheint – der Umstand, dass es in Einbürgerungsverfahren zu unzutreffenden Loyalitätserklärungen gekommen ist, noch lange nicht den Schluss zu rechtfertigen, dass alle anderen Einbürgerungsbewerber mit ihren Loyalitätserklärungen die Einbürgerungsbehörden genauso täuschen. Deshalb gilt nach wie vor: für eine Anfrage beim Verfassungsschutz ohne einen solchen konkreten Anlass oder gar für eine Regelanfrage ohne Berücksichtigung der Umstände des Einzelfalls keine rechtliche Befugnis.

Abgesehen davon ist zweifelhaft, ob Anfragen der Einbürgerungsbehörden beim Landesamt für Verfassungsschutz überhaupt geeignet sind, gerichtsverwertbare Einbürgerungshindernisse in Erfahrung zu bringen. Erkenntnisse des Verfassungsschutzes sind nämlich bekanntermaßen gerade im Bereich des Ausländerextremismus aus Gründen des Quellenschutzes geheimhaltungsbedürftig. Sie nützen deshalb der Einbürgerungsbehörde, selbst wenn sie die Erkenntnisse vom Verfassungsschutz erfährt, nichts, weil sie diese dem Einbürgerungsbewerber nicht offenbaren darf und deshalb im Einbürgerungsverfahren nicht berücksichtigen kann.

Das Innenministerium ließ mich wissen, dass es an der Regelanfrage über Einbürgerungsbewerber festhalten will. Mit dem geltenden Recht steht dies nicht im Einklang. Hätte der Gesetzgeber die Regelanfrage gewollt, hätte er dies mit der gebotenen Deutlichkeit in den Regelungen über das Einbürgerungsverfahren zum Ausdruck bringen müssen. Das hat er jedoch nicht getan. Ich weiß wohl, dass im Zuge der Terroranschläge vom 11. September 2001 Forderungen laut geworden sind, bei der Einbürgerung von Ausländern die Regelanfrage für Einbürgerungsbewerber einzuführen und sich der Bundesrat diesen zwischenzeitlich angeschlossen hat. Per Verwaltungsvorschrift, wie dies der Bundesrat verlangt, lässt sich das jedoch nicht machen. Die zwingende Beteiligung des Verfassungsschutzes im Einbürgerungsverfahren, der seine Erkenntnisse mit nachrichtendienstlichen Mitteln beschaffen kann, bringt einen gravierenden Eingriff in das Grundrecht auf Datenschutz der betroffenen Bürger mit sich. Solche Eingriffe bedürfen nach der Rechtsprechung des Bundesverfassungsgerichts einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für den Bürger erkennbar ergeben und die dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Deshalb muss, wie es sich in einer Demokratie gehört, das Parlament über eine solche Forderung entscheiden.

2. Die Ausländerbehörde vergisst nichts!

Ausländer, die sich in Deutschland aufhalten, unterliegen der Überwachung durch die Ausländerbehörden. Lassen sie sich etwas zu Schulden kommen, müssen sie unter Umständen mit ihrer Ausweisung rechnen und dann Deutschland verlassen. Erhalten andere Behörden Kenntnis von einem Aus-

weisungsgrund, haben sie darüber die Ausländerbehörden zu unterrichten. Ausgewiesen werden kann ein Ausländer beispielsweise, wenn er die freiheitlich demokratische Grundordnung gefährdet oder sich bei der Verfolgung politischer Ziele an Gewalttätigkeiten beteiligt oder einen nicht nur vereinzelten oder geringfügigen Verstoß gegen Rechtsvorschriften begangen hat. Immerhin ist damit auch klar, dass bei vereinzelten oder geringfügigen Verstößen eine Mitteilung unterbleibt. Als geringfügig sind Ordnungswidrigkeiten anzusehen, wenn die dafür festgesetzte Geldbuße nicht mehr als 1.000 DM beträgt. Straftaten gelten als geringfügig, wenn das Ermittlungsverfahren ohne oder gegen eine Geldauflage von weniger als 1.000 DM eingestellt oder wenn der Täter zu einer Geldstrafe von weniger als 30 Tagessätzen verurteilt worden ist. Für die Behördenpraxis folgt daraus, dass Ausländerbehörden nur rechtskräftige Strafurteile und Bußgeldbescheide zu ihren Ausländerakten nehmen dürfen, wenn die verhängten Sanktionen die Geringfügigkeitsgrenze überschreiten. Das bedeutet freilich nicht, dass die Ausländerbehörden vor dem rechtskräftigen Abschluss eines Bußgeld- oder Strafverfahrens eingegangene Mitteilungen als Luft behandeln müssten. Sie dürfen solche Mitteilungen gleichwohl zu ihren Ausländerakten nehmen, müssen sie aber wieder entfernen, wenn das Verfahren eingestellt oder eine Sanktion verhängt worden ist, die unterhalb der Geringfügigkeitsgrenze liegt.

Dieser Rechtslage tragen die Ausländerbehörden, wie wir bei Kontrollen festgestellt haben, nicht immer Rechnung. Sie nehmen Mitteilungen über Anzeigen wegen Straftaten und Ordnungswidrigkeiten sowie Strafbefehle und Strafurteile stets zu ihren Ausländerakten und belassen sie dort selbst dann, wenn der Ausländer später freigesprochen oder das Verfahren eingestellt worden ist. Selbst Mitteilungen der Polizei über nächtliche Ruhestörungen haben wir in Ausländerakten gefunden. Auch kommt es oft vor, dass Jahre alte Mitteilungen über Anzeigen wegen einer Straftat oder einer Ordnungswidrigkeit in den Ausländerakten liegen, ohne dass daraus ersichtlich wäre, wie das Bußgeld- oder Ermittlungsverfahren seinerzeit ausgegangen ist. Um diesen untragbaren Zustand zu ändern, bat ich Anfang Juli 2001 das Innenministerium sicherzustellen, dass die Ausländerbehörden künftig bei der Aufbewahrung von Mitteilungen über Straf- und Bußgeldverfahren der geschilderten Rechtslage Rechnung tragen. Dabei schlug ich vor, die gemeinsame Verwaltungsvorschrift des Innenministeriums, des Justizministeriums und des Sozialministeriums über die Ausweisung von Ausländern entsprechend zu ergänzen. Ob das Innenministerium meinem Petitum nachkommen wird, weiß ich nicht. Es hüllt sich bislang noch in Schweigen.

3. Fragen an den Ehegatten

Darf eine Ausländerbehörde vor Erteilung oder Verlängerung einer Aufenthaltserlaubnis von einem Ausländer und seinem (ausländischen oder deutschen) Ehepartner eine schriftliche Erklärung zur ehelichen Lebensgemeinschaft einholen und darin danach fragen, ob sie getrennt leben, ob die Ehe geschieden ist, die Scheidung beantragt ist oder ob Scheidungsabsichten bestehen? Ein Rechtsanwalt, der uns mit dieser Frage konfrontiert hatte, weil eine Ausländerbehörde von seinem Mandanten und von dessen Ehefrau eine solche Erklärung erbeten hatte, meinte nein, weil den Ehepartner im aufenthaltsrechtlichen Verfahren nach dem Ausländergesetz weder eine Mitwirkungsobliegenheit noch eine Pflicht zu Angaben gegenüber der Ausländerbehörde treffe. Mit diesem Hinweis hatte der Anwalt recht. Doch beantwortet war damit seine Frage noch nicht. Die Sache ist nämlich verzwickter:

Einem ausländischen Ehegatten eines in Deutschland lebenden Ausländers kann nach den Vorschriften des Ausländergesetzes ein Aufenthaltsrecht gewährt werden; unter Umständen hat er sogar einen Anspruch darauf. Entsprechendes gilt für den ausländischen Ehegatten eines Deutschen. Voraussetzung ist jedoch, dass beide in Deutschland bereits in familiärer Lebensgemeinschaft leben oder hier eine solche Lebensgemeinschaft begründen wollen. Ob diese Voraussetzungen vorliegen, haben die Ausländerbehörden in jedem Einzelfall von Amts wegen zu prüfen. Dazu können sie den Antragsteller befragen oder von ihm Angaben in schriftlichem Wege einholen. Dem Ausländer obliegt es, die für ihn günstigen Umstände, die für die Ent-

scheidung über seinen Antrag erheblich sind, gegenüber der Ausländerbehörde geltend zu machen. Handelt es sich um Umstände aus seiner persönlichen Sphäre, muss er sie sogar beweisen. Zu Letzeren gehört auch die Frage, ob ein Ausländer mit seinem Partner in ehelicher Lebensgemeinschaft lebt. Er muss diese Voraussetzung für die Erteilung oder Verlängerung einer Aufenthaltserlaubnis zum Ehegattennachzug demnach nicht nur vortragen, sondern auch einen geeigneten Nachweis dafür erbringen, will er nicht Gefahr laufen, dass sein Antrag abgelehnt wird. Deshalb und weil sich beispielsweise mit der Vorlage einer Heiratsurkunde nicht belegen lässt, dass tatsächlich eine familiäre Lebensgemeinschaft besteht, und weil Befragungen Dritter durch die Ausländerbehörden oder gar Kontrollen vor Ort einen viel gravierenderen Eingriff in die Privatsphäre darstellen, ließ ich den Rechtsanwalt wissen, dass sich aus der Sicht des Datenschutzes die Einholung einer Erklärung zur ehelichen Lebensgemeinschaft nicht beanstanden lässt.

4. Wohin mit der Haftungsübernahmeerklärung?

Eine Frau, die seit mehreren Jahren immer wieder Au-pair-Mädchen in ihrem Haushalt beschäftigt hatte, wollte wieder eine junge Ausländerin für eine solche Tätigkeit einladen. Nach den dafür maßgeblichen Vorschriften dürfen aber Personen aus bestimmten Staaten nur nach Deutschland kommen, wenn ihr Gastgeber für ihren Lebensunterhalt und für die Rückreisekosten bürgt. Weil das neue Au-pair-Mädchen wieder aus einem solchen Land stammte, sprach die Frau beim Ausländeramt vor, um erneut eine solche Haftungsübernahmeerklärung abzugeben. Als dieses sie aufforderte, zum Beleg ihrer Erklärung einen Gehaltsnachweis, Unterlagen über die Größe ihrer Wohnung und Geburtsurkunden ihrer Kinder vorzulegen, kamen der Frau Bedenken. Sie hatte diese Nachweise dem Ausländeramt auf dessen Bitte bereits im Zusammenhang mit der Haftungsübernahmeerklärung bei der Vorgängerin und der Vorvorgängerin des neuen Au-pair-Mädchens überlassen. Diese Unterlagen waren indes nicht mehr vorhanden. Man hatte sie kurzer Hand jeweils zur Ausländerakte der beiden Au-pair-Mädchen genommen und diese Akte den Ausländerämtern übersandt, in deren Zuständigkeitsbereich sie verzogen waren.

Keine Frage: Die Unterlagen, die die Frau zum Beleg ihrer Haftungsübernahmeerklärung dem Ausländeramt vorgelegt hatte, hatten bei den anderen Ausländerämtern nichts zu suchen; diese brauchten sie zur Erfüllung ihrer Aufgaben nicht. Ursächlich dafür, dass die Unterlagen dennoch dort landeten, waren zwei Fehler, die dem Ausländeramt unterlaufen waren. Sein Kardinalfehler war, dass es die Ausländerakten über die Au-pair-Mädchen mit den Akten über die Haftungsübernahmeerklärung verquickt hatte, anstatt sie gesondert zu führen. Das auf die Abgabe einer Haftungsübernahmeerklärung gerichtete Verfahren ist ein eigenständiges Verwaltungsverfahren, in dem derjenige, der die Übernahmeerklärung abgibt, Verfahrensbeteiligter ist, nicht aber der Ausländer, zu dessen Gunsten die Erklärung abgegeben wird. Deswegen hätte das Ausländeramt dafür eine eigenständige, von der Ausländerakte des begünstigten Au-pair-Mädchens getrennte Akte anlegen müssen. Diese Akte hätte es beim Umzug der Mädchen selbstverständlich nicht weitergeben dürfen, weil die Ausländerämter, in deren Bereich die beiden verzogen waren, diese Akte zur Erfüllung ihrer Aufgabe gar nicht benötigen. Der zweite Fehler war, dass das Ausländeramt dem in Behördenkreisen weitverbreiteten Hang gefolgt ist, alle Unterlagen, die ein Bürger zum Beleg seiner Angaben vorlegt, in Kopie zu den Akten zu nehmen. Nach dem Landesdatenschutzgesetz dürfen aber Behörden personenbezogene Informationen in Akten nur festhalten, soweit sie für das weitere Verfahren und für die Dokumentation einzelner Verfahrensschritte erforderlich sind. Deshalb dürfen Schriftstücke, die ein Verfahrensbeteiligter bei einer Behörde zum Beleg seiner Angaben vorlegt, nur dann zu den Akten genommen werden, wenn dies über den bloßen Nachweis der Angaben hinaus geboten ist. Dabei ist der Grundsatz der Verhältnismäßigkeit zu beachten. Dies gilt insbesondere dann, wenn die Schriftstücke mehr personenbezogene Informationen – oftmals auch über Dritte – enthalten als für den Nachweis der entscheidungserheblichen Angaben unbedingt notwendig ist. Statt solche Schriftstücke einfach zu kopieren und zu den Akten zu nehmen,

müssen sich die Behörden deshalb darauf beschränken, dort zu vermerken, dass die Angaben belegt worden sind. Hätte das Ausländeramt dies beherzigt, wäre bei der Weitergabe der Akten für die Datenschutzrechte der Frau schon einiges gerettet gewesen. In Zukunft will es – wie es mir versichert hat – die Akten trennen und beim Kopieren Zurückhaltung üben.

4. Abschnitt: Sonstiges

1. Die Suche nach Altlasten durch ein Ingenieurbüro

Altlasten sind tickende Zeitbomben. Sie zu erfassen ist deshalb dringend geboten. Das Landesabfallgesetz hat diese Aufgabe den Landratsämtern übertragen. Sie müssen altlastverdächtige Flächen systematisch erheben und auf ihr Gefährdungspotential untersuchen. Dazu können sie auf Unterlagen anderer Behörden, die Aufschluss darüber geben können, ob und wo Altlasten zu vermuten sind, zugreifen, also z. B. auf Bau- und Gewerbeakten.

So weit, so gut. Aber wie sieht es aus, wenn ein Landratsamt die notwendigen Erhebungen nicht selbst vornimmt und stattdessen ein privates Ingenieurbüro beauftragt? Genau diese Frage stellte mir eine Stadt. Das Landratsamt Konstanz hatte ein Ingenieurbüro beauftragt, eine vor einigen Jahren durchgeführte flächendeckende Erhebung altlastverdächtiger Flächen für den gesamten Landkreis fortzuschreiben. Im Rahmen dieses Auftrags hatte sich das Ingenieurbüro an Gewerbe- und Baurechtsbehörden gewandt, um Einsicht in die Unterlagen von Betrieben zu nehmen, die seit der letzten Erhebung stillgelegt worden waren.

Hierzu muss man Folgendes wissen: Eine Behörde muss ihre Aufgaben grundsätzlich selbst wahrnehmen. Sie darf diese nur dann auf andere Stellen übertragen, wenn eine Rechtsvorschrift dies erlaubt. Eine solche Rechtsvorschrift existiert in Baden-Württemberg für die Altlastenerhebung gerade nicht. Es besteht jedoch die Möglichkeit, dass eine Behörde eine andere Stelle mit der Erledigung ihr obliegender Aufgaben betraut. Die Behörde bleibt dann nach wie vor für die Erfüllung der Aufgabe verantwortlich. Die beauftragte Stelle wird nur als verlängerter Arm der Behörde tätig. Sie handelt in diesem Fall als sog. Verwaltungshelfer. Dieser darf sich nur in dem Umfang und in der Weise Informationen beschaffen, wie es auch die Behörde dürfte. Umgekehrt dürfen und müssen Dritte dem Verwaltungshelfer nur die Daten zur Verfügung stellen, die sie auch an die Behörde herausgeben müssten. Schließlich müssen Bürger, über die von einem Verwaltungshelfer Informationen eingeholt und genutzt werden, auch nur in dem Maß Eingriffe in ihr Grundrecht auf Datenschutz hinnehmen, wie sie dies gegenüber der Behörde tun müssten. Die Einschaltung eines Verwaltungshelfers hat nur einen Haken: Diese Rechtswirkungen treten nicht automatisch ein. Die Landesregierung hatte es bei der Novellierung des Landesdatenschutzgesetzes leider abgelehnt, dies dort festzuschreiben. Deshalb müssen die Behörde und der Verwaltungshelfer vertraglich festlegen, dass dieser verpflichtet ist, die datenschutzrechtlichen Regelungen zu beachten, die auch von der zuständigen Behörde zu befolgen wären, wenn sie ihre Aufgabe in vollem Umfang selbst erledigen würde. Nur wenn dies sichergestellt und gesetzlich nichts anderes bestimmt ist, darf die zuständige Behörde einen Dritten beauftragen.

Eine Nachfrage beim Landratsamt Konstanz ergab, dass die mit dem Ingenieurbüro abgeschlossenen Vereinbarungen diesen Anforderungen bei weitem nicht Rechnung trugen. Ich forderte deshalb das Landratsamt im Dezember 2000 zur Nachbesserung auf. Darauf tat sich trotz wiederholter Erinnerungsschreiben lange Zeit nichts. Erst zehn Monate später bequemte sich das Landratsamt dazu, mir eine Kopie des überarbeiteten Vertrages zuzuleiten. Damit Ende gut, alles gut? Leider nein. Denn auch die aktualisierte Vereinbarung entsprach nicht vollständig den datenschutzrechtlichen Anforderungen. Ich musste das Landratsamt daher ein weiteres Mal zur Nachbesserung auffordern.

2. Schulen im World Wide Web

„Schulen ans Netz“, so lautet das Motto das deutlich macht, dass das Internet landauf, landab auch in den Schulen Einzug gehalten hat oder noch wird. Dabei geht es aber nicht nur darum, elektronische Post auszutauschen und zu lernen, wie man Internet-Angebote finden und nutzen kann. Vielmehr wollen sich zunehmend auch die Schule, die Lehrkräfte und die Schüler im Internet präsentieren. Während sich manche Schulen dabei, wie Eingaben zu entnehmen ist, offenbar keine Gedanken über den Datenschutz von Lehrern und Schülern machen, fragen andere nach, ob und ggf. welche Daten sie ohne deren Einwilligung in das Internet einstellen dürfen. Einige Grundsätze dazu habe ich bereits im 18. Tätigkeitsbericht 1997, LT-Drs. 12/2242, S. 17, dargestellt. Überträgt man diese auf die Schule ist zu fragen, ob es zur Erfüllung der Aufgaben der Schule nötig ist, Schüler- und Lehrerdaten ins Internet einzustellen. Die Frage stellen heißt, sie sogleich zu verneinen. Die weltweite Verbreitung von Daten eines Lehrers ohne dessen Einwilligung verbieten § 113d des Landesbeamtengesetzes und § 36 Abs. 1 des Landesdatenschutzgesetzes (LDSG). Für die Schülerdaten gilt nach § 18 LDSG das Gleiche, weil die Schüler durchaus ein schutzwürdiges Interesse daran haben können, dass ihre Daten nicht weltweit gestreut werden. Die Schule darf also Daten von Eltern und Schülern – dazu zählen auch Fotos – nur dann in das Internet einstellen, wenn sie zuvor deren schriftliche Einwilligung eingeholt hat. Bei Schülern unter 14 Jahren müssen in jedem Fall die Eltern die Einwilligung erteilen.

Das Kultusministerium hat die Schulen bereits 1997 in einem Erlass auf diese Rechtslage aufmerksam gemacht. Er findet aber offenbar bei den Schulen nicht die nötige Beachtung, denn sonst gäbe es die Anfragen bei meinem Amt dazu gar nicht.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
am 1. Oktober 2001

Sondertreffen der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z. B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus – mit den Worten des Bundesverfassungsgerichts – auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich-demokratischen Gemeinwesens“.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zulasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahre gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der Strafprozessordnung zu ergreifen, führt zu Eingriffen in das Persönlich-

keitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internet-Provider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

Biometrische Merkmale in Personalausweisen und Pässen

Im Entwurf eines Terrorismusbekämpfungsgesetzes ist vorgesehen, die Möglichkeit zu eröffnen, in deutschen Personalausweisen und Pässen neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie zum Beispiel Fingerabdrücke, Handgeometrie, Gesichtsgeometrie u. a. aufzunehmen. Auch die Verwendung genetischer Daten wird nicht ausgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass diese Maßnahme schon allein wegen des technischen und zeitlichen Aufwandes, der mit der Einführung derartiger Dokumente verbunden wäre, keinen kurzfristigen Beitrag zur Lösung der mit dem internationalen Terrorismus derzeit verbundenen Probleme leisten kann, zumal Ausländerinnen und Ausländer, die sich in Deutschland aufhalten, nicht erfasst werden.

Die Nutzung biometrischer Merkmale in Personalausweisen und Pässen sowie die damit verbundenen Folgeprobleme (zum Beispiel Art und Ort der Speicherung von Referenzdaten; Vermeidung von Überschussinformationen) werfen eine Vielzahl schwieriger Fragen auf, die einer ausführlichen Diskussion bedürfen. Die zuständigen Stellen werden hierzu aufgefordert, die Notwendigkeit und die rechtlichen und technischen Einzelheiten einer Realisierung dieser Maßnahmen darzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist bereit, sich unter diesen Voraussetzungen mit der Frage zu befassen, ob und wie es möglich ist, mit Hilfe geeigneter zusätzlicher Merkmale in Identifikationspapieren deren Missbrauch zu verhindern, ohne dabei die Grundsätze des Datenschutzes zu verletzen.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 10. Mai 2001
zum

Entwurf der Telekommunikations-Überwachungsverordnung

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße „Surfen“ zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienste-Staatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

Grundsätze zur Übermittlung von Telekommunikationsverbindungsdaten

Die Bundesregierung hat den Gesetzentwurf für eine Nachfolgeregelung zu § 12 Fernmeldeanlagengesetz (FAG) vorgelegt, der eine Reihe datenschutzrechtlich positiver Ansätze enthält. Der Bundesrat hat sich demgegenüber in seiner Stellungnahme für eine Regelung ausgesprochen, die wesentlichen datenschutzrechtlichen Anforderungen nicht gerecht wird. Die Datenschutzbeauftragten des Bundes und der Länder lehnen den Vorschlag des Bundesrates entschieden ab.

Sie halten es für nicht vertretbar, Auskünfte über zurückliegende Aktivmeldungen von Mobiltelefonen auch bei reinem Stand-by-Betrieb zu erteilen und Diensteanbieter zur Aufzeichnung von Telekommunikationsverbindungsdaten eigens für Zwecke der Strafverfolgung zu verpflichten.

Auch die vom Bundesrat vorgeschlagene Regelung des § 18a BVerfSchG zur Übermittlung von Telekommunikationsverbindungsdaten an die Verfassungsschutzbehörden halten die Datenschutzbeauftragten des Bundes und der Länder für nicht akzeptabel. Sie fordern eine deutliche Klarstellung im Wortlaut des Gesetzes, dass Verbindungsdaten an den Verfassungsschutz nur dann übermittelt werden dürfen, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine in § 3 Abs. 1 G 10 genannte Straftat plant, begeht oder begangen hat oder sonst an gewalttätigen Bestrebungen oder sicherheitsgefährdenden Tätigkeiten teilnimmt. Eine Übermittlung der Verbindungsdaten für den gesamten Aufgabenbereich des Verfassungsschutzes ginge dagegen erheblich zu weit.

Ferner halten es die Datenschutzbeauftragten für geboten, hinsichtlich der Kennzeichnung und Zweckbindung der Daten, der Mitteilungen an Betroffene und der parlamentarischen Kontrolle einen dem G 10 möglichst gleichwertigen Standard zu gewährleisten.

Die Bundesregierung und der Deutsche Bundestag werden gebeten, diese datenschutzrechtlichen Mindestanforderungen im weiteren Gesetzgebungsverfahren zu berücksichtigen.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2001

Novellierung des G 10-Gesetzes

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u. a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,
- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und
- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.
- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.
- Alle Neuregelungen wie z. B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.
- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.
- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.
- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.
- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

- Dem BND wird nicht mehr nur die „strategische Überwachung“ des nicht leitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.
- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischer Überwachung“ nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2001

Datenschutz bei der Bekämpfung von Datennetzkriminalität

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[1)]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden.[2)]

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

- Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,
- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,
- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,
- Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

[1)] European Committee on Crimes Problems (CDPC), Committe of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY (2000) Draft No. 25).

[2)] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26. Januar 2001 – KOM (2000) 890 endgültig.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 12. März 2001

Anlasslose DNA-Analyse aller Männer verfassungswidrig

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den Vorschlag zurück, den „genetischen Fingerabdruck“ aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potentielle Straftäter behandelt, ist verfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

Zur „neuen Medienordnung“

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

Anhang 10

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

- Informationsaustausch mit Partnern

  Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und -stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

- Verarbeitung personenbezogener Daten

  Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

- Ermittlungsindex und Dateien

  Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

- Auskunftsrecht

  Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

- Änderung, Berichtigung und Löschung

  Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

- Speicherungsfristen

  Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z. B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

- Datensicherheit

  Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

- Gemeinsame Kontrollinstanz

  Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindenden Charakter haben.

- Rechtsschutz

  Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

- Rechtsetzungsbedarf

  Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.

  Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

Anhang 11

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2001

Datenschutz beim elektronischen Geschäftsverkehr

Die Konferenz wendet sich mit Entschiedenheit gegen Anträge, die gegenwärtig dem Bundesrat zum Entwurf eines Gesetzes zum elektronischen Geschäftsverkehr (BR-Drs. 136/01) vorliegen. Danach sollen Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste übermittelt werden. Darüber hinaus sollen die Anbieterinnen und Anbieter zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden.

Die Datenschutzbeauftragten weisen darauf hin, dass sich anhand dieser Daten nachvollziehen lässt, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen nachgeht. Eine pauschale Registrierung jeder Inanspruchnahme von Telediensten zur staatlichen Überwachung greift tief in das Persönlichkeitsrecht der betroffenen Nutzerinnen und Nutzer ein und berührt auf empfindliche Weise deren Informationsfreiheit. Der Bundesrat wird daher aufgefordert, diese Anträge abzulehnen.

Anhang 12

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
am 24. April 2001

Veröffentlichung von Insolvenzinformationen im Internet

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, auf Grund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 9. März 1988 – 1 BvL 49/86 – zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 der Insolvenzordnung verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

Anhang 13

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
am 8./9. März 2001

Novellierung des Melderechtsrahmengesetzes

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.
2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf – wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internets durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.
3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.
4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.
5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.
6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist .

Bei Enthaltung Thüringens zu Ziffer 6.

Anhang 14

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“
(Medikamentenchipkarte)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als *Pflichtkarte*. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden *(Grundsatz der Freiwilligkeit)*.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,
- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
- welche ihrer Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und
- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem „Arzneimittelpass“ keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den „Arzneimittelpass“ auf der *Krankenversichertenkarte* gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die „Funktion Krankenversichertenkarte“ von der „Funktion Arzneimittelpass“ informationstechnisch getrennt würde, sodass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu of-

fenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offen legen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z. B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

Anhang 15

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

Zur gesetzlichen Regelung von genetischen Untersuchungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung – in der Strafprozessordnung bereits normiert – sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegenzunehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Anlage zur Entschließung der Datenschutzbeauftragten des Bundes und der Länder zur gesetzlichen Regelung von genetischen Untersuchungen vom 24./25. Oktober 2001

Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen

Allgemeines

Gegenstand

Zu regeln ist die Zulässigkeit genetischer Untersuchungen beim Menschen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten. Neben allgemeinen Regelungen sind besondere Bestimmungen zu genetischen Untersuchungen

1. zu medizinischen Zwecken
2. im Zusammenhang mit Arbeits- und Versicherungsverhältnissen
3. zur Abstammungsklärung und Identifizierung außerhalb der Strafverfolgung
4. zu Forschungszwecken

zu treffen.

Ziel, Benachteiligungsverbot

(1) Ziel der Regelungen ist der Schutz der Menschenwürde, der Persönlichkeit und der informationellen Selbstbestimmung der Betroffenen bei genetischen Untersuchungen.

(2) Niemand darf wegen seiner Erbanlagen oder wegen der Weigerung, eine genetische Untersuchung bei sich durchführen zu lassen, benachteiligt werden.

Begriffe

1. *Genetische Untersuchungen:* Untersuchungen auf Chromosomen-, Genprodukt- oder molekularer DNS/RNS-Ebene, die darauf abzielen, Informationen über das Erbgut zu erhalten;
2. *Prädiktive Untersuchungen:* vor- oder nachgeburtliche genetische Untersuchungen mit dem Ziel, Erbanlagen einer Person, insbesondere Krankheitsanlagen vor dem Auftreten von Symptomen oder einen Überträgerstatus, zu erkennen;
3. *Überträgerstatus:* Erbablagen, die erst in Verbindung mit entsprechenden Erbanlagen eines Partners oder einer Partnerin eine Krankheitsanlage bei den gemeinsamen Nachkommen ausbilden;
4. *Pränatale Untersuchungen:* vorgeburtliche genetische Untersuchungen mit dem Ziel, während der Schwangerschaft Informationen über das Erbgut des Embryos oder des Fötus zu gewinnen;
5. *Reihenuntersuchung:* genetische Untersuchungen, die systematisch der gesamten Bevölkerung oder bestimmten Gruppen der Bevölkerung angeboten werden, ohne dass bei den Betroffenen Anhaltspunkte dafür bestehen, dass die gesuchten Erbanlagen bei ihnen vorhanden sind;
6. *Diagnostische genetische Untersuchungen:* genetische Untersuchungen zur Abklärung der Diagnose einer manifesten Erkrankung oder zur Vorbereitung oder Verlaufskontrolle einer Behandlung;
7. *Probe:* die für eine genetische Untersuchung vorgesehene oder genutzte biologische Substanz;
8. *Genetische Daten:* im Zusammenhang mit genetischen Untersuchungen erlangte Informationen über eine Person;
9. *Betroffene Person:* die Person, von der eine Probe vorliegt oder deren genetische Daten erhoben, verarbeitet oder genutzt werden; bei pränatalen Untersuchungen auch die schwangere Frau.

10. Verarbeiten: das Speichern, Verändern, Übermitteln, Sperren und Löschen erhobener personenbezogener genetischer Daten.

Zulässigkeit genetischer Untersuchungen

Genetische Untersuchungen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten bedürfen der freiwilligen, schriftlichen Einwilligung der betroffenen Person nach Aufklärung. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen zu regelnden und in der Strafprozessordnung geregelten Ausnahmen.

Zulassung zur Durchführung genetischer Untersuchungen

(1) Wer genetische Untersuchungen durchführen will, bedarf hierfür der Zulassung durch die zuständige Aufsichtsbehörde des Landes.

(2) Die Zulassung wird erteilt, wenn Gewähr dafür besteht, dass

- die Untersuchungen und ihre Auswertungen sorgfältig und nach dem Stand von Wissenschaft und Technik durchgeführt werden,
- die Regelungen gemäß diesen Vorschlägen eingehalten, insbesondere Information und Beratung der betroffenen Person und die Datensicherheit gewährleistet werden und
- in der antragstellenden Person die berufsrechtlichen und gewerberechtlichen Voraussetzungen vorliegen.

(3) Das Nähere regelt die Bundesregierung durch Rechtsverordnung.

Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen

Genetische Testverfahren dürfen nur für den Gebrauch durch Ärztinnen, Ärzte oder Labors eingeführt oder in Verkehr gebracht werden. Das öffentliche Angebot, genetische Untersuchungen zu medizinischen Zwecken ohne individuelle Beratung der betroffenen Person durchzuführen, ist unzulässig. Die Berufsfreiheit, Artikel 12 Absatz 1 Satz 2 Grundgesetz, wird insoweit eingeschränkt.

Zweckbindung

Die für die genetische Untersuchung vorgesehene oder genutzte Probe und die genetischen Daten dürfen nur für den Zweck verwandt und für die Dauer aufbewahrt werden, zu denen die betroffene Person ihre Einwilligung erklärt hat oder zu denen ein Gericht oder eine Verwaltungsbehörde eine Anordnung getroffen hat. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen geregelten Ausnahmen.

Datensicherheit

(1) Proben und genetische Daten sind vor dem Zugriff unbefugter Dritter wirksam zu schützen. Dies gilt auch in Bezug auf Mitarbeiterinnen und Mitarbeiter der untersuchenden und Daten verarbeitenden Stelle, die an der genetischen Untersuchung, Aufklärung und Beratung nicht beteiligt sind oder waren.

(2) Genetische Daten sind von anderen Datenarten gesondert zu speichern.

(3) Im Übrigen gilt hinsichtlich der genetischen Daten die Bestimmung des Bundesdatenschutzgesetzes über die technischen und organisatorischen Maßnahmen der Datensicherheit in der jeweils geltenden Fassung.

Einsichts- und Auskunftsrecht

Die betroffene Person hat das Recht, unentgeltlich Einsicht in die Dokumentationen zur genetischen Untersuchung einschließlich Aufklärung und Beratung zu nehmen und Auskunft über die zu ihr gespeicherten Daten zu verlangen.

Genetische Untersuchungen zu medizinischen Zwecken

Grundsatz

(1) Zu medizinischen Zwecken dürfen prädiktive Untersuchungen nur durchgeführt werden, wenn sie nach ärztlicher Indikation der Vorsorge, der Behandlung oder der Familienplanung der betroffenen Person dienen.

(2) Eine genetische Untersuchung zum Erkennen eines Überträgerstatus ist nur zu Zwecken der konkreten Familienplanung zulässig.

(3) Für diagnostische genetische Untersuchungen gelten nur die Anforderungen gemäß dem Arztvorbehalt (siehe unten) und an diagnostische genetische Untersuchungen bei behinderten Personen (siehe am Ende dieses Abschnitts).

Pränatale Untersuchungen

Pränatale Untersuchungen sind auf das Erkennen solcher Krankheiten zu richten, die vorgeburtlich behandelt werden können. Für darüber hinausgehende genetische Untersuchungen gelten die Richtlinien der Bundesärztekammer zur pränatalen Diagnostik. Das Geschlecht darf gezielt nur zu medizinischen Zwecken festgestellt werden.

Ob darüber hinaus auch schwere Behinderungen und Anlagen für schwere, nicht behandelbare Krankheiten Ziele pränataler DNA-Untersuchungen sein dürfen, muss der gesellschaftspolitischen Diskussion, der fachmedizinischen Bewertung und der Verantwortung des Gesetzgebers überlassen bleiben.

Genetische Untersuchungen bei Minderjährigen und nicht einsichtsfähigen Erwachsenen

(1) Genetische Untersuchungen bei Minderjährigen sind nur zulässig, wenn ihre Durchführung vor Erreichen der Volljährigkeit erforderlich ist, um den Ausbruch einer Krankheit zu vermeiden oder zu verzögern, eine Heilung oder Verlaufsmilderung zu erreichen oder spätere besonders belastende Untersuchungen zu vermeiden. Bei Aufklärung, Beratung und Einwilligung (siehe unten) ist die Einsichtsfähigkeit der betroffenen minderjährigen Person zu berücksichtigen.

(2) Prädiktive Untersuchungen bei nicht einsichtsfähigen Erwachsenen dürfen sich nur auf das Erkennen von Krankheiten richten, deren Ausbruch vermieden oder verzögert oder bei denen eine Heilung oder Verlaufsmilderung erreicht werden kann. Die Einwilligung obliegt dem gesetzlichen Vertreter.

Reihenuntersuchungen

(1) Genetische Reihenuntersuchungen bedürfen der Zulassung durch die zuständige Landesbehörde.

(2) Voraussetzung für die Zulassung ist, dass

- die Reihenuntersuchung gerichtet ist auf das Erkennen von verbreiteten oder schweren Krankheiten, die unverzüglich nach dem Untersuchungsergebnis behandelt werden können, oder von Krankheiten, deren Ausbruch verhindert werden kann,
- die Untersuchungsmethode eindeutige Ergebnisse liefert,
- die Freiwilligkeit der Teilnahme und die genetische Beratung gewährleistet und
- der Datenschutz gesichert ist.

Arztvorbehalt

(1) Prädiktive Untersuchungen dürfen nur von Fachärztinnen und Fachärzten für Humangenetik veranlasst werden. Diagnostische genetische Untersuchungen dürfen auch von anderen zur Berufsausübung zugelassenen Ärztinnen und Ärzten veranlasst werden.

(2) Die veranlassende Ärztin oder der veranlassende Arzt hat die Aufklärung und Beratung (siehe nachstehend) und die Einholung und Dokumentation der Einwilligung (siehe unten) sicherzustellen.

Aufklärung und Beratung

(1) Vor und nach einer prädiktiven genetischen Untersuchung ist die betroffene Person umfassend aufzuklären und zu beraten, um ihr eine selbstbestimmte Entscheidung gemäß den Anforderungen an die Einwilligung (siehe unten) zu ermöglichen.

(2) Die betroffene Person und gegebenenfalls ihr gesetzlicher Vertreter muss insbesondere aufgeklärt werden über

- Ziel, Art, Aussagekraft und Risiko der Untersuchung und die Folgen ihrer Unterlassung;
- mögliche, auch unerwartete Ergebnisse der Untersuchung;
- mögliche Folgen des Untersuchungsergebnisses, einschließlich physischer und psychischer Belastungen der betroffenen Person oder ihrer Familie;
- Behandlungsmöglichkeiten für die gesuchte Krankheit;
- den geplanten Umgang mit der Probe und den genetischen Daten einschließlich des Orts und der Dauer der Aufbewahrung bzw. Speicherung;
- die Einflussmöglichkeiten und Datenschutzrechte der betroffenen Person;
- weitere Beratungs- und Unterstützungsmöglichkeiten.

(3) Aufklärung und Beratung dürfen nur der individuellen und familiären Situation der betroffenen Person und den möglichen psychosozialen Auswirkungen des Untersuchungsergebnisses auf sie und ihre Familie Rechnung tragen.

(4) Bei Reihenuntersuchungen kann in begründeten Ausnahmefällen die Aufklärung in standardisierter Form erfolgen, wenn zugleich die Möglichkeit einer zusätzlichen individuellen Beratung angeboten wird.

(5) Bei pränatalen Untersuchungen ist der Partner der betroffenen Frau in die Beratung einzubeziehen, sofern die Frau einwilligt. Auf Stellen der Schwangerschaftskonfliktberatung ist hinzuweisen.

(6) Bei genetischen Untersuchungen zum Erkennen eines Überträgerstatus soll der Partner oder die Partnerin der betroffenen Person in die Aufklärung und Beratung einbezogen werden.

Einwilligung

(1) Nach der Aufklärung und Beratung entscheidet die betroffene Person nach angemessener Bedenkzeit in freier Selbstbestimmung darüber,

- ob die genetische Untersuchung durchgeführt werden soll,
- welches Ziel die genetische Untersuchung hat,
- ob sie auch unvermeidbare weitere Untersuchungsergebnisse zur Kenntnis nehmen will,
- wie gegebenenfalls mit der Probe und den genetischen Daten weiter verfahren werden soll.

Soweit die betroffene Person vom Ergebnis, auf das die Untersuchung zielt, keine Kenntnis nehmen will, soll außer bei Reihenuntersuchungen grundsätzlich auf die genetische Untersuchung verzichtet werden.

(2) Die betroffene Person oder ihr gesetzlicher Vertreter hat die vorherige Aufklärung und Beratung schriftlich zu bestätigen und die Einwilligung in die genetische Untersuchung und in den vereinbarten Umgang mit der Probe und den genetischen Daten schriftlich zu erklären.

(3) Die Einwilligung kann widerrufen werden mit der Folge, dass noch nicht erfolgte Maßnahmen unterbleiben, schon vorliegende Proben vernichtet und die im Zusammenhang mit der Untersuchung erhobenen und gespeicherten Daten gelöscht werden.

Unterrichtung über das Untersuchungsergebnis

(1) Die veranlassende Ärztin oder der veranlassende Arzt teilt das Ergebnis der genetischen Untersuchung nur der betroffenen Person, bei Minderjährigen

auch oder nur ihrem gesetzlichen Vertreter mit und berät über die möglichen Folgen und Entscheidungsalternativen.

(2) Ist das Ergebnis nach ärztlicher Erkenntnis auch für Verwandte der betroffenen Person von Bedeutung, hat die Ärztin oder der Arzt bei der nachgehenden Beratung der betroffenen Person auch auf das Recht der Verwandten hinzuweisen, ihre Erbanlagen nicht zur Kenntnis zu nehmen. Will die betroffene Person die Verwandten gleichwohl unterrichten, soll die Beratung auch die Möglichkeit umfassen, die Ärztin oder den Arzt mit der Unterrichtung von Verwandten der betroffenen Person zu beauftragen.

(3) Gegen den Willen der betroffenen Person oder ihres gesetzlichen Vertreters darf die veranlassende Ärztin oder der veranlassende Arzt Verwandte oder Partner der betroffenen Person nur dann von dem Untersuchungsergebnis unterrichten, wenn und soweit dies zur Wahrung erheblich überwiegender Interessen dieser Personen erforderlich ist.

Diagnostische genetische Untersuchung bei behinderten Personen

Bei diagnostischen genetischen Untersuchungen, die sich auf die Ursache einer Behinderung der betreffenden Person beziehen, gelten die Anforderungen an die Einwilligung und Unterrichtung über das Untersuchungsergebnis entsprechend.

Genetische Untersuchungen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen

Grundsatz

Arbeitgebern und Versicherern ist es verboten, als Voraussetzung für einen Vertragsabschluss oder während des Vertragsverhältnisses prädiktive genetische Untersuchungen an betroffenen Arbeits- oder Versicherungsvertragsbewerbern oder Vertragspartnern durchzuführen oder zu veranlassen oder Ergebnisse von genetischen Untersuchungen zu verlangen, entgegenzunehmen oder sonst zu nutzen. Aus einer wahrheitswidrigen Beantwortung können Arbeitgeber oder Versicherer grundsätzlich keine Rechte ableiten (Ausnahmen siehe unten).

Arbeitsverhältnis

Bleibt der Arbeitsplatz trotz vorrangiger Arbeitsschutzmaßnahmen mit einer erhöhten Erkrankungs- oder Unfallgefahr verbunden, für deren Einritt nach dem Stand der Wissenschaft eine bestimmte Genstruktur der Betroffenen von Bedeutung ist, ist eine Arbeitsplatzbewerberin oder ein Arbeitsplatzbewerber hierauf hinzuweisen. Die Betriebsärztin oder der Betriebsarzt soll die betroffene Person hinsichtlich einer geeigneten genetischen Untersuchung beraten und ihr dafür zugelassene Ärztinnen oder Ärzte benennen.

Ausnahmen für das Versicherungsverhältnis

(1) Strebt die betroffene Person eine Versicherung mit einer Leistungssumme über 250.000 € an, ist der Versicherer berechtigt zu fragen, ob und gegebenenfalls wann bei der betroffenen Person eine prädiktive genetische Untersuchung durchgeführt wurde. Bei arglistigem Verschweigen kann der Versicherer den Versicherungsvertrag kündigen.

(2) Bestehen konkrete Anhaltspunkte, insbesondere auf Grund des Zeitabstandes zwischen genetischer Untersuchung und Versicherungsantrag, dafür, dass die Höhe der gewünschten Versicherungsleistung mit dem Ergebnis der genetischen Untersuchung zusammenhängt, kann der Versicherer das Ergebnis der genetischen Untersuchung verlangen. Dies gilt nicht für eine genetische Untersuchung, die bei der betroffenen Person pränatal oder während der Minderjährigkeit oder einer Einsichtsunfähigkeit durchgeführt wurde. In diesen Fällen darf der Versicherer das Ergebnis der genetischen Untersuchung von der betroffenen Person nicht entgegennehmen.

Genetische Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb der Strafverfolgung

Grundsatz

(1) Zu Zwecken der Abstammungsklärung und der Identifizierung dürfen nur die dazu geeigneten und erforderlichen genetischen Untersuchungen (DNA-Identifizierungsmuster) durchgeführt werden. Diagnostische oder prädiktive Untersuchungen nach Krankheitsanlagen oder Merkmalen der betroffenen Person sind unzulässig. Abgesehen vom Merkmal Geschlecht sind unvermeidliche Überschussinformationen so früh wie möglich zu vernichten.

(2) Die untersuchende Stelle hat selbst die Proben bei der betroffenen Person zu entnehmen und dies zu dokumentieren.

(3) Die Proben sind zu vernichten, wenn die betroffene Person dies wünscht oder ein Gericht die Vernichtung anordnet, im Übrigen wenn die genetische Untersuchung durchgeführt ist. Die Dokumentation ist 10 Jahre aufzubewahren.

Einwilligung

Genetische Untersuchungen zu Zwecken der Abstammungsklärung oder Identifizierung dürfen nur mit schriftlicher Einwilligung der betroffenen Person oder ihres gesetzlichen Vertreters oder auf gerichtliche oder behördliche Anordnung durchgeführt werden. Für genetische Untersuchungen zur Abstammungsklärung bei Minderjährigen gilt § 1629 BGB.

Anordnung genetischer Untersuchungen zu Identifizierungszwecken

(1) In gerichtlichen und Verwaltungsverfahren kann das Gericht bzw. die Verwaltungsbehörde eine genetische Untersuchung zu Identifizierungszwecken anordnen, wenn die Identität einer Partei, eines Beteiligten oder einer für das Verfahren wichtigen dritten Person oder Leiche in Zweifel steht und nicht auf andere Weise geklärt werden kann. Ist die Identitätsfeststellung Voraussetzung für die Gewährung von behördlichen Genehmigungen oder Leistungen an die betroffene Person, ist die genetische Untersuchung nur mit ihrer Einwilligung zulässig.

(2) Die Anordnung hat die Art der Probe, das Ziel der Untersuchung sowie den Zeitpunkt der Vernichtung der Probe und der Löschung der genetischen Daten festzulegen. Bei lebenden Personen ist die Probe ohne Eingriff in die körperliche Unversehrtheit zu entnehmen, es sei denn, die betroffene Person willigt in einen Eingriff ein.

Genetische Untersuchungen zu Forschungszwecken

Konkrete, zeitlich befristete Forschungsvorhaben

(1) Für konkrete, zeitlich befristete Forschungsvorhaben ist die genetische Untersuchung von Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten zulässig, wenn

1. die Proben und die genetischen Daten der betroffenen Person nicht mehr zugeordnet werden können oder
2. im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert, die betroffene Person nach den Anforderungen für Forschungsvorhaben eingewilligt hat (siehe unten) oder
3. im Falle, dass weder auf die Zuordnungsmöglichkeit verzichtet noch die Einwilligung eingeholt werden kann, das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt und der Forschungszweck nicht auf andere Weise zu erreichen ist.

(2) In den Fällen der Ziffer (1) Nr. 2 und 3 sind bei Proben vor der Untersuchung, bei genetischen Daten vor der Verarbeitung oder Nutzung die Merkmale, mit denen ein Personenbezug hergestellt werden kann, gesondert zu speichern. Die Zuordnungsmöglichkeit ist aufzuheben, sobald der Forschungszweck es erlaubt und schutzwürdige Interessen der betroffenen Person gemäß der Regelung über deren Rechte (siehe unten) nicht entgegenstehen.

(3) Die Proben dürfen nur im Rahmen des Forschungsvorhabens untersucht, die genetischen Daten dürfen nur zu den Zwecken verarbeitet oder genutzt werden, für die sie im Rahmen des Forschungsvorhabens erhoben wurden.

(4) Mit Beendigung des Forschungsvorhabens sind die Proben zu vernichten und die genetischen Daten zu löschen. Ist ihre Aufbewahrung oder Speicherung zum Zwecke der Selbstkontrolle der Wissenschaft erforderlich, ist dies in pseudonymisierter Form für einen Zeitraum von längstens 10 Jahren zulässig.

(5) Konkrete, zeitlich befristete Forschungsvorhaben nach Ziffer (1) bedürfen der vorherigen Zustimmung der zuständigen Ethikkommission.

Sammlungen von Proben und genetischen Daten

(1) Das Sammeln von Proben einschließlich isolierter DNS oder RNS oder von genetischen Daten zu allgemeinen Forschungszwecken ist nur zulässig, wenn die betroffenen Personen über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurden und in die Entnahme der Probe sowie die Aufnahme von Probe und Daten in die Sammlung eingewilligt haben (siehe unten). Satz 1 gilt entsprechend für die Übernahme bereits vorhandener Proben oder genetischer Daten.

(2) Die Zuordnung der Probe und der genetischen Daten zur betroffenen Person ist vor der Aufnahme in die Sammlung aufzuheben. Erfordert der Zweck der Sammlung die Möglichkeit einer Zuordnung, sind die Proben und die genetischen Daten vor der Aufnahme in die Sammlung bei Treuhändern zu pseudonymisieren.

(3) Vor einer Weitergabe von Proben und einer Übermittlung genetischer Daten für konkrete Forschungsvorhaben ist die Möglichkeit der Zuordnung zur betroffenen Person aufzuheben oder, wenn der Forschungszweck dem entgegensteht, eine weitere Pseudonymisierung gemäß den Regelungen bei Treuhändern (siehe unten) vorzunehmen.

(4) Der Träger einer Sammlung hat eine kontinuierliche interne Datenschutzkontrolle sicherzustellen. Bei Trägerwechsel gehen alle Verpflichtungen aus diesem Gesetz auf den neuen Träger über. Soll eine Sammlung beendet werden, sind die Proben zu vernichten und die genetischen Daten sowie die beim Treuhänder (siehe unten) gespeicherten Daten zu löschen.

(5) Die Einrichtung einer neuen und die Übernahme einer bestehenden Sammlung nach Ziffer (1) bedürfen der Zustimmung durch die zuständige Ethikkommission. Die Einrichtung ist mit dem Votum der Ethikkommission und unter Darlegung der in den Vorschlägen zur Sammlung von Proben und genetischen Daten, zur Aufklärung und Einwilligung, über die Rechte der betroffenen Person und über die Treuhänder geforderten Maßnahmen bei der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen. Betriebs- und Geschäftsgeheimnisse sind kenntlich zu machen. Die Anzeige ist jeweils nach 5 Jahren mit einer Begründung der weiteren Speicherung zu erneuern. Ebenso sind die Vernichtung oder Löschung von Sammlungen nach Ziffer (1), die Löschung der Zuordnungsmerkmale bei Treuhändern und Trägerwechsel nach Ziffer (4) anzuzeigen.

Aufklärung und Einwilligung

(1) Die betroffene Person ist vor ihrer Einwilligung im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert (siehe oben), oder bei Sammlungen von Proben oder genetischen Daten (siehe oben) insbesondere aufzuklären über

- den verantwortlichen Träger des Forschungsvorhabens oder der Sammlung,
- das Ziel der Forschung oder bei Sammlungen die möglichen Forschungsrichtungen,
- ihre Rechte bei Patentanmeldungen und gewerblichen Nutzungen,
- die Dauer der Aufbewahrung von Proben und der Speicherung der genetischen Daten,
- Zeitpunkt und Art der Pseudonymisierung von Proben und genetischen Daten sowie über die mögliche Wiederherstellung der Zuordnung zur betroffenen Person,

– ihr Recht – vorbehaltlich der pseudonymisierten Verarbeitung nach Beendigung des Forschungsvorhabens (siehe oben) –, die Vernichtung der Probe und die Löschung der genetischen Daten oder die Aufhebung der Zuordnungsmöglichkeit zu verlangen, wenn sie die Einwilligung widerruft,

– ihr Recht, Ergebnisse von Untersuchungen nicht zur Kenntnis zu nehmen oder unter Nutzung eines darzustellenden Ent-Pseudonymisierungsverfahrens zu erfahren,

– ihr Recht, Auskunft über die zu ihr gespeicherten genetischen Daten zu verlangen.

Die Aufklärung hat schriftlich und mündlich zu erfolgen.

(2) Die Einwilligung soll die Entscheidung darüber umfassen, ob die betroffene Person vom Ergebnis der Untersuchung Kenntnis nehmen will oder nicht.

(3) Die Einwilligung kann eine Schweigepflichtentbindung für zu benennende behandelnde Ärzte einschließen, wenn die betroffene Person über Art und Umfang der Patientendaten informiert wird, die der Arzt für das Forschungsvorhaben (siehe oben) oder die Sammlung von Proben oder genetischen Daten (siehe oben) übermittelt.

Rechte der betroffenen Person

(1) Hinsichtlich der genetischen Daten stehen der betroffenen Person die im Bundesdatenschutzgesetz geregelten Rechte zu. Widerruft die betroffene Person ihre Einwilligung (siehe oben), sind entweder die Probe zu vernichten und die genetischen Daten zu löschen oder die Zuordnungsmerkmale zu löschen.

(2) Erbringt ein Forschungsvorhaben Ergebnisse, die für die betroffene Person von Bedeutung sind, veranlasst der Träger des Forschungsvorhabens eine Unterrichtung der betroffenen Person. Dies gilt nicht, wenn die betroffene Person erklärt hat, von dem Untersuchungsergebnis keine Kenntnis nehmen zu wollen (siehe oben).

Treuhänder

(1) Die Pseudonymisierung von Proben und genetischen Daten erfolgt durch einen Treuhänder. Er vergibt die Pseudonyme unverzüglich, verwahrt und verwaltet die Zuordnungsmerkmale und sichert die Rechte der betroffenen Person (siehe oben). Soweit erforderlich, kann er für diese Zwecke Kontakt mit der betroffenen Person aufnehmen. Er hat keinen Zugriff auf genetische Daten.

(2) Treuhänder kann eine natürliche Person sein, die von Berufs wegen einer besonderen Schweigepflicht unterliegt und vom Träger des Forschungsprojekts oder der Sammlung von Proben oder genetischen Daten unabhängig ist. Im Vertrag zwischen dem Treuhänder und dem Träger des Forschungsvorhabens oder der Sammlung von Proben oder genetischen Daten sind insbesondere die Anlässe und das Verfahren zur Wiederherstellung des Personenbezuges, die Nutzungsformen durch die Selbstkontrollgremien der Wissenschaft sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit festzulegen. Der Vertrag ist vorab der für die Datenschutzkontrolle zuständigen Behörde vorzulegen.

Schlussvorschläge

Ordnungswidrigkeit

Ordnungswidrig handelt, wer

– eine Reihenuntersuchung ohne die erforderliche Zulassung durchführt oder

– den Anzeigepflichten bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung von Proben oder genetischen Daten oder bei bestehenden Proben- oder genetischen Datensammlungen nicht fristgemäß nachkommt.

Straftaten

(1) Wer genetische Testverfahren unter Verstoß gegen die Anforderungen an das Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen einführt oder in Verkehr bringt oder genetische Untersuchungen ohne eine individuelle Beratung öffentlich anbietet, wird mit ... ... bestraft. Handelt die Täterin oder der Täter gewerbsmäßig, ist die Strafe ... .

(2) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu medizinischen Zwecken durchführt, ohne

- Arzt oder Ärztin zu sein,
- die für die genetischen Untersuchungen zu medizinischen Zwecken festgelegten Beschränkungen der Untersuchungszwecke einzuhalten,
- die geforderte Aufklärung und Beratung unternommen bzw. sichergestellt zu haben oder
- die Einwilligung der betroffenen Person eingeholt zu haben,

wird mit ... ... bestraft.

(3) Wer als Arbeitgeber oder als Versicherer gegen das Verbot genetischer Untersuchungen verstößt, ohne dass die vorgesehene Ausnahmeregelung eingreift, wird mit ... ... bestraft.

(4) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu Zwecken der Abstammungsklärung oder Identifizierung in unzulässiger Weise auf prädiktive oder diagnostische Ziele ausrichtet oder ohne die geforderte Einwilligung durchführt, wird mit ... ... bestraft.

(5) Wer vorsätzlich oder fahrlässig personenbeziehbare Proben, DNS-/RNS-Teile oder genetische Daten entgegen den Regelungen für genetische Untersuchungen zu Forschungszwecken

- ohne Einwilligung oder Aufklärung zu Forschungszwecken nutzt oder
- in Sammlungen für Forschungszwecke zur Verfügung stellt,

wird mit ... ... bestraft.

Antrag

Die oben aufgeführten Straftaten werden nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person und die für die Datenschutzkontrolle zuständige Behörde.

Befristung

Die Regelungen sind auf zehn Jahre zu befristen. Acht Jahre nach Inkrafttreten haben die für die Datenschutzkontrolle zuständigen Behörden unter Federführung des Bundesbeauftragten für den Datenschutz dem Gesetzgeber einen Bericht über die Wirksamkeit der vorgeschlagenen Regelungen und über neue Gefährdungen für das Persönlichkeitsrecht sowie zu möglichen Rechtsvereinfachungen vorzulegen. Diesem Bericht sind Stellungnahmen des Ethikrates und der Deutschen Forschungsgemeinschaft beizufügen.

Übergangsvorschrift

Träger von bestehenden Proben- und genetischen Datensammlungen haben der Anzeigepflicht bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung innerhalb von sechs Monaten nach Inkrafttreten dieses Gesetzes nachzukommen. Innerhalb dieser Frist ist den Anforderungen an die Einwilligung zu entsprechen. Vor Inkrafttreten dieses Gesetzes ohne Einwilligung gewonnene Proben und erhobene genetische Daten sind spätestens nach zwei Jahren zu vernichten bzw. zu löschen. Dies ist der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen.

Anhang 16

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2001

Zur Lkw-Maut auf Autobahnen und zur allgemeinen Maut auf privat errichteten Bundesfernstraßen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten. Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechungszwecke verwendet werden.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen. Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbeziehbarer Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.
- Es ist sicherzustellen, dass anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

Anhang 17

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2001

Äußerungsrecht der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne – wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen – vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.

Anhang 18

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2001

Informationszugangsgesetze

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien Zugang zu behördeninternen, amtlichen Informationen nicht entgegensteht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der Voraussetzung entsprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.