Landtag von Baden-Württemberg **Drucksache 12 / 5740**

12. Wahlperiode **04. 12. 2000**

Mitteilung

des Landesbeauftragten für den Datenschutz

Einundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 4. Dezember 2000:

Anbei übersende ich Ihnen den 21. Tätigkeitsbericht meines Amts, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag zu erstatten ist.

Schneider

Eingegangen: 04. 12. 2000 / Ausgegeben: 19. 12. 2000

Einundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

1. Teil: Zur Situation

1. Wie geht es weiter? 6
2. Das Amt 7

2. Teil: Technik und Organisation

1. E-Government 8
   1.1 Elektronische Bürgerdienste in Baden-Württemberg 8
   1.2 Bereitstellung der erforderlichen Chipkarten 9
2. Internet-Probleme 9
   2.1 Firewall-Outsourcing 10
   2.2 Computerviren – ein hartnäckiges Problem 10
   2.3 Höhere Sicherheit vor Viren und anderen Schadensprogrammen 11
   2.4 Cookies 12
3. Fernsteuerungssoftware 13
4. Telearbeit 14
5. Auftragsdatenverarbeitung 17
   5.1 Outsourcing der Bürokommunikation 17
   5.2 Outsourcing des Landesverwaltungsnetzes 18
   5.3 Das Gemeinschaftsprojekt Polizei-Online 18
   5.4 Test mit Echtdaten der Polizei 19
6. Chipkarten 20
   6.1 Gesetzliche Anforderungen an Chipkarten 20
   6.2 Chipkarteneinsatz bei einer Fachhochschule 21

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit 23
1. Datenschutz im Krankenhaus 23
   1.1 Verarbeitung von Patientendaten außerhalb des Krankenhauses: Was geht wie und was geht nicht? 23
   1.2 Wozu die Staatsangehörigkeit? 25
   1.3 Der bedürftige Krankenhauspatient 26
   1.4 ... nur eine Tür 27
2. Gesundheitsdatenschutz im Regierungspräsidium 28
   2.1 Postlauf versus Datenschutz? 28
   2.2 Der Briefkasten 29
   2.3 Nicht nur Behörden sind Sünder! 29
3. Das Gesundheitsamt 30
   3.1 Der Kontrollbesuch 30
      3.1.1 Das Gesundheitsamt vergisst nichts 30
      3.1.2 Der fehlerhafte EDV-Einsatz 32
   3.2 Wie ein Gesundheitsamt über das Ziel hinausschoss 33
4. Datenschutz in der medizinischen Forschung 33

2. Abschnitt: Die Sozialversicherung 34
1. Kranken- und Pflegeversicherung 34
1.1 Jedes Jahr die gleiche Frage: Was darf die Krankenkasse wissen und was nicht? 34
1.1.1 Sozialbericht der Drogenberatungsstelle 35
1.1.2 Ärztlicher Entlassungsbericht der Reha-Einrichtung 36
1.2 Neue Aufgaben für den MDK – das Arzneimittel-Clearing 37
1.3 Beitragsüberwachung des Rentenversicherungsträgers bei der Pflegekasse 38
1.4 Der vergebliche Widerspruch 38
2. Die Kassenärztlichen Vereinigungen 39
2.1 J 06.9 oder: Wer schafft den „gläsernen" Patienten? 39
2.2 Die Drogenersatztherapie 40

3. Abschnitt: Soziales 41
1. Aus der täglichen Arbeit der Sozialämter 41
1.1 Von der Wiege bis zur Bahre: Formulare, Formulare! 42
1.2 Kfz-Halteranfragen durch Online-Zugriff 43
1.3 Sorgfältiger arbeiten! 44
2. Nochmals: Die Gemeinden als Sozialämter? 45
3. Aus der Arbeit der Jugendämter 46
3.1 Der Vordruck in der Jugendhilfe 46
3.2 Der getäuschte Arbeitgeber 46
3.3 Wo ist das Jugendamt? 47
3.4 Datenschutz auch bei der Familienhilfe! 48
3.5 Die Pflegefamilie und der Sozialdatenschutz 49
3.6 Schweigepflicht des Berufspsychologen gegenüber seinem Vorgesetzten 50

4. Teil: Justiz und Polizei

1. Abschnitt: Die Justiz 51
1. Die vereitelte Kontrolle beim Verwaltungsgericht Stuttgart 53
2. Das Schlichtungsverfahren – wo bleibt der Datenschutz? 55
3. DNA-Analysen im Ermittlungsverfahren 56
4. Ärztliche Schweigepflicht ausgehebelt 58
5. Macht der Gewohnheit? 59

2. Abschnitt: Die Polizei 61
1. Videoüberwachung von Kriminalitätsbrennpunkten 61
2. Aussonderungsprüffristen für polizeiliche personenbezogene Sammlungen 63
3. Einzelfälle 65
3.1 Ein Schwachpunkt des Schengener Informationssystems und seine Notlösung 65
3.2 In der PAD gelöscht 66

5. Teil: Andere Bereiche

1. Abschnitt: Kommunales 68
1. Meldewesen 68
1.1 Adressen von Wahlberechtigten – Begehrte Objekte 68
1.2 Der Widerspruch gegen die Veröffentlichung im Adressbuch – formlos, fristlos und manchmal fruchtlos 69
1.3 Melderegisterauskünfte an der Meldebehörde vorbei – genial oder rechtswidrig? 70
2. Umgang mit Abbuchungsermächtigungen fehlerhaft 70
3. Nachdenken! 71

2. Abschnitt: Personalwesen 72
1. Die aufgeblähte Personalnebenakte 72
1.1 Das alte Lied und Leid mit dem Personalbogen 73
1.2 Der Lebenslauf – gebräuchlich, aber fehl am Platz 73
1.3 Ärztliche Zeugnisse 73
2. Suchtprobleme coram publico? 74
3. Kein Datenschutz in der Familie? 75

3. Abschnitt: Schulen und Hochschulen 75
1. Antworten der Schüler sind gefragt 75
1.1 IGLU mit kleinen Mängeln 76
1.2 Runde Tische ecken an 76
2. Prüfungsergebnisse via Internet 78

4. Abschnitt: Die Archive 78
1. Die Zwangsarbeiter 78
1.1 Wohin mit den Unterlagen? 78
1.2 Die Arbeitgeber 79
2. Das Archiv als Hilfsregistratur 79

5. Abschnitt: Das Finanzamt 80
1. Fair zum Steuerbürger! 80
2. Und sie bewegt sich doch! 81

Inhaltsverzeichnis des Anhangs 83

1. Teil: Zur Situation

1. Wie geht es weiter?

Es ist schon eine eigenartige Situation. Da werden im Bund und in den Ländern Datenschutzgesetze geändert, und kaum jemand redet darüber. Den Medien sind diese Gesetzesvorhaben allenfalls eine kurze Notiz wert. Welch Gegensatz zu den Auseinandersetzungen, die in der Vergangenheit bei der Novellierung von Datenschutzgesetzen geführt worden sind. Zu verstehen ist dieses Phänomen allemal, denn die Gesetzesänderungen, die – wie z. B. in Baden-Württemberg – bereits beschlossen sind oder noch zur Beschlussfassung anstehen, sind wahrlich nicht dazu angetan, darüber große Debatten zu führen. Letztlich handelt es sich bei ihnen nämlich in den Augen vieler im Wesentlichen nur um ungeliebte, von der Europäischen Gemeinschaft auferlegte Pflichtübungen, denen man sich nicht entziehen kann, sondern die man nolens volens akzeptieren muss. Damit haben sie sicher nicht ganz Unrecht. Zwar ist anzuerkennen, dass in einigen Punkten sehr wohl Fortschritte in Richtung besserer Datenschutz erzielt worden sind und noch erzielt werden sollen. Aber alles in allem muss die Bilanz dieser Gesetzgebungsaktivitäten doch einigermaßen ernüchternd ausfallen. Der große Wurf, ein Quantensprung nach vorn fand und findet nicht statt. Das war von der Politik auch gar nicht beabsichtigt.

Diesen mangelnden Ehrgeiz kann man nur bedauern, denn eines müsste klar sein: Das Datenschutzrecht in der Bundesrepublik bedarf einer grundlegenden Revision. Es ist unübersichtlich, inhomogen und vielfach nicht in sich stimmig geworden. Dies erschwert es den Bürgern, den Datenschutz zu verstehen und mindert deshalb seine Akzeptanz. Aber auch die Daten verarbeitenden Stellen und die dort beschäftigten Personen selbst haben vielfach Probleme damit zu erkennen, was sie tun dürfen und was nicht. Das Datenschutzrecht hat sich zu einem Rechtsgebiet für Spezialisten entwickelt. Ich führe dies ganz wesentlich auf einen Webfehler zurück, der dem modernen Datenschutzrecht seit seiner Entstehung in den 70er Jahren anhaftet. Als damals die erste Generation der Datenschutzgesetze entstand, war es ja keineswegs so, dass damit völliges Neuland in Sachen Datenschutz betreten wurde. Vielmehr gab es schon zur damaligen Zeit eine Vielzahl von Rechtsvorschriften, die regelten, wie mit personenbezogenen Daten umgegangen werden darf. Alle diese Regelungen in die Datenschutzgesetze zu integrieren, wäre schlicht und einfach nicht machbar gewesen. Deshalb beschränkte man sich darauf, die Datenschutzgesetze als Auffang-Gesetze zu konzipieren, die einen gewissen Mindeststandard an Datenschutz garantieren und im Übrigen nur Wirkung zeigen sollten, soweit der Umgang mit personenbezogenen Daten nicht bereits in anderen Rechtsvorschriften geregelt ist. Vom Prinzip her war und ist kaum eine andere Konzeption denkbar. Ein sich auf die Weiterentwicklung des Datenschutzrechts verhängnisvoll auswirkender Fehler wurde dann nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dez. 1983 begangen. Anstatt dieses Urteil, das ja den Datenschutz auf eine ganz neue Grundlage gestellt hatte, zum Anlass zu nehmen, zunächst einmal die Datenschutzgesetze den vom Bundesverfassungsgericht festgestellten Anforderungen unserer Verfassung anzupassen und dann darauf aufbauend nach möglichst einheitlichen Kriterien für einzelne Bereiche deren Besonderheiten Rechnung tragende sog. bereichsspezifische Regelungen zu treffen, ging man leider den umgekehrten Weg. Man begann, ohne erkennbares System, quasi willkürlich mit der Schaffung eben solcher speziellen Regelungen in zahlreichen Einzelgesetzen mit dem Ergebnis, dass sich das Datenschutzrecht heute wie ein Flickenteppich mit vielen großen und kleinen Löchern darstellt.

Ein weiterer Aspekt, der eine grundlegende Revision des Datenschutzrechts notwendig macht, kommt hinzu: Die Entwicklung der Informations- und Kommunikationstechnik und ihr rasant zunehmender Einsatz in allen Lebensbereichen zwingt dazu, überkommene Strukturen und Verhaltensweisen zu überdenken und sich zu überlegen, mit welchen Instrumenten den sich aus ihrem Einsatz ergebenden Risiken für das Persönlichkeitsrecht der Menschen am besten begegnet werden kann.

Die EG-Datenschutzrichtlinie vom 24. Okt. 1995 und die sich daraus ergebende Notwendigkeit, das derzeitige Datenschutzrecht ihren Anforderungen anzupassen, hätte eigentlich ein guter Anlass für eine solche Generalrevision des Datenschutzrechts sein können. Doch leider wurde diese Chance vertan, ganz einfach deshalb, weil die Vorgängerin der jetzigen Bundesregierung keine Notwendigkeit zu einer solch umfassenden Überarbeitung sah und sich deshalb von vornherein darauf beschränken wollte, nur das zu regeln, was wegen der EG-Datenschutzrichtlinie unbedingt zu regeln war. Da ihr aber nicht einmal dies gelang, steht die jetzige Bundesregierung unter Zeitdruck, denn der Termin, bis zu dem die Anpassung hätte erfolgen müssen, ist schon längst verstrichen. Die Folge ist, dass die Änderungen, die das Bundesdatenschutzgesetz in Bälde erfahren wird, neben der notwendigen Anpassung an die EG-Datenschutzrichtlinie nur einige wenige, im Übrigen aber durchaus begrüßenswerte Verbesserungen mit sich bringen werden. Nur, an der Notwendigkeit der Generalrevision ändert sich dadurch nichts. Das sieht auch die Bundesregierung so. Sie will deshalb in einer zweiten Stufe eine Neustrukturierung des Datenschutzrechts in Angriff nehmen. Angesichts der Komplexität der Materie ist dies gewiss eine äußerst schwierige Aufgabe. Ganz sicher kann dabei nicht allen, teilweise recht hoch geschraubten Erwartungen, die daran geknüpft werden, Rechnung getragen werden, zumal ja auch die Interessenlage der daran Beteiligten und der davon Betroffenen höchst unterschiedlich ist. Begrüßenswert und einen Versuch wert ist ein solches Vorhaben aber allemal. Es betrifft zwar zunächst unmittelbar nur das Bundesrecht. Die dabei erzielten Ergebnisse werden aber zweifellos auch Auswirkungen auf die Weiterentwicklung des Datenschutzrechts von Baden-Württemberg haben.

2. Das Amt

Das wichtigste Ereignis im Berichtsjahr war die durch die EG-Datenschutzrichtlinie notwendig gewordene Novellierung des Landesdatenschutzgesetzes. Was aus meiner Sicht zum Gesetzentwurf der Landesregierung zu sagen war, habe ich in meinem letzten Tätigkeitsbericht (LT-Drs. 12/4600, S. 10) im Einzelnen ausgeführt. Meine Bemühungen, im Rahmen der parlamentarischen Beratungen des Gesetzentwurfs wenigstens noch die eine oder andere Verbesserung zu erreichen, fanden im Landtag leider nicht die notwendige Unterstützung. Der Regierungsentwurf wurde so auch als Gesetz beschlossen. Schade, eine gute Gelegenheit, den Datenschutz zu stärken, blieb ungenutzt. Die Novelle ist am 1. Sept. 2000 in Kraft getreten. Man wird abwarten müssen, wie die Praxis damit zurechtkommt.

Nach Max Weber bedeutet Politik ein starkes, langsames Durchbohren von harten Brettern mit Leidenschaft und Augenmaß zugleich. Besser kann man eigentlich auch die Arbeit der Datenschutzkontrolle nicht umschreiben. Wer glaubt, schnell, ohne große Anstrengung und Mühe spektakuläre Erfolge erzielen zu können, ist hier fehl am Platze. Bei dieser Aufgabe braucht man Geduld und einen langen Atem, muss mit Rückschlägen leben und immer neue Anläufe nehmen. Das zeigte sich auch wieder im Berichtsjahr. Ein Schwerpunkt der Kontrollen war die Frage, wie Behörden Informationen bei Bürgern anfordern. Ob sie sich an die dafür geltenden Spielregeln halten und ob sie die Bürger insbesondere so über ihre Rechte und Pflichten informieren, dass diese sich in Kenntnis der Sach- und Rechtslage entscheiden können, ob sie die gewünschten Informationen zur Verfügung stellen wollen. Wie sich insbesondere im Bereich der Sozial- und Jugendhilfe, aber auch anderswo gezeigt hat, bestehen hier noch erhebliche Defizite. In einer Zeit, in der zu Recht eine bürgerfreundliche Verwaltung angemahnt, der Dienstleistungscharakter der Verwaltung betont wird und, in völliger Verkennung der Bedeutung dieses Begriffs, Bürger zu Kunden erklärt werden, habe ich dafür wenig Verständnis. Freilich, um den durch das Datenschutzrecht gestellten Anforderungen an die Aufklärung der Bürger über ihre Rechtsstellung gerecht zu werden, bedarf es mühsamer Kleinarbeit und exakter Einarbeitung in die maßgeblichen Rechtsvorschriften. Eine Verwaltung, die den Anspruch erhebt, den Bürger ernst zu nehmen, muss sich gleichwohl dieser Aufgabe stellen und so zeigen, dass sie gewillt ist, diesem Anspruch Rechnung zu tragen, auch wenn damit keine wählerwirksame Publicity zu erzielen ist.

Die Kontrollerfahrungen sind wie immer zwiespältig. Wie schon in der Vergangenheit wechseln sich Licht und Schatten ab. In manchen Fällen bedarf es schon einiger Anstrengungen, um überhaupt die gewünschten Antworten und Stellungnahmen zu erhalten. In anderen wiederum rennen wir offene Türen ein. Gar nicht so selten dürfen wir uns über Erfolgserlebnisse freuen, Ereignisse, die uns manche Enttäuschung verschmerzen lassen und Mut machen, unsere Arbeit fortzusetzen.

Einen immer größeren Umfang nimmt die Beratungstätigkeit an, bei der es keineswegs nur um größere Projekte wie etwa das Outsourcing der Bürokommunikation in der Landesverwaltung, die IKNPOL-Dezentralisierung der Polizei, die Einführung Neuer Steuerungsinstrumente in der Landesverwaltung oder die Entwicklung eines einheitlichen Personalverwaltungssystems für die Landesverwaltung geht. Der Sachverstand meines Amtes ist vielmehr auch gefordert bei vielen Anfragen zu Einzelproblemen sowohl von Behörden als auch von anderen öffentlichen Stellen. Ob Bürgermeisterämter, Krankenhäuser, Ministerien, Kfz-Zulassungsstellen oder Schulen, für alle ist mein Amt zum Ansprechpartner geworden, an den man sich wenden kann, wenn man Beratungsbedarf hat. Leider sind wir nicht immer in der Lage, das zu leisten, was von uns erwartet wird, und zwar schlicht und einfach deshalb, weil uns das dazu notwendige Personal fehlt. Auf diesen Mangel habe ich bereits in meinem letzten Tätigkeitsbericht (LT-Drs. 12/4600, S. 11) hingewiesen. Meine dort zum Ausdruck gebrachte Erwartung, im Rahmen der Beratungen des Haushaltsplans für die Jahre 2000/2001 wenigstens eine zusätzliche Stelle für einen Informatiker zu erhalten, ist leider nicht in Erfüllung gegangen, obwohl ich im Landtag, von einer offensichtlich desinformierten Ausnahme abgesehen, nur Stimmen gehört habe, die für mein Anliegen Verständnis gezeigt haben. Dies lässt mich hoffen, dass ihm in absehbarer Zeit vielleicht doch noch entsprochen wird.

2. Teil: Technik und Organisation

1. E-Government

Wer ein Buch bestellen, seinen aktuellen Kontostand abfragen oder Geld überweisen möchte, kann dies längst auch über das Internet tun. Tele-Banking und E-Commerce machen es möglich. Die öffentliche Verwaltung will da nicht zurückstehen und plant ebenfalls, ihre Dienstleistungen elektronisch anzubieten. E-Government lautet das Ziel. Und dabei soll weit mehr möglich sein als das einfache Abrufen von Informationen und Formularen. Geplant ist, dass Bürger elektronische Anträge mit einer digitalen Signatur versehen an die Behörden senden und auf gleichem Wege Antwort von der Behörde erhalten können. Bis der elektronische Austausch von rechtsverbindlichen Anträgen und Bescheiden zum Behördenalltag gehören wird, sind allerdings noch einige Hürden zu überwinden. Kernproblem ist die Einführung digitaler Signaturen. Dazu hat der Bund schon vor einiger Zeit im Signaturgesetz einen Standard für zuverlässige und sichere digitale Signaturen festlegt. Da das Signaturgesetz jedoch nichts darüber aussagt, in welchen Bereichen des täglichen Lebens handschriftliche Unterschriften durch digitale Signaturen ersetzt werden können, sind noch entsprechende Gesetzesänderungen nötig, bevor Behörden digital signierte Anträge der Bürger entgegennehmen und bearbeiten können. Angesichts der wachsenden Bedeutung elektronischer Behördengänge haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (vgl. Anhang 10) deutlich gemacht, dass sie dieser Entwicklung, die mehr Bürgernähe bewirken kann, positiv gegenüberstehen. Da Bürger und Behörden die Gewähr haben müssen, dass sowohl ihre Anträge als auch die Bescheide der Behörden unterwegs nicht von Personen gelesen werden können, für die sie nicht bestimmt sind, und unverfälscht den jeweiligen Adressaten erreichen, stellen Datenschutz und Datensicherheit entscheidende Voraussetzungen für die Zulässigkeit und Akzeptanz dieser neuen Angebote dar.

1.1 Elektronische Bürgerdienste in Baden-Württemberg

Einen bedeutenden Schritt hin zur Realisierung elektronischer Bürgerdienste ging das Land, indem es in diesem Jahr das e-Bürgerdienste-Gesetz verabschiedete, das die Verwendung digitaler Signaturen in acht

Verwaltungsbereichen gestattet. Dieses Gesetz gibt dazu allerdings nur einen groben Rahmen vor. Weitere Details müssen, bevor die einzelnen Bürgerdienste genutzt werden können, noch vom jeweiligen Fachministerium in einer Verordnung festgelegt werden. Für den Bereich des Meldewesens liegt bereits ein vom Innenministerium ausgearbeiteter Entwurf einer Verordnung vor. An dessen Abfassung hat mein Amt beratend mitgewirkt. Dabei konnte mit dem Innenministerium Übereinstimmung über die festzulegenden technischen und organisatorischen Sicherheitsmaßnahmen erzielt werden:

- Da bei im Internet übertragenen Daten die Gefahr besteht, dass sie mitgelesen werden, sind sie während des Transports zu verschlüsseln.
- Die Meldebehörde muss nachweisen können, dass die eingesetzte Technik den Anforderungen des Signaturgesetzes entspricht, die eingesetzten Programme ordentlich freigegeben worden sind und ordnungsgemäß betrieben werden.
- Ferner muss die Meldebehörde festlegen, auf welche Weise sie die Identität des Meldepflichtigen anhand der digitalen Signatur überprüft und welche zu dessen Identifizierung notwendigen Angaben sie wie lange speichert.

Es ist damit zu rechnen, dass die Verordnung in Bälde in Kraft treten wird.

1.2 Bereitstellung der erforderlichen Chipkarten

Wollen Internet-Nutzer rechtsverbindliche Anträge und Erklärungen abgeben können, genügt es nicht, über einen Standard-PC mit Internet-Anschluss zu verfügen. Da sich Signaturen, die mit dem Signaturgesetz konform gehen, nur mit Hilfe einer Chipkarte erzeugen lassen, muss an den heimischen PC ein Chipkartenlesegerät angeschlossen werden. Ferner müssen Trust Center zur Verfügung stehen, die Chipkarten unter Beachtung strenger Sicherheitsanforderungen herstellen und für deren Zuordnung zu den jeweiligen Nutzern garantieren. Unvermeidlich kommen damit auch Kosten auf alle Bürger zu, die solche Bürgerdienste nutzen wollen. Allein schon aus diesem Grund ist es nicht vorstellbar, dass jede Behörde eine eigene Chipkarte ausgibt. Deshalb überlegt man, eine sog. Baden-Württemberg-Card zu realisieren, mit der staatliche und kommunale E-Bürgerdienste in ganz Baden-Württemberg genutzt werden können. Aber selbst wenn dies geschieht ist fraglich, ob viele Bürger eine Karte erwerben würden, die nur für Verwaltungsdienstleistungen nutzbar ist. Das Innenministerium favorisiert daher, die zur Signatur erforderlichen Funktionen auf Chipkarten zu realisieren, die bereits von anderen Stellen, etwa den Banken und Sparkassen, an ihre Kunden ausgegeben werden und dadurch schon weit verbreitet sind. Aus Sicht des Datenschutzes ist in diesem wie auch in anderen Fällen der Nutzung sog. multifunktionaler Chipkarten darauf zu achten, dass im Zuge jeder einzelnen Nutzungsart jeweils nur auf die dafür bestimmten Daten und Funktionen einer Chipkarte zugegriffen werden kann.

2. Internet-Probleme

Fast schon gebetsmühlenartig weisen Datenschutzbeauftragte und Sicherheitsexperten seit Jahren darauf hin, dass der Anschluss an das Internet mit erheblichen Risiken für den Datenschutz und die Datensicherheit verbunden ist. Erfreulicherweise sind mittlerweile die meisten das Internet nutzende Stellen von der Notwendigkeit überzeugt, Firewalls einzusetzen, um ihr eigenes Netz vor Angriffen aus dem Internet zu schützen. Darüber, wie ein solcher Anschluss am besten realisiert werden kann, beriet mein Amt zwei Ministerien. Dass es aber nicht ausreicht, sich nur auf die Firewall zu verlassen, zeigte sich deutlich bei der Verbreitung des „I love you“-Virus, das auch PC befiel, deren Internet-Anschluss durch eine Firewall gesichert war. Die Zunahme insbesondere der sog. Makro-Viren erfordert verstärkte Anstrengungen, um auch künftig einen gesicherten Internet-Anschluss realisieren zu können. Gefahren für den Datenschutz, wenn auch ganz anderer Art, gehen von den im Internet verwendeten Cookies aus. Sie können zur Bildung von Persönlichkeitsprofilen verwendet werden. Doch nun der Reihe nach:

2.1 Firewall-Outsourcing

Ein Ministerium möchte, dass künftig ein privates Unternehmen seine Firewall betreibt. Im Rahmen einer beratenden Stellungnahme machten wir auf einige Defizite seines Firewall-Betriebskonzeptes aufmerksam:

– Festlegungen teilweise unverbindlich

Einige der für den Betrieb der Firewall wichtigen Festlegungen waren in unverbindliche „kann-“ oder „sollte-“Aussagen gekleidet. Stattdessen ist es aber erforderlich, klare und verbindliche Festlegungen im Betriebskonzept zu treffen.

– Filterung auf Paket- und Anwendungsebene

Aufgabe einer jeden Firewall ist, den zwischen lokalem Computernetz und dem Internet fließenden Datenverkehr auf seine Zulässigkeit hin zu prüfen. Während es allgemein als notwendig angesehen wird, eine solche Überprüfung sowohl auf der sog. Datenpaketebene als auch auf der Ebene der Anwendungen durchzuführen, sah das Betriebskonzept zunächst nur die Prüfung auf einer dieser Ebenen vor.

– Beschränkung der Dienste

Beim Betrieb einer Firewall dürfen nur die unbedingt erforderlichen Datenströme zwischen lokalem Netz und Internet zugelassen werden. Angesichts der Kommunikationswünsche des Ministeriums kamen Zweifel auf, ob diese in dem genannten Umfang tatsächlich erforderlich waren und beispielsweise jeder Mitarbeiter des Ministeriums die Möglichkeit haben muss, Internet-Radio zu hören.

– Auswertung der Protokolldateien präzisieren

Firewall-Protokolle, die Auskunft über sicherheitsrelevante Vorkommnisse geben, müssen regelmäßig ausgewertet werden. Das Betriebskonzept nahm nur unzureichend dazu Stellung, in welcher Weise diese Auswertung zu geschehen hat.

– Schutz der Fernadministration und Fernüberwachung vor Missbrauch

Der Auftragnehmer sollte die Firewall nicht vor Ort, sondern über eine Online-Verbindung administrieren. Dabei muss besonders darauf geachtet werden, dass diese für Systemverwalter bestimmte Zugriffsmöglichkeit nicht unberechtigt genutzt werden kann. Dieser Frage schenkte das Betriebskonzept noch nicht die notwendige Aufmerksamkeit.

– Überwachungsmöglichkeiten durch den Auftraggeber

Bei einem Outsourcing-Projekt muss der Auftraggeber prüfen können, ob der Auftragnehmer die mit dem Auftrag verbundenen datenschutzrechtlichen Anforderungen einhält. Dies ist natürlich bei der Administration einer so sicherheitskritischen Einrichtung wie einer Firewall von besonderer Bedeutung. Der Auftraggeber muss sich dabei unter anderem davon überzeugen können, dass der Auftragnehmer neben den dienstlich benötigten keine weiteren Kommunikationswege öffnet, auf denen Daten zwischen Internet und dem lokalen Netz ausgetauscht werden können. Wie dies bewerkstelligt werden soll, ließ sich dem Konzept noch nicht entnehmen.

Das Ministerium teilte unsere Einschätzung und gab die Anpassung des Betriebskonzepts in Auftrag.

2.2 Computerviren – ein hartnäckiges Problem

Wie eine Lawine überrollte in diesem Jahr das sog. „I love you“-Virus die weltweite Internet-Gemeinde. Noch nie schlug ein Schadensprogramm so schnell und so flächendeckend zu. Millionen Computer, die mit dem Betriebssystem Windows und dem Programm Outlook ausgestattet waren, waren betroffen. Darunter auch etliche Computer öffentlicher Stellen, zu deren Schutz Firewalls und Virenscanner vorhanden waren. Das Virus verbreitete sich so:

Anfang Mai dieses Jahres landeten E-Mails mit dem Betreff „I love you“ in einer Vielzahl elektronischer Postfächer. Der verlockenden Botschaft „Ich liebe dich“ konnten Millionen Computernutzer nicht widerstehen, zumal es sich beim jeweiligen Absender der Mail um keinen Unbekannten handelte, sondern um jemanden, von dem man in der Regel bereits früher elektronische Nachrichten erhalten hatte. Sie öffneten die als Anhang zu dieser E-Mail versandte Datei, begierig darauf zu erfahren, was sich denn hinter der elektronischen Liebeserklärung verbirgt. Damit nahm dann das Unheil seinen Lauf. Die Datei enthielt, obwohl sie wie ein harmloser Text daherkam, ein sog. Makro-Programm, das nach dem Öffnen der Datei sofort ausgeführt wurde: Das Programm sandte Kopien der ursprünglichen „I-love-you“-Nachricht an alle Mail-Adressen, die der Empfänger in seinem Outlook-Adressbuch hinterlegt hatte. Die Lawine kam in Gang. Zudem löschte das Virus bestimmte Dateien.

Eines macht dieses Vorkommnis schlagartig klar: Es ist unerlässlich, dass die für die Datenverarbeitung verantwortlichen Stellen dagegen Vorkehrungen treffen. Darüber hinaus muss in unserer vernetzten Informationsgesellschaft aber auch jeder einzelne Benutzer für die Viren-Gefahren sensibilisiert sein und sich richtig verhalten. Denn ein Schaden entsteht nach bisherigem Kenntnisstand erst dann, wenn die Benutzer erhaltene elektronische Post öffnen. Insbesondere sollten sie Folgendes beachten:

– Bei jeder eingegangenen elektronischen Post sollte der Empfänger den Betreff sorgfältig lesen. Vorsicht ist bei auffälligen Betreff-Angaben geboten. Dazu gehören englischsprachige Betreffs wie
„I love you“, „Important Message from...“ oder „Pics for you“,
selbst wenn diese von ihm bekannten Absendern stammen. Derartigen E-Mails angeschlossene Anlagen dürfen unter keinen Umständen geöffnet werden; stattdessen ist der Systemverantwortliche umgehend zu benachrichtigen.

– Vorsicht ist ebenfalls geboten, wenn man von einem deutschen Absender plötzlich elektronische Post mit einem englischsprachigen Betreff erhält. Auch in solchen Fällen dürfen die Anlagen der eingegangenen elektronischen Post nicht geöffnet werden.

– Wer per elektronischer Post als Anlage ein ausführbares Programm erhält (Dateien mit den Endungen .com, .bat, .sys, .bin, .exe, .vbs etc.) sollte dieses nur starten, wenn der Versand der Anlage mit dem Absender zuvor abgestimmt wurde. Unangekündigt eingegangene ausführbare Programme sollten dagegen nicht in Gang gesetzt werden. Stattdessen ist entweder Kontakt mit dem Absender der elektronischen Post aufzunehmen oder der Systemverantwortliche der Dienststelle zu unterrichten. In der gleichen Weise sollte der verfahren, der per elektronischer Post komprimierte Dateien (in aller Regel an der Dateiendung .zip erkennbar) erhält und beim Dekomprimieren feststellt, dass ausführbare Programme übersandt wurden.

– Das Herunterladen von Freeware- oder Shareware-Programmen sollte grundsätzlich ebenso unterbleiben wie das Herunterladen von Spielen.

In einer beratenden Stellungnahme gegenüber dem Innenministerium haben wir auf diese Verhaltensregeln hingewiesen. Dieses hat inzwischen, was ich sehr begrüße, eine Handreichung erarbeitet, die detailliert beschreibt, welche Schutzvorkehrungen zur Abwehr von Viren getroffen werden sollten.

2.3 Höhere Sicherheit vor Viren und anderen Schadensprogrammen

Virenattacken à la „I love you“ lösten auch Diskussionen um die Sicherheit von Firewalls aus. Denn sie machten deutlich, dass selbst Firewalls keinen ausreichenden Schutz vor Computerviren, die aus dem Internet stammen und via E-Mail versandt werden, bieten können. Unzulänglich schützen Firewalls aber auch vor sog. aktiven Inhalten, die beim Surfen im World Wide Web (WWW) auf interne PC gelangen können und dort vielfach automatisch ausgeführt werden. Es handelt sich dabei um Scha-

densprogramme, die als Javascript-Anwendungen, Java-Applets oder Active-X-Controls realisiert sein können. Nicht auszuschließen ist, dass Viren und aktive Inhalte gezielt dazu eingesetzt werden, den Firewall-Schutz zu durchlöchern und schutzbedürftige Daten heimlich ins Internet zu schleusen. Es gilt daher, die Sicherheitstechnik so fortzuentwickeln, dass sie auch solchen Angriffen standhalten kann. Ansätze hierfür sind vorhanden, unter anderem:

– Signatur für Makros

  Mittlerweile lassen sich einige Programme, mit denen Computerbenutzer ihre elektronischen Postfächer leeren, so einstellen, dass ein in einem E-Mail-Anhang enthaltenes Makroprogramm nur dann ausgeführt wird, wenn es durch eine digitale Signatur als vertrauenswürdig gekennzeichnet ist. Nicht-signierte Makros werden dagegen nicht ausgeführt. Es ist zu begrüßen, dass die Landesverwaltung diese Möglichkeit künftig nutzen will.

– Auslagerung des Browsers

  Aktive Inhalte des WWW können Schaden anrichten, wenn sie auf einen internen Computer gelangen und dort von dem Browser ausgeführt werden, den man zum Surfen im WWW benutzt. Eine Möglichkeit, Schaden durch aktive Inhalte des World Wide Web abzuwehren, beruht auf der Idee, den Internet-Browser aus dem internen Netz zu verbannen und auf einen Computer zu verlagern, der außerhalb des internen Netzes angesiedelt ist und auf dem keine sicherheitsrelevanten oder schutzbedürftigen Daten gespeichert sind. Damit das Internet-Surfen aber weiterhin auch von internen Computern aus möglich ist, wird auf den internen Computern ein Programm eingesetzt, das lediglich den Bildschirminhalt des auf dem externen Computer installierten Browsers, letztlich also eine Menge von Bildpunkten, wiedergibt. Entscheidend ist dabei, dass aktive Inhalte auf diesem Weg gar nicht erst ins interne Netz gelangen können.

– Verschlüsselung schutzbedürftiger Daten

  Eine anderer Ansatz zum Schutz der im internen Netz gespeicherten personenbezogenen Daten geht von der Feststellung aus, dass ein hundertprozentiger Schutz vor Angriffen aus dem Internet nicht zu erreichen ist, und setzt deshalb auf die Verschlüsselung aller im internen Netz gespeicherten personenbezogenen Daten. Selbst wenn es einem Angreifer gelänge, sich diese Daten zu verschaffen, so wären diese Informationen für ihn wertlos, da er sie nicht im Klartext lesen könnte.

Diese Maßnahmen spiegeln nur einen Teil der Überlegungen wider, die gegenwärtig zur Verbesserung der Sicherheit beim Internet-Anschluss angestellt werden. Wichtig ist, dass die von Land, Kommunen und anderen öffentlichen Stellen betriebenen Internet-Anschlüsse möglichst bald technisch so gestaltet werden, dass Makro-Viren oder aktive Inhalte mit Schadensfunktionen keine Chance mehr haben.

2.4 Cookies

Cookies („Kekse“) sind nicht nur kulinarische Leckerbissen, es gibt sie inzwischen auch im Internet: Ruft man Informationen im World Wide Web ab, so kann es sein, dass der Informationsanbieter auf dem PC des Internet-Nutzers eine kleine Datei, eben das Cookie, speichert. Ruft der Surfer von seinem PC aus später das Web-Angebot erneut auf, so wird das Cookie vom heimischen PC zurück an den Informationsanbieter übertragen, der anhand der im Cookie abgelegten Informationen einen Zusammenhang zwischen dem früheren und dem aktuellen Abruf herstellen kann. Vielfach geht die Speicherung von Cookies sogar unbemerkt vom Surfer vonstatten. Zwar stellen Cookies, im Gegensatz zu Viren, keine ausführbaren Programme dar und können daher den betroffenen PC nicht unmittelbar schädigen. Unbedenklich ist der Einsatz von Cookies gleichwohl nicht. Mit ihrer Hilfe lassen sich nämlich Interessenprofile erzeugen. Besonders aussagekräftige Profile entstehen bei

Internet-Werbeunternehmen, die sog. Werbebanner in Web-Angebote anderer Informationsanbieter einblenden. Das geht wie folgt vor sich:

Ruft ein Internet-Nutzer das Angebot z. B. eines Gebrauchtwagenhändlers auf, auf dessen Web-Seiten Banner eines Werbeunternehmens eingeblendet werden, so kann dieses Unternehmen auf dem PC des Surfers ein Cookie anlegen und darin festhalten, dass sich dieser für Gebrauchtwagen interessiert. Besucht unser Mann danach von seinem PC aus das WWW-Angebot eines Warenhauses, das vom gleichen Werbeunternehmen mit Banner-Werbung bestückt wird, so sendet der PC das bereits vorhandene Cookie an das Werbeunternehmen. Dieses kann ihm entnehmen, dass sich der Surfer zuvor für Gebrauchtwagen interessiert hat. Es kann dann an diesem PC gezielt dafür werben. Interessiert sich der Internet-Nutzer beim Besuch des Warenhaus-Angebotes besonders für Jugendstilmöbel, so kann das Werbeunternehmen auf dem PC des Internet-Nutzers ein Cookie speichern, in dem neben dem bereits vorher bekannten Interesse für „Gebrauchtwagen“ nun auch das für „Jugendstilmöbel“ dokumentiert wird.

Zwar erfährt das Werbeunternehmen auf diese Weise nicht, welche Person die Informationen abrief, gleichwohl entsteht, einem Mosaik gleich, Stück für Stück ein Interessenprofil. Dass große Werbeunternehmen mit vielen tausend Inhaltsanbietern zusammenarbeiten, lässt erahnen, wie detailliert diese Mosaike werden können. Teilt der Surfer, beispielsweise bei der Teilnahme an einem Internet-Preisausschreiben, dann noch seinen Namen mit, so können auch diese Angaben in das Profil aufgenommen und dieses damit unmittelbar auf den Surfer bezogen werden. Aber auch wenn die Interessenprofile zunächst noch keinen unmittelbaren Personenbezug aufweisen, ist dies problematisch, da nicht auszuschließen ist, dass dieser später hergestellt wird. Dabei ist auch zu bedenken, dass für die im Ausland ansässigen Internet-Werbeunternehmen mitunter wesentlich geringere Datenschutzanforderungen gelten, als dies hierzulande der Fall ist. Daher empfiehlt sich aus Sicht des Datenschutzes generell ein restriktiver Umgang mit Cookies. Die einfachste Möglichkeit dazu ist, den eigenen Internet-Browser so einzustellen, dass er keine Cookies annimmt.

Manche Internet-Angebote setzen diese aber auch sinnvoll ein, etwa dann wenn es beim Tele-Shopping darum geht, beim Händler verschiedene Waren gleichzeitig zu bestellen. Ohne den Einsatz von Cookies könnten diese nicht quasi in einem Warenkorb auf einmal, sondern jeweils nur einzeln geordert werden. Will man solche Angebote nutzen, sollte man den Browser so einstellen, dass der Surfer über den Cookie-Einsatz informiert wird und ihn im Zweifel ablehnen kann. Hat man einmal Cookies akzeptiert, so sollte man diese nach Abschluss der Internet-Recherche löschen.

3. Fernsteuerungssoftware

Wer mit dem Computer arbeitet, kann ein Lied davon singen: Mal funktioniert ein Programm nicht so wie erwartet, mal streikt der Drucker, mal gibt es eine andere Störung. Wer so in seiner Arbeit unterbrochen wird, ist als Benutzer naturgemäß sehr froh, wenn ihm schnell geholfen wird. Umgekehrt haben auch die EDV-Verantwortlichen ein Interesse daran, die Störung rasch zu beheben, denn sie müssen mit meist wenig Personal die Betreuung möglichst effektiv und kostengünstig schultern. Dabei ist es schon eine große Erleichterung, wenn sich der Administrator zur Fehlersuche und -behebung nicht ständig vor Ort an den Server oder den PC der einzelnen Benutzer begeben muss, sondern von seinem PC aus tätig werden kann. Genau in diese Richtung zielt Fernsteuerungssoftware. Sie ermöglicht dem Administrator, von seinem Arbeitsplatz aus sowohl einen Server als auch einen Arbeitsplatz-PC über das Netzwerk zu steuern. Zudem kann sich der Administrator alles, was auf dem Bildschirm des Benutzers erscheint, auch auf seinem eigenen anzeigen lassen. Er kann in den Dialog eingreifen und – anstelle des Benutzers – Eingaben tätigen, aus der Ferne Installationsarbeiten an dessen PC durchführen oder sich als Administrator anmelden. Fernsteuerungssoftware ist damit ein wirkungsvolles Werkzeug zur Fehlersuche und Fehlerbeseitigung.

Bei all diesen nützlichen Funktionen darf freilich nicht außer Acht gelassen werden, dass mit dem Einsatz von Fernsteuerungssoftware auch Risiken für den Datenschutz einhergehen. Sie lässt sich nämlich auch zur Überwachung von Mitarbeitern verwenden. Zudem besteht die Gefahr, dass damit unberechtigt auf gespeicherte Daten zugegriffen wird. Es gilt also, geeignete Sicherheitsmaßnahmen vorzusehen, um den Einsatz von Fernsteuerungssoftware datenschutzgerecht zu gestalten. Wie sich aber bei Kontrollen und Beratungen gezeigt hat, schenken die Daten verarbeitenden Stellen dieser Frage oft genug nicht die gebotene Aufmerksamkeit. Zu beachten ist insbesondere Folgendes:

– Eine Fernsteuerung eines Arbeitsplatz-PC darf nur möglich sein, wenn der Benutzer aktiv am Zustandekommen der Fernsteuerungsverbindung mitgewirkt hat. Denn wer hat es schon gern, dass ein anderer seine Arbeit am PC von der Ferne aus unbemerkt überwachen kann? Diese notwendige Mitwirkung lässt sich beispielsweise durch eine am Bildschirm angezeigte Maske sicherstellen, die der Benutzer bestätigen muss, um die Fernsteuerung in Gang zu setzen. Eigentlich sollte eine solche Vorgehensweise selbstverständlich sein. Dem ist jedoch, wie mein Amt bei zwei Stellen feststellte, nicht immer so: Dort war die Aufschaltung auf den PC der einzelnen Benutzer ohne weiteres möglich. Beide verwiesen zwar darauf, dass der Administrator dem Benutzer eine Aufschaltung jeweils telefonisch ankündigen würde; dies ändert jedoch nichts an dem Umstand, dass eine Aufschaltung auch ohne vorherigen telefonischen Kontakt möglich war.

– Die Benutzer sollten ferner über die Installation und die Wirkungsweise der Fernsteuerungssoftware unterrichtet werden. Denn schließlich setzt die bereits angesprochene aktive Mitwirkung des Benutzers voraus, dass er weiß, welche Folgen seine Mitwirkung hat. Neben der Unterrichtung ist zudem geboten, dass die Daten verarbeitende Stelle ihre Mitarbeiter anweist, wie sie sich zu verhalten haben. Dabei verlangt eine datenschutzgerechte Vorgehensweise, dass der Benutzer Bildschirm-Masken mit personenbezogenen Daten vor der Aufschaltung nach Möglichkeit schließt. Ansonsten besteht die Gefahr, dass dem Administrator bei der Fernsteuerung personenbezogene Daten bekannt werden, auf die er ansonsten nicht zugreifen kann und die er für die Fernsteuerung auch gar nicht benötigt.

– Fernsteuerungsarbeiten sind in angemessener Weise zu protokollieren. Zumindest sind Datum, Beginn und Ende der Fernsteuerung, die Adressen der beiden Computer, zwischen denen eine Fernsteuerungsverbindung hergestellt wurde, sowie die Kennung desjenigen aufzuzeichnen, der die Fernsteuerung initiierte.

– Weil der Einsatz von Fernsteuerungssoftware in aller Regel auch den Zugriff auf personenbezogene Daten ermöglicht, muss die Dienststelle ihre Verwendung schriftlich freigeben. Der Freigabe muss eine Prüfung vorangehen, ob die für den Einsatz vorgesehene Fernsteuerungssoftware datenschutzrechtlichen Anforderungen genügt.

Weitere Hinweise zum Einsatz von Fernsteuerungssoftware können Interessierte einem von meinem Amt ausgearbeiteten Merkblatt zu diesem Thema entnehmen. Dieses kann auch über mein Internet-Angebot (www.baden-wuerttemberg.datenschutz.de) abgerufen werden.

4. Telearbeit

Nichts bleibt so wie es ist. Dies gilt auch und gerade für die Arbeitswelt. Lange Zeit mussten die meisten Beschäftigten, soweit sie nicht selbständig tätig waren, die Wohnung verlassen, um ihren Dienst, sei es in einem Betrieb, in einer Behörde oder sonstwo, zu verrichten. Doch heutzutage ist dies längst keine Selbstverständlichkeit mehr. Flexibilisierung der Arbeit ist angesagt. Formen der sog. Telearbeit kommt dabei zentrale Bedeutung zu. Der Beschäftigte „geht nicht zur Arbeit“, sondern die Arbeit kommt zu ihm. Die gebräuchlichste Form der Telearbeit ist die Tätigkeit zu Hause. Mit Hilfe moderner Informations- und Kommunikationstechniken wie E-Mail, Internet oder Videokonferenzen ist der Beschäftigte für den Arbeitgeber bei

vielen Tätigkeiten fast so gut verfügbar, wie wenn er sich am Arbeitsplatz aufhielte. Die moderne Technik macht es zum Kinderspiel, Informationen aus dem Computernetzwerk des Arbeitgebers abzurufen, Arbeitsergebnisse dorthin zu überspielen oder mit Kolleginnen oder Kollegen zu kommunizieren. Telearbeit ist für viele u. a. deshalb verlockend, weil sie durch die Arbeit zu Hause Familie und Beruf besser miteinander vereinbaren können.

Nachdem Telearbeit in der Privatwirtschaft schon länger üblich ist, sind Telearbeitsplätze nun auch in der öffentlichen Verwaltung auf dem Vormarsch. Deshalb befasste ich mich im letzten Jahr verstärkt mit Telearbeit, indem ich dem Wunsch von Behörden, sie bei der Planung und Einrichtung von Telearbeitsplätzen zu beraten, nachkam und kontrollierte, welche Vorkehrungen andere Behörden bei eingerichteten Plätzen getroffen haben, um den Datenschutz zu gewährleisten. Denn es kann keine Frage sein, dass die Telearbeit zusätzliche datenschutzrechtliche Anforderungen stellt, die es zu erfüllen gilt. Immerhin ermöglicht dabei der Arbeitgeber, dass von außen auf sein Computernetzwerk zugegriffen wird. Er muss daher sicherstellen, dass nicht Hinz und Kunz, sondern nur berechtigte Personen, dies tun können. Wenn zudem auch Unterlagen mit personenbezogenen Daten die Räume des Arbeitgebers verlassen, birgt das weitere Risiken in sich, denn es ist natürlich ein großer Unterschied, ob ein Bediensteter personenbezogene Daten im Büro oder per Telearbeit in den eigenen vier Wänden bearbeitet. Telearbeitsplätze sind deshalb sorgfältig zu planen, um die zusätzlichen Risiken für den Datenschutz durch geeignete Maßnahmen auf ein vertretbares Minimum zu reduzieren. Ist dies nicht erreichbar, ist auf die Einrichtung eines Telearbeitsplatzes zu verzichten. Die wichtigsten bei der Einrichtung von Telearbeitsplätzen zu beachtenden Punkte sind im Folgenden aufgeführt, denn die Erfahrungen in der Praxis zeigen, dass es mit ihrer Umsetzung teilweise erheblich hapert.

– Planung eines Telearbeitsplatzes

  Generell sollte eine Dienststelle prüfen, ob bei der Telearbeit die Verarbeitung personenbezogener Daten unbedingt notwendig ist. Aus der Sicht des Datenschutzes besser wäre es, wenn bei ihr nur anonymisierte oder pseudonymisierte Daten verarbeitet würden. Wegen ihrer herausgehobenen Schutzbedürftigkeit sollte sie besonders sensible personenbezogene Daten nicht in Telearbeit bearbeiten lassen. Darunter fallen Daten, die Berufs- oder besonderen Amtsgeheimnissen unterliegen, wie Sozial-, Personal- und Steuerdaten sowie Beihilfedaten und medizinische Daten.

– Dokumentierte Regelung

  Die Dienststelle sollte die Rahmenbedingungen der Telearbeit in einer Dienstvereinbarung oder einer Dienstanweisung regeln. Darin sind die Pflichten der Telearbeiterinnen und Telearbeiter festzulegen. Regelungsbedürftig sind u. a. die Teilnahmevoraussetzungen, Fragen zur Arbeitszeit und zum Arbeitsmittel sowie Kontrollrechte am Telearbeitsplatz. Die Dienststelle sollte dann über die Einrichtung der einzelnen Telearbeitsplätze auf der Grundlage dieser Rahmenbedingungen entscheiden. Im Einzelfall nötige zusätzliche Regelungen sind gegenüber der Telearbeiterin oder dem Telearbeiter zu treffen. Neben der schriftlichen Regelung der Rahmenbedingungen der Telearbeit sollte die Dienststelle die technischen und organisatorischen Maßnahmen, die von ihr getroffen worden sind, um einen ausreichenden Datenschutz bei Telearbeit zu gewährleisten, in einem Sicherheitskonzept dokumentieren.

– Arbeitsmittel

  Zur Grundausstattung eines Telearbeitsplatzes gehören in aller Regel ein PC samt Programmen und Anschlusstechnik, um den Telearbeits-PC mit dem Computernetzwerk der Dienststelle zu verbinden. Bei den bereitgestellten Arbeitsmitteln sollte die Dienststelle von vornherein für klare Verhältnisse sorgen. Bei sämtlichen Arbeitsmitteln sollte es sich um dienstliche Geräte und Programme handeln, die die Dienststelle beschafft, installiert, konfiguriert und administriert. Eine private Nutzung der Arbeitsmittel sollte ausgeschlossen sein. Denn jede Privatnutzung erhöht das Risiko, dass etwa Computerviren oder sonstige Programme mit

Schadensfunktionen auf den Telearbeits-PC gelangen und die Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigen.

– Nutzung des Telearbeits-PC

  Die Nutzung des Telearbeits-PC darf nur demjenigen möglich sein, der seine Berechtigung dafür, etwa durch Eingabe eines Passworts, nachweist. Selbstredend dürfen beispielsweise Familienangehörige dieses Passwort nicht erfahren. Nach wenigen, mehrmaligen Anmeldefehlversuchen (maximal fünf) ist der PC zu sperren, um etwaigen Missbrauch zu verhindern.

  Darüber hinaus sind Unterbrechungen durch Kinder, Besucher oder Anrufer bei Tele-Heimarbeit nichts Ungewöhnliches. Wenn die Telearbeiterin oder der Telearbeiter den PC verlässt, ist dieser aber offen wie ein Scheunentor. Jeder Mitbewohner kann die gespeicherten Daten zur Kenntnis nehmen und unter Umständen gar verändern. Wichtig ist folglich, dass die Telearbeiterin oder der Telearbeiter beim Verlassen des Arbeitsplatzes den Bildschirm in Sekundenschnelle per Knopfdruck sperren kann. Weil das Sperren per Hand aber leicht einmal vergessen wird, ist als zusätzlicher Schutz sicherzustellen, dass nach einer gewissen Zeitspanne, in der keine Eingaben erfolgen, der Bildschirm automatisch gesperrt wird.

– Verarbeitung personenbezogener Daten auf dem Telearbeits-PC

  Auch wenn Beschäftigte im Rahmen von Telearbeit personenbezogene Daten außer Haus verarbeiten: Die Dienststelle bleibt verantwortlich dafür, dass die Telearbeiterin oder der Telearbeiter mit den Daten datenschutzgerecht umgeht. Aus diesem Grund muss die Dienststelle klare Vorgaben machen, in welchem Umfang personenbezogene Daten mit welchen Programmen auf dem Telearbeits-PC zu verarbeiten sind und wann welche gespeicherten Daten wieder zu löschen sind. Aus Sicherheitsgründen sollten personenbezogene Daten auf dem Telearbeits-PC verschlüsselt gespeichert werden.

– Häuslicher Bereich

  An Tele-Heimarbeit Interessierte müssen nicht gleich ihre Wohnung oder ihr Haus komplett umbauen. Aber ein paar Bedingungen müssen schon erfüllt sein: So benötigt die Telearbeiterin oder der Telearbeiter einen Raum, in dem sich ungestört arbeiten lässt. Papierunterlagen und Datenträger sind nicht zwischen den Fotoalben, sondern vor dem Zugriff von Familienangehörigen gesichert, etwa in einem abschließbaren Schrank, aufzubewahren.

– Kontrollrechte

  Aufgrund der im Grundgesetz garantierten Unverletzlichkeit der Wohnung darf der Arbeitgeber nicht einfach in die Privatsphäre hineinplatzen, um zu sehen, was die Telearbeiterin oder der Telearbeiter am Telearbeitsplatz so alles treibt. Auch der Landesbeauftragte für den Datenschutz darf nicht ohne weiteres in einer Privatwohnung seiner Kontrollaufgabe nachgehen. Da es aber keinen (datenschutz-)kontrollfreien Raum geben darf, muss die Telearbeiterin oder der Telearbeiter darin einwilligen, dass sowohl die Dienststelle als auch der Landesbeauftragte für den Datenschutz die Datenverarbeitung am Telearbeitsplatz überprüfen können. Die Dienststelle darf den Telearbeitsplatz nicht genehmigen, wenn die Einwilligung nicht erteilt wird.

– Sicherer Transport von Unterlagen

  Telearbeit ist Vertrauenssache. Ob die Telearbeiterin oder der Telearbeiter Akten auf dem schnellsten Weg von der Dienststelle zur Privatwohnung transportiert oder ob sie oder er unterwegs noch einen Einkaufsbummel einschiebt und die Tasche mit Akten dann an einen Einkaufswagen hängt, kann die Dienststelle letztendlich nicht mehr beeinflussen. In jedem Falle sollte sie aber festlegen, dass die Telearbeiterin oder der Telearbeiter Unterlagen auf sichere Weise, möglichst in einem verschlossenen Behälter, zu transportieren hat.

– Anbindung des Telearbeits-PC an das DV-System der Dienststelle

  Durch geeignete Maßnahmen wie Rückruf, Rufnummernüberprüfung oder durch Einsatz spezieller Authentifikationsprotokolle sind ein unzulässiger Verbindungsaufbau und Missbrauch des Computernetzwerks der Dienststelle zu unterbinden. Personenbezogene Daten, die zwischen dem Telearbeits-PC und der Dienststelle ausgetauscht werden, sollten während des Transports aus Sicherheitsgründen verschlüsselt werden.

Summa summarum ist festzuhalten: Sofern nicht gerade besonders sensible personenbezogene Daten in Tele-Heimarbeit bearbeitet werden sollen, lassen sich die Datenschutzrisiken durch die beschriebenen Maßnahmen hinreichend minimieren.

5. Auftragsdatenverarbeitung

Manch eine Behörde, die personenbezogene Daten elektronisch verarbeitet, betreibt die dazu notwendigen Computer nicht selbst, sondern beauftragt damit ein privates Unternehmen oder eine andere öffentliche Stelle. Dabei kann es sich um zeitlich und inhaltlich beschränkte Aufträge, beispielsweise zur Störungsbehebung, handeln oder aber um Outsourcing-Projekte, bei denen der Auftragnehmer mit dem EDV-Betrieb zusammenhängende Aufgaben auf Dauer erledigt. Das Landesdatenschutzgesetz lässt eine solche Auftragsdatenverarbeitung zu, sofern u. a. der Auftrag schriftlich erteilt wird und darin die notwendigen technischen und organisatorischen Datenschutzmaßnahmen genannt werden, die der Auftragnehmer ergreifen muss. Mehrere große EDV-Projekte boten uns im vergangenen Jahr Anlass, auf ein datenschutzgerechtes Vorgehen bei der Auftragsdatenverarbeitung hinzuwirken:

5.1 Outsourcing der Bürokommunikation

Vor zwei Jahren beauftragten zwei Ministerien erstmals ein privates Unternehmen mit dem Betrieb ihrer PC-Netzwerke und der Bürokommunikationsprogramme (BK-Outsourcing). Mittlerweile ist das Unternehmen mit dem Betrieb von ca. 9 500 PC in Kultusverwaltung, Justiz und im Wissenschaftsministerium betraut; eine Ausdehnung auf weitere Zweige der Landesverwaltung ist in Sicht. Wie schon in der Vergangenheit (vgl. 20. Tätigkeitsbericht 1999, LT-Drs. 12/4600, S. 16/17 und 18. Tätigkeitsbericht 1997, LT-Drs. 12/2242, S. 20/21) nahm mein Amt auch im laufenden Jahr beratend zu diesem Projekt Stellung. Im Mittelpunkt stand dabei die Frage, wie sich personenbezogene oder andere schutzbedürftige Daten, die dem Auftragnehmer nicht bekannt werden dürfen, am besten vor unberechtigter Kenntnisnahme schützen lassen. Zwar konnten wir bereits früher erreichen, dass auf allen von dem Unternehmen betreuten PC ein Programm zur Verschlüsselung schutzbedürftiger Daten bereitgestellt wird. Da dieses jedoch unter den speziellen Bedingungen des BK-Outsourcings nicht als erste Wahl anzusehen ist, bat ich das federführende Innenministerium, die Eignung anderer Verschlüsselungsprodukte zu prüfen, die einen besseren Schutz versprachen. Nach anfänglichem Zögern lenkte das Innenministerium ein und wies den Auftragnehmer an, ein solches Produkt im Outsourcing-Betrieb zu testen. Sofern sich dabei die Praxistauglichkeit bestätigt, soll das Produkt künftig zum Standard beim BK-Outsourcing werden.

Nachdem damit die Diskussionen über die mit dem Projekt verbundenen allgemeinen Datenschutzfragen zu einem vorläufigen Abschluss gekommen sind, lässt sich insgesamt eine positive Bilanz für den Datenschutz ziehen:

– Entgegen den ursprünglichen Plänen erfolgt die Fernbetreuung der PC des Landes nicht von der Firmenzentrale des Auftragnehmers aus. Stattdessen richtete dieser eigens für die Betreuung der Behörden des Landes ein Betreuungszentrum in Ludwigsburg ein.

– Um eine bessere Auswertung der beim Betrieb der Computer anfallenden Protokolldaten zu ermöglichen, setzt der Auftragnehmer ein zusätzliches Auswertungsprogramm ein und ermöglicht, dass auch die Auftraggeber dieses jederzeit nutzen können.

– Um zu verhindern, dass Mitarbeiter des Auftragnehmers unberechtigt auf schutzbedürftige Daten zugreifen können, richtete der Auftragnehmer an allen PC-Arbeitsplätzen eine Verschlüsselungsmöglichkeit ein. An deren Verbesserung wird, wie oben beschrieben, noch gearbeitet.

5.2 Outsourcing des Landesverwaltungsnetzes

Weniger erfreulich fällt aus Sicht des Datenschutzes die bisherige Bilanz beim Outsourcing des Landesverwaltungsnetzes (LVN) aus. Nach Abschluss der entsprechenden Verträge ersetzt der Auftragnehmer gegenwärtig das bisherige, vom landeseigenen Zentrum für Kommunikationstechnik und Datenverarbeitung (ZKD) betriebene LVN durch ein von ihm betriebenes Netz. Wie stets bei der Auftragsdatenverarbeitung, liegt auch hier die Verantwortung für die datenschutzgerechte Abwicklung des Auftrags beim Auftraggeber, also den Behörden. Dazu müssen klare Absprachen darüber getroffen werden, was der Auftragnehmer zu tun hat, um den Auftrag datenschutzgerecht auszuführen. Zentrale Bedeutung kommt dabei dem Datenschutzkonzept zu, das der Auftragnehmer zu erstellen und umzusetzen hat. Der Entwurf dieses Konzepts enthielt nur sehr wenige und zudem vage Aussagen darüber, welche Maßnahmen der Auftragnehmer ergreift, um den Datenschutz zu wahren. Wir haben daher empfohlen, dieses Konzept nicht abzunehmen, sondern vom Auftragnehmer eine Nachbesserung zu fordern. Dem trat das Innenministerium entgegen und meinte, die Behörden des Landes seien nicht verpflichtet, sich genauer mit den Datenschutzmaßnahmen zu befassen, denn man schließe Outsourcing-Aufträge ja gerade mit dem Ziel ab, mit solchen konzeptionellen Fragen nicht mehr behelligt zu werden. Das ändert aber nichts daran, dass sie als Auftraggeber für die Einhaltung des Datenschutzes verantwortlich bleiben. Sie müssen sich daher zumindest so weit mit den vom Auftragnehmer getroffenen technischen und organisatorischen Schutzmaßnahmen befassen, dass sie diese Verantwortung übernehmen können.

Bislang ließ sich noch keine Annäherung in der Sache erzielen. Das Innenministerium möchte nun die strittigen Fragen in einem für Anfang Dezember geplanten Gespräch klären. Bleibt zu hoffen, dass sich dort endlich Fortschritte erzielen lassen.

5.3 Das Gemeinschaftsprojekt Polizei-Online

Gemeinsam mit einem großen Telekommunikationsunternehmen realisiert das Innenministerium das Verfahren Polizei-Online. Die Polizeibeamten im Land können damit an ihrem Arbeitsplatz Gesetze, Verordnungen sowie sonstige Informationen lesen, aktuelle Fragen in Diskussionsforen erörtern und sich zu Fortbildungsveranstaltungen anmelden. Obwohl längst noch nicht alle Polizeidienststellen über geeignete PC verfügen, können heute schon ca. 4 000 Bedienstete Polizei-Online nutzen. Dieses Projekt ist für den Datenschutz von Bedeutung, da damit auch personenbezogene Daten verarbeitet werden: Um solche handelt es sich sowohl bei den Fahndungsmitteilungen des Landeskriminalamts und einzelner Polizeidirektionen wie auch bei den in Diskussionsforen geäußerten Meinungen und den für die Teilnahme an Fortbildungsveranstaltungen eingegebenen Daten. Sicherheitsrelevant ist zudem, dass Computer des Auftragnehmers unmittelbar mit dem Computernetz der Polizei gekoppelt werden.

Da die zum Projekt Polizei-Online gehörenden Server nicht von der Polizei selbst, sondern von einem privaten Kooperationspartner betrieben werden, liegt hier eine Auftragsdatenverarbeitung vor. Unzulänglich war dabei Folgendes:

– Bislang hat das Innenministerium dem Auftragnehmer noch keinen schriftlichen Auftrag erteilt. Auf unseren Hinweis will das Innenministerium diesen Mangel abstellen und den Auftrag möglichst bald auch schriftlich fixieren.

– Das für das Projekt erarbeitete Datenschutz- und Sicherheitskonzept behandelte nur solche Datenschutzrisiken, die sich auf die in Polizei-

Online verarbeiteten personenbezogenen Daten beziehen, also beispielsweise auf die Daten von Teilnehmern an Fortbildungsveranstaltungen. Da Computer des Auftragnehmers aber mit dem polizeilichen Computernetz gekoppelt werden, besteht die Gefahr, dass polizeiliche Daten unberechtigt gelesen oder geändert werden können, die in anderen polizeilichen Verfahren als Polizei-Online gespeichert werden. Unverständlich war daher, wieso diese Risiken ausdrücklich aus dem Datenschutz- und Sicherheitskonzept ausgeklammert wurden. Dies gilt umso mehr, als die Sensibilität der in den übrigen polizeilichen EDV-Verfahren gespeicherten Daten zum Teil erheblich höher ist als die in Polizei-Online selbst verarbeiteten Informationen. Erfreulicherweise ist das Innenministerium nach einigem Hin und Her bereit, im Datenschutz- und Sicherheitskonzept auch auf solche Risiken einzugehen, die zwar durch das Projekt verursacht werden, sich aber auf Daten beziehen, die außerhalb des Verfahrens Polizei-Online gespeichert sind.

5.4 Test mit Echtdaten der Polizei

Nach mehrjähriger Planungs- und Entwicklungszeit nahm die Polizeidirektion Waiblingen Mitte dieses Jahres ein neues, speziell für polizeiliche Anforderungen entwickeltes Softwarepaket in Betrieb, das künftig landesweit eingesetzt werden und die polizeiliche Vorgangsbearbeitung wesentlich besser unterstützen soll, als dies bisher möglich war. Dabei traten Fehler auf, die vor Ort weder von der Polizei noch von dem mit der Entwicklung beauftragten Softwarehaus behoben werden konnten. Die Polizei stellte daher das fehlerhafte System inklusive der darin gespeicherten personenbezogenen Daten einem österreichischen Unternehmen zur Verfügung und beauftragte dieses mit der Fehlersuche und -behebung. Dabei ging sie allerdings nicht so vor, wie es der Datenschutz verlangt.

Zwar erteilte das Landeskriminalamt dem Unternehmen einen schriftlichen Auftrag und nannte darin auch technische und organisatorische Maßnahmen, die das Unternehmen beim Umgang mit den personenbezogenen Daten beachten muss. Dabei machte es sich die Sache allerdings einfach und zitierte im Auftrag lediglich die für jegliche Art der automatisierten Datenverarbeitung geltenden allgemeinen Anforderungen aus dem Landesdatenschutzgesetz. Damit lag es zwar nicht falsch, unzulänglich war dabei aber, dass das Landeskriminalamt aus den ganz allgemein formulierten Sicherheitszielen keine konkreten, auf die besonderen Umstände dieses Auftrags bezogenen Anforderungen ableitete. Folgende, an eine solche Testsituation zu stellende konkrete Anforderungen fehlten beispielsweise in dem Auftrag:

– Beschreibung des Testsystems und dessen Abschottung gegenüber anderen Computern

  Es ist festzulegen, an welchem Firmenstandort die Tests stattfinden und wie die Testarbeiten durchzuführen sind. Festzulegen ist ferner, wie es räumlich und netztechnisch von anderen Computern und Anwendungen innerhalb und außerhalb der Firma abzuschotten ist.

– Zugriffsbeschränkungen innerhalb des Testteams

  Den Mitarbeitern, die an den Testarbeiten beteiligt sind, sind Benutzerkennungen zur Verfügung zu stellen, die den unterschiedlichen Testaufgaben entsprechende Zugriffsberechtigungen bieten. Keinesfalls dürfen alle Tests mit Systemverwalterberechtigungen durchgeführt werden.

– Datensparsamkeit beim Testbetrieb

  Vor jedem Testschritt ist zu prüfen, ob die beabsichtigten Tests mit nicht-personenbezogenen Testdaten durchgeführt werden können. Nur wenn dies nicht möglich ist, darf auf personenbezogene Daten zurückgegriffen werden. In diesem Fall ist darauf zu achten, dass Daten möglichst weniger Personen in den Test einbezogen werden.

– Umgang mit Datenträgern

  Es ist näher zu beschreiben, wo die für die Tests benötigten Datenträger mit personenbezogenen Daten aufbewahrt werden und wer darauf zugreifen darf.

– Auswahl und Einsatz des Personals

  Die Tests sollten so gestaltet sein, dass dabei nur möglichst wenige Mitarbeiter personenbezogene Daten zur Kenntnis nehmen können. Außerdem sollten nur fest angestellte Mitarbeiter eingesetzt werden.

– Dokumentation

  Damit der Auftraggeber nachvollziehen kann, dass jeweils nur notwendige Arbeiten mit Testdaten ausgeführt wurden, sind die einzelnen Testschritte zu dokumentieren. Neben dem Testziel ist dabei anzugeben, in welchem Umfang personenbezogene Echtdaten für den entsprechenden Testschritt benötigt werden.

– Datenlöschung

  Es ist näher zu vereinbaren, wie die Datenlöschung auf Festplatten und Datenträgern nach Beendigung der Tests durchzuführen ist.

Ich forderte das Innenministerium, das mich um eine Stellungnahme gebeten hatte, auf, den Vertrag entsprechend zu präzisieren. Selbstverständlich muss es dabei das Rad nicht neu erfinden: Sofern der Auftragnehmer bereits über entsprechende Sicherheitskonzeptionen verfügt, kann darauf im Auftrag verwiesen werden.

6. Chipkarten

In Gestalt von Telefon- oder Krankenversichertenkarten nehmen Chipkarten bereits einen festen Platz in unserem Alltag ein. Auch in der öffentlichen Verwaltung gewinnen sie immer mehr Bedeutung. Nicht nur, dass sie eine zentrale Rolle bei elektronischen Bürgerdiensten spielen. Auch dort, wo bislang noch keine elektronischen Signaturen geleistet werden müssen, setzen öffentliche Stellen immer häufiger auf diese Technik. Beispielsweise gibt bereits eine Reihe von Hochschulen Chipkarten an ihre Studenten aus, die sich damit u. a. in jedem Semester zurückmelden, zu Prüfungen anmelden oder Fotokopien bezahlen können.

6.1 Gesetzliche Anforderungen an Chipkarten

Aus Sicht des Datenschutzes wirft der Umgang mit Chipkarten eine Reihe neuer Fragen auf. Dabei geht es um Folgendes:

– Obwohl die Karten den Bürgern ausgehändigt werden, sind sie Teil eines Datenverarbeitungssystems der ausgebenden und nutzenden Stellen. Diese müssen daher dafür sorgen, dass auch für die Chipkarten ausreichende technische und organisatorische Schutzmaßnahmen getroffen werden, um beispielsweise zu verhindern, dass Personen, die dazu nicht berechtigt sind, die auf der Chipkarte gespeicherten Daten lesen. Das ist insbesondere dann wichtig, wenn eine Karte nicht nur von einer Einrichtung, sondern gleich von mehreren gemeinsam genutzt wird, es sich also um eine sog. multifunktionale Karte handelt. Speichern beispielsweise ein Nahverkehrsunternehmen, eine Bank und eine Hochschule personenbezogene Daten auf ein und derselben Chipkarte, so muss sichergestellt sein, dass jede dieser Stellen nur auf die für sie bestimmten Daten zugreifen kann. Wichtig ist auch, dass der Karteninhaber weiß, an wen er sich halten kann, wenn er wissen will, welche Daten auf der Karte gespeichert sind, oder wenn er deren Berichtigung oder Löschung veranlassen will.

– Ein weiteres mit dem Einsatz von Chipkarten verbundenes Problem ist die Löschung: Auch bei der Speicherung personenbezogener Daten auf Chipkarten ist die speichernde Stelle verpflichtet, diese zu löschen, sobald sie nicht mehr benötigt werden. Da sich die Karten nicht bei ihr befinden, kann sie diese Löschung in der Regel nicht ohne weiteres zum vorgesehenen Zeitpunkt durchführen. Der Frage,

wie sich gleichwohl eine möglichst fristgerechte Löschung bewerkstelligen lässt, ist daher besondere Aufmerksamkeit zu schenken.

– Schließlich ist zu berücksichtigen, dass Chipkarten mittlerweile auch kontaktlos gelesen oder beeinflusst werden können. Schon das Vorübergehen an einem Lese- oder Schreibgerät genügt, um einen Datenaustausch zwischen der Karte und diesem Gerät zu ermöglichen. Beim Einsatz dieser Technik sollte sichergestellt sein, dass die gespeicherten Daten nur mit Wissen des Inhabers gelesen oder verändert werden können.

Damit bei öffentlichen Stellen des Landes die mit dem Einsatz von Chipkarten verbundenen Risiken soweit wie möglich minimiert werden, schlug ich vor, entsprechende Vorgaben in das Landesdatenschutzgesetz aufzunehmen. Der Gesetzgeber ist meinen Vorschlägen jedoch nur teilweise gefolgt. Das neu gefasste Landesdatenschutzgesetz sieht nun Folgendes vor:

– Die Karteninhaber sind über ihre Datenschutzrechte (also z. B. das Recht auf Auskunft über die gespeicherten Daten) zu informieren.

– Die Wahrnehmung dieser Rechte muss für den Chipkarteninhaber ohne unvertretbaren Aufwand möglich sein.

– Auch müssen diese darüber informiert werden, welche Folgen der Verlust der Karte hat und was in einem solchen Fall zu tun ist.

– Werden auf der Karte gespeicherte Daten gelesen oder auf andere Weise verarbeitet, hat die verantwortliche Stelle dafür zu sorgen, dass der Karteninhaber dies erkennen kann.

Das novellierte Landesdatenschutzgesetz zählt im Übrigen den Einsatz von Chipkarten zu den Fällen, in denen die Datenverarbeitung mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann. Wer Chipkarten einsetzen will, muss dies daher zuvor im Rahmen einer sog. Vorabkontrolle prüfen sowie schriftlich darlegen, dass diese Gefahren nicht bestehen oder durch geeignete technische und organisatorische Maßnahmen verhindert werden können und das Ergebnis der Untersuchung dem zuständigen Beauftragten für den Datenschutz zur Prüfung vorlegen.

6.2 Chipkarteneinsatz bei einer Fachhochschule

Um zu erfahren, wie der Chipkarteneinsatz in der Praxis aussieht und welche datenschutzrechtlichen Aspekte damit verbunden sind, überprüften wir das Projekt einer Fachhochschule, die seit zwei Jahren Chipkarten an ihre Studenten ausgibt. Diese können sich damit an speziellen Selbstbedienungs-Stationen (SB-Stationen) zurückmelden, Studienbescheinigungen ausdrucken, den Semesterbetrag oder die Langzeitstudiengebühr per Lastschrift bezahlen, die Semesteranschrift ändern, sich zu Prüfungen an- oder abmelden und sich die über ihre Person gespeicherten Daten anzeigen lassen. Außerdem ist auf der Chipkarte eine „Geldbörse“ installiert, in die an einem speziellen Gerät Geldbeträge per Lastschrift oder durch Bareinzahlung aufgeladen werden können. Das Guthaben kann genutzt werden, um an mehreren Fotokopierern Kopien zu bezahlen. Nicht alle für diese Vorgänge benötigten Daten werden in einem computerlesbaren Datenspeicher auf der Chipkarte abgelegt: Die Fachhochschule hat sich vielmehr darauf beschränkt, dort nur die Matrikel-Nummer, die Gültigkeitsdauer, das Geldbörsenguthaben sowie einige systemtechnische Daten wie Kartentyp und Seriennummer zu speichern. Die meisten der für die einzelnen Vorgänge benötigten Daten speichert die Fachhochschule auf einem mit den SB-Stationen vernetzten Server. Jedes Mal, wenn eine Studentin oder ein Student an einer solchen Station die Chipkarte einlegt, stellt der Server dieser zahlreiche zusätzliche personenbezogene Daten des jeweiligen Karteninhabers zur Verfügung. Dieser Ansatz, möglichst wenige Daten auf der Chipkarte selbst zu speichern, ist aus Sicht des Datenschutzes zu begrüßen.

Gleichwohl waren auch einige Unzulänglichkeiten beim Umgang mit den Chipkarten festzustellen:

– Unzureichende Kenntnisse der sicherheitsrelevanten Chipkarten-Eigenschaften

  Will man sich ein Urteil darüber bilden, ob das Chipkartensystem datenschutzgerecht arbeitet, so benötigt man Kenntnisse über dessen technische Realisierung, beispielsweise über den verwendeten Typ der Karte, die Möglichkeiten, darauf nachträglich weitere Datenarten zu speichern oder die Sicherheitstechniken, die unberechtigtes Lesen oder Manipulation an den Daten verhindern. Alle diese Fragen konnte die Fachhochschule nicht beantworten. Sie besaß keine schriftliche Dokumentation des eingesetzten Systems, dem solche Informationen hätten entnommen werden können.

– Protokolldaten teilweise unrechtmäßig gespeichert

  Die Fachhochschule dokumentiert sämtliche von den Studenten an den SB-Stationen durchgeführten Vorgänge, also auch die Fälle, in denen sich ein Student lediglich die zu seiner Person gespeicherten Daten anzeigen oder Studienbescheinigungen ausdrucken ließ. Diese detaillierten Protokolle deckten zum Zeitpunkt unserer Kontrolle einen Zeitraum von ca. 6 Monaten ab und umfassten 13 MB Daten: Eine Datenmenge, die ausreicht, um ca. 6 500 Schreibmaschinenseiten zu füllen. Diese lückenlose Aufzeichnung aller Vorgänge und deren monatelange Speicherung war nicht notwendig und deshalb auch nicht zulässig.

– Zu lange Speicherung von Protokolldaten aufgrund fehlender Löschfristen

  Neben der bereits erwähnten umfassenden Protokollierung dokumentierte die Fachhochschule jeweils gesondert die einzelnen Bargeldaufbuchungen, die Bezahlung von Fotokopien und die Lastschriftaufträge. Löschfristen hatte die Fachhochschule für alle diese Protokolldaten nicht festgelegt. Dies hatte zur Folge, dass einige dieser Daten seit Einführung des Chipkartensystems nie gelöscht und somit länger als zulässig gespeichert waren.

– Unzureichende Information der Chipkarteninhaber

  Weil der Einsatz von Chipkarten für die Inhaber mit besonderen Risiken verbunden ist, muss die verantwortliche Stelle, so verlangt es der Gesetzgeber, sicherstellen, dass diese erkennen können, wann und wo Daten mittels des Chipkartensystems verarbeitet werden. Das betrifft insbesondere Einlasskontrollen, bei denen beim Passieren einer bestimmten Stelle eine „Buchung“ auf der Karte erfolgt, ohne dass der Karteninhaber seine Chipkarte in ein Terminal einführen muss. Zum anderen müssen die Stellen, die Chipkarten einsetzen, die Kartenbesitzer bereits bei der Ausgabe der Karten in verständlicher Form über die ihnen zustehenden Rechte informieren. Diesen im neugefassten Landesdatenschutzgesetz erstmals festgelegten Verpflichtungen kam die kontrollierte Fachhochschule bislang noch nicht nach. Zwar erklärt sie den Studenten auf einem Hinweisblatt, welche Funktionen sie mit der Chipkarte ausführen können, z. B. Prüfungsergebnisse abfragen oder sich im automatisierten Verfahren zurückmelden. Dies genügt den gesetzlichen Vorgaben jedoch nicht. Vielmehr muss sie die Studenten auf folgende Punkte hinweisen:

  • Der Karteninhaber muss wissen, wie er seinen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten geltend machen kann.

  • Er muss darüber informiert werden, dass und wie er die Berichtigung, Löschung oder Sperrung dieser Daten verlangen kann.

  • Die Fachhochschule muss ihn darauf aufmerksam machen, dass ihm ein Recht auf Auskunft aus dem Verfahrensverzeichnis zusteht und wie er dieses wahrnehmen kann.

  • Ferner muss ihm bekannt sein, dass ihm Schadensersatzansprüche infolge fehlerhafter Datenverarbeitung zustehen können.

- Auch muss er darüber aufgeklärt werden, dass und wie er schutzwürdige, in seiner persönlichen Situation begründete Interessen gegen die Verarbeitung seiner Daten in dem Chipkartensystem vorbringen kann. Dazu muss er wissen, welche Stellen an dem System beteiligt sind, welche Daten diese zu welchem Zweck erheben und ob bzw. welche Informationen sie regelmäßig an andere Stellen weitergeben.
- Dem Karteninhaber muss jeweils gesagt werden, von welchen Voraussetzungen die Nutzung der Karte im Einzelfall abhängt. Die Fachhochschule muss ihn also beispielsweise darauf hinweisen, dass die elektronische Rückmeldung nur möglich ist, wenn der Semesterbeitrag und gegebenenfalls die Langzeitstudiengebühr beglichen und diese Informationen bereits im System gespeichert worden sind. Sonst kann es passieren, dass das System die begehrte Rückmeldung verweigert, ohne dass dem Benutzer klar wird, worin dies seinen Grund hat und was er veranlassen muss, damit ihm die elektronische Rückmeldung doch noch ermöglicht wird.
- Die Fachhochschule muss jeden neuen Kartenbesitzer darüber unterrichten, was er im Falle des Verlustes der Chipkarte veranlassen muss.
- Last not least muss sie die Karteninhaber darüber aufklären, dass sie den Landesbeauftragten für den Datenschutz anrufen können, wenn sie der Ansicht sind, dass sie bei der Verarbeitung ihrer Daten in ihren Rechten verletzt worden sind.

Ich bat also die Fachhochschule ein Merkblatt auszuarbeiten, das diesen Anforderungen gerecht wird, und dieses künftig den Studenten bei der Ausgabe der Karten zur Verfügung zu stellen. Darüber und über den Chipkarteneinsatz insgesamt wird in Bälde ein Gespräch mit den Fachhochschulen stattfinden.

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

1. Datenschutz im Krankenhaus

Bedauerlicherweise erfreuen sich nur wenige zeitlebens einer so guten Gesundheit, dass sie niemals die Dienste eines Krankenhauses in Anspruch nehmen müssen. Beginnend mit der Geburt, die meist in einer Klinik stattfindet, bis zum Tod sieht man sich mehr oder weniger oft in der Situation, stationär behandelt werden zu müssen. Die meisten machen sich in solchen Fällen am wenigsten Gedanken darüber, was eigentlich mit den vielen Informationen über den persönlichen Gesundheitszustand geschieht, die im Laufe des Krankenhausaufenthalts dort gesammelt werden. Von der Last der Leiden befreit und in der gewohnten Umgebung zurück, stellen sich dann aber vielleicht doch Fragen, wie etwa: Wer erfährt eigentlich was über mich und meine Krankheit? Sind meine Daten gegen die Kenntnisnahme Unbefugter hinreichend geschützt? Wie kann ich herausfinden, was über mich wo gespeichert ist? Nicht zuletzt auch angesichts der zunehmend kommerziellen Bedeutung medizinischer Informationen über den Einzelnen ist die Sorge um den ordnungsgemäßen Umgang mit solchen Daten verständlich. Sie aufzugreifen und dem Schutzbedürfnis des Patienten auch in diesem Bereich Geltung zu verschaffen, ist eine meiner Aufgaben. Um ihr Rechnung zu tragen, sind wir vielen Eingaben von Bürgern nachgegangen, haben in Kontakten mit Krankenhäusern und der Baden-Württembergischen Krankenhausgesellschaft Beratungshilfe geleistet und einem Krankenhaus einen Kontrollbesuch abgestattet. Dabei haben sich u. a. folgende Probleme und Mängel gezeigt:

1.1 Verarbeitung von Patientendaten außerhalb des Krankenhauses: Was geht wie und was geht nicht?

Krankenhäuser sehen sich vielfach aus Kostengründen dazu veranlasst, Teile ihrer Datenverarbeitung privaten Dritten zu übertragen. In

aller Regel handelt es sich um Schreibarbeiten, Mikroverfilmung, Archivierung von Patientenunterlagen und Aktenvernichtung. Zu bedenken ist dabei, dass zum einen jedes Offenbaren von Patientengeheimnissen eine Durchbrechung der ärztlichen Schweigepflicht darstellt, die nur zulässig ist, wenn entweder eine Entbindung von der Schweigepflicht durch den Patienten vorliegt oder eine Rechtsvorschrift die Weitergabe erlaubt. Zum anderen sind die Patientendaten außerhalb des Krankenhauses rechtlich schlechter geschützt als in den Räumen des Krankenhauses. Bisher war die Rechtslage in dieser Frage unklar, weil der Wortlaut des § 48 Abs. 2 des Landeskrankenhausgesetzes (LKHG), der die Auftragsdatenverarbeitung regelt, nicht eindeutig zum Ausdruck brachte, was der Gesetzgeber eigentlich festlegen wollte. Die Entstehungsgeschichte belegt nämlich, dass eine Auftragsdatenverarbeitung allenfalls durch Rechenzentren erlaubt werden sollte. Dem Wortlaut des Gesetzes, der von einer Auftragsdatenverarbeitung „durch eine andere Stelle“ sprach, war dies indes nicht mit der erforderlichen Eindeutigkeit zu entnehmen. Die Folge war, dass ich wiederholt auf die Unzulässigkeit der Praxis einzelner Krankenhäuser hinweisen musste (19. Tätigkeitsbericht 1998, LT-Drs. 12/3480, S. 29; 16. Tätigkeitsbericht 1995, LT-Drs. 11/6900, S. 57). Mit Artikel 2 des Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze vom 23. Mai 2000 (GBl. S. 450) hat der Gesetzgeber in dieser Frage nun Klarheit geschaffen. Seit In-Kraft-Treten dieses Artikels am 10. Juni 2000 ist nur noch eine Datenverarbeitung im Auftrag durch ein *Rechenzentrum* zulässig, wobei diese Datenverarbeitung *automatisiert* erfolgen muss. Damit ist jetzt klar, dass die oben dargestellten externen Verarbeitungen künftig nicht mehr uneingeschränkt zulässig sind. Manchen Krankenhäusern bereitet dies, wie nicht anders zu erwarten war, Probleme, da man an der bisherigen Praxis möglichst festhalten möchte. Die Frage ist daher: Was ist nach der neuen Rechtslage noch möglich?

– Externe Büros dürfen nur noch dann mit dem Schreiben von Arztbriefen und anderen Schriftstücken beauftragt werden, wenn vor der Weitergabe der Krankenhausunterlagen an den Auftragnehmer der Personenbezug der Patientendaten beseitigt wird. Dies kann dadurch geschehen, dass die Personen identifizierenden Merkmale verschlüsselt werden. Wird so verfahren, wird es dem Auftragnehmer, aber auch Dritten, die eventuell Einblick in die Unterlagen nehmen, – jedenfalls im Regelfall – faktisch nicht möglich sein, die Daten einer konkreten Person zuzuordnen. Damit ist die Anonymität des Patienten hinreichend gewahrt.

– Eine Mikroverfilmung durch Dritte ist unter folgenden Voraussetzungen akzeptabel:

  • Die Arbeiten, zu denen auch die Entwicklung der Mikrofilme gehört, werden in den Räumen des Krankenhauses erbracht;

  • das vom Auftragnehmer eingesetzte Personal unterliegt dem Direktionsrecht des Krankenhauses, was vertraglich abzusichern ist;

  • in öffentlichen Krankenhäusern werden diejenigen, die die Arbeiten ausführen, nach dem Verpflichtungsgesetz verpflichtet;

  • die sonstigen für die Sicherstellung von Datenschutz und Datensicherheit erforderlichen Maßnahmen werden schriftlich festgelegt.

– Eine externe Archivierung von Patientenunterlagen ist

  • bei Aktenarchivierung in der Form möglich, dass das Krankenhaus die benötigten Räumlichkeiten anmietet und zur Verwaltung der Akten eigenes Archivpersonal einsetzt. Nur so ist der Gewahrsam des Krankenhauses an den Unterlagen sichergestellt;

  • in elektronischer Form nur zulässig, wenn die Daten auf den Rechnern des Auftragnehmers verschlüsselt und von Daten anderer Auftragnehmer wirksam abgeschottet gespeichert werden.

– Die Aktenvernichtung kann auf zwei Arten erfolgen:

  • Der Auftragnehmer vernichtet die Unterlagen im Krankenhaus und unter Aufsicht von Krankenhauspersonal; der Einsatz mobiler Vernichtungsanlagen ist schon heute keine Seltenheit mehr.

  • Die zu vernichtenden Unterlagen werden in einem verschließbaren Behältnis gesammelt und dem Unternehmen zur Vernichtung übergeben. Dabei ist sicherzustellen, dass vor der eigentlichen Vernichtung, insbesondere während des Transports, nicht auf die Unterlagen zugegriffen werden kann. Dies ist beispielsweise nicht sichergestellt, wenn dem Fahrer des Transportfahrzeugs der Schlüssel für das Behältnis ausgehändigt wird. Um hier die erforderliche Sicherheit zu gewährleisten, muss der Transport von einem Mitarbeiter des Krankenhauses begleitet werden. Dessen Aufgabe muss es auch sein, die eigentliche Vernichtung zu kontrollieren und dabei darauf zu achten, dass während des Vernichtungsvorgangs keine Akten unbefugt gelesen werden.

Viele Krankenhäuser überlegen sich, anstelle der oben dargestellten Verfahren die Einwilligung der Patienten in die Auftragsdatenverarbeitung einzuholen. Aus der Sicht des Datenschutzes kann ein solches Vorgehen nicht befürwortet werden. Einzuräumen ist zwar, dass es letztlich jeder selbst in der Hand hat, ja oder nein zu sagen und der Gesetzgeber dem Krankenhaus jedenfalls nicht verboten hat, so zu verfahren. Die Einwilligungslösung ist jedoch deshalb bedenklich, weil der Patient eines Krankenhauses in seiner besonderen Situation in aller Regel nicht die innere Freiheit besitzt, sich auch gegen den Wunsch des Krankenhauses zu entscheiden. Die datenschutzrechtliche Einwilligung setzt aber gerade eine solche innere Freiheit voraus. Hinzu kommt, dass es bei der steigenden Zahl der Erklärungen, die man bei der Aufnahme in ein Krankenhaus abgeben soll, zunehmend schwerer fällt, den Überblick zu wahren. Entscheidet sich ein Krankenhaus aber gleichwohl für diesen Weg, ist jedenfalls der Zeitpunkt, in dem es den Patienten um die Einwilligung ersucht, so zu wählen, dass wenigstens ein Mindestmaß an tatsächlicher Entscheidungsfreiheit gewährleistet ist. Dies wird regelmäßig erst dann der Fall sein, wenn die Behandlung abgeschlossen ist und der Patient entlassen wird. Der Patient ist dabei über alle Umstände aufzuklären, unter denen die Datenverarbeitung stattfindet. Vor allem ist er auf die Freiwilligkeit der Einwilligung, auf sein Widerrufsrecht sowie darauf hinzuweisen, welche Folgen eine Verweigerung der Einwilligung haben kann.

1.2 Wozu die Staatsangehörigkeit?

Bei Kontrollbesuchen in Krankenhäusern stellen wir immer wieder fest, dass bei der Aufnahme zu viele Daten erhoben werden. Diese Problematik habe ich in den Tätigkeitsberichten der vergangenen Jahre wiederholt dargestellt. Ins Grübeln kamen wir aber, als ein Krankenhaus, das mein Amt aufgefordert hatte, bei der Aufnahme nicht nach der Staatsangehörigkeit zu fragen, auf § 25 des Meldegesetzes (MG) hinwies. Diese Bestimmung verlangt vom Krankenhaus, ein Verzeichnis über die stationär aufgenommenen Personen zu führen, in dem unter anderem auch die Staatsangehörigkeit anzugeben ist. Nach dieser muss das Krankenhaus natürlich erst fragen. Ergebnis der Überlegungen war:

Wenn das Krankenhaus im Meldegesetz verpflichtet wird, ein Verzeichnis mit den dort näher beschriebenen Angaben zu führen, dann dient dies ausschließlich melderechtlichen Zwecken. Soweit die zur Erfüllung melderechtlicher Verpflichtungen erfragten Angaben nicht gleichzeitig auch für krankenhauseigene Zwecke (Patientenversorgung, verwaltungsmäßige Abwicklung des Behandlungsverhältnisses) benötigt werden, dürfen sie nicht in die Patientenakte übernommen werden. Bei der Staatsangehörigkeit handelt es sich um eine solche Angabe. Denn um den Patienten behandeln zu können, muss diese in der Regel nicht

bekannt sein. Die melderechtliche Verpflichtung des Krankenhauses überlagert also nicht das Verbot, für krankenhauseigene Zwecke nicht erforderliche Daten zu verarbeiten. Zu bedenken ist auch Folgendes: Die bei der Aufnahme erhobenen Daten werden im Zweifel mindestens zehn, meistens aber 30 Jahre aufbewahrt. Das Meldegesetz sieht dagegen vor, dass das Verzeichnis und damit die in diesem enthaltenen Daten bereits nach Ablauf des auf die Entlassung folgenden Jahres zu vernichten sind. Würde die Staatsangehörigkeit in der Patientenakte gespeichert, hätte dies zur Folge, dass die melderechtliche Löschungspflicht leer läuft. Dies kann und muss schon von vornherein vermieden werden.

Im Ergebnis ist es also so, dass das Krankenhaus zwar (auch) nach der Staatsangehörigkeit fragen, diese aber nicht in den Patientenunterlagen vermerken darf. Außerdem müssen öffentliche Krankenhäuser die Patienten nach § 14 Abs. 1 Satz 1 des Landesdatenschutzgesetzes (LDSG) darüber unterrichten, wozu dieses Datum erhoben wird und dass es unter Umständen der Meldebehörde und der Polizei mitgeteilt werden muss. Diese Unterrichtungspflicht erstreckt sich übrigens auch auf die anderen nach § 25 Abs. 3 MG im Verzeichnis anzugebenden Daten.

1.3 Der bedürftige Krankenhauspatient

Empfängt jemand Sozialhilfe und muss ins Krankenhaus, so trägt das Sozialamt auch dafür in der Regel die Kosten. Anderes gilt im Wesentlichen nur, wenn der Hilfebedürftige krankenversichert ist. Es kommt nun immer wieder vor, dass jemand ins Krankenhaus eingeliefert und behandelt wird, ohne dass dem Krankenhaus die Hilfebedürftigkeit bekannt ist und die Frage der Kostentragung mit dem Sozialamt vor Behandlungsbeginn abgeklärt werden kann. Für diese Eilfälle sieht § 121 des Bundessozialhilfegesetzes (BSHG) vor, dass dem Krankenhaus, das ungeachtet dieser Unklarheiten Leistungen erbringt, seine Aufwendungen auf Antrag vom Sozialamt erstattet werden (sog. „Nothelferanspruch“). Voraussetzung ist allerdings, dass das Sozialamt bei rechtzeitiger Kenntnis der Sachlage Hilfe gewährt haben würde. In der Praxis ist es nun meist so, dass der Antrag des Krankenhauses an das Sozialamt auch Angaben über die Einkommens- und Vermögensverhältnisse des Patienten enthält. Diese erfragt es beim Patienten und trägt sie in den Antragsvordruck ein, um es dem Sozialamt zu ermöglichen, seine Leistungspflicht zu prüfen. Wie sich anlässlich der Kontrolle in einem Krankenhaus außerdem zeigte, nehmen Krankenhäuser offenbar Kopien solcher Anträge in die Krankenhausakten auf. Dies darf jedoch nicht sein.

Ein Krankenhaus darf nur die Daten seiner Patienten erheben und speichern, die es zur Erfüllung seiner eigenen Aufgaben benötigt. Die Einkommens- und Vermögensverhältnisse der Patienten gehören regelmäßig nicht dazu. Für die medizinische Behandlung selbst sind sie jedenfalls uninteressant. Was die Abrechnung angeht, gilt: Besteht Versicherungsschutz, was in der Regel durch Vorlage einer Krankenversichertenkarte bestätigt wird, braucht sich das Krankenhaus keine Sorgen um die Bezahlung seiner Leistungen zu machen. Aber auch in den Fällen, in denen der Patient hilfebedürftig im Sinne des Bundessozialhilfegesetzes ist, ist das Wissen um die finanzielle Situation des Patienten allein für das Sozialamt von Bedeutung. Nur dieses muss auf der Grundlage entsprechender Informationen prüfen, ob die Voraussetzungen für eine Hilfeleistung nach dem Bundessozialhilfegesetz vorliegen.

Das von uns besuchte Krankenhaus bat ich deshalb dafür Sorge zu tragen, dass in solchen Fällen die Angaben der Patienten über ihre Einkommens- und Vermögensverhältnisse nicht mehr in die Akten des Krankenhauses gelangen. Dies könne z. B. dadurch erreicht werden, dass die Angaben nicht mehr auf dem Vordruck für den Antrag nach § 121 BSHG eingetragen, sondern dem Patienten ein Antragsvorduck des Sozialamts auf Sozialhilfeleistungen ausgehändigt wird. Diesen soll der Patient eigenständig oder allenfalls – falls dies gewünscht wird – unter Mithilfe eines geeigneten Krankenhausmitarbeiters, vorzugsweise eines Mitarbeiters oder einer Mitarbeiterin des sozialen Dienstes, ausfüllen.

Der Antrag kann dann in einen zu verschließenden Umschlag gesteckt und dem Antrag des Krankenhauses nach § 121 BSHG beigefügt werden. Das Krankenhaus hat zugesagt, diesem Vorschlag nachzukommen. Ich meine, dies sei eine Verfahrensweise, der sich auch andere Krankenhäuser anschließen sollten.

In dem von meinem Amt besuchten Krankenhaus war es darüber hinaus üblich, in den Fällen, in denen eine Krankenkasse nicht gleich eine Kostenzusage erteilte, „vorsorglich" einen Antrag nach § 121 BSHG zu stellen. Kam die Zusage der Krankenkasse später dann doch noch, nahm das Krankenhaus seinen Antrag wieder zurück. Eine solche vorsorgliche Antragstellung ist unzulässig.

Mit jedem Antrag an das Sozialamt erfährt dieses nämlich, wer sich zur Behandlung in das Krankenhaus begeben hat. Und zwar auch dann, wenn sich hinterher herausstellt, dass der Patient gar nicht sozialhilfebedürftig ist. Allein der Umstand, dass jemand im Krankenhaus behandelt wird, fällt aber schon unter die ärztliche Schweigepflicht. Eine Durchbrechung ist nur gerechtfertigt, wenn der Patient einwilligt oder dies durch Gesetz zugelassen ist. Darüber hinaus muss die Datenübermittlung erforderlich sein. Keinesfalls dürfen Patientengeheimnisse unnötigerweise offenbart werden. Dies wäre aber dann der Fall, wenn das Krankenhaus dem Sozialamt den Krankenhausaufenthalt einer Person mitteilen würde, obwohl sie krankenversichert ist und bei der deshalb das Sozialamt von vornherein als Kostenträger ausscheidet. Darüber muss sich das Krankenhaus Gewissheit verschaffen, bevor es sich an das Sozialamt wendet. Die Praxis der vorsorglichen Antragstellung steht damit nicht in Einklang. Die Sozialhilferichtlinien nennen für die Antragstellung nach § 121 BSHG einen Zeitraum von in der Regel zwei Monaten als angemessene Frist. Innerhalb dieser Frist muss es dem Krankenhaus möglich sein, eine definitive Entscheidung der Krankenkasse darüber herbeizuführen, ob Versicherungsschutz besteht oder nicht oder aus welchem Grund eine Kostengarantie-Zusage nicht erfolgt. Erst wenn dies klar ist, kann eine Antragstellung beim Sozialamt in Betracht kommen. Das Krankenhaus hat zugesagt, die Praxis der vorläufigen Antragstellung aufzugeben.

1.4 ... nur eine Tür

Manchmal verschlägt es einem fast die Sprache, wie manche Stellen auf unsere Prüffeststellungen reagieren. Folgendes Beispiel hierzu:

Im Juni 1999 besuchte mein Amt das Kreiskrankenhaus Freudenstadt. Was uns dort besonders auffiel, war der buchstäblich „offene" Umgang mit den Patientenakten (20. Tätigkeitsbericht 1999, LT-Drs. 12/4600, S. 42). Zur Erinnerung: Das zentrale Schreibbüro und das Krankenhausarchiv sind beide in demselben Raum untergebracht. Damit kann sich praktisch jede Mitarbeiterin des Schreibdienstes – jedenfalls nach Dienstende des Registraturpersonals – nach Lust und Laune jederzeit Zugang zu den Patientenakten verschaffen. Ein unmöglicher Zustand, den wir so in anderen Krankenhäusern auch bisher nirgends angetroffen haben. Im Gegenteil, jedes bisher kontrollierte Krankenhaus hat größten Wert darauf gelegt, dass nur das eigens hierfür bestellte Personal über die sensiblen Daten verfügen konnte, und streng geregelt, wer unter welchen Voraussetzungen Patientenakten in die Hand bekommt.

Auf meine Beanstandung hin wollte das Krankenhaus erst einmal nichts unternehmen. Ich hatte vorgeschlagen, das Archiv einfach durch den Einbau einer verschließbaren Tür gegen das Schreibbüro abzuschotten. Aufgrund der Räumlichkeiten wäre dies verhältnismäßig einfach zu machen gewesen. Nach über einem Jahr und erst nach mehrfacher Erinnerung hat das Kreiskrankenhaus vor kurzem mitgeteilt, um „die Eintönigkeit der Arbeiten im Archiv besser auffangen" zu können, habe man veranlasst, dass künftig alle Mitarbeiterinnen des Schreibdienstes auch Registraturarbeiten wahrnehmen. Da damit ja nun alle in dem Raum beschäftigten Personen (auch) Registraturmitarbeiter seien, sei eine räumliche Abschottung der beiden Bereiche gegeneinander nicht mehr nötig. Eine wahrhaft geniale Lösung! Deutlicher hätte man nun

wirklich nicht mehr zum Ausdruck bringen können, welchen Stellenwert man der Wahrung des Patientengeheimnisses beimisst! Gesundheitsdaten gehören mit zu den sensibelsten Daten überhaupt. Die Patienten eines Krankenhauses dürfen zu Recht erwarten, dass alles getan wird, um den Kreis derjenigen, die diese Daten zur Kenntnis nehmen können, so klein wie möglich zu halten. Das Datenschutzbewusstsein der Krankenhausverwaltung scheint insoweit eher unterentwickelt zu sein. Erstaunen muss auch, dass sich offenbar von ärztlicher Seite keinerlei Widerstand regt. Denn immerhin geht es um Daten, die der ärztlichen Schweigepflicht unterliegen.

Meine Kritik an dieser mangelhaften Organisation der Aktenaufbewahrung habe ich dem Landrat des Landkreises Freudenstadt vorgetragen. In seiner Antwort betonte er die – von mir nie bezweifelte – Vertrauenswürdigkeit der Mitarbeiterinnen des Schreibdienstes. Um meinen Bedenken Rechnung zu tragen, will er nun nur noch auf drei der Schreibkräfte Archivtätigkeiten übertragen. Außerdem soll die Arbeitszeit des Archivpersonals der des Schreibdienstes angeglichen werden, damit niemand unbemerkt an die Akten komme.

Ich habe meine Zweifel daran, dass dies alles so funktioniert, wie es sollte. Dass das Krankenhausarchiv nicht räumlich und funktional vom Schreibdienst abgeschottet ist, ist nach wie vor nicht in Ordnung. Es hätte, wie gesagt, nur einer Tür bedurft.

2. Gesundheitsdatenschutz im Regierungspräsidium

Das Regierungspräsidium als staatliche Mittelinstanz hat aufgrund seiner Bündelungsfunktion vielfältige Aufgaben. Sicher nicht allgemein bekannt ist, dass es auch Gesundheitsdaten einzelner Bürger verarbeitet, wenn auch nur in geringem Umfang. Anlässlich eines Kontrollbesuchs beim Regierungspräsidium Stuttgart konnten wir uns ein Bild davon machen, wie dies in der Praxis läuft. Folgendes ist erwähnenswert:

2.1 Postlauf versus Datenschutz?

Üblicherweise ist es so, dass Post, die an eine Behörde gerichtet ist, in einer zentralen Poststelle eingeht, dort geöffnet wird und von Boten durch das Haus an die zuständigen Einheiten gebracht wird. Bis der Referent oder Sachbearbeiter die Post auf dem Tisch hat, ist sie meist durch viele Hände gegangen. Das ist im Allgemeinen auch hinzunehmen. Denn wer sich an eine Behörde als solche wendet, ohne zu wissen, wer dort konkret für seine Angelegenheit zuständig ist, von dem kann angenommen werden, er akzeptiere, dass sein Schreiben im Rahmen des Üblichen „verwaltet“ wird. Etwas anders muss man dies dann sehen, wenn es um personenbezogene Daten geht, die besonders schützenswert sind. Dazu gehören vor allem auch von einem Arzt erhobene und deshalb der ärztlichen Schweigepflicht unterliegende Gesundheitsdaten von Bürgern.

Das Regierungspräsidium erhält solche Gesundheitsdaten im Zusammenhang mit seiner Aufgabe, den Vollzug des Betäubungsmittelgesetzes zu überwachen, und in seiner Eigenschaft als Landesprüfungsamt für Medizin und Pharmazie. Im Bereich Betäubungsmittel prüft das Regierungspräsidium, ob die Ärzte die Betäubungsmittelrezepte ordnungsgemäß ausgefüllt und die vorgeschriebenen Höchstmengen eingehalten haben. Zu diesem Zweck lässt es sich von den Ärzten die innerhalb eines bestimmten Zeitraums ausgestellten Rezepte vorlegen. Im Prüfungsbereich ist es so, dass derjenige, der aus gesundheitlichen Gründen von der Prüfung zurücktreten will, seine Prüfungsunfähigkeit durch ein ärztliches Gutachten untermauern muss. In beiden Fällen geht es um Unterlagen, die sensible, der ärztlichen Schweigepflicht unterliegende Informationen enthalten. Hier ist es nicht angemessen, diese Post wie jede andere auch zu behandeln. Vielmehr muss sie so gut es geht gegen Kenntnisnahme durch solche Mitarbeiter geschützt werden, die nicht unmittelbar mit der Sachbearbeitung befasst sind.

Dem Regierungspräsidium empfahl ich deshalb, dafür Sorge zu tragen, dass in den Anschreiben an die Betroffenen und in den herausgegebenen

Informationsschreiben dazu aufgefordert wird, Briefe, mit denen solche Unterlagen übersandt werden, äußerlich deutlich erkennbar als vertrauliche Arztsache zu deklarieren. Intern sollte es durch Dienstanweisung sicherstellen, dass so gekennzeichnete Post ungeöffnet an den zuständigen Bearbeiter gelangt. Erfreulicherweise hat sich das Regierungspräsidium sofort bereit erklärt, diesen Empfehlungen nachzukommen.

Bei dieser Gelegenheit behob es auch gleich zwei weitere Mängel:

– Eine stichprobenweise Durchsicht alter Betäubungsmittelakten hatte ergeben, dass in diesen zahlreiche Kopien von Betäubungsmittelrezepten und ärztlichen Berichten über die gesundheitlichen und sozialen Umstände von Patienten abgelegt waren. Diese Unterlagen stammten noch aus der Zeit vor der letzten Änderung der Betäubungsmittel-Verschreibungsverordnung. Nach derzeitiger Rechtslage sind solche Unterlagen nach Abschluss der Prüfung wieder zurückzugeben (was, wie sich gezeigt hat, vom Regierungspräsidium auch beachtet wird). Auf unsere Bitte hin, nicht mehr erforderliche Akten auszusondern, reagierte das Regierungspräsidium zustimmend.

– Der andere Punkt war, dass das Landesprüfungsamt ärztliche Gutachten, die ihm zugegangen waren, bisher wie jedes andere Schriftstück auch zu den Akten genommen hatte. Dies ist aus Datenschutzgründen sehr problematisch. Denn ein wirksamer Schutz dagegen, dass nicht mit der Sachbearbeitung befasste Mitarbeiter unbemerkt solche Gutachten lesen, kann so nicht gewährleistet werden. Angesichts der Sensibilität und Schutzbedürftigkeit dieser Gesundheitsdaten habe ich das Regierungspräsidium aufgefordert, die Gutachten wenigstens in einem verschlossenen Umschlag zu den Akten zu nehmen. Damit ist zwar noch keine 100-prozentige Sicherheit erreicht, denn der Umschlag kann auch von Unbefugten geöffnet werden. Einem unbemerkten Lesen ist damit aber ein Riegel vorgeschoben. Lieber hätte ich es gesehen, wenn die Gutachten sicherer untergebracht worden wären, etwa in einem verschlossenen Schrank beim zuständigen Referenten. Mehr als die Umschlagslösung, der das Regierungspräsidium zugestimmt hat, war aber nicht zu erreichen. Immerhin eine kleine Verbesserung!

2.2 Der Briefkasten

Wer kennt das nicht: Man kommt nach Hause und der Briefkasten quillt über. Ärgerlich, aber meist ist es Reklame, die man umgehend entsorgt. Ähnliches musste ein Medizinstudent feststellen, der an einem Samstag seine Anmeldung zur Prüfung persönlich in den Briefkasten des Regierungspräsidiums Stuttgart einwerfen wollte. Der Briefkasten sei so voll gewesen, dass er erst ordentlich habe drücken und Platz schaffen müssen, um seinen Umschlag noch unterbringen zu können. Wenn er gewollt hätte, so schrieb er weiter, hätte er – so wie der Briefkasten konstruiert gewesen sei – ohne Schwierigkeiten Briefe heraus- und mitnehmen können. Wir prüften dies vor Ort nach und stellten fest, dass diese Schilderung zutraf. Prüfungsanwärter hätten also ganz erheblich in Schwierigkeiten kommen können.

Das Regierungspräsidium, von mir aufgefordert, hier für ordentliche Verhältnisse zu sorgen, hat umgehend zugesagt, die notwendigen Maßnahmen zu treffen. Die Frage bleibt, warum es das Problem nicht selbst erkannt und schon früher für Abhilfe gesorgt hat.

2.3 Nicht nur Behörden sind Sünder!

Das Regierungspräsidium Stuttgart ist im Land zentral für die Approbation von psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten zuständig. Die Psychotherapeuten, die schon vor dem In-Kraft-Treten des Psychotherapeutengesetzes diesen Beruf ausgeübt hatten und nunmehr von der in diesem Gesetz eingeräumten Möglichkeit, die Approbation zu erlangen, Gebrauch machen wollten, mussten ihre auf diesem Gebiet in den letzten Jahren gewonnene Berufserfahrung nachweisen. Unter Mühen konnten die Datenschutzbeauftrag-

ten gerade auch auf Drängen der Psychotherapeuten erreichen, dass die für die Prüfung der bisherigen beruflichen Tätigkeit erforderlichen Unterlagen, soweit sie Auskunft über Patienten geben, nur in anonymisierter Form vorgelegt werden mussten. Bei einer beim Kontrollbesuch gezogenen Stichprobe der Approbationsakten zeigte sich, dass die von den Psychotherapeuten eingereichten Unterlagen oft nur mehr als oberflächlich anonymisiert waren. Name und Adresse von Patienten waren häufig nur so schwach geschwärzt, dass mühelos zu erkennen war, um wen es konkret ging. Angesichts der sehr detaillierten Darstellung der physischen und psychischen Verfassung sowie der sozialen Situation der Patienten, einschließlich der Personen in ihrem Umfeld, ist dies ein unmöglicher Umstand! Offenbar waren sich manche der Antragsteller nicht bewusst, dass die Gleichstellung mit Ärzten auch Pflichten mit sich bringt, so auch die Pflicht, anvertraute Geheimnisse nicht unbefugt zu offenbaren. Da dieser Mangel allerdings nicht dem Regierungspräsidium anzulasten war, das in seinen Merkblättern deutlich auf die Möglichkeit der Anonymisierung hingewiesen hatte, mussten wir uns damit begnügen, diesen Sachverhalt – wenn auch mit Kopfschütteln – zur Kenntnis zu nehmen.

3. Das Gesundheitsamt

Das Aufgabenspektrum eines Gesundheitsamts moderner Prägung ist breit gefächert. Neben den „klassischen“ Aufgaben wie beispielsweise der Seuchenbekämpfung obliegen ihm die Gesundheitsförderung und -prävention sowie Gesundheitsberichterstattung und epidemiologische Untersuchungen. Angesichts der Vielzahl und Vielfalt der Aufgaben, die überwiegend die menschliche Gesundheit betreffen (eine uns von einem Gesundheitsamt vorgelegte Zusammenstellung weist allein 78 Untersuchungsanlässe auf!), liegt es auf der Hand, dass sich mein Amt immer wieder mit Fragen des Datenschutzes beim Gesundheitsamt zu befassen hat. Häufig wenden sich Bürger an uns und tragen ihre Sorgen und Nöte vor. Häufig werden wir aber auch von Amtsärzten um Rat gefragt, wie sie sich in bestimmten Situationen verhalten sollen. Kontrollbesuche, bei denen festgestellt werden soll, ob Sein und Sollen übereinstimmen, runden das Bild ab. Was gibt es zu berichten?

3.1 Der Kontrollbesuch

Unser Kontrollbesuch galt in diesem Jahr dem städtischen Gesundheitsamt Mannheim. Bekannt war uns, dass dieses das verhältnismäßig neue EDV-Verfahren Octoware einsetzt. Dessen praktischen Betrieb wollten wir uns einmal vorführen lassen. Daneben war aber auch die Datenverarbeitung im Übrigen Gegenstand unserer Kontrolle.

3.1.1 Das Gesundheitsamt vergisst nichts

Dass das Gesundheitsamt, wie jede andere Behörde auch, Akten über „seine“ Patienten anlegt und diese archiviert, ist keine Besonderheit. Es ist sogar dazu verpflichtet, wobei sich diese Pflicht auch aus dem Umstand ableitet, dass es hier um ärztliches Handeln geht und Ärzte nach ihrer Berufsordnung ihre Feststellungen und Maßnahmen dokumentieren müssen. Das ist an sich gar kein Problem. Problematisch wird es nur dann, wenn zu viel zu lange gespeichert wird und das noch in einer Form, die eine rechtlich unbefugte Kenntnisnahme der Daten ermöglicht. Wie so etwas praktisch aussieht, war wieder einmal in Mannheim festzustellen, nämlich am leidigen Problem der sog. Personenakte. Zur Erinnerung:

Die Anlässe, sich im Gesundheitsamt untersuchen zu lassen, sind sehr zahlreich. Manche nehmen die Dienste des Gesundheitsamts mehrfach in Anspruch, und das nicht immer freiwillig. Zwischen einzelnen Untersuchungen können Jahre liegen, die Untersuchungsanlässe haben sachlich nicht immer etwas gemeinsam. Das Gesundheitsdienstgesetz sieht in seinen Datenverarbeitungsbestimmungen vor, dass personenbezogene Daten, die im Rahmen einer bestimmten Untersuchung für einen konkreten Zweck er-

hoben worden sind, für einen anderen Zweck nur unter ganz bestimmten engen Voraussetzungen genutzt werden dürfen. Um dieser klaren gesetzlichen Vorgabe Rechnung zu tragen, müssen die im Rahmen der einzelnen Untersuchung erhobenen Daten jeweils für sich gespeichert werden. Die Akte, die diese Daten enthält, darf für den gleichen Zweck bedenkenlos, für andere Zwecke nur unter den dafür im Gesundheitsdienstgesetz festgelegten Voraussetzungen herangezogen werden. Allein dies ist im Übrigen mit der ärztlichen Schweigepflicht vereinbar, die grundsätzlich auch unter Berufskollegen gilt. Wie schon in den Tätigkeitsberichten von 1997 und 1998 dargestellt (18. Tätigkeitsbericht 1997, LT-Drs. 12/2242, S. 57 f.; 19. Tätigkeitsbericht 1998, LT-Drs. 12/3480, S. 34 f.), sieht die Praxis der wohl meisten Gesundheitsämter allerdings anders aus. Dort wird nämlich nicht nach Untersuchungsanlässen unterschieden, sondern es werden grundsätzlich fast alle jemals über den Patienten erhobenen Daten in einer Akte zusammengefasst gespeichert. Jeder Arzt des Gesundheitsamts, der die Akte in die Hand nimmt, erfährt so auch, was die Kollegen über den Patienten festgestellt haben und erhält damit einen vollständigen Überblick über die „Gesundheitsamtskarriere“ des Betroffenen. Und das unabhängig davon, ob die Daten im konkreten Zusammenhang überhaupt gebraucht werden. Wir haben dies immer kritisiert, und so auch im Fall des Gesundheitsamts Mannheim. Dieses führt ebenfalls Personenakten, wobei man sich der datenschutzrechtlichen Problematik dieser Praxis nicht einmal bewusst war. Hinzu kam Folgendes:

Als meine Mitarbeiter beim Besuch die amtsärztliche Registratur näher anschauten, fanden sie dort Akten und Akteninhalte, die zum Teil mehr als 50 Jahre alt waren. Tatsächlich ist es so, dass das Gesundheitsamt keinerlei Konzept dafür hat, wann es Akten aussondert, dem zuständigen Archiv anbietet und wann es sie vernichtet. Im Klartext heißt dies: Was das Gesundheitsamt einmal schriftlich erfasst und zu den Akten genommen hat, bleibt dort auf unbegrenzte Zeit gespeichert. Dies verstößt nachhaltig gegen Datenschutzrecht.

Die Speicherung personenbezogener Daten ist grundsätzlich nur so lange zulässig, als diese Daten zur Aufgabenerfüllung erforderlich sind. Der Einzelne wird in seinem Recht auf Datenschutz verletzt, wenn eine öffentliche Stelle zeitlich unbegrenzt und ohne sachliche Notwendigkeit Informationen über seine Person vorhält. Die Frage, wie lange Akten aufbewahrt werden müssen, richtet sich regelmäßig nach den Umständen des Einzelfalls. Lassen sich Einzelfälle typisieren, können hierfür auch generelle Löschfristen bestimmt werden. Für die Tätigkeit der Amtsärzte kann in Anlehnung an die ärztliche Berufsordnung von einer regelmäßigen Aufbewahrungsdauer von zehn Jahren nach Abschluss der Untersuchung ausgegangen werden. Für bestimmte Bereiche mag eine längere Aufbewahrungsdauer erforderlich sein, für andere wiederum kann eine kürzere Aufbewahrung genügen. Dies zu bestimmen und in einer Aussonderungs- und Löschkonzeption zu regeln, ist Aufgabe des Gesundheitsamts.

Auf unsere Kritik an dieser Praxis des Gesundheitsamts reagierte der Oberbürgermeister der Stadt Mannheim insoweit rasch, als er ankündigte, die Aktenablage erfolge „nunmehr“ getrennt nach unterschiedlichen Untersuchungsanlässen, bereits angelegte Akten würden im Rahmen einer erneuten Untersuchung des Patienten nach denselben Kriterien getrennt. Dies entspricht unserem Vorschlag. Bei der Aktenaussonderung will man dagegen weit hinter unseren Forderungen zurückbleiben. Akten sollen generell 30 Jahre lang aufbewahrt werden. Die Stadt überträgt damit die bei Krankenhäusern üblichen Aufbewahrungsfristen auf das Gesundheitsamt. Tatsächlich ist es so, dass Krankenhäuser vielfach ihre Akten aus versichungsrechtlichen Gründen und wegen der späten Verjährung von Schadensersatzansprüchen erst nach 30 Jahren

vernichten. Die Situation eines Krankenhauses ist aber nicht mit der eines Gesundheitsamts zu vergleichen. Wenn dort eine Akte über einen so langen Zeitraum archiviert werden soll, muss es schon gute Gründe dafür geben. Solche hat die Stadt bisher aber noch nicht vorgebracht.

3.1.2 Der fehlerhafte EDV-Einsatz

Mit dem von einem privaten Unternehmen entwickelten EDV-Verfahren „Octoware“ verarbeitet das Gesundheitsamt Mannheim Daten, die im Zusammenhang mit amtsärztlichen Untersuchungen sowie der Erfassung meldepflichtiger Krankheiten anfallen. Keine Frage, dass es sich dabei um sehr schützenswerte personenbezogene Daten handelt. Das Gesundheitsamt hätte deshalb allen Anlass gehabt sorgfältig zu prüfen, welche technischen und organisatorischen Maßnahmen es treffen muss, um eine datenschutzgerechte Verarbeitung seiner Daten sicherzustellen. Dem war jedoch nicht so:

– Völlig unzureichend war der Zugriffsschutz. Die Anmeldemaske von Octoware sah zwar Eingabefelder für die Benutzerkennung und ein Passwort vor. Die Eingabe eines Passworts war jedoch gar nicht erforderlich, um das Verfahren in Gang zu bringen. Vielmehr genügte die Eingabe einer Benutzerkennung und schon konnte es losgehen. Damit war aber jedem Octoware-Benutzer möglich, sich sowohl unter seiner eigenen als auch unter einer beliebigen anderen Benutzerkennung, die ihm auf irgendeine Weise bekannt geworden war, anzumelden, um Zugriffsrechte zu erhalten, die ihm gar nicht zustanden. Besonders gravierend wäre gewesen, wenn sich ein Benutzer unter der Identität des Verfahrensbetreuers angemeldet hätte, weil dieser aufgrund seiner verantwortungsvollen Tätigkeit über besonders weit reichende Zugriffsberechtigungen verfügt. Da Benutzerkennungen nicht geheim sind, war die Vorgehensweise des Gesundheitsamts ausgesprochen mangelhaft. Ein ordnungsgemäßer Einsatz der Software war nicht sichergestellt.

– Hinzu kam noch ein weiterer erheblicher Mangel. Das Gesundheitsamt installierte Octoware auf einem PC. Über sog. Dateifreigaben und daran geknüpfte Zugriffsrechte konnte auch von anderen PC aus auf das Programm und die gespeicherten Daten zugegriffen werden. Das Gesundheitsamt stellte die Zugriffsrechte so ein, dass nicht jeder PC-Benutzer, sondern nur diejenigen Mitarbeiter, die mit Octoware arbeiten sollten, das Verfahren aufrufen konnten. Es übersah freilich, dass jeder PC-Nutzer diese eingerichteten Zugriffsrechte nach eigenem Gusto verändern konnte. So hätte etwa ein PC-Benutzer die eingestellten Zugriffsrechte erweitern und sich selbst das Recht einräumen können, Octoware aufzurufen. Summa summarum hätten also auch solche Mitarbeiter des Gesundheitsamts, die gar nicht mit Octoware arbeiten sollten, die Anmeldemaske des Verfahrens aufrufen können. Da, wie bereits ausgeführt, für den Start des Verfahrens kein Passwort einzugeben war, hätten sie mit Octoware arbeiten können, indem sie einfach eine zugelassene Benutzerkennung eingetippt hätten. So geht es natürlich nicht! Wer welche Zugriffsrechte auf ein Verfahren erhält und wer in welchem Umfang personenbezogene Daten zu bearbeiten hat, ergibt sich aus der Geschäftsverteilung der jeweiligen Dienststelle. Zugriffsrechte darf nur der Benutzerverwalter verändern, nicht dagegen der einzelne Benutzer.

  Diese gravierenden Mängel musste ich beanstanden. Die Stadt hat zwar Besserung gelobt. Aufgrund technischer Probleme dauert der seit Einführung von Octoware beim Gesundheitsamt Mannheim im November 1999 bestehende datenschutzwidrige Zustand aber an.

3.2 Wie ein Gesundheitsamt über das Ziel hinausschoss

Stellen Sie sich vor, es klingelt an Ihrer Tür. Sie öffnen und ein Mitarbeiter des Gesundheitsamts eröffnet Ihnen, Ihr Kind sei nicht gegen Mumps geimpft, es unterliege deshalb der seuchenrechtlichen Überwachung und müsse den Anweisungen des Gesundheitsamts Folge leisten. Unvorstellbar? Offenbar nicht, wenn es nach dem Gesundheitsamt Heidelberg geht.

Harmlos fing es damit an, dass ein Arzt meinem Amt einen Erhebungsvordruck mit der Bitte vorlegte, diesen datenschutzrechtlich zu prüfen. Der Vordruck nebst einer Elterninformation war vom Gesundheitsamt Heidelberg an Schulen über Lehrer an Kinder der 6. Klasse ausgegeben worden. Unter der Überschrift „Impfschutz für alle – Impfberatungsaktion Herbst 1999“ sollten sich die Kinder vom Arzt bestätigen lassen, ob und gegen was sie geimpft sind. Diese Bestätigungen sollte der Klassenlehrer wieder einsammeln und an das Gesundheitsamt weiterleiten.

Dem Gesundheitsamt musste ich sagen, dass es so, wie die ganze Aktion tatsächlich ablief, nicht geht. Datenschutzrechtlich zu beachten war beispielsweise, dass die Teilnahme an der Umfrage freiwillig ist. Hierauf hätte in der Information an die Eltern hingewiesen werden müssen. Ebenso hätte darauf hingewiesen werden müssen, dass die Nichtteilnahme an der Befragung keine Nachteile für das Kind haben werde. Außerdem konnten wir keinen sachlichen Grund dafür erkennen, weshalb die Rückmeldung offen beim Lehrer abzugeben sein sollte. Denn immerhin unterliegen die dort gemachten Angaben der ärztlichen Schweigepflicht. Eine Rückgabe in einem verschlossenen Briefumschlag ohne Absenderangabe wäre völlig ausreichend.

Zunächst sah es so aus, als wolle uns das Gesundheitsamt folgen. Es sagte zu, die Eltern über die Freiwilligkeit der Teilnahme zu informieren, auch sollten Briefumschläge für die Rückmeldung zur Verfügung gestellt werden. Als wir jedoch wegen einiger Unklarheiten in der Antwort des Gesundheitsamts dort noch mal nachhakten, änderte sich plötzlich die Richtung. Markig wurde nun die Auffassung vertreten, wer nicht gegen Masern, Mumps und Röteln geimpft sei, der sei „ansteckungs- oder ausscheidungsverdächtig“ im Sinne des Bundes-Seuchengesetzes. Und wer ansteckungsverdächtig sei, der unterliege nun einmal der seuchenrechtlichen Beobachtung durch das Gesundheitsamt und müsse die erforderlichen Untersuchungen durch dieses dulden. Deshalb seien die Eltern auch verpflichtet, an der Erhebungsaktion teilzunehmen, ein Hinweis auf die Freiwilligkeit der Teilnahme sei nicht erforderlich. Alles Bemühen, das Gesundheitsamt wieder auf den rechten Weg zu bringen, blieb erfolglos. Nachdem sich sogar die von mir eingeschaltete, juristisch beschlagene Leitung des Landratsamts die irrige Auffassung des Gesundheitsamts zu Eigen gemacht hatte, blieb mir keine andere Möglichkeit, als die Vorgehensweise des Gesundheitsamts gegenüber dem Sozialministerium förmlich zu beanstanden. Dieses teilte mir daraufhin mit, das Gesundheitsamt Heidelberg werde bei künftigen Impfberatungsaktionen meine Hinweise beachten. Warum denn nicht gleich so?

4. Datenschutz in der medizinischen Forschung

Die Tumorzentren (TZ) und Onkologischen Schwerpunkte (OSP) betreiben klinische Krebsforschung. Dazu verwenden sie ihre Tumordokumentation. Im Rahmen dieser Arbeiten interessiert es sie natürlich auch, was aus den Krebspatienten geworden ist, die sie einmal behandelt haben. Die Arbeitsgruppe Tumordokumentation und EDV der Tumorzentren und Onkologischen Schwerpunkte wandte sich in diesem Zusammenhang mit der Frage an uns, wie es denn datenschutzrechtlich zu bewerten sei, wenn die kommunalen Rechenzentren im Land den Tumorzentren und Onkologischen Schwerpunkten jährlich eine Liste aller im Lauf des Jahres verstorbener Personen zur Verfügung stellen würden. Diese Listen könnten mit dem klinischen Tumorregister abgeglichen und so ohne viel Aufwand festgestellt werden, wer von den ehemaligen Patienten noch lebt. Der Arbeitsgruppe teilte ich mit, dass ich diese Lösung nicht befürworte. Drei Gründe gaben dafür den Ausschlag:

– Zum einen lässt die derzeitige Rechtslage eine solche regelmäßige Übermittlung von Sterbejahrgängen durch die Meldebehörden nicht zu. Das Meldegesetz und die Meldeverordnung sehen dies nicht vor.

– Zum anderen würde die jährliche Übermittlung solcher Sterbelisten durch jedes kommunale Rechenzentrum im Lande an alle Tumorzentren und Onkologischen Schwerpunkte zu einer Art „Datentourismus“ führen, der unverhältnismäßig wäre.

– Schließlich gibt es für die Tumorzentren und Onkologischen Schwerpunkte auch andere, datenschutzfreundlichere Möglichkeiten, an die benötigten Informationen zu kommen. So hat der Landtag erst kürzlich eine Regelung in das Landeskrankenhausgesetz eingefügt, nach der das Krankenhaus berechtigt ist, beim Meldeamt gezielt danach zu fragen, ob eine bestimmte Person noch lebt oder ggf. wann sie gestorben ist. Bei solchen Anfragen ist allerdings streng darauf zu achten, dass dem Meldeamt keinerlei Hinweise darauf gegeben werden, woran die erfragte Person erkrankt war. Hierzu kann es auch erforderlich sein, einen „unauffälligen“ Briefbogen zu verwenden. Soweit die Möglichkeit besteht, solche Anfragen in einer Form an das Meldeamt oder das von diesem eingeschaltete Rechenzentrum zu richten, die einen automatisierten Abgleich ermöglicht, ohne dass dabei von den Namen Kenntnis genommen werden muss, ist von dieser Möglichkeit Gebrauch zu machen.

Alternativ dazu kann das Informationsbedürfnis der Tumorzentren und Onkologischen Schwerpunkte auch dadurch gestillt werden, dass die Möglichkeiten, die das Krebsregister bietet, stärker genutzt werden. Seit letztem Sommer ist das Krebsregister berechtigt (§ 9 Abs. 8 des Landeskrebsregistergesetzes), einem meldeberechtigten Krankenhaus die Sterbedaten seiner ehemaligen Patienten zu übermitteln. Unter der Voraussetzung, dass die Tumorzentren und Onkologischen Schwerpunkte ihre Krebspatienten (verschlüsselt) melden und auch die Gesundheitsämter gemäß ihrer gesetzlichen Verpflichtung dem Krebsregister die Leichenschauscheine übermitteln, liegen diesem zentral alle Informationen vor, für die sich die Tumorzentren und Onkologischen Schwerpunkte sonst an die vielen Meldebehörden wenden müssten. Dieser Weg, den Vitalstatus zu erheben, verdient aus datenschutzrechtlicher Sicht eindeutig den Vorzug.

2. Abschnitt: Die Sozialversicherung

1. Kranken- und Pflegeversicherung

Krank sein wird immer teurer. Dass deshalb gespart werden muss, ist allen klar. Geht es aber um das „Wie“ und „Wo“, ist es mit der Einigkeit schnell vorbei. Auch der Datenschutz bleibt bei dieser Diskussion nicht außen vor. Auf der Suche nach Auswegen aus dem Dilemma versucht man, was ja auch nahe liegt, auf einer möglichst breiten Wissensbasis diejenigen auszumachen, die durch ihr Verhalten die Solidargemeinschaft über Gebühr in Anspruch nehmen. Diese Wissensbasis zu schaffen setzt voraus, dass Daten fließen – Daten über Leistungserbringer und über Versicherte gleichermaßen. In diesem Geflecht zum Teil stark gegenläufiger, meist wirtschaftlicher Interessen die Flagge des Datenschutzes hochzuhalten, ist oft nicht ganz einfach. Lorbeeren ernten kann man dabei gewiss nicht, darum geht es aber auch gar nicht. So unbefriedigend es manches Mal ist, wenn gute Argumente kein Gehör finden und aus Sicht des Datenschutzes problematische oder gar unzulässige Datenverarbeitungen trotz Intervention meines Amtes weitergeführt werden, so freut es uns andererseits auch wieder, wenn in einem konstruktiven Dialog tragfähige Lösungen gefunden werden. Licht und Schatten lagen so auch im Berichtszeitraum wieder eng beieinander. Genug zu tun gab es allemal.

1.1 Jedes Jahr die gleiche Frage: Was darf die Krankenkasse wissen und was nicht?

Beinahe täglich hören und lesen wir, dass wir in einer Informationsgesellschaft leben. Wissen sei der Rohstoff der Zukunft. Auch Krankenkassen (aber nicht nur die) scheinen dies verinnerlicht zu haben. Immer

wieder musste sich nämlich mein Amt mit der Frage auseinander setzen, was eine Krankenkasse eigentlich an Informationen über Versicherte braucht, um ihrer Arbeit nachkommen zu können, und was sie nicht erfahren darf. Bereits im letzten Tätigkeitsbericht (20. Tätigkeitsbericht 1999, LT-Drs. 12/4600, S. 50 f.) hatte ich mich mit Einzelfragen zu dieser Thematik befasst. Auch in diesem Jahr gab es Anlass, einzelne Facetten näher zu beleuchten. Der Anstoß hierzu kam vor allem von einem Kontrollbesuch bei einer Betriebskrankenkasse.

1.1.1 Sozialbericht der Drogenberatungsstelle

Stationäre Rehabilitationsmaßnahmen für Abhängigkeitskranke werden nicht nur von den Rentenversicherungsträgern, sondern auch von Krankenkassen erbracht. Wer wann zuständig ist, ist in der sog. Sucht-Vereinbarung näher geregelt. Nach dieser ist dem Antrag auf Reha-Leistungen auch ein Sozialbericht einer Drogenberatungsstelle beizufügen. Wie wir beim Kontrollbesuch feststellen mussten, finden sich solche Sozialberichte in Versichertenakten der Krankenkassen wieder. Dies darf nicht sein.

Im Unterschied zu anderen Sozialversicherungsträgern dürfen die Krankenkassen medizinische Daten ihrer Versicherten nur mit Einschränkungen verarbeiten. Die Schranken ergeben sich aus dem Umstand, dass es in der gesetzlichen Krankenversicherung eine besondere Einrichtung, nämlich den Medizinischen Dienst der Krankenversicherung (MDK), gibt. Diesem hat der Gesetzgeber – auch bezogen auf die Datenverarbeitung – eigene Rechte und Pflichten eingeräumt. An den §§ 275 ff. SGB V einerseits und den §§ 284 ff. SGB V andererseits zeigt sich das Verhältnis der Krankenkasse zum MDK: Die Krankenkasse hat die abschließende Entscheidung über die Gewährung oder Versagung von Leistungen zu treffen. Sind hierfür medizinische Sachverhalte zu beurteilen, ist der MDK, bei dem der medizinische Sachverstand vorhanden ist, zu Rate zu ziehen. Da die Krankenkasse selbst in der Regel keine Ärzte beschäftigt, fehlt ihr dieser medizinische Sachverstand. Sie kann folglich Unterlagen mit medizinischen Inhalten, wie beispielsweise Arztgutachten, nicht sachgerecht beurteilen. Und da sie dies nicht kann, ist auch die Anforderung solcher Unterlagen bei Dritten nicht zulässig. Es fehlt an der Erforderlichkeit als Grundvoraussetzung einer jeden Datenverarbeitungsbefugnis.

Eindeutig ergibt sich diese Rollenverteilung aus § 276 Abs. 2 Satz 1, 2. Halbsatz SGB V. Dort nämlich ist bestimmt, dass die Leistungserbringer verpflichtet sind, dem MDK und nur diesem die für dessen Gutachtertätigkeit erforderlichen Daten zu übermitteln. Nun ist es zwar so, dass im Wortlaut dieser Bestimmung ausdrücklich nur die „Leistungserbringer“ von Sozialversicherungsleistungen genannt sind. Die Drogenberatungsstellen, um auf den Ausgangspunkt zurückzukommen, gehören nicht dazu. Sie erbringen keine Sozialversicherungsleistung, sondern sie werden vielmehr im Auftrag des Versicherten tätig, der (im hier gegebenen Zusammenhang) den Sozialbericht als Teil seiner Antragsunterlagen vorlegen muss, wenn er Reha-Leistungen erhalten will. Gleichwohl wird man zumindest den Rechtsgedanken, der hinter den §§ 275 ff. SGB V, insbesondere dem § 276 Abs. 2 Satz 1, 2. Halbsatz SGB V steckt, auch hier anwenden müssen. Vergegenwärtigt man sich, dass der Sozialbericht sensibelste Angaben über den gesundheitlichen und psychosozialen Zustand des Betroffenen enthält, die fachgerecht zu beurteilen regelmäßig eine ärztliche Ausbildung voraussetzen, liegt es auf der Hand, dass solche Informationen ausschließlich in die Hände von Ärzten gehören und nicht im Bürobetrieb einer Krankenkasse landen dürfen. Die Krankenkassenmitarbeiter können mit solchen Informationen nichts anfangen, wie uns die Mitarbeiter der von uns besuchten Betriebskrankenkasse freimütig eingeräumt haben. Ich habe deshalb gefordert, dass in den Fällen, in denen die Krankenkasse über Reha-Leistungen für

Abhängigkeitskranke zu entscheiden hat, der Sozialbericht der Drogenberatung ausschließlich und unmittelbar dem MDK zugehen muss. Dieser hat ihn auch nach Erstattung seines Gutachtens bei sich aufzubewahren. Die Krankenkasse darf ihn weder im Original noch als Kopie erhalten. Verfahrensmäßig kann das so erreicht werden, dass die Krankenkasse den Betroffenen und/oder die Beratungsstelle auffordert, den Bericht entweder unmittelbar dem MDK zuzuleiten oder ihn in einem verschlossenen Umschlag zur Weiterleitung an den MDK der Krankenkasse zuzusenden.

Diese Auffassung habe ich den Spitzenorganisationen der Krankenkassen auf Landesebene mitgeteilt. Die AOK Baden-Württemberg hat geantwortet, dass sie schon bisher so verfahre. Die IKK Baden-Württemberg hat erklärt, sie teile unsere Auffassung und werde ihre Regionaldirektionen entsprechend unterrichten. Lediglich der BKK Landesverband wollte nicht folgen. Ich hoffe aber, ihn doch noch überzeugen zu können.

1.1.2 Ärztlicher Entlassungsbericht der Reha-Einrichtung

Bei dem Besuch der BKK stießen wir noch auf ein weiteres datenschutzrechtliches Problem. Es war dort Praxis, sich von Reha-Krankenhäusern neben einer Kurzfassung des ärztlichen Entlassungsberichts hin und wieder auch dessen vollständige Fassung übermitteln zu lassen. Dazu muss man Folgendes wissen:

Benötigt jemand einen stationären Kuraufenthalt, ist dies in den meisten Fällen Sache des für ihn zuständigen Rentenversicherungsträgers. Nach Abschluss der Kur erstellt die Kurklinik einen Entlassungsbericht. Dieser enthält eine umfassende Darstellung des Gesundheitszustands des Betroffenen und der vorgenommenen therapeutischen Maßnahmen, einschließlich eines ausführlichen Arztberichts. Der Entlassungsbericht hat für den Rentenversicherungsträger den Stellenwert eines sozial-medizinischen Gutachtens. Er dient ihm als Wissensbasis für die weitere Betreuung des Versicherten.

Nun ist es so, dass auch die Krankenkasse nach Abschluss der Reha-Behandlung verpflichtet sein kann, Leistungen der gesetzlichen Krankenversicherung zu gewähren. Sie muss beispielsweise die weitere Arbeitsunfähigkeit beurteilen oder prüfen, ob eine stufenweise Wiedereingliederung in Betracht kommt. Darf ihr zu diesem Zweck der vollständige Entlassungsbericht übermittelt werden? Die Antwort ist: Nein!

Die im ärztlichen Entlassungsbericht enthaltenen Angaben über den Patienten unterliegen der ärztlichen Schweigepflicht. Die Ärzte der Reha-Einrichtung dürfen diese Daten zwar dem Rentenversicherungsträger als Kostenträger übermitteln; dieser holt hierzu grundsätzlich die Einwilligung des Versicherten ein. Der Krankenkasse dürfen sie diese Daten hingegen nicht überlassen. Eine Rechtsvorschrift, die dies erlauben würde, gibt es nicht. Zwar könnte der Versicherte gefragt werden, ob er mit einer solchen Übermittlung einverstanden ist. Dabei wäre allerdings Folgendes zu beachten:

Wie bereits oben dargestellt, ist es im Rahmen der Prüfung, ob Leistungen der gesetzlichen Krankenversicherung erbracht werden müssen, Aufgabe des MDK, medizinische Sachverhalte zu klären. Nur der MDK, nicht dagegen die Krankenkasse selbst, ist berechtigt, Informationen über den Gesundheitszustand des Versicherten einzuholen. Im gegebenen Zusammenhang bedeutet dies, dass die Reha-Einrichtung den vollständigen ärztlichen Entlassungsbericht ausschließlich dem MDK zuleiten darf. Aus § 76 SGB X, insbesondere dessen Absatz 3, ergibt sich, dass es für eine solche Übermittlung keines Einverständnisses des Versicherten bedarf; er hat nicht einmal ein Widerspruchsrecht. Anders sieht es dagegen aus, wenn, was in der Praxis üblich ist und auch von den Daten-

schutzbeauftragten akzeptiert wird, der Krankenkasse (lediglich) Blatt 1 des Entlassungsberichts – routinemäßig – übersandt wird. Blatt 1 enthält nur allgemeine Auskünfte über die Diagnose, den Erfolg der Maßnahme und Vorschläge für nachfolgende Maßnahmen. Hier ist allerdings zu beachten, dass der Rentenversicherungsträger oder die von ihm beauftragte Reha-Einrichtung entsprechend § 76 Abs. 2 Nr. 1 SGB X verfahren und den Versicherten darauf hinweisen müssen, dass er der Weitergabe dieser Informationen widersprechen kann.

Im Dialog mit den Landesversicherungsanstalten Baden und Württemberg konnte erreicht werden, dass sie ihre bisherige Praxis, den Krankenkassen selbst auf deren Anforderung den vollständigen Entlassungsbericht zu übermitteln oder durch die Reha-Einrichtung übermitteln zu lassen, geändert haben. Künftig wird der Versicherte ausführlich darüber informiert, was mit dem ärztlichen Entlassungsbericht geschieht. Er hat die Möglichkeit, der Weitergabe von Blatt 1 des Berichts an die Krankenkasse zu widersprechen. Eine Übermittlung des vollständigen Entlassungsberichts erfolgt nur noch unmittelbar an den MDK. Damit konnte erneut eine einvernehmliche Lösung zugunsten eines verbesserten Datenschutzes erreicht werden.

1.2 Neue Aufgaben für den MDK – das Arzneimittel-Clearing

„Was notwendig im krankenversicherungsrechtlichen Sinne ist, wird vornehmlich durch den medizinischen Zweck der Leistung bestimmt“, so das Bundessozialgericht. Der Medizinische Dienst der Krankenversicherung (MDK) wurde eigens dazu eingerichtet, um die Fachkompetenz der Krankenkassen in sozialmedizinischen Fragen sicherzustellen. Im Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – sind die Aufgaben des MDK und sein Verhältnis zu den Krankenkassen detailliert geregelt. Wir haben uns deshalb zunächst schwer getan, als sich der MDK Baden-Württemberg mit Folgendem an uns wandte:

Bei der Arzneimittelverschreibung durch Vertragsärzte seien Missstände festgestellt worden. Um hier regulierend einschreiten zu können, seien die Krankenkassen daran interessiert, die Arzneimittelabrechnungsdaten arztbezogen kassenartenübergreifend zusammenzuführen und auszuwerten. Sie hätten den MDK als „Arzneimittel-Clearingstelle“ damit beauftragt, dies zu tun.

Um es vorweg zu sagen: Die Krankenkassen hatten von vornherein nicht beabsichtigt, dem MDK die zur Erfüllung dieser Aufgabe erforderlichen Daten versichertenbezogen zuzuleiten. Dies wäre aus der Sicht des Datenschutzes mehr als problematisch gewesen. Jedoch wollten die Krankenkassen dem MDK die Rezeptdaten arzt- und damit gleichfalls personenbezogen übermitteln. Im Rücklauf sollten die einzelnen Krankenkassen – auch wieder arztbezogen – eine ausgewertete Zusammenstellung des Verschreibungsverhaltens jedes einzelnen Arztes erhalten. Dies war der datenschutzrechtlich relevante Sachverhalt, dessentwegen uns der MDK um Rat fragte.

Nach § 84 Abs. 2 SGB V sind die Krankenkassen berechtigt, „Arbeitsgemeinschaften nach § 219“ damit zu beauftragen, Arzneimitteldaten zusammenzuführen und an die Kassenärztliche Vereinigung zu übermitteln. Dass der MDK, der nach § 278 SGB V als Arbeitsgemeinschaft der Landesverbände der Orts-, Betriebs- und Innungskrankenkassen, der Landwirtschaftlichen Krankenkasse und der Verbände der Ersatzkassen errichtet wurde und dessen Organisation, Aufgaben und Befugnisse im Neunten Kapitel des SGB V geregelt sind, möglicherweise nicht als Arbeitsgemeinschaft nach § 219 SGB V gesehen werden kann, hielt ich letztlich nicht für ausschlaggebend. Auf Grund der Rechtslage war den Krankenkassen jedenfalls nicht das Recht abzusprechen, solche Auswertungen durchführen zu lassen. Viel wichtiger erschien es mir deshalb, darauf zu dringen, dass der Umgang des MDK mit den erhaltenen Daten dem Interesse der betroffenen Ärzte an der Wahrung ihrer Datenschutz-

rechte weitestmöglich entspricht. Ich habe deshalb verlangt, dass der MDK durch technische und organisatorische Maßnahmen dafür Sorge zu tragen hat, dass die Daten ausschließlich zweckentsprechend verarbeitet werden können. Als Folge dieser Forderung hat der MDK meinem Amt ein ausführliches Datenschutz- und -sicherheitskonzept vorgelegt. Dieses sieht unter anderem vor, dass die Clearingdaten auf eigens hierfür bestimmten Rechnern verarbeitet werden, die in einem separaten und zugangsgesicherten Raum stehen und die von ausgewähltem, namentlich genanntem Personal betreut werden.

1.3 Beitragsüberwachung des Rentenversicherungsträgers bei der Pflegekasse

Das Sozialgesetzbuch (SGB) Elftes Buch (XI) – Gesetzliche Pflegeversicherung – regelt, dass, wer die häusliche Pflege von pflegebedürftigen Personen übernimmt, sozial abgesichert sein soll. Die Träger der Pflegeversicherung, meist also die bei den Krankenkassen errichteten Pflegekassen, sind dementsprechend verpflichtet, für die Pflegepersonen Rentenversicherungsbeiträge zu entrichten. Sache der Landesversicherungsanstalten als Träger der Rentenversicherung ist es darauf zu achten, dass die Pflegekassen die Pflichtbeiträge rechtzeitig und vollständig zahlen. Die Pflegekassen werden in diesen Fällen wie Arbeitgeber behandelt und sind verpflichtet, über alle Tatsachen Auskunft zu geben, die für die Erhebung der Beiträge und demgemäß auch für die Überprüfung der Korrektheit der Zahlungen notwendig sind. Und genau das lief, wie wir feststellen mussten, in der Praxis nicht so, wie es sein sollte.

Um die Richtigkeit der Beitragszahlungen zu prüfen, müssen die Prüfer der Landesversicherungsanstalt wissen, wer die Pflegeperson ist, welche Stufe der Pflegebedürftigkeit vorliegt und wie weit der medizinisch notwendige Pflegeumfang reicht. Diese Informationen sind in der Pflegeakte, genauer in dem dort enthaltenen Pflegegutachten des MDK enthalten. Folglich haben sich die Prüfer der LVA stets die kompletten Pflegeakten vorlegen lassen. Damit konnten sie aber weit mehr erfahren, als sie brauchten. Insbesondere konnten sie in dem Pflegegutachten die doch sehr sensiblen Angaben über den gesundheitlichen Zustand der pflegebedürftigen Person nachlesen.

Die hierzu befragte AOK Baden-Württemberg wie auch die beiden Landesversicherungsanstalten meinten zunächst, zu dieser Verfahrensweise gebe es keine Alternative. Wir haben nicht locker gelassen und darauf gedrängt, dass ein Verfahren gefunden wird, das eine Beitragsprüfung unter gleichzeitiger Wahrung des Sozialgeheimnisses ermöglicht. Hierauf hat sich vor allem die AOK Baden-Württemberg intensiv bemüht, nach Lösungsmöglichkeiten zu suchen. Ergebnis war, dass die Struktur des Pflegegutachtens geändert wurde. Künftig wird es so sein, dass die prüfungsrelevanten Angaben auf einem Zusatzblatt zum Gutachten zusammengefasst werden. Die LVA-Prüfer können dann ihre Informationen diesem Blatt entnehmen, ohne in das Gutachten selbst schauen zu müssen. Der BKK Landesverband und die IKK Baden-Württemberg haben sich dem angeschlossen. Dieser Fall hat die erfreulich gute und konstruktive Zusammenarbeit der Krankenkassen mit unserem Amt erneut bestätigt und gezeigt, dass mit gutem Willen Datenschutz und Verwaltungspraxis durchaus miteinander vereinbar sind.

1.4 Der vergebliche Widerspruch

Normalerweise sind die datenschutzrechtlichen Spielregeln klar: Zulässig ist eine Datenverarbeitung dann, wenn eine Rechtsvorschrift sie erlaubt oder wenn der Betroffene in sie einwilligt. In seltenen Fällen hat sich der Gesetzgeber allerdings für eine Lösung entschieden, die etwa in der Mitte liegt. In solchen Fällen ist eine Datenverarbeitung zwar vom Gesetz zugelassen, widerspricht der Betroffene allerdings, darf sie nicht (mehr) erfolgen. Solche Widerspruchsregelungen sind in der Praxis offenbar nicht immer bekannt. Anders jedenfalls lässt sich das Verhalten einer Krankenkasse nicht erklären, das mir ein Bürger so schilderte:

Nachdem er arbeitsunfähig krank geworden sei, habe er nach Ablauf der Entgeltfortzahlung bis Anfang des Jahres von seiner Krankenkasse Krankengeld bezogen. Die Zahlungen seien eingestellt worden, nachdem eine sozialmedizinische Begutachtung ergeben habe, dass eine Arbeitsaufnahme oder eine Arbeitsvermittlung wieder möglich sei. Er sei aufgefordert worden, zu diesem Zweck beim Arbeitsamt vorzusprechen. Dem habe er widersprochen und ein ärztliches Attest vorgelegt, wonach er weiterhin arbeitsunfähig krank sei.

Wie die Krankenkasse später auch bestätigte, rief einer ihrer Mitarbeiter daraufhin beim zuständigen Arbeitsamt an und fragte nach, ob der Betroffene schon zwecks Arbeitsvermittlung vorgesprochen habe. Das Arbeitsamt verneinte dies und teilte weiter mit, es sei bereits eine arbeitsmedizinische Untersuchung durch den arbeitsamtsärztlichen Dienst in die Wege geleitet. Wenig später fragte die Krankenkasse schriftlich beim Arbeitsamt nach, ob die Untersuchung bereits stattgefunden habe. Das Arbeitsamt bejahte dies und teilte mit, aufgrund des Untersuchungsergebnisses könne Arbeitslosengeld bewilligt werden.

Ein Punkt bei diesem Informationsaustausch war besonders zu kritisieren: Bevor sich nämlich die Krankenkasse an das Arbeitsamt mit der Bitte gewandt hatte, Auskunft über die Begutachtung zu erhalten, hatte der Betroffene in einem Schreiben gegenüber der Krankenkasse klipp und klar erklärt, er sei damit nicht einverstanden. Die Krankenkasse setzte sich einfach darüber hinweg.

Dieses Vorgehen der Krankenkasse war nicht mit dem Datenschutzrecht vereinbar. Denn zum einen hätte die Krankenkasse ihre Informationen beim Betroffenen selbst anfordern können und müssen. Es gilt nämlich der Grundsatz des Vorrangs der Datenerhebung beim Betroffenen. Bei Dritten dürfen Daten nur unter ganz bestimmten Voraussetzungen eingeholt werden. Die Krankenkasse hat nichts vorgetragen, was darauf schließen ließe, dass sie hierzu berechtigt gewesen sei. Zum anderen ist es so, dass ein medizinisches Gutachten, das ein Sozialversicherungsträger für einen bestimmten Zweck hat erstellen lassen, nach § 76 Abs. 2 Nr. 1 SGB X nur dann an einen anderen Sozialversicherungsträger übermittelt werden darf, wenn der Versicherte dem nicht widerspricht. Gleiches muss auch gelten, wenn es nicht um die Übermittlung des Gutachtens, sondern nur um Auskunft daraus geht. Hier hat der Versicherte nun nicht gegenüber dem Arbeitsamt der Übermittlung an die Krankenkasse, sondern gegenüber der Krankenkasse der Erhebung beim Arbeitsamt widersprochen. Gleichwohl hätte die Krankenkasse dies respektieren und das Arbeitsamt zumindest auf diesen Widerspruch hinweisen müssen. Dieses hätte dann, um rechtmäßig zu handeln, jegliche Auskunft im Zusammenhang mit dem Gutachten verweigern müssen.

Wir haben der Krankenkasse deutlich gemacht, dass sie hier falsch gehandelt hat und sie aufgefordert, künftig sorgfältiger über ihre Berechtigungen nachzudenken, bevor sie sich wegen eines Versicherten an andere Behörden wendet.

2. Die Kassenärztlichen Vereinigungen

2.1 J 06.9 oder: Wer schafft den „gläsernen“ Patienten?

„Ach, noch einer mit J 06.9“, lautete die Überschrift über einem Artikel in der Tagespresse Anfang des Jahres. Es ging um die mit Jahresbeginn einsetzende Verpflichtung der Vertragsärzte, bei der Abrechnung ihrer Leistungen die Diagnosen künftig nicht mehr in Klartext anzugeben, sondern nach der stark differenzierten Internationalen statistischen Klassifikation der Krankheiten und verwandter Gesundheitsprobleme, kurz ICD-10, zu codieren. Die Vorgaben des Bundesministeriums für Gesundheit führten zu teilweise heftigen Reaktionen in der Ärzteschaft. In zahlreichen Eingaben beschworen Ärzte das Schreckensbild des „gläsernen“ Patienten herauf und forderten mich auf, dem entgegenzutreten. Es war nicht ganz einfach, meinen Standpunkt deutlich zu machen.

Richtig ist, dass die Verwendung der ICD-10 im Vergleich mit der bisherigen Praxis zu einer differenzierteren Abbildung von Krankheiten und Gesundheitsproblemen führen wird. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits im Jahr 1996 wegen der Einführung der ICD-10 datenschutzrechtliche Bedenken angemeldet. Dies hatte mit dazu beigetragen, dass die ICD-10 speziell für die Bedürfnisse des SGB V überarbeitet worden ist. Den damals vorgetragenen Bedenken wurde weitgehend Rechnung getragen. Angesichts dieser Vorgeschichte und der insoweit eindeutigen Gesetzeslage sah ich keine Veranlassung, der Einführung der ICD-10 unter Hinweis auf den Datenschutz entgegenzutreten.

Ich sehe auch nicht, dass allein die Verwendung der ICD-10 den „gläsernen“ Patienten schaffen würde. Denn an der gesetzlich geregelten Form der Abrechnung von Kassenarztleistungen hat sich nichts geändert. Schon seit 1993 gilt, dass die Kassenärztliche Vereinigung die ihr von den Vertragsärzten vorgelegten Abrechnungsunterlagen nicht versicherten-, sondern nur fallbezogen an die Krankenkassen weiterleiten dürfen (§ 295 Abs. 2 SGB V). Von den Arbeitsunfähigkeitsbescheinigungen und den (Ausnahme-) Fällen abgesehen, in denen Abrechnungsdaten zu Prüfzwecken versichertenbezogen mit medizinischen Inhalten und Diagnoseangaben mitgeteilt werden, können die Krankenkassen somit auch die nach ICD-10 verschlüsselten Diagnosen keinem konkreten Patienten zuordnen. Ihnen liegen nach wie vor nur „Fälle“ vor.

Die Gefahr des „gläsernen“ Patienten geht für mich eher vom Verhalten der Kassenärztlichen Vereinigungen aus. Denn entgegen der schon seit 1993 bestehenden Verpflichtung, diese Unterlagen den Krankenkassen nicht versichertenbezogen zu übermitteln, haben sie zum Teil bis heute immer dann, wenn Ärzte bei der Abrechnung keine EDV einsetzten, sondern noch manuell abrechneten, die Abrechnungsunterlagen mitsamt der Angaben zur Person des Versicherten an die Krankenkassen weitergeleitet. Ich habe diese Praxis deshalb gegenüber den Kassenärztlichen Vereinigungen beanstandet. Dabei habe ich deutlich gemacht, dass nach mittlerweile mehr als sieben Jahren seit Einführung der Verpflichtung zur fallbezogenen Abrechnung auch der anfangs noch vertretbare Übergangsbonus verbraucht sei. Die Reaktion war erfreulicherweise einhellig. Alle Kassenärztlichen Vereinigungen sagten zu, ihre Praxis zu ändern. Während die Kassenärztliche Vereinigung Südbaden mitteilte, sie habe das Verfahren schon seit 1. Januar 2000 umgestellt, wollten die Kassenärztlichen Vereinigungen Südwürttemberg und Nordbaden bis zum Jahresende soweit sein, aber unabhängig davon zwischenzeitlich keine Krankenscheine mehr an die Krankenkassen weiterleiten. Lediglich die Kassenärztliche Vereinigung Nord-Württemberg will sich mehr Zeit lassen. Sie schreibt, als „Zeitziel“ für die Umstellung des Verfahrens sei der 1. Januar 2002 vorgesehen. Hierüber wird noch zu reden sein.

2.2 Die Drogenersatztherapie

In der gesetzlichen Krankenversicherung dürfen bestimmte Untersuchungen und Behandlungen zu Lasten der Krankenkassen nur erbracht werden, wenn die Bundesausschüsse der Ärzte und Krankenkassen entsprechende Empfehlungen in Form von Richtlinien abgegeben haben. Diese Richtlinien haben gesetzesähnlichen Charakter.

Wer drogenabhängig ist, dem bezahlt die Krankenkasse unter gewissen Voraussetzungen eine Substitutionsbehandlung. Früher in den sog. Methadon-Richtlinien geregelt, findet sich das Verfahren heute in den „Richtlinien zur substitutionsgestützten Behandlung Opiatabhängiger“, kurz: AUB-Richtlinien (**A**nerkannte **U**ntersuchungs- und **B**ehandlungsmethoden).

Wesentliche Voraussetzung für die von den Krankenkassen finanzierte Substitution ist das Vorliegen einer medizinischen Indikation. Im Antrag an die Kassenärztliche Vereinigung, der durch den zur Substitution berechtigten Arzt gestellt werden muss, muss die Indikation vorgetragen werden. Bei der Kassenärztlichen Vereinigung ist eine Beratungs-

kommission eingerichtet, die die Indikationsstellung überprüft. In diesem Zusammenhang hat sie der zuständigen Krankenkasse Gelegenheit zur Stellungnahme zu geben.

Aus datenschutzrechtlicher Sicht stellt sich bei diesem Verfahren die Frage, wer eigentlich alles die sehr sensiblen Gesundheitsdaten des Patienten zu Gesicht bekommen darf oder muss.

Die AUB-Richtlinien verpflichten den Arzt, Beginn und Beendigung einer Substitution der Kassenärztlichen Vereinigung und der Krankenkasse anzuzeigen. Der Kassenärztlichen Vereinigung muss er zusätzlich noch eine schriftliche Begründung vorlegen, die die für eine Überprüfung durch die Beratungskommission erforderlichen Angaben enthält. Dazu, wie mit den persönlichen Daten des Patienten im Übrigen umgegangen werden darf, schweigen sich die Richtlinien aus. Wie mein Amt feststellen musste, war die Praxis der vier Kassenärztlichen Vereinigungen im Lande sehr unterschiedlich. Überwiegend war es so, dass sie der Krankenkasse die kompletten Antragsunterlagen übersandten. Hierfür verlangten sie dem Patienten zuvor eine Einwilligung ab, um den Arzt von seiner Schweigepflicht zu entbinden. Mein Amt hatte deshalb zunächst einmal grundsätzlich zu klären, was aus Gründen des Datenschutzes geht und was nicht.

Wir kamen zu dem Ergebnis, dass

- eine Mitteilung des Arztes an die Krankenkasse über beabsichtigte oder eingeleitete psychotherapeutische, psychiatrische oder psychosoziale Begleitmaßnahmen nicht erforderlich ist. Die AUB-Richtlinien sehen insoweit nur eine Mitteilung über Beginn und Ende der Substitution vor, mehr nicht. Diese Information reicht aus, damit die Krankenkasse feststellen kann, ob eine Mehrfachsubstitution erfolgt;
- keine Notwendigkeit besteht, dass die Kassenärztlichen Vereinigungen der Beratungskommission Daten personenbezogen weitergeben. Die Kommission ist auch dann in der Lage, den „Fall“ anhand der Unterlagen zu beurteilen, wenn sie den Namen des Patienten nicht kennt;
- die Krankenkasse im Rahmen der Anhörung durch die Beratungskommission nicht die kompletten Antragsunterlagen erhalten darf. Die Überprüfung der Indikationsstellung ist allein der Beratungskommission übertragen. Die Krankenkasse kann der Kommission ihr bekannte Sachverhalte mitteilen, die für die Überprüfung eventuell bedeutsam sind. Allein dazu dient die Anhörung. Um solche Informationen geben zu können, muss die Krankenkasse allerdings nicht mehr wissen, als den Namen desjenigen, um den es geht. Der Inhalt der ärztlichen Unterlagen ist insoweit irrelevant.

Diese Rechtsauffassung habe ich sowohl den Kassenärztlichen Vereinigungen als auch den Krankenkassen mitgeteilt. Erfreulicherweise waren die Kassenärztlichen Vereinigungen bereit, dem zu folgen. In mühevoller Kleinarbeit konnte erreicht werden, dass alle vier annähernd gleich lautende Einwilligungsformulare verwenden, die dem Patienten nicht mehr abverlangen, als nach geltendem Recht notwendig ist. Alle Kassenärztlichen Vereinigungen haben erklärt, die vom Arzt erhaltenen Unterlagen vor der Weiterleitung an die Beratungskommission zu codieren, so dass die Beratung selbst faktisch anonym erfolgt. Schließlich werden die Kassenärztlichen Vereinigungen den Krankenkassen auch keine Gesundheitsdaten des Patienten mehr übersenden. Und offenbar funktioniert dieses Verfahren in der Praxis auch. Bisher habe ich jedenfalls noch nichts Gegenteiliges gehört.

3. Abschnitt: Soziales

1. Aus der täglichen Arbeit der Sozialämter

Die Aufgaben der Sozialämter bringen es mit sich, dass sie viele, häufig sehr sensible Informationen über Hilfesuchende und ihre Angehörigen sammeln müssen. Kein Wunder, dass der Datenschutz dabei in hohem Maße gefordert ist.

1.1 Von der Wiege bis zur Bahre: Formulare, Formulare!

Kaum jemand erkennt den Sinngehalt dieses Spruchs besser als Sozialhilfeempfänger. Bis ein Hilfesuchender die dringend benötigte Hilfe zum Lebensunterhalt in Empfang nehmen kann, muss er sich durch einen wahren Wust von Erklärungs- und Erhebungsvordrucken durcharbeiten, werden von ihm Einverständniserklärungen erwartet und Auskünfte bei Dritten eingeholt. Dagegen ist im Grundsatz nichts einzuwenden, da nach dem Bundessozialhilfegesetz (BSHG) Sozialhilfe nur dem zu gewähren ist, der seinen notwendigen Lebensunterhalt nicht oder nicht ausreichend aus eigenen Kräften und Mitteln, vor allem aus seinem Einkommen und Vermögen, bestreiten kann. Um prüfen zu können, ob diese Voraussetzungen vorliegen, benötigen die Sozialämter Informationen. Da es sich bei der Gewährung von Sozialhilfe um ein Massengeschäft handelt, setzen sie dazu Vordrucke und Formulare ein. Dies vereinfacht ihnen auf der einen Seite die Arbeit, birgt aber auf der anderen Seite die Gefahr in sich, dass in vielerlei Weise generalisiert und deshalb zu viel gefragt wird. Die nicht selten 8-seitigen Antragsvordrucke enthalten so neben Fragen nach Einkommen und Vermögen von Hilfesuchenden auch Fragen nach den Verhältnissen von Personen, deren Beantwortung für die beantragte Leistung irrelevant ist. Dafür einige Beispiele aus unserer Prüfpraxis:

– Sozialhilfe ist grundsätzlich nicht dazu da, Unterhaltspflichtige von ihrer Unterhaltspflicht gegenüber dem Hilfesuchenden zu entlasten. Gewährt das Sozialamt Sozialhilfe, geht deshalb ein etwaiger Unterhaltsanspruch des Hilfeempfängers auf das Sozialamt über. Allerdings hat der Gesetzgeber dieser Rückgriffsmöglichkeit Grenzen gesetzt. Das Sozialamt kann nur Kinder und Eltern des Hilfeempfängers zum Unterhalt heranziehen, nicht aber die Großeltern und Enkel. Gleichwohl werden Hilfesuchende in Antragsvordrucken vielfach nach unterhaltspflichtigen Angehörigen, deren Anschrift, Alter, Beruf und Arbeitgeber gefragt. Bei Großeltern und Enkel sind diese Angaben für die Sozialhilfegewährung aber irrelevant. Die Sozialämter dürfen deshalb auch nicht danach fragen und schon gar nicht die Leistung von der Beantwortung abhängig machen.

– Ist der Hilfesuchende nicht willens oder in der Lage, sein Arbeitseinkommen nachzuweisen, kann sich das Sozialamt an seinen Arbeitgeber halten. Dieser ist aber nur verpflichtet, über die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst des bei ihm beschäftigten Hilfesuchenden Auskunft zu geben. Diese Angaben allein scheinen aber den Aufwand für die Erstellung eines Vordrucks nicht zu rechtfertigen. Deshalb finden sich in solchen Formularen unter Hinweis auf die Auskunftspflicht des Arbeitgebers vielfach auch noch Fragen nach der Krankenkasse des Hilfesuchenden, seinen Krankheitszeiten, Zeiten des Fernbleibens von der Arbeit, möglichen Entlassungsgründen, zum evtl. neuen Arbeitgeber, der Berufstätigkeit des Ehegatten des Hilfesuchenden, einer zweiten Lohnsteuerkarte, dem Durchschnittsverdienst im Betrieb sowie der Veranlagung zur Einkommensteuer. Ein solches Vorgehen stellt eine grobe Irreführung der Arbeitgeber dar und ist schlicht und einfach unzulässig.

– Ist ein Verwaltungsverfahren erst einmal in Fahrt gebracht, soll der Hilfesuchende neben den Angaben zu seinen persönlichen und finanziellen Verhältnissen in einem Aufwasch auch gleich noch verschiedene Ermächtigungen erteilen und Erklärungen abgeben. Unter anderem soll er das Sozialamt ermächtigen, Akten anderer Sozialleistungsträger einzusehen. Behörden und Bankinstitute soll er beauftragen, Auskünfte über seine Vermögensverhältnisse zu erteilen. Den behandelnden Arzt, die Klinik und den ärztlichen Gutachter soll er gegenüber dem Sozialamt von der Schweigepflicht entbinden. Der Hilfesuchende soll sich weiter damit einverstanden erklären, dass das Bürgermeisteramt seiner Wohnortgemeinde eine Mehrfertigung des Sozialhilfebescheids erhält. Auch soll er einwilligen, dass das Sozialamt die erforderlichen Daten an Arbeitgeber, Behörden oder sonstige Beteiligte weitergeben darf. Diesen teils geforderten, teils auf frei-

willliger Basis erbetenen formularmäßigen Einwilligungserklärungen ist in der Regel gemeinsam, dass sie zu pauschal und unbestimmt abgefasst sind. Der Erklärende vermag daraus nicht zu erkennen, auf was er sich mit der Abgabe einer solchen Erklärung einlässt. Außerdem tragen sie regelmäßig auch den sonstigen Anforderungen, die der Gesetzgeber gerade an derartige Erklärungen gestellt hat, nicht hinreichend Rechnung. Der Einwilligende ist nach § 67 b Abs. 2 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) auf den Zweck der Speicherung oder einer vorgesehenen Datenübermittlung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung und der Hinweis bedürfen der Schriftform. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Mangelhafte Vordrucke und unzureichende formularmäßige Einwilligungserklärungen sind Erscheinungen, mit denen mein Amt schon seit Beginn seiner Tätigkeit ständig konfrontiert wird (vgl. 3. Tätigkeitsbericht 1982, LT-Drs. 8/3450, S. 8/9; 10. Tätigkeitsbericht 1989, LT-Drs. 10/2730, S. 64 ff.; 20. Tätigkeitsbericht 1999, LT-Drs. 12/4600, S. 62/63). Offensichtlich tun sich die Sozialämter schwer damit, wie gerade auch Kontrollen im vergangenen Jahr gezeigt haben. Manche zeigten sich unseren Hinweisen gegenüber aufgeschlossen und wollen ihnen zumindest teilweise nachkommen. Immer wieder hörten wir aber auch die Antwort: Man beziehe die Vordrucke von Verlagen und sei daher nicht der richtige Ansprechpartner. Einmal hieß es, das Sozialamt gehe davon aus, dass der Verlag über die rechtliche Entwicklung auf dem neuesten Stand sei und die angebotenen Vordrucke demzufolge dem neuesten Rechtsstand auch anpasse. Ein weiteres Landratsamt schlug vor, die „zuständige Fachaufsichtsbehörde für den Sozialdatenschutz“ einzuschalten – was immer darunter auch zu verstehen ist, denn eine solche Behörde existiert nicht.

Diese Sozialämter liegen mit diesen Auffassungen voll daneben. Allein sie tragen nämlich die Verantwortung für das datenschutzgerechte Erheben und Verarbeiten personenbezogener Angaben. Sie können die Verantwortung für die Rechtmäßigkeit ihres Tuns nicht dem Hersteller der von ihnen eingesetzten Vordrucke überbürden oder sich darauf berufen, die Vordrucke würden von den Gemeinden und nicht von ihnen beschafft. Die Frage ist, wie man erreichen kann, dass bei den Sozialämtern endlich datenschutzgerechte Vordrucke zum Einsatz kommen. Ein erster Schritt schien im Jahr 1989 bereits getan. Damals hatte sich der Landkreistag bereit erklärt, in Zusammenarbeit mit Städtetag, Gemeindetag und meinem Amt eine Musterformularsammlung zu erstellen. Bei dieser Absichtserklärung ist es dann allerdings geblieben. Wegen ihrer starken Arbeitsbelastung war es den Kommunalen Landesverbänden nicht möglich, ihren Vorsatz in die Tat umzusetzen. Meinem erneuten Vorstoß in dieser Frage im vergangenen Jahr war aus dem gleichen Grund leider wieder kein Erfolg beschieden. Ich werde im nächsten Jahr wohl oder übel einen erneuten Versuch starten müssen.

1.2 Kfz-Halteranfragen durch Online-Zugriff

Für das Sozialamt ist es zweifellos von Bedeutung, ob ein Hilfeempfänger ein Kraftfahrzeug, das ja einen Vermögenswert besitzt, sein Eigen nennt. Der Gesetzgeber hat die Sozialämter deshalb zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe u. a. ermächtigt, auch einen automatisierten Datenabgleich mit der für sie zuständigen Kraftfahrzeugzulassungsstelle durchzuführen. Dabei darf aber im Ergebnis nur überprüft werden, ob ein Hilfeempfänger Halter eines Kraftfahrzeugs ist.

Ein von uns kontrolliertes Sozialamt begnügt sich nicht damit, von Zeit zu Zeit einen solchen automatisierten Datenabgleich durchzuführen. Dort haben vielmehr das Sozialamt und die Kraftfahrzeugzulassungsstelle ein automatisiertes Abrufverfahren eingerichtet. Dieses ermöglicht es Sachbearbeitern des Sozialamts, per Mausklick auf den Datenbestand der

Zulassungsstelle zuzugreifen und sich dann, wenn der Hilfeempfänger Kfz-Halter ist, auch Angaben über Hersteller, Art, Typ, Aufbau und Farbe des Kraftfahrzeugs, das Datum der Erstzulassung und das Kennzeichen anzeigen zu lassen. Ich erinnerte das Sozialamt deshalb an die Vorschrift des § 117 Abs. 3 Satz 4 Buchst. f BSHG, die nur die Überprüfung der Haltereigenschaft erlaubt. Die Erwiderung des Sozialamts war erstaunlich: Die gesetzliche Regelung strebe die Vermeidung missbräuchlicher Inanspruchnahme von Sozialhilfe an. Dahingehend seien die Gesetzesbegriffe „Eigenschaft als Kraftfahrzeughalter" auch zu definieren. Es sei deshalb notwendig, dass das Sozialamt „näherungsweise zumindest Anhaltspunkte darüber erhält, ob und in welchem Umfang sich aufgrund der Tatsache, dass jemand Halter eines Kraftfahrzeugs ist, wegen der Art, Beschaffenheit oder des Wertes des Fahrzeugs Auswirkungen auf den Sozialhilfeanspruch ergeben können". Ganz offensichtlich war hier der Wunsch der Vater des Gedankens. Der klare Gesetzeswortlaut sagt etwas anderes und daran hat sich auch das kontrollierte Sozialamt zu halten. Inzwischen hat es sich eines Besseren besonnen.

Es prüft jetzt nämlich, ob der Direktabruf auf die Prüfung der Haltereigenschaft begrenzt werden kann. Sollte dies nicht möglich sein, will das Sozialamt zukünftig ganz auf die Nutzung des Online-Zugriffs verzichten.

Als Fazit bleibt festzustellen: Wird anstelle eines von Zeit zu Zeit stattfindenden automatisierten Datenabgleichs ein mit besonderen Risiken verbundenes automatisiertes Abrufverfahren eingerichtet, muss Folgendes beachtet werden:

- Die Zugriffe müssen so ausgestaltet sein, dass ausschließlich die Haltereigenschaft, nicht jedoch weitere Daten über das jeweilige Kraftfahrzeug abgerufen werden können.
- Es muss darauf hingewirkt werden, dass Missbrauchsmöglichkeiten beim Zugriff auf Kfz-Halterdaten schon technisch minimiert werden. Online-Zugriffe müssen deshalb in jedem Fall protokolliert und zumindest stichprobenweise überprüft werden.
- Es muss gewährleistet sein, dass, bevor ein Zugriff auf Kfz-Halterdaten erfolgen kann, der zugriffsberechtigte Sachbearbeiter zumindest den Namen, den Vornamen und das Geburtsdatum des Betroffenen eingeben muss.
- Außerdem empfehle ich, die Hilfesuchenden in geeigneter Weise darauf hinzuweisen, dass ihre Angaben zur Kfz-Haltereigenschaft durch Direktzugriff auf den Datenbestand der Zulassungsstelle überprüft werden können. Ein solcher Hinweis hat präventive Wirkung, ein Effekt, an dem jedem Sozialamt gelegen sein müsste.

1.3 Sorgfältiger arbeiten!

Sehr verwundert war eine Bürgerin aus Norddeutschland, als ihr im September 1998 ein städtisches Sozialamt eine sog. Anzeige zur Überleitung von Unterhaltsansprüchen ins Haus schickte und dabei mitteilte, sie sei als Mutter eines mit Namen bezeichneten Sozialhilfeempfängers diesem gegenüber zum Unterhalt verpflichtet. Nachdem sie das Sozialamt darauf hingewiesen hatte, dass es sich bei dem Hilfeempfänger mitnichten um ihren Sohn handelt, nahm das Sozialamt dann auch die Überleitungsanzeige zurück. Damit schien der Fall erledigt, aber weit gefehlt: Rund ein Jahr später erhielt die Bürgerin wieder eine Mitteilung vom Sozialamt. Dabei gab dieses wieder an, ihr Sohn erhalte jeden Monat Sozialhilfe in bestimmter Höhe. Ein etwaiger Unterhaltsanspruch des Hilfeempfängers gegen sie sei auf das Sozialamt übergegangen. Sie möge ihre persönlichen und wirtschaftlichen Verhältnisse darlegen, damit die Höhe des Unterhaltsanspruchs festgestellt werden könne. Auch ihr Ehemann sei auskunftspflichtig. Zu Recht verärgert, erinnerte die Frau das Sozialamt an den Vorgang aus dem Jahr 1998. Daraufhin reagierte dieses immer noch sehr gelassen. Die Rechtswahrungsanzeige könne als gegenstandslos betrachtet werden, verlautete es aus dem Sozialamt. Zur Begründung seines Vorgehens meinte es, die Akte über

den Vorgang im Jahr zuvor habe nicht vorgelegen. Der Hilfeempfänger habe eine bestimmte Person als Mutter angegeben. Diese Angaben seien „telefonisch über diverse Einwohnermeldeämter“ verfolgt worden. Welche Ämter dies gewesen seien, lasse sich nicht mehr sagen, da die Anfragen ja telefonisch erfolgt seien. Bei der Mutter des Hilfeempfängers und der Bürgerin bestehe Namensgleichheit und einiges mehr. Diese Feststellung erstaunte mich sehr, denn tatsächlich haben beide Frauen nur den nicht gerade seltenen Vornamen Gisela gemeinsam.

Das Sozialamt verhielt sich bei diesem Drama in zwei Akten gleich mehrmals datenschutzwidrig: Es gab auf der Grundlage einer völlig unzureichenden Recherche die Sozialdaten eines Hilfeempfängers an eine unbeteiligte Bürgerin weiter. Es berichtigte seinen Aktenbestand nicht in allen Teilen, obwohl dies nach dem ersten Anschreiben sehr wohl notwendig gewesen wäre. Schließlich traf das Sozialamt auch nicht die organisatorischen Maßnahmen, die erforderlich sind, um den Anforderungen des Sozialdatenschutzes gerecht zu werden. Dazu gehört, dass die Datenverarbeitung so organisiert wird, dass sie nachprüfbar ist und dem Akteneinsichtsrecht und Auskunftsanspruch des Betroffenen Rechnung getragen werden kann. Daran mangelte es bei dem Sozialamt. Es konnte selbst nur noch vermuten, bei welchen Stellen es zuvor welche Auskünfte eingeholt hatte und wie es zur Annahme einer Personenidentität kam. Dies ist jedoch absolut inakzeptabel. Datenabgleiche mit anderen Ämtern sind zu dokumentieren.

Da das Sozialamt weder gegenüber der von ihm zu Unrecht als Unterhaltspflichtige bezeichneten Bürgerin noch in seiner meinem Amt gegenüber abgegebenen Stellungnahme ein ausreichendes Problembewusstsein erkennen ließ, habe ich seine Vorgehensweise förmlich beanstandet. Der Oberbürgermeister der Stadt zeigte mehr Verständnis. Er räumte die Fehler seines Amtes ein und sagte das dortige Bemühen zu, künftig derartige Fehlsch(l)üsse zu vermeiden.

2. Nochmals: Die Gemeinden als Sozialämter?

Auch im abgelaufenen Jahr mussten wir uns wiederum mit der Rolle der Wohnortgemeinden bei der Beantragung und Gewährung von Leistungen der Sozialhilfe befassen. Zur Erinnerung: Bereits im 19. Tätigkeitsbericht meines Amtes für das Jahr 1998 (LT-Drs. 12/3480, S. 14/15) wies ich darauf hin, dass die Wohnortgemeinden nur die Aufgabe haben, Anträge auf Sozialhilfe entgegenzunehmen und diese dem örtlichen Träger der Sozialhilfe zuzuleiten. Eine eigene Prüfzuständigkeit dieser Anträge ist damit für die Wohnortgemeinden nicht verbunden. Sie sind nicht befugt, in das Recht auf informationelle Selbstbestimmung des Antragstellers einzugreifen. Ihnen gegenüber ist der Antragsteller auch nicht zur Mitwirkung verpflichtet. Anders ist dies nur, wenn der Träger der Sozialhilfe der Gemeinde nach § 4 AG-BSHG Aufgaben ganz oder teilweise überträgt oder sie im Einzelfall beauftragt.

Dennoch hält sich bei manchen Gemeinden ganz offensichtlich hartnäckig die Vorstellung, dass sie als Vor-Ort-Sozialamt fungieren. So rechtfertigte ein Bürgermeisteramt seine Praxis, von den zur Weiterleitung an das Landratsamt dort eingereichten Anträgen auf Gewährung von Sozialhilfe regelmäßig jeweils eine komplette Mehrfertigung in einer Akte aufzubewahren, u. a. damit, es nehme bei der Entgegennahme von Sozialhilfeanträgen die Aufgaben des Landratsamts im Rahmen des Bundessozialhilfegesetzes und des Ersten Sozialgesetzbuchs wahr. So geht es nicht! Mehrfertigungen oder Kopien von Sozialhilfeanträgen gehören nicht in die Akten der Bürgermeisterämter von Wohnortgemeinden.

Es ist nichts dagegen einzuwenden, wenn das Bürgermeisteramt Antragsteller berät, z. B. ihnen Datenfelder erläutert oder sie auf offensichtliche Unvollständigkeiten bei ihren Eintragungen aufmerksam macht. Zum Nachweis der Entgegennahme des Antrags genügt es aber, wenn das Bürgermeisteramt Antragsteller, Anschrift und Daten der Entgegennahme und Weiterleitung des Antrags bei sich vermerkt. Keinesfalls ist es dagegen erforderlich, dass die Wohnortgemeinden die Angaben über Einkommen und Vermögen des Antragstellers und seines Ehegatten/Lebensgefährten, Ver-

sicherungsverhältnisse, Arbeitsfähigkeit, Schuldverpflichtungen, Schul- und Berufsausbildungsabschluss, Unterhaltspflichtige, frühere Ehegatten usw. bei sich verwahren. Höchste Zeit, dass diese Rechtslage, auf die mein Amt schon vor einigen Jahren hingewiesen hat (vgl. 16. Tätigkeitsbericht 1995, LT-Drs. 11/6900, S. 69), endlich beachtet wird.

3. Aus der Arbeit der Jugendämter

Die Jugendämter sollen vor allem junge Menschen in ihrer Entwicklung fördern, Kinder und Jugendliche vor Gefahren für ihr Wohl schützen, aber auch Eltern und Erziehungsberechtigte beraten und unterstützen. Dazu benötigen sie eine Vielzahl von Informationen, speichern und nutzen sie und geben sie weiter. Die dafür maßgebenden Regelungen finden sich im Achten und im Zehnten Buch des Sozialgesetzbuchs (SGB VIII und SGB X).

3.1 Der Vordruck in der Jugendhilfe

Wer glaubt, dass der Einsatz von Erhebungsvordrucken allein für Sozialämter ein datenschutzrechtliches Problem ist, täuscht sich. Auch in der Jugendhilfe schießen Erhebungsvordrucke oftmals über das Ziel hinaus. Hier nur ein Beispiel aus der Prüfpraxis meines Amtes:

Die Jugendhilfe kostet Geld. Deshalb sieht das SGB VIII vor, dass die Jugendämter Kinder oder Jugendliche und ihre Eltern in allerdings unterschiedlichem Umfang zu den Kosten der Jugendhilfemaßnahmen heranzuziehen haben. Das gilt freilich nicht für die Kosten von ambulanten Erziehungshilfen. Dazu gehören die Erziehungsbeistandschaft, die Familienhilfe und die soziale Gruppenarbeit. Verschiedene Jugendämter verwenden ein und denselben Antragsvordruck für eine Reihe von Maßnahmen. Er wird eingesetzt, ganz gleich ob Tagespflege, Vollzeitpflege, Heimerziehung, eine sonstige Maßnahme oder eine ambulante Erziehungshilfe beantragt wird. Dieser Vordruck sieht u. a. auch Angaben über Einkommens- und Vermögensverhältnisse vor. Das hat zur Folge, dass sich die Antragsteller dazu genötigt sehen, diese Angaben auch dann zu machen, wenn es nur um ambulante Erziehungshilfen geht, obwohl sie dafür völlig irrelevant sind.

Ganz ähnlich verhält es sich, wenn Kinder und Jugendliche zu einem Kostenbeitrag herangezogen werden sollen. Maßgebend dafür ist nur das Einkommen, nicht aber das Vermögen. Angaben zum Vermögen sind deshalb nicht erforderlich, ihre Erhebung damit unzulässig. Gleichwohl sieht der dafür eingesetzte Vordruck solche Fragen vor.

3.2 Der getäuschte Arbeitgeber

Das am 1. Juli 1998 in Kraft getretene Beistandsgesetz schaffte die gesetzliche Amtspflegschaft für nichteheliche Kinder ab und führte die Beistandschaft als allgemeines Rechtsinstitut für allein erziehende Elternteile ein. Bei der Beistandschaft (Amtsbeistandschaft) handelt es sich um eine öffentliche Aufgabe des Jugendamts. Sie ist in den §§ 1712 ff. des Bürgerlichen Gesetzbuches (BGB) geregelt. Das Jugendamt, genauer gesagt ein Mitarbeiter/eine Mitarbeiterin des Jugendamts, dem/der die Ausübung der Beistandschaft übertragen wird (§ 55 Abs. 2 SGB VIII), wird damit auf Antrag zum gesetzlichen Vertreter des Kindes. Eine Aufgabe des Beistands kann es sein, den Unterhaltsanspruch des Kindes gegen den unterhaltspflichtigen Elternteil geltend zu machen. Dazu kann der Beistand von diesem Auskunft über sein Einkommen und sein Vermögen verlangen, soweit dies zur Feststellung eines Unterhaltsanspruchs erforderlich ist. Darüber hinaus kann er von ihm Belege, insbesondere Bescheinigungen des Arbeitgebers über die Höhe der Einkünfte anfordern. Dabei kann es hin und wieder Probleme geben. So auch in einem an mich herangetragenen Fall:

Der Beistand eines nichtehelichen Kindes hatte zunächst versucht, sich vom Vater des Kindes die für die Berechnung der Unterhaltshöhe notwendigen Angaben über dessen derzeitiges Arbeitseinkommen geben zu lassen. Da dieser dem nicht vollständig nachkam, wandte er sich an den Arbeitgeber des Vaters, der ihm dann auch die gewünschten Informa-

tionen mitteilte. Dass der Beistand den Arbeitgeber um Auskunft anging, nachdem zuvor Anfragen beim Vater erfolglos geblieben waren, war durchaus korrekt. Auch wenn der Arbeitgeber dabei von der Existenz eines nichtehelichen Kindes seines Mitarbeiters erfährt, kann ein Beistand diesen Weg jedenfalls dann gehen, wenn der Unterhaltspflichtige zur Erteilung der notwendigen Auskünfte und Vorlage der Nachweise nicht oder nur unvollständig bereit ist. Nicht korrekt war dann allerdings, dass der Beistand bei seiner Anfrage beim Arbeitgeber des Vaters den Eindruck erweckte, der Arbeitgeber sei zur Erteilung der gewünschten Auskunft verpflichtet. Eine solche Auskunftspflicht besteht nämlich nicht. Einem Jugendamt ist es aber auch in seiner Funktion als Beistand wegen seiner Bindung der Verwaltung an Gesetz und Recht verwehrt, sich durch eine Täuschung Informationen zu verschaffen. Ich habe deshalb das Jugendamt aufgefordert dafür Sorge zu tragen, dass ein solches Vorgehen künftig unterbleibt.

3.3 Wo ist das Jugendamt?

Wer den Organisationsplan des Landratsamts Alb-Donau-Kreis liest, wird dort vergeblich nach dem Jugendamt suchen. Eine Organisationseinheit Jugendamt existiert dort nämlich nicht mehr. Wie in anderen Landratsämtern gibt es dort zwar ein Sozialdezernat. Dieses ist aber nicht wie anderswo in die Bereiche Sozialamt, Jugendamt und u. U. Ausgleichsamt, sondern nur noch in die Ämter 1 und 2 untergliedert. In diesen Ämtern werden insgesamt 9 Sachgebiete mit entsprechender Sachgebietsleitung gebündelt. Ein Sachgebiet umfasst z. B. die Bereiche Sozialhilfe und wirtschaftliche Jugendhilfe, ein weiteres den Bezirkssozialdienst, die Schuldnerberatung, die vorbeugende Jugendhilfe, das Aufgabengebiet Mutter-Kind, die Adoptionen sowie die Alten- und Behindertenhilfe. Ein Sachgebiet beinhaltet die Jugendpflege, die Suchtvorbeugung, die Jugendgerichtshilfe, die Betreuung von Spätaussiedlern und Flüchtlingen.

Diese Organisationsstruktur des Landratsamts ignoriert die historisch gewachsene Organisation des örtlichen Trägers der öffentlichen Jugendhilfe, wie sie auch im SGB VIII vorgesehen ist. Nach § 69 Abs. 3 SGB VIII hat nämlich jeder örtliche Träger der öffentlichen Jugendhilfe – hier der Landkreis – für die Wahrnehmung der Aufgaben nach dem SGB VIII ein Jugendamt zu errichten. Die Aufgaben des Jugendamtes werden nach § 70 Abs. 1 SGB VIII durch den Jugendhilfeausschuss und die Verwaltung des Jugendamtes wahrgenommen. Aus diesen gesetzlichen Regelungen folgt die Verpflichtung des Landkreises, ein Jugendamt als selbstständige Organisationseinheit innerhalb seiner Verwaltung zu organisieren. Dafür ist es natürlich nicht zwingend erforderlich, die Organisationseinheit als „Amt“ einzurichten. Die Aufgaben der Jugendhilfe können nach der Organisationshoheit des Landkreises auch einer anderen Ebene zugeordnet werden. Entscheidend ist allein, und dies ist das Gebot dieser Vorschriften, dass die Erfüllung der Aufgaben der Jugendhilfe einer selbstständigen zweigliedrigen (Jugendhilfeausschuss und Verwaltung) Organisationseinheit obliegt. Die vom Landratsamt praktizierte Zusammenlegung von Aufgaben und Ämtern, insbesondere die Auflösung des Jugendamtes, steht damit in offenkundigem Widerspruch zu § 69 Abs. 3 SGB VIII und sollte deshalb auch ein Fall für die Rechtsaufsicht sein.

Diese beim Landratsamt praktizierte Organisationsform des Sozialdezernats ist aber auch aus Sicht des Datenschutzes bedenklich. Dabei geht es vor allem um die Auflösung des Jugendamtes. Die Zusammenlegung seiner Aufgabenbereiche mit den Aufgaben des Landkreises als örtlicher Träger der Sozialhilfe und mit staatlichen Aufgaben des Landratsamts, wie der Flüchtlingsunterbringung, in gemeinsamen Sachgebieten birgt die Gefahr in sich, dass das Recht auf informationelle Selbstbestimmung der Hilfesuchenden und Leistungsempfänger nicht hinreichend gewahrt wird. Für die einzelnen Aufgaben sind personenbezogene Angaben nach ganz unterschiedlichen rechtlichen Regelungen zu erheben und zu verarbeiten. Diese Angaben dürfen, wenn überhaupt, nur unter ganz bestimmten Voraussetzungen ausgetauscht und für andere Aufgaben ver-

wendet werden. So können insbesondere Sozialhilfedaten und Jugendhilfedaten als Sozialdaten nur nach Maßgabe besonderer Vorschriften des SGB X sowie ergänzender und abweichender besonderer Vorschriften des SGB VIII von einem Bereich zu einem anderen übermittelt werden. Mit der beim Landratsamt praktizierten Organisation ist aber insbesondere die vom Gesetzgeber geforderte Abschottung der Aufgaben des Jugendhilfeträgers nicht mehr zu gewährleisten. Der Gesetzgeber hielt es für angezeigt, für die vielfältigen Aufgaben des Jugendamtes einen jugendhilfespezifischen Datenschutz in das SGB VIII einzufügen. Danach sind sogar Vorgänge innerhalb des Jugendamtes gegenüber anderen Aufgaben des Jugendamtes streng abzuschotten. Was für Aufgaben innerhalb des klassischen Jugendamtes gilt, muss erst recht für die datenschutzgerechte Abgrenzung dieser Aufgaben im Verhältnis zu anderen Organisationseinheiten gelten.

Ich forderte deshalb das Landratsamt auf, zu der Organisationsstruktur zurückzukehren, wie sie dem SGB VIII zugrunde liegt. Wie nicht anders zu erwarten, stieß ich damit auf wenig Gegenliebe. Die Organisationsstruktur des Sozialdezernats trage sehr wohl der Regelung des § 69 Abs. 3 SGB VIII Rechnung, heißt es jetzt von Seiten des Landratsamtes. Die Aufgabenerledigung erfolge innerhalb des Sozialdezernats selbstständig in der vorgesehenen zweigliedrigen Organisationseinheit. Dass dies nach der beschriebenen Struktur aber gerade nicht möglich ist, wird beim Landratsamt offensichtlich verdrängt. Diese Antwort des Landratsamts kann nicht das letzte Wort gewesen sein.

3.4 Datenschutz auch bei der Familienhilfe!

Die sozialpädagogische Familienhilfe ist eine Leistung der Jugendhilfe. Nach § 31 SGB VIII soll die sozialpädagogische Familienhilfe durch intensive Betreuung und Begleitung Familien in ihren Erziehungsaufgaben, bei der Bewältigung von Alltagsproblemen, bei der Lösung von Konflikten und Krisen sowie im Kontakt mit Ämtern und Institutionen unterstützen und Hilfe zur Selbsthilfe geben. Sie ist in der Regel auf längere Dauer angelegt und erfordert die Mitarbeit der Familie. Mit diesem Profil nimmt die Hilfe eine Sonderform im Katalog der Erziehungshilfen ein, da nicht einzelne Personen Adressat eines Angebots des Jugendamts sind, sondern die Familie als Ganzes im Zentrum der Hilfe steht. Die Familienhilfe ist ein fester Bestandteil der Angebotspalette der Jugendämter. Sie tritt organisatorisch in verschiedenen Formen auf. Mal sind die Familienhelfer/innen Bedienstete der Landratsämter, mal sind sie freie Mitarbeiter/innen bei den Landratsämtern, mal wird die gesamte Familienhilfe an einen freien Träger vergeben.

Bei zwei Kontrollbesuchen nahmen wir u. a. die datenschutzgerechte Organisation der Familienhilfe unter die Lupe. Wir stellten fest, dass der Datenschutz dabei nicht ausreichend berücksichtigt worden ist.

Bereits mit dem Begriff „ambulante Erziehungshilfe“ wird deutlich, dass die Familienhelfer/innen ihre Arbeit ganz überwiegend in der Familie verrichten. Aufgrund der zuweilen sehr großen Zahl der in diesem Leistungsfeld Tätigen stehen in der Regel auch keine Büroräume im Jugendamt zur Verfügung. Vielmehr sind Familienhelfer/innen für Vor- und Nachbereitung ihrer Tätigkeit regelmäßig auf ihre Privaträume angewiesen. Geschieht dies, haben die Familienhelfer/innen auch dort gewisse organisatorische und technische Anforderungen zu beachten. Jeder Bürger hat nämlich das Recht auf eine ordnungsgemäße Verarbeitung seiner personenbezogenen Daten. Das muss auch gewährleistet sein, wenn die Datenverarbeitung in der häuslichen Umgebung der Familienhelfer/innen stattfindet. Gerade dort sind nämlich personenbezogene Angaben einer erhöhten Gefahr zufälliger Kenntnisnahme durch Familienmitglieder oder Besucher ausgesetzt. Deshalb sollten Familienhelfer/innen bei der Verarbeitung von Sozialdaten in den eigenen Räumen zumindest folgenden Anforderungen Rechnung tragen:

– Es sind geeignete Maßnahmen zu treffen, die eine Kenntnisnahme, Nutzung und Manipulation der personenbezogenen Daten durch Mitbewohner/innen oder Bezugspersonen ausschließen.

– Im Falle eines Aktentransports oder Transports elektronischer Datenträger zwischen dem Amt oder dem Anstellungsträger und dem häuslichen Arbeitsbereich sollten verschlossene Behältnisse verwendet werden.

– Beim Einsatz von PC ist sicherzustellen, dass nur dem/der Familienhelfer/in ein Zugriff auf die gespeicherten Daten möglich ist.

Handelt es sich um einen Bediensteten/eine Bedienstete des Jugendhilfeträgers, sollte sich die Beachtung dieser Vorgaben von selbst verstehen. Aber auch bei der Wahrnehmung der Aufgaben der Familienhilfe durch einen freien Träger gilt mitnichten das Prinzip „Aus den Augen aus dem Sinn“. Das Jugendamt muss vielmehr zunächst den freien Träger darauf hinweisen, dass übermittelte Sozialdaten dort im gleichen Umfang geheim zu halten sind, wie dies auch für die Geheimhaltung beim Jugendamt gilt. Zudem sind die vom Jugendamt an den freien Träger übermittelten Daten dort nur zu dem Zweck zu verwenden, zu dem sie ihm mitgeteilt wurden (§ 78 SGB X). Damit aber nicht genug. Beteiligt nämlich – wie hier – ein Leistungsträger einen Dritten an der Wahrnehmung seiner Aufgaben, so muss er sicherstellen, dass dieser Dritte die Gewähr für eine sachgerechte, die Rechte und Interessen der Betroffenen wahrende Erfüllung der Aufgaben bietet. Zu diesen Rechten gehört auch der Sozialdatenschutz. Deshalb muss mit dem freien Träger zumindest vertraglich vereinbart werden, dass die Bestimmungen zum Schutz der Sozialdaten (§ 35 SGB I, §§ 67 bis 84 a SGB X) zu beachten sind und die dazu notwendigen technischen und organisatorischen Schutzvorkehrungen getroffen werden müssen.

Zu fordern ist auch, dass sich das Jugendamt ein Kontrollrecht vor Ort vertraglich einräumen lässt. Es ist nämlich gerade nicht, wie ein Landratsamt geäußert hat, allein Sache des freien Trägers, sich um den dortigen Datenschutz zu bemühen. Vielmehr trifft das Jugendamt eine Sicherstellungspflicht.

3.5 Die Pflegefamilie und der Sozialdatenschutz

Das SGB VIII sieht die sog. Vollzeitpflege als eine Leistung der Jugendhilfe vor (§ 33 SGB VIII). Diese Hilfe zur Erziehung soll u. a. entsprechend Alter und Entwicklungsstand dem Kind oder dem Jugendlichen in einer anderen Familie eine zeitlich befristete Erziehungshilfe oder eine auf Dauer angelegte Lebensform bieten. Die Vollzeitpflege ist keine typische Leistung des Jugendamts selbst, sondern eine Hilfe im privaten Raum unter Beteiligung des Jugendamts. Die Leistung wird dabei durch Personen erbracht, die für diese Aufgabe nicht eigens ausgebildet sind.

Ein Jugendamt wandte sich in diesem Zusammenhang gleich mit mehreren Fragen an mich. Hintergrund seiner Anfrage war u. a., dass ein Pflegevater mit personenbezogenen Angaben des Pflegekindes und dessen leiblicher Familie die Öffentlichkeit gesucht hatte. Das Jugendamt wollte deshalb wissen,

– wie und wo der Datenschutz bei Vollzeitpflegefamilien gesetzlich geregelt ist,

– in welchen Grenzen die Pflegeeltern den Datenschutz zu beachten haben,

– welche Pflichten für den Träger der öffentlichen Jugendhilfe daraus entstehen und

– was es bei Datenschutzverstößen durch die Pflegeeltern tun kann.

Die Pflegefamilie, die sich auf Betreiben des Jugendamts eines Kindes/Jugendlichen annimmt, ist trotz der gesetzlichen Regelung der Vollzeitpflege keine öffentliche Stelle oder gar ein Institut der Jugendhilfe. Sie wäre dann auch einer ständigen Kontrolle zugänglich. Das darf nicht sein. Schon von daher findet das Landesdatenschutzgesetz auf die Pflegefamilie keine Anwendung. Auch das Bundesdatenschutzgesetz, das die Datenverarbeitung im nichtöffentlichen Bereich regelt, ist nicht

einschlägig. Dieses Gesetz macht nämlich nur Vorgaben für geschäftsmäßige, für berufliche oder für gewerbliche Zwecke stattfindende private Datenverarbeitung. Schließlich erfassen auch die Vorschriften des Sozialdatenschutzes im Zehnten Buchs des Sozialgesetzbuchs (SGB X) die Pflegefamilie nicht unmittelbar. Werden aber Personen, die nicht selbst Leistungsträger sind, Sozialdaten übermittelt, wie hier der Pflegefamilie, die durch das Jugendamt Angaben zu dem Pflegekind erfährt, so sieht § 78 Abs. 1 SGB X einen sog. verlängerten Sozialdatenschutz vor. Danach müssen die Empfänger die Daten in demselben Umfang geheim halten wie das Jugendamt und dürfen diese Daten auch nur zu dem Zweck verwenden, zu dem sie ihnen übermittelt wurden. Dem verlängerten Sozialdatenschutz und der Zweckbindung unterfallen alle Angaben, die das Jugendamt der Pflegefamilie über das Pflegekind und über dessen leibliche Eltern übermittelt.

Der Verwendung dieser Daten durch die Pflegefamilie sind damit Grenzen gezogen. Sie darf sie nur im Rahmen der Hilfe zur Erziehung und zum Wohle des Kindes oder Jugendlichen in ihrer Funktion als Pflegefamilie verwenden.

Das Jugendamt ist nach § 78 Abs. 2 SGB X verpflichtet, die Pflegeeltern auf die Zweckbindung sowie den verlängerten Sozialdatenschutz ausdrücklich hinzuweisen. Möchte das Jugendamt die Einhaltung von Datenschutzbestimmungen bei der Pflegefamilie einfordern, so muss es die Beachtung des Datenschutzes zum Gegenstand der Pflegevereinbarung machen. Haben sich die Pflegeeltern vertraglich gebunden, können sie auch zur Einhaltung der Schutzvorschriften aufgefordert werden.

3.6 Schweigepflicht des Berufspsychologen gegenüber seinem Vorgesetzten

Es ist mehr als erstaunlich, dass die in § 203 Abs. 1 des Strafgesetzbuches (StGB) aufgeführten Berufsgeheimnisse Behörden immer wieder Probleme bereiten. Insbesondere Vorgesetzte tun sich schwer damit, die Reichweite dieser Geheimhaltungspflichten zu akzeptieren. So wollte ein Landratsamt, dessen Jugendamtsleiter Einsicht in die Klientenakten von dort beschäftigten Psychologen begehrte, von mir Folgendes wissen:

- Besteht die Schweigepflicht des Psychologen auch gegenüber dem Jugendamtsleiter?
- Ist der Schweigepflicht genügt, wenn die Namen der Betroffenen unkenntlich gemacht werden?
- Reicht für eine Entbindung von der innerbehördlichen Schweigepflicht eine entsprechende Information des Klienten vor Beginn der Therapie aus?

Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung dürfen nach § 203 Abs. 1 Nr. 2 StGB all das, was ihnen bei der Ausübung dieser Tätigkeit anvertraut oder sonst bekannt wird, namentlich ein zum persönlichen Lebensbereich gehörendes fremdes Geheimnis, nicht unbefugt offenbaren. Eine Offenbarung liegt dabei immer schon dann vor, wenn das Geheimnis einer nicht an der Behandlung oder Beratung beteiligten Person mitgeteilt wird. Deshalb kann es keine Frage sein, dass die Schweigepflicht auch behördenintern zu beachten ist. Eine gesetzliche Befugnis, die es einem Psychologen erlaubt, solche Geheimnisse seinem nicht unmittelbar in die Beratung eingeschalteten Vorgesetzten mitzuteilen, existiert nicht. Insbesondere legitimiert das dienstrechtliche Weisungsrecht nicht die Durchbrechung der Schweigepflicht. Für die Praxis bedeutet das: Gewährt ein Psychologe einem nicht in die Beratung einbezogenen Vorgesetzten Einblick in Beratungsprotokolle, dann offenbart er Geheimnisse i. S. von § 203 Abs. 1 StGB. Er darf das deshalb nur tun, wenn dafür eine Befugnis gegeben ist. Ansonsten bricht er seine Schweigepflicht und macht sich strafbar. In der Regel wird in solchen Fällen als Befugnis lediglich die Einwilligung des Klienten in Betracht kommen.

Anders wäre die Rechtslage nur dann, wenn die Protokolle vor der Einsichtnahme z. B. durch Schwärzung so verändert würden, dass nicht

mehr festzustellen ist, auf welche Personen sich die darin enthaltenen Angaben beziehen. In diesem Falle wäre nämlich die Schweigepflicht nicht tangiert. Das bloße Unkenntlichmachen des Namens des Klienten wird dafür allerdings nicht ausreichen. Mit Hilfe der übrigen Einzelangaben und des für einen Vorgesetzten beschaffbaren Zusatzwissens kann meist noch ein Personenbezug hergestellt werden.

Im Ergebnis bedeutet dies, dass ein Vorgesetzter nur dann Einblick in die Beratungsakte erhalten darf, wenn der Klient sein Einverständnis hierzu erteilt. Dazu muss man den Klienten vor der Beratung unmissverständlich darauf hinweisen, dass auch der an der Beratung nicht beteiligte Vorgesetzte Kenntnis vom Gegenstand der Gespräche und Einblick in die Aufzeichnungen über die Beratung nehmen wird.

Eine effektive Beratung setzt freilich voraus, dass zwischen Beratenem und Berater ein Vertrauensverhältnis entsteht. Man stelle sich nun vor, einem Klienten wird vor der Beratung und Therapie eröffnet, dass auch Dritte über das, was dabei gesprochen wird, informiert werden. Wie soll unter dieser Voraussetzung eine Vertrauensbasis entstehen? Ich empfahl deshalb dringend, im Interesse einer effektiven Beratung von der Einholung einer derartigen Einwilligung abzusehen. Schon gar nicht sollte die Beratung von der Abgabe einer entsprechenden Einwilligungserklärung abhängig gemacht werden.

4. Teil: Justiz und Polizei

1. Abschnitt: Die Justiz

Justiz und Justizverwaltung kann man sich ohne Verarbeitung personenbezogener Daten gar nicht vorstellen. Jedem, der sich schon einmal mit diesem Thema befasst hat, ist dies ohne weiteres klar. Er weiß spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 aber auch, dass Behörden und Gerichte Angaben über Personen wegen des damit einhergehenden Eingriffs in das Grundrecht auf informationelle Selbstbestimmung nur erheben, speichern, verwenden oder weitergeben dürfen, wenn und soweit dies der Gesetzgeber im überwiegenden Allgemeininteresse zugelassen hat. Nimmt man Justiz und Justizverwaltung unter diesem Blickwinkel in Augenschein, fällt der Befund unterschiedlich aus. Neben Bereichen, in denen auch heute noch – wie etwa in der Zivilprozeßordnung und in der Verwaltungsgerichtsordnung – weiße Flecken vorherrschen, stehen andere, in denen es inzwischen eine komplette gesetzliche Regelung der Informationsverarbeitung gibt. Beispielsweise ist im Justizmitteilungsgesetz vom 18. Juni 1997 geregelt, welche Mitteilungen die ordentliche Gerichtsbarkeit und die Staatsanwaltschaften in Zivil- und Strafsachen an andere Stellen machen dürfen. Seit dem 4. Strafvollzugsänderungsgesetz vom 26. Aug. 1998 gibt es im Strafvollzugsgesetz Regelungen darüber, unter welchen Voraussetzungen die Justizvollzugsanstalten personenbezogene Daten von Strafgefangenen und anderen Personen verarbeiten dürfen. Eine gesetzliche Regelung der Informationsverarbeitung ist freilich kein Wert an sich. Es kommt vielmehr darauf an, inwieweit dabei dem Grundrecht auf Datenschutz Rechnung getragen worden ist. Dies ist bei diesen beiden Gesetzesvorhaben nicht im gebotenen Maße gelungen (vgl. 18. Tätigkeitsbericht 1997, Landtags-Drucksache 12/2242, S. 28 f.). Dieses Fazit gilt auch für die vor kurzem in die Strafprozeßordnung eingefügten Datenverarbeitungsregelungen. Nachdem es der Gesetzgeber jahrelang versäumt hatte, für die in Strafverfahren anfallenden hoch sensiblen personenbezogenen Informationen Datenschutzregelungen zu verabschieden, und mehrere Entwürfe eines Strafverfahrensänderungsgesetzes am Widerstand der Länder gescheitert waren, komplettierte er mit dem Strafverfahrensänderungsgesetz 1999 vom 2. Aug. 2000 die Datenverarbeitungsvorschriften in der Strafprozeßordnung. Dieses Gesetzesvorhaben stand von Anfang an unter keinem guten Stern. Der von der Bundesregierung 1999 vorgelegte Gesetzentwurf verschlechterte sogar die aus der Sicht des Datenschutzes ohnehin unzureichenden Regelungen der vorherigen Entwürfe. Der Bundesrat tat noch ein Übriges: Weil ihm das Datenschutzniveau des Gesetzesbeschlusses des Bundestags immer noch zu hoch war, rief er

den Vermittlungsausschuss an. Diese Entwicklung veranlasste meine Kollegen und mich, den Vermittlungsausschuss aufzufordern, die Änderungsanträge des Bundesrats zurückzuweisen (vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 zum Strafverfahrensänderungsgesetz 1999, Anhang 2). Herausgekommen ist ein Gesetz, das Kritik vor allem deshalb verdient, weil die Zweckbindung von Daten zur Gefahrenabwehr und der Strafverfolgung nahezu vollständig aufgehoben wird, die Staatsanwaltschaften Daten aus Ermittlungsverfahren auch zur Verfolgung künftiger Straftaten in Dateien speichern dürfen, obwohl die Polizei solche Datensammlungen auf bundesrechtlicher Grundlage bereits seit langem besitzt, ein gemeinsamer Datenpool der Justizbehörden eingeführt wird unabhängig davon, ob die Informationen für die konkreten Aufgaben wirklich erforderlich sind und weil nicht am Strafverfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die gesetzliche Regelung der Informationsverarbeitung ist eine Sache, die Umsetzung des Datenschutzes in der täglichen Behördenpraxis eine andere. Dass dabei die Datenschutzrechte der Bürger zum Tragen kommen, ist eine der Aufgaben, die das Landesdatenschutzgesetz meinem Amt anvertraut hat. Dazu können wir Eingaben von Bürgern nachgehen, die sich an uns wenden, weil sie der Ansicht sind, bei der Verarbeitung ihrer personenbezogenen Daten durch eine öffentliche Stelle in ihren Rechten verletzt worden zu sein, generelle Kontrollen vor Ort durchführen oder – was einen immer breiteren Raum unserer Tätigkeit ausmacht – Behörden in Datenschutzfragen beraten und ihnen dabei Empfehlungen geben. Wenn wir dann aber auf die erbetene Äußerung zu unseren Vorschlägen und Beanstandungen warten und warten müssen oder unsere Argumente wie an einer Wand abprallen, ist dies nicht nur für uns unerquicklich, sondern steht vor allem der gebotenen Stärkung des Grundrechts auf Datenschutz unserer Bürger entgegen. Gerade solches passierte uns beim Justizministerium:

– Mitte September 1999 ließ ich dem Justizministerium einen umfassenden Bericht über die bei einer Kontrolle des EDV-Einsatzes in zwei Justizvollzugsanstalten festgestellten Mängel zukommen. Für seine Äußerung zu meinen Beanstandungen, Hinweisen und Vorschlägen setzte ich ihm eine angemessene Frist; es waren gut sieben Wochen. Dazu bin ich nach § 30 des Landesdatenschutzgesetzes (LDSG) gehalten, damit den festgestellten Mängeln unverzüglich nachgegangen wird. Kurz vor Ablauf der Äußerungsfrist stellte uns das Justizministerium vor vollendete Tatsachen: Es habe mit anderen Dingen alle Hände voll zu tun, ließ es mich wissen und vertröstete uns auf Februar/März 2000. Ob ich angesichts der festgestellten gravierenden Mängel der EDV-Verfahren, die es zügig zu beheben galt, damit einverstanden bin, fragte es mich erst gar nicht. Tatsächlich gekommen ist die Stellungnahme dann am 19. Mai 2000. Eine solche Vorgehensweise steht nicht nur mit dem Landesdatenschutzgesetz nicht im Einklang. Sie ist auch für meine Mitarbeiter, die oft nicht wissen, nach welcher Akte sie zuerst greifen sollen, ineffektiv, weil sie sich nach so langer Zeit praktisch wieder neu in die Materie einarbeiten müssen.

– In meinem Tätigkeitsbericht für das Jahr 1998 habe ich eingehend dargelegt, in welche Schwierigkeiten die Staatsanwaltschaften die Bürgermeisterämter hierzulande dadurch bringen, dass sie diesen bei Mitteilungen in Strafsachen zum Wählerverzeichnis nicht auch das Ende des durch eine strafgerichtliche Verurteilung eingetretenen Ausschlusses von der Wählbarkeit mitteilen (vgl. Landtags-Drucksache 12/4380, S. 41 ff.). Meinem Vorschlag, die Staatsanwaltschaften könnten doch in einem Zuge mit der Mitteilung über das Ende des Ausschlusses von der Wählbarkeit, die sie sowieso an das Bundeszentralregister absetzen müssen, auch die Bürgermeisterämter davon unterrichten, zeigte das Justizministerium die kalte Schulter; dies verursache zu viel Aufwand. Weil dies mit dem besten Willen nicht nachvollziehbar war, hakte ich nach. Wiederum führte das Justizministerium den hohen Verwaltungsaufwand ins Feld. Als ich es darauf hinwies, dass seiner Haltung unzutreffende Annahmen zugrunde liegen, beendete das Justizministerium die Diskussion. Jetzt, Ende Oktober 2000, leitete es mir eine Reihe von Vor-

schlägen zur Änderung der Anordnung über Mitteilungen in Strafsachen zu, die es einvernehmlich mit den anderen Justizverwaltungen erarbeitet hatte. Darin plädierte es – ich traute meinen Augen kaum – dafür, dass die Staatsanwaltschaften den Bürgermeisterämtern den Tag des Ablaufs des Verlustes der Wählbarkeit mitteilen sollen, weil sie diesen Zeitpunkt ja ohnehin für das Bundeszentralregister errechnen müssen. Schon recht so! Die Frage aber ist: Warum nicht gleich so und warum der hartnäckige Widerstand gegen meinen identischen Vorschlag von vor zwei Jahren?

Mancher, der all dies gelesen hat, wird sich fragen, welchen Stellenwert der Datenschutz eigentlich im Justizministerium einnimmt. Womöglich hilft es ihm weiter, wenn er weiß, wie sich das Justizministerium einer beabsichtigten Kontrolle beim Verwaltungsgericht Stuttgart in den Weg gestellt hat.

1. Die vereitelte Kontrolle beim Verwaltungsgericht Stuttgart

   In meinem Tätigkeitsbericht für das Jahr 1999 ist nachzulesen, wie das Justizministerium gesetzwidrig eine Datenschutzkontrolle verhindert hat. Wir wollten prüfen, ob die Amtsgerichte bei ihren Computern die technischen und organisatorischen Vorkehrungen getroffen haben, die für einen datenschutzgerechten Einsatz der EDV-Technik unerlässlich sind (vgl. Landtags-Drucksache 12/4600, S. 68 f.). Dies war kein einmaliger Ausrutscher. Im Berichtsjahr stellte es sich erneut einer Datenschutzkontrolle in den Weg. Dazu kam es so:

   Ein Mann aus dem Stuttgarter Raum, der seit 1991 mehrere Prozesse beim Verwaltungsgericht Stuttgart geführt hatte, kam bei einer Vorsprache an dessen Pforte darüber ins Grübeln, dass diese – wie er uns schrieb – am Computer Angaben über alle seine Prozesse abrufen konnte und ihm mir nichts dir nichts Auskunft darüber gab. Um uns ein näheres Bild davon machen zu können, baten wir das Verwaltungsgericht Stuttgart im schriftlichen Weg, uns die Praxis der Auskunftserteilung an seiner Pforte näher zu schildern und dabei insbesondere mitzuteilen, ob und wie sich jemand legitimieren muss, der dort vorspricht oder anruft und um eine Auskunft nachsucht, sowie welche Informationen die Pforte dazu im EDV-System des Verwaltungsgerichts Stuttgart abrufen kann. Das Verwaltungsgericht Stuttgart bestätigte, dass an seiner Pforte die Posteingangsstelle bestimmte Auskünfte erteilt und dabei Zugriff auf die in seinem EDV-Verfahren JULIA erfassten kompletten Stammdaten der Prozessparteien hat. Weil damit nicht alle unsere Fragen geklärt waren, wollten wir uns beim Verwaltungsgericht einen eigenen Eindruck vom Einsatz des JULIA-Verfahrens verschaffen und boten ihm dafür zwei Termine zur Auswahl an. Das rief das Justizministerium auf den Plan. Nach einem Telefonat mit ihm gab sich das bis dahin recht kooperative Verwaltungsgericht plötzlich ziemlich zugeknöpft und schwenkte auf die Linie des Justizministeriums ein: Keine Kontrollbefugnis, lautete jetzt die Devise. Auf meine Einwände legte es die Sache dem Justizministerium vor, das mir vor kurzem schrieb, es bleibe bei seinem Standpunkt. Die Ausstattung der Verwaltungsgerichte mit dem Verfahren JULIA sei für Zwecke der Rechtspflege erfolgt und unterliege damit nicht der Datenschutzkontrolle meines Amtes.

   Diese Auffassung des Justizministeriums beruht auf einer Verkennung der Reichweite der meinem Amt durch das Landesdatenschutzgesetz eingeräumten Kontrollzuständigkeit. Von dieser sind die Gerichte mit Rücksicht auf die verfassungsrechtlich garantierte Unabhängigkeit der Richter ausgenommen, soweit sie nicht in Verwaltungsangelegenheiten, sondern in Ausübung der Rechtsprechung tätig werden. So war dies in § 24 Abs. 4 des alten Landesdatenschutzgesetzes geregelt, unter dessen Ägide die Malaise beim Verwaltungsgericht Stuttgart begonnen hatte. So bestimmt dies auch § 2 Abs. 3 des neuen Landesdatenschutzgesetzes, denn diese Regelung stimmt insoweit mit der alten Vorschrift überein. Sie nimmt – wie die Gesetzesbegründung betont – die unabhängige Aufgabenerledigung der Gerichte von der Kontrollbefugnis meines Amtes aus. Anders gesagt: Wo die Gerichte nach den einschlägigen Verfahrensgesetzen in sachlicher Unabhängigkeit entscheiden, unterliegen sie der

Datenschutzkontrolle meines Amtes nicht. Dies habe ich seit jeher respektiert. Ist ihre Tätigkeit dagegen Weisungen durch das Justizministerium zugänglich und verarbeiten sie dabei personenbezogene Daten, unterliegen sie insoweit im Interesse eines effektiven Schutzes des informationellen Selbstbestimmungsrechts der betroffenen Bürger der Datenschutzkontrolle durch mein Amt. Gerade so liegen die Dinge im vorliegenden Fall.

– Dass mein Amt EDV-Verfahren bei Gerichten daraufhin überprüfen kann, ob die Justizverwaltung für dieses Verfahren die nach § 9 LDSG gebotenen technischen und organisatorischen Maßnahmen getroffen hat, habe ich bereits in meinem Tätigkeitsbericht für das Jahr 1999 (vgl. Landtags-Drucksache 12/4600, S. 68 f.) eingehend dargelegt. Diese Überlegungen gelten auch für das JULIA-Verfahren. Eine Kontrolle der richterlichen Datenverarbeitung oder gar der richterlichen Arbeitsweise am Fall – wie das Justizministerium befürchtet – findet dabei nicht statt. Die Überprüfung, ob bei der den Gerichten von der Justizverwaltung vorgegebenen EDV die nach § 9 LDSG gebotenen technischen und organisatorischen Maßnahmen getroffen sind, lässt sich sehr wohl ohne Rückgriff auf die konkrete richterliche Datenverarbeitung bewerkstelligen. Die nach dieser Vorschrift zu treffenden Datensicherungsmaßnahmen knüpfen nämlich an den von der Justizverwaltung eingesetzten EDV-Systemen und gerade nicht an den mit ihrer Hilfe von Richtern verarbeiteten personenbezogenen Daten an. Fragen zur Datensicherung wie etwa – um nur ein Beispiel zu nennen – zur Abschottung des internen Computernetzes eines Gerichtes gegenüber dem Internet oder zur Sicherheit der EDV-Anlage berühren die Arbeit eines Richters am Einzelfall nicht. Abgesehen davon kann die Verantwortung für die Gewährleistung der Sicherheit einer EDV-Anlage nicht auf die einzelnen Richter übertragen werden, weil diese Aufgabe nur mit EDV-Spezialwissen zu bewältigen ist und Richter hierfür nicht ausgebildet sind.

– Das Verwaltungsgericht setzt das EDV-Verfahren JULIA keineswegs nur für die Durchführung der einzelnen gerichtlichen Verfahren ein. Die Daten bleiben vielmehr auch noch nach Abschluss der gerichtlichen Verfahren gespeichert. Die sog. Stammdaten werden zu nahezu allen im Geschäftsbetrieb des Verwaltungsgerichts anfallenden Arbeiten genutzt. So z. B. können nicht nur alle Richter, sondern auch die Eingangsgeschäftsstelle online auf diese Stammdaten zugreifen und Recherchen durchführen. Soweit das Verwaltungsgericht die in JULIA gespeicherten personenbezogenen Daten auch noch nach Abschluss der gerichtlichen Verfahren weiter speichert und für in seinem Geschäftsbetrieb anfallende Arbeiten nutzt, wird es nicht mehr in Ausübung der Rechtsprechung tätig. Wenn das Justizministerium gleichwohl die Kontrollzuständigkeit meines Amtes negiert, übersieht es, dass von dieser nach dem Landesdatenschutzgesetz nur die unabhängige Aufgabenerledigung der Gerichte ausgenommen ist. So liegen die Dinge hier aber gerade nicht. Vielmehr handelt es sich dabei wie bei der Aufbewahrung von Akten nach Abschluss der Verfahren um eine Verwaltungsangelegenheit. Dass es sich bei der Aktenaufbewahrung nicht um Recht sprechende Tätigkeit, sondern um eine Angelegenheit der Justizverwaltung handelt, zeigt sich u. a. auch daran, dass das Justizministerium sich dazu berechtigt hält, die Aktenaufbewahrung in einer Verwaltungsvorschrift zu regeln. Es ist deshalb sehr wohl Aufgabe meines Amtes zu prüfen, wie lange personenbezogene Daten nach Abschluss von gerichtlichen Verfahren mit Hilfe des EDV-Verfahrens JULIA gespeichert bleiben dürfen und inwieweit das Bereithalten dieser Daten zur Verwendung für andere Verfahren sowie andere im Geschäftsbetrieb des Verwaltungsgerichts anfallende Aufgaben und die damit einhergehende Zweckänderung durch eine den Anforderungen unserer Verfassung an Eingriffe in das Recht auf informationelle Selbstbestimmung genügende Rechtsvorschrift gedeckt ist.

Was ist das Fazit? Beharrt das Justizministerium auf seiner Position und behält seine Wagenburgmentalität bei, steht letztendlich der Bürger als

Verlierer da. Der unabhängigen Datenschutzkontrolle, deren Beteiligung – so das Bundesverfassungsgericht – für den effektiven Schutz des Grundrechts auf Datenschutz von erheblicher Bedeutung ist, wären im Bereich der Gerichte praktisch die Hände gebunden.

2. Das Schlichtungsverfahren – wo bleibt der Datenschutz?

Wer in Nachbarschaftsstreitigkeiten, in Streitigkeiten wegen einer Verletzung seiner persönlichen Ehre, die nicht in Presse oder Rundfunk begangen worden ist, oder in Streitigkeiten wegen Ansprüchen auf Zahlung von Geld bis zu einem Betrag von 1500 DM die Hilfe der Amtsgerichte in Anspruch nehmen will, muss seit Juli 2000 zuvor ein Schlichtungsverfahren durchlaufen. Man verspricht sich davon, dass einvernehmliche Lösungen eher geeignet sind, dauerhaft Rechtsfrieden zu stiften, als gerichtliche Entscheidungen. Vor allem aber soll das Schlichtungsverfahren eine Entlastung für die Justiz bringen. Dazu werden bei den Amtsgerichten sog. Gütestellen eingerichtet. Den wesentlichen Part spielen dort die sog. Schlichtungspersonen. Ihre Sache ist vor allem die Durchführung der Schlichtungsverhandlung mit dem Ziel, den Streit unter den beteiligten Parteien zu bereinigen. Als Schlichter sollen in Baden-Württemberg in erster Linie Rechtsanwälte tätig werden. So ist es im Schlichtungsgesetz geregelt, das aus der Feder des Justizministeriums stammt und das am 1. Juli 2000 in Kraft getreten ist. An der Erarbeitung dieses Gesetzes hat das Justizministerium mein Amt nicht beteiligt, obwohl in den Vorschriftenrichtlinien der Landesregierung klipp und klar steht, dass meinem Amt frühzeitig Gelegenheit zu geben ist, zu Entwürfen von Gesetzen, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben, Stellung zu nehmen (vgl. Gemeinsames Amtsblatt 1997, S. 365 ff.). Seinen Gesetzentwurf bekamen wir erstmals zu Gesicht, als ihn die Landesregierung schon in den Landtag eingebracht und der Landtag ihn uns via Landtags-Drucksache 12/5033 ins Haus geliefert hatte. Darin konnten wir nicht nur sehen, dass das Justizministerium eine Vielzahl von öffentlichen Stellen und Verbänden bis hin zum ADAC – ganz anders als uns – um ihre Meinung zu seinem Gesetzesvorhaben gefragt hatte, sondern vor allem auch, dass eine Beteiligung meines Amtes bei der Erarbeitung des Gesetzentwurfs dringend geboten gewesen wäre. Der zentrale Schwachpunkt war: Der Gesetzentwurf des Justizministeriums enthielt keinerlei Regelung zur Datenverarbeitung im Schlichtungsverfahren. Kein Wort insbesondere dazu, aufgrund welcher Rechtsvorschriften die Gütestellen personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs (z. B. Haftpflichtversicherungen o. Ä.) übermitteln dürfen. Kein Wort dazu, ob und, wenn ja, unter welchen Voraussetzungen die Gütestellen solchen Personen oder Stellen Einsicht in ihre Akten über Schlichtungsverfahren geben dürfen. Keine Regelung für Mitteilungen der Gütestellen an öffentliche Stellen. Nichts dazu, welche technischen und organisatorischen Regelungen die Schlichtungspersonen treffen müssen, um einen datenschutzgerechten Umgang mit den von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten.

Die Antwort des Justizministeriums, das ich auf diese Schwachpunkte hingewiesen habe, erstaunte. Eine Datenübermittlung durch die Gütestellen und eine Einsichtnahme in ihre Akten sei im Schlichtungsgesetz nicht vorgesehen und deshalb konsequenterweise nicht geregelt, ließ es mich wissen. Weil es ihm offenbar doch dämmerte, dass es damit die Augen vor den Bedürfnissen der Praxis verschließen würde, ergänzte es sibyllinisch, es sei „im Einzelfall unter Berücksichtigung aller tatsächlichen Umstände zu entscheiden, ob der vorrangige Geheimhaltungsschutz für Berufs- und Amtsgeheimnisse, eine analoge Anwendung von § 299 ZPO oder die allgemeinen Datenschutzregelungen Anwendung finden“. Weil damit bei der späteren Praktizierung des Schlichtungsgesetzes Unklarheiten geradezu vorprogrammiert waren, schlug ich dem Justizministerium vor, im Rahmen des laufenden Gesetzgebungsverfahrens klarzustellen, dass für die Verarbeitung von personenbezogenen Daten durch die Gütestellen uneingeschränkt das Landesdatenschutzgesetz gilt; eine Rechtslage, die im Übrigen auch bei den von Körperschaften des öffentlichen Rechts (z. B. Landesärztekammer, Industrie- und Handelskammer) eingerichteten Gütestellen zu beachten ist. Mein Vorschlag fand leider keine Resonanz.

Eine klare Position hatte das Justizministerium dagegen von Anfang an in der Frage der Reichweite der Kontrollbefugnis meines Amtes bei der Datenverarbeitung der Gütestellen. Obwohl die Einschaltung der Gütestellen der Klageerhebung vorgeschaltet und als eigenständiges Verfahren ausgestaltet ist, das im Schlichtungsgesetz ausdrücklich als „außergerichtlich" bezeichnet wird, schlug das Justizministerium die Gütestellen kurzerhand den Gerichten zu. Dabei übersah es, dass die Gütestelle und nicht das Gericht, bei dem sie eingerichtet ist, nach der dem Landesdatenschutzgesetz zugrunde liegenden funktionalen Betrachtungsweise Daten verarbeitende Stelle und damit Adressat einer datenschutzrechtlichen Kontrolle ist. Ich kann die Haltung des Justizministeriums nicht akzeptieren und sehe darin einen weiteren Versuch, die als lästig empfundene unabhängige Datenschutzkontrolle zurückzudrängen und ihre Prüfmöglichkeiten zu beschneiden.

3. DNA-Analysen im Ermittlungsverfahren

Ein Mann aus der Ortenau schrieb uns, die bei der Polizeidirektion Offenburg gebildete Sonderkommission habe ihn im Zuge ihrer Ermittlungen zur Aufklärung von drei Mordfällen, die sich im Herbst 1999 im Stadtgebiet von Kehl zugetragen hatten, um die Abgabe einer Speichelprobe für eine DNA-Analyse gebeten. Er habe die Speichelprobe abgegeben. Die Einverständniserklärung habe er unter der Bedingung unterschrieben, dass all seine Daten nach Abschluss der Untersuchung vernichtet werden. Zu Hause habe er sich die Einverständniserklärung und die schriftlichen Erläuterungen dazu in Ruhe nochmals durchgelesen. Er könne sich danach mit dem besten Willen nicht vorstellen, was genau mit seiner Speichelprobe passiert und welche Informationen die Polizei und wer sonst noch über ihn speichert. Deshalb habe er tags darauf sein Einverständnis zurückgezogen.

Weil die Polizeidirektion Offenburg und die Staatsanwaltschaft Offenburg im Zuge der Ermittlungen wegen der drei Mordfälle 2800 Männer einem DNA-Test unterzogen hatten, der – wie ebenfalls in der Zeitung zu lesen war – samt und sonders ergeben hatte, dass die bei den Mordopfern aufgefundenen Tatspuren nicht von diesen Männern stammen, stand die Frage im Raum, wie Staatsanwaltschaft Offenburg und Polizeidirektion Offenburg dabei verfahren sind. Und das Ergebnis sieht so aus:

– Seit 1997 ist die Anwendung von DNA-Analysen zur Aufklärung von Straftaten in der Strafprozeßordnung geregelt (§ 81 e, § 81 f StPO). Nach diesen Vorschriften dürfen Speichelproben molekulargenetisch u. a. danach untersucht werden, ob aufgefundenes Spurenmaterial von dem Beschuldigten stammt. Solche Untersuchungen dürfen nach § 81 f StPO nur durch den Richter angeordnet werden. Wenn Staatsanwaltschaft Offenburg und Polizeidirektion Offenburg trotzdem meinten, in allen 2800 Fällen auf eine richterliche Anordnung verzichten und die DNA-Analyse mit schriftlichem Einverständnis der Männer vornehmen zu können, hätten sie diese zuvor wenigstens so aufklären müssen, dass sie sich eine im Wesentlichen zutreffende Vorstellung über die Verarbeitung ihrer Daten im Zusammenhang mit ihrer DNA-Analyse hätten machen können. Nur wenn so verfahren worden wäre, hätten die Männer die Tragweite ihrer Entscheidung erkennen und mithin wirksam einwilligen können. Diesen Anforderungen genügte die Vorgehensweise von Staatsanwaltschaft Offenburg und Polizeidirektion Offenburg bei der Einholung der Einverständniserklärungen nicht. Das dazu verwendete Hinweisblatt war auf eine ganz andere Fallgestaltung zugeschnitten und schon deshalb für die gebotene, umfassende Aufklärung der 2800 Männer nicht nur nicht geeignet, sondern teilweise sogar irreführend. Darin mussten sie lesen, die DNA-Analyse erfolge „zum Zwecke der Identitätsfeststellung im künftigen Strafverfahren". Zudem war darin davon die Rede, ihre Personalien und die DNA-Ergebnisse würden beim Bundeskriminalamt gespeichert. Tatsächlich erfolgten die DNA-Analysen zur Aufklärung der besagten drei Mordfälle; gespeichert wurden die Daten der Männer nicht beim Bundeskriminalamt – wofür es im Übrigen keine Rechtsgrundlage gegeben hätte –, sondern bei der Polizeidirektion Offenburg und bei den mit den DNA-Analysen befassten Stellen, von denen gleich noch die Rede sein wird. Um welche Stellen es sich dabei handelte und welche Daten dort über sie gespeichert werden, war dem

Hinweisblatt ebenso wenig zu entnehmen wie Angaben darüber, welche Daten im Einzelnen bei der Polizeidirektion Offenburg gespeichert und an welche andere Stellen von dort aus weitergegeben werden. Dass die den 2800 Männern in dem Hinweisblatt gegebene Zusicherung, die Speichelproben würden anonym an die Untersuchungsstellen weitergegeben und unverzüglich nach Feststellung des DNA-Identifizierungsmusters vernichtet, in der Praxis dann doch nicht eingehalten wurde, passte ins Bild. Kurzum: Den 2800 Männern waren beim Unterschreiben der Einverständniserklärung die für ihre Entscheidung für eine Teilnahme an den DNA-Tests maßgeblichen Umstände nicht bekannt. Diese unzureichende Aufklärung musste ich beanstanden.

Das Innenministerium antwortete mir vor kurzem. Obwohl der Leiter der Sonderkommission meinem Mitarbeiter auf Nachfrage erklärt hatte, dass das besagte Hinweisblatt in allen Fällen verwendet worden war und obwohl das Innenministerium einräumen musste, dass die Polizeidirektion Offenburg in ihren Akten gar nicht festgehalten hat, welchem Mann sie welches Hinweisblatt bei der Einholung der Einverständniserklärung ausgehändigt hatte, soll sie jetzt plötzlich den Männern im Großen und Ganzen die richtigen Hinweisblätter ausgehändigt und sich nur bei etwa 10 % der Fälle beim Einverständnisformular vergriffen haben. Insoweit sei die Einwilligung in der Tat unwirksam. Ferner meinte es, anhand der Informationen auf dem Hinweisblatt habe sich der Betroffene eine klare Vorstellung von Sinn und Tragweite seiner Entscheidung machen können. Das mag für einen Insider der polizeilichen Datenverarbeitung so sein, für andere Personen, auf die es hier maßgeblich ankommt, gilt dies jedoch nicht. Wenn es nach dem Innenministerium geht, braucht die Polizei den Personen, die in eine DNA-Analyse einwilligen, auch nicht sagen, welche Stelle sie mit der DNA-Analyse beauftragt. Haben es diese Personen, die ja mit der Polizei kooperieren, wirklich verdient, insoweit schlechter gestellt zu werden als diejenigen, die nicht einwilligen und bei denen Polizei und Staatsanwaltschaft deshalb auf die Herbeiführung einer richterlichen Anordnung angewiesen sind? Diese Personen können nämlich in der richterlichen Anordnung nachlesen, welche Stelle die DNA-Analyse durchführt; der Richter muss sie nach § 81 f StPO in seiner Anordnung bestimmen.

– Muss jemand aufgrund einer richterlichen Anordnung eine DNA-Analyse hinnehmen, ist dem Sachverständigen das Untersuchungsmaterial ohne Angabe des Namens, der Anschrift und des Geburtstages und -monats zu übergeben. Diesen Geheimnisschutz, den der Gesetzgeber in § 81 f StPO wegen den mit DNA-Analysen einhergehenden besonderen Risiken für das informationelle Selbstbestimmungsrecht vorgesehen hat, haben auch Personen wie die 2800 Männer aus dem Kehler Raum verdient, die der Bitte von Staatsanwaltschaft Offenburg und Polizeidirektion Offenburg nachgekommen sind und ohne richterliche Anordnung eine Speichelprobe für eine DNA-Analyse abgegeben haben. Dass die Speichelproben dem entgegen mit Familien- und Vorname sowie vollständigem Geburtsdatum beschriftet an das Rechtsmedizinische Institut der Universität Freiburg weitergegeben worden waren, habe ich ebenfalls beanstandet. Entscheidend fiel dabei ins Gewicht, dass sich die Polizeidirektion Offenburg über ihre in den Hinweisen zur Einverständniserklärung gegebene Zusage, das Untersuchungsmaterial dem Rechtsmedizinischen Institut ohne Mitteilung des Namens und des Geburtstages und -monats zu übergeben, hinweggesetzt hat. Seit August 2000 verfährt die Polizeidirektion Offenburg – wie das Innenministerium mich auf die Beanstandung wissen ließ – korrekt.

– Nach § 81 a der Strafprozeßordnung sind Speichelproben unverzüglich zu vernichten, wenn sie für Zwecke des der Entnahme zugrunde liegenden oder eines anderen anhängigen Ermittlungsverfahrens nicht mehr erforderlich sind. Diese gesetzliche Vorgabe war in dem Hinweisblatt, das die Sonderkommission den 2800 Männern bei der Einholung ihres Einverständnisses in die DNA-Analysen ausgehändigt hatte, dahingehend präzisiert, dass das „Untersuchungsmaterial nach Feststellung des DNA-Identifizierungsmusters unverzüglich vernichtet (wird)“. Diese Zusage war nicht mehr als recht und billig. Denn ab diesem Zeitpunkt war nach

dem Ergebnis der DNA-Analyse eindeutig belegt, dass der betreffende Mann mit der Person, von der das bei den Mordopfern aufgefundene Spurenmaterial herrührt, nicht identisch ist. Man kann nämlich – wie DNA-Experten betonen – davon ausgehen, dass es mit Ausnahme von eineiigen Zwillingen keine zwei Menschen auf der Welt gibt, die ein identisches DNA-Identifizierungsmuster besitzen. Auf unsere Fragen mussten Staatsanwaltschaft Offenburg und Polizeidirektion Offenburg einräumen, dass sie die Speichelproben keineswegs, wie versprochen, nach Feststellung des DNA-Identifizierungsmusters vernichtet hatten, sondern weiterhin aufbewahrten. Inzwischen sind – wie uns das Innenministerium schrieb – die Speichelproben in Freiburg und die Speichelproben, die das Rechtsmedizinische Institut der Universität Freiburg wegen Überlastung seiner Kapazitäten an das Gerichtsmedizinische Institut Innsbruck zur molekulargenetischen Untersuchung weitergegeben hatte, vernichtet.

4. Ärztliche Schweigepflicht ausgehebelt

Die Schweigepflicht des Arztes ist Grundlage für eine vom Vertrauen des Patienten getragene wirkungsvolle Behandlung. Sie dient zugleich dem Interesse der Allgemeinheit an einer effektiven ärztlichen Gesundheitspflege. Deshalb hat ein Arzt über das, was ihm in Ausübung seines Berufes anvertraut oder bekannt geworden ist, zu schweigen. Diese Schweigepflicht reicht bis in den Strafprozess. Dort hat ihr der Gesetzgeber den Vorrang vor dem gewiss nicht unbedeutenden Allgemeininteresse an der restlosen Erforschung von Straftaten eingeräumt. Nach § 53 der Strafprozeßordnung (StPO) müssen Ärzte über das, was ihnen in dieser Eigenschaft anvertraut worden ist, keine Aussagen machen. Damit dieses Zeugnisverweigerungsrecht nicht umgangen werden kann, dehnt die Strafprozeßordnung dieses Recht auf die ärztlichen Hilfspersonen aus und belegt Aufzeichnungen, auf die sich das Zeugnisverweigerungsrecht erstreckt, mit einem Beschlagnahmeverbot. Diese Regelungen waren dem Polizeirevier Uhingen und dem zuständigen Staatsanwalt der Staatsanwaltschaft Ulm offenbar wenig vertraut. Anders ist die Art und Weise, wie sie sich unter Mitwirkung des Amtsgerichts Göppingen über die ärztliche Schweigepflicht hinwegsetzten, nicht zu erklären. Dazu kam es so:

In einer Filstalgemeinde war es an zwei Tagen im Mai praktisch an ein und derselben Stelle zu Blechschäden an zwei am Straßenrand geparkten Autos gekommen. Die Schäden lagen zwischen 1 500 DM und 2 000 DM. Die Verursacher hatten sich unerkannt davon gemacht. Das Polizeirevier Uhingen nahm die Ermittlungen auf. Weil die Polizeibeamten vermuteten, die Blechschäden könnten von Autofahrern beim Ausparken aus den auf der anderen Straßenseite liegenden Parkplätzen zweier Arztpraxen verursacht worden sein, sprachen sie in den Praxen vor und baten anhand der Terminkalender festzustellen, wer an den fraglichen Tagen Patient in den Arztpraxen war und anhand der Behandlungsunterlagen deren Adressen herauszusuchen. Die Ärzte lehnten die Bitte unter Berufung auf ihre Schweigepflicht ab. Statt dies zu akzeptieren, wandte sich das Polizeirevier Uhingen mit dem Ziel an die Staatsanwaltschaft Ulm, eine richterliche Anordnung für die Durchsuchung der Büros der beiden Arztpraxen, die Beschlagnahme der Terminkalender für die beiden Tage, an denen es zu den Blechschäden gekommen war, und der Anschriften der darin notierten Patienten herbeizuführen. Die Staatsanwaltschaft Ulm beantragte beim Amtsgericht Göppingen einen solchen Durchsuchungs- und Beschlagnahmebeschluss. Dieses gab dem Antrag umgehend statt. Mit dem Durchsuchungs- und Beschlagnahmebeschluss versehen, erwirkte das Polizeirevier Uhingen die Herausgabe von fünf Blättern aus den Terminkalendern der beiden Arztpraxen und der Anschriften von 43 Patienten. Das Ergebnis der polizeilichen Nachforschungen, bei denen das Polizeirevier Uhingen das Zentrale Verkehrsinformationssystem des Kraftfahrt-Bundesamtes und die polizeiliche Sachfahndungsdatei zu Rate zog und die Autos auf Lackschäden inspizierte, war: Keiner der überprüften Patienten hatte etwas mit den Blechschäden zu tun.

Keine Frage: Das Polizeirevier Uhingen hätte weder die Ärzte um die freiwillige Herausgabe der Patientenanschriften ersuchen noch bei der Staatsanwaltschaft Ulm anregen dürfen, einen richterlichen Durchsuchungs- und

Beschlagnahmebeschluss herbeizuführen. Die Staatsanwaltschaft Ulm hätte das Ansinnen des Polizeireviers zurückweisen müssen. Denn mit ihrem Vorgehen haben Polizeirevier Uhingen und Staatsanwaltschaft Ulm nicht nur unzulässigerweise Namen und Anschriften von 43 Patienten sowie Informationen darüber, wann sie bei welchem Arzt welcher Fachrichtung als Patient in Behandlung gewesen sind, erhoben, sondern auch bewirkt, dass die Ärzte aufgrund des ihnen präsentierten richterlichen Durchsuchungs- und Beschlagnahmebeschlusses notgedrungen ihre ärztliche Schweigepflicht brechen und Daten über ihre Patienten an das Polizeirevier Uhingen herausgeben mussten. Weil das Polizeirevier Uhingen die unzulässigerweise erlangten Angaben über die Patienten nicht verwenden durfte, war auch deren Überprüfung im Zentralen Verkehrsinformationssystem und in der polizeilichen Sachfahndungsdatei unzulässig.

Der Leiter der Staatsanwaltschaft Ulm hat erfreulicherweise die Verwendung der Patientendaten für die weiteren Ermittlungen sofort untersagt, als er von der Sache erfuhr, und uns wissen lassen, er werde den Fall zum Anlass nehmen, bei der nächsten Dienstbesprechung seine Dezernenten und die Polizeidienststellen seines Sprengels auf die Rechtslage hinzuweisen. Das Polizeirevier Uhingen hat die Kopien aus den Terminkalendern der beiden Arztpraxen und die Anschriften der Patienten vernichtet. Das Landgericht Ulm hat auf die Beschwerde eines Arztes den Durchsuchungs- und Beschlagnahmebeschluss des Amtsgerichts Göppingen aufgehoben; zwei Sätze reichten ihm angesichts der klaren Rechtslage zur Begründung aus. Dass diese den an diesem Fall beteiligten Personen, also Polizeibeamten, Staatsanwalt und Richter, anscheinend nicht bekannt war, muss nachdenklich stimmen.

5. Macht der Gewohnheit?

Manches wiederholt sich im Behördenalltag so oft, dass die Erledigung zur Routine wird. Wie leicht man dann mit dem Datenschutz in Konflikt kommen kann, zeigen folgende Beispiele:

– Wer bekommt schon gerne Post vom Gerichtsvollzieher? Mancher ärgert sich schon darüber, wenn ein Gerichtsvollzieher einen Benachrichtigungszettel offen in den Briefkasten wirft, in dem er aufgefordert wird, sich doch an einem der kommenden Sprechtage mit diesem in Verbindung zu setzen. Ein solches Vorgehen mag im Normalfall gerade noch angehen. Anders liegen die Dinge aber dann, wenn der Gerichtsvollzieher auf seinem Benachrichtigungszettel konkrete Angaben über laufende Zwangsvollstreckungsverfahren vermerkt. Hier hat der Schuldner ganz bestimmt ein berechtigtes Interesse daran, dass diese aus dem Blickwinkel Dritter regelmäßig als besonders negativ bewerteten Informationen anderen Personen nicht bekannt werden. Weil aber der Gerichtsvollzieher nicht weiß, wer alles die Post aus dem Briefkasten des Schuldners holen kann, muss er in einem solchen Fall seine Benachrichtigungszettel in einen Briefumschlag stecken. Nur so lässt sich verhindern, dass kompromittierende Informationen über laufende Zwangsvollstreckungsverfahren Dritten bekannt werden, die Zugriff auf den Briefkasten des Schuldners haben. Der dabei für den Gerichtsvollzieher entstehende Mehraufwand scheint im Hinblick auf die schutzwürdigen Interessen des Schuldners akzeptabel, zumal der Gerichtsvollzieher nach der Gerichtsvollzieherordnung verpflichtet ist, zur Wahrung seiner Pflicht zur Amtsverschwiegenheit dafür zu sorgen, dass sein gesamtes Schriftgut vor dem Einblick Unberechtigter gesichert ist. Darauf wies ich einen Amtsgerichtsdirektor hin, in dessen Bezirk ein Gerichtsvollzieher seine um Hinweise zu laufenden Zwangsvollstreckungsverfahren ergänzten Benachrichtigungszettel einem Schuldner offen in den Briefkasten geworfen hatte. Weil der Schuldner – wie er mir schrieb – gerade im Krankenhaus gelegen und Bekannte gebeten hatte, seinen Briefkasten zu leeren, erhielten diese Kenntnis von den Zwangsvollstreckungsverfahren.

– Gerichte verschicken tagtäglich Akten. Dabei kann es zu Unzuträglichkeiten für den Datenschutz kommen, wenn beim Versand die Besonderheiten des Einzelfalles außer Betracht bleiben. Dies zeigte sich im Falle

eines Mannes, der vor einem Sozialgericht im Lande einen Prozess führte. Um sich auf die Verhandlung vorbereiten zu können und weil ihm die Fahrt zum Gericht wegen seiner angeschlagenen Gesundheit zu beschwerlich gewesen wäre, hatte er das Gericht gebeten, die Akten zur Einsichtnahme an das Bürgermeisteramt seiner Heimatstadt zu übersenden. Das Gericht entsprach seiner Bitte. Weil es die Akte – wie üblich – in ein Kuvert gesteckt und so zur Post gegeben hatte, lag die Akte für jeden, der bei der Stadtverwaltung mit dem Öffnen der Post und mit der Benachrichtigung des Mannes über den Eingang der Akte beschäftigt war, mitsamt den darin befindlichen ärztlichen Gutachten über seinen Gesundheitszustand offen auf dem Tisch.

Als wir das Sozialgericht darauf ansprachen, betonte es, die Entscheidung über die Versendung einer Akte zur Einsichtnahme durch einen Verfahrensbeteiligten sei Sache des jeweiligen Kammervorsitzenden. Darum ging es mir nicht; dies stand und steht außer Frage. Mein Anliegen war vielmehr, die Richterinnen und Richter des Sozialgerichts auf die geschilderte Problematik aufmerksam zu machen. Zu ihrer Lösung schlug ich vor, die Akte in einen extra Umschlag zu stecken, diesen zuzukleben und den verschlossenen Umschlag sodann in einem Kuvert an die Stelle zu schicken, bei der die Akteneinsicht stattfinden soll. Meinen Vorschlag hat das Sozialgericht – wie es mich wissen ließ – seinen Richterinnen und Richtern bekannt gegeben.

– Über Personen, die eine Freiheitsstrafe oder – weil sie ihre Geldstrafe nicht zahlen (können) – eine Ersatzfreiheitsstrafe verbüßen, erstatten die Justizvollzugsanstalten dem Landeskriminalamt zu Beginn der Haft eine Aufnahmemitteilung und am Ende eine Entlassmitteilung. Handelt es sich um einen ausländischen Mitbürger, erhält auch das für seinen Wohnsitz zuständige Ausländeramt diese Mitteilungen. Das Ausländeramt nimmt die Mitteilungen zu seinen Akten. Das Landeskriminalamt ergänzt anhand der Mitteilungen die Haftdatei, in der bundesweit alle Polizeibeamte rund um die Uhr Personen abfragen können, die in Haft sind oder gewesen sind. Wie schnell man wegen einer solchen Mitteilung mit einem falschen Etikett versehen werden kann und wie lange es dauert, bis man es wieder los ist, zeigte sich im Fall eines Mannes aus Kroatien. Er musste in einer Justizvollzugsanstalt zwei Ersatzfreiheitsstrafen verbüßen; eine davon wegen Verletzung der Unterhaltspflicht nach § 170 b des Strafgesetzbuches (StGB). Statt diesen Tatvorwurf speicherte die Justizvollzugsanstalt „§ 178 StGB; sexuelle Nötigung“ in den Datensatz des Mannes ein. Entsprechende Aufnahmemitteilungen gingen an das Landeskriminalamt und das Ausländeramt mit der Folge, dass er in den Akten des Ausländeramtes und in der bundesweiten Haftdatei als Sexualtäter dastand. Als der Mann nach der Verbüßung eines Teils seiner Ersatzfreiheitsstrafen von dem unzutreffenden Eintrag in der EDV der Justizvollzugsanstalt erfuhr, bat er diese um eine umfassende Berichtigung. Die Justizvollzugsanstalt änderte in ihrer EDV den Tatvorwurf von „sexueller Nötigung“ auf „§ 170 b StGB; Verletzung der Unterhaltspflicht“. Weil der Mann nach seiner Haftentlassung bei einer Vorsprache im Ausländeramt sah, dass dort immer noch „sexuelle Nötigung“ in seiner Akte stand, erstattete er Strafanzeige. Die Polizei ermittelte und sah bei einer Abfrage der Haftdatei, dass auch diese noch nicht berichtigt war. Nach Abschluss ihrer Ermittlungen legte sie der Staatsanwaltschaft die Ermittlungsakte mit der Bitte vor, die Justizvollzugsanstalt anzuweisen, sämtliche vorhandene Eigen- und Fremddateien/Akten zu ändern. Die Staatsanwaltschaft stellte das Ermittlungsverfahren mangels hinreichendem Tatverdacht ein und übersandte uns die Akten, worum der Mann sie gebeten hatte. Als wir die Justizvollzugsanstalt mit den unzutreffenden Einträgen konfrontierten, berief sie sich darauf, ihre Änderungsmitteilungen, die sie im Zuge der Berichtigung ihrer EDV abgesetzt habe, seien beim Landeskriminalamt und beim Ausländeramt offenbar nicht angekommen. Die Änderungen seien jetzt aber erfolgt. Dies war auch dringend geboten, weil der Tatvorwurf einer sexuellen Nötigung in der Tat geeignet war, ein schiefes Licht auf den Mann zu werfen.

2. Abschnitt: Die Polizei

1. Videoüberwachung von Kriminalitätsbrennpunkten

„Kameras sollen Plätze überwachen“, „Kriminalität verstärkt mit Videokameras bekämpfen“, mit diesen oder ähnlich lautenden Schlagzeilen brachten Presseberichte immer wieder erhobene Forderungen von Sicherheitspolitikern, das Polizeigesetz entsprechend zu ändern, auf einen kurzen Nenner. Solche Forderungen fanden mancherorts rasch Resonanz. Die Stadt Mannheim beispielsweise war besonders agil. Bereits Ende Juli 2000 war in der Zeitung zu lesen: „Stadt bereitet Kamera-Überwachung in der City vor. Paradeplatz, Marktplatz, Breite Straße und Kurpfalzkreisel sollen künftig mit Video-Augen überwacht werden.“ Als wir die Stadt fragten, nach welchen Kriterien diese Plätze für die Videoüberwachung ausgewählt worden waren und sie auf die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 zu den Risiken und Grenzen der Videoüberwachung (vgl. Anhang 1) hinwiesen, hörten wir lange nichts. Vor kurzem ließ die Stadt uns wenig erhellend wissen, die Auswahlentscheidung beruhe auf der Polizeistatistik. Obwohl der Gesetzentwurf des Innenministeriums, mit dem die Videoüberwachung von Kriminalitätsbrennpunkten im Polizeigesetz geregelt werden soll, den Landtag noch gar nicht erreicht hatte, begann die Stadt schon einmal damit, alles, was dazu notwendig ist, ins Werk zu setzen. Inzwischen hat die Landesregierung den Gesetzentwurf in den Landtag eingebracht. Im Hinblick auf die anstehenden Beratungen des Gesetzentwurfs habe ich die Landtagsfraktionen auf einige Schwachpunkte des Gesetzentwurfs hingewiesen. Mir geht es um Folgendes:

Keine Frage: Wäre eine Videoüberwachung tatsächlich mit dem Einsatz eines Fernglases durch einen Polizeibeamten vergleichbar, wäre hier nicht viel Aufhebens zu machen. Dieser Vergleich, den das Innenministerium in der Gesetzesbegründung anstellt, hinkt aber erheblich. Er verkennt nicht nur die technischen Möglichkeiten moderner Videoüberwachungsanlagen, sondern lässt auch die Auswirkungen einer Videoüberwachung außer Acht. Moderne Videoüberwachungsanlagen haben ständig alle Personen im Blick, die sich im kameraüberwachten Bereich aufhalten. Dabei wird nicht nur deren Anwesenheit an einer bestimmten Örtlichkeit registriert, sondern auch wie sie sich dabei geben, wie sie gekleidet sind, was sie dabei haben, mit wem sie sich dort aufhalten, wie sie sich etwaigen Begleitern oder Begleiterinnen gegenüber verhalten und ob ihr Auftreten in ein bestimmtes Raster passt oder nicht. Videobilder lassen sich mit Hilfe eingebauter Zoom-Objektive bis ins Detail vergrößern und über schon heute vorhandene Bildvergleichssysteme auswerten. Angesichts der sich ständig weiterentwickelnden Auswertungstechnik lassen sich die Verwendungsmöglichkeiten der Videobilder kaum abschätzen. Hinzu kommt:

Von einer Videoüberwachung, wie sie mit dem Gesetzentwurf ermöglicht werden soll, werden unterschiedslos sämtliche Personen, die in den Bereich der Videokameras kommen, erfasst, und damit ganz überwiegend völlig unverdächtige Personen gezielt durch den Staat ins Visier genommen. Erfassung, Übertragung und Aufzeichnung der Videobilder sind in der Regel für sie nicht durchschaubar. Sie können die durch die ständig fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten der aufgenommenen Bilder weder abschätzen noch überblicken. Die daraus resultierende Ungewissheit erzeugt einen latenten Anpassungsdruck. Im Grunde weiß nämlich schon jedes Kind: Wer sich unter Beobachtung wähnt oder tatsächlich unter Beobachtung steht, verhält sich anders als sonst. Er versucht eine Rolle zu spielen, vermeidet dieses und inszeniert jenes, übt erwünschte, vermeintlich oder tatsächlich verlangte Verhaltensmuster ein und verinnerlicht sie am Ende sogar unbemerkt. Die Fragen lagen damit offen: Soll angesichts dieser Auswirkungen und der damit einhergehenden gravierenden Eingriffe in das Persönlichkeitsrecht vieler völlig unverdächtiger Personen eine Videoüberwachung überhaupt zugelassen werden? Muss sich wirklich jedermann gefallen lassen, dass auf öffentlichen Straßen und Plätzen sozusagen das elektronische Weitwinkelauge der Polizei ständig auf ihn gerichtet ist, ohne dass irgendein Verdacht einer strafbaren Handlung oder einer Störung der öffentlichen Ordnung gegen ihn besteht? Ist es nicht

geradezu paradox, dass von der polizeilichen Videoüberwachung, die – wie ihre Befürworter gerne betonen – denjenigen gelten soll, die die Sicherheit öffentlicher Straßen und Plätze beeinträchtigen, tatsächlich jedoch ganz überwiegend völlig rechtstreue Bürger betroffen werden? Kann eine Videoüberwachung nicht dazu führen, dass der Argwohn gegen nicht-überwachte Bereiche steigt und die Videoüberwachung damit letztendlich gerade dem Misstrauen in die Sicherheit öffentlicher Plätze Vorschub leistet, dem sie eigentlich entgegenwirken soll? Fragen über Fragen also. Eine öffentliche Debatte darüber wäre spannend gewesen; sie fand bisher leider nicht statt.

Unterzieht man den vorliegenden Gesetzentwurf einer näheren Inspektion, fällt eine merkwürdige Inkongruenz zwischen Gesetzesbegründung und öffentlichen Erklärungen des Innenministeriums auf der einen und dem beabsichtigten Gesetzestext auf der anderen Seite auf. Der Gesetzesbegründung und den öffentlichen Erklärungen zufolge soll eine Videoüberwachung nur an Kriminalitätsbrennpunkten stattfinden. Polizeibeamte sollen am Monitor die Geschehnisse live verfolgen, damit ein schnelles Eingreifen im Ernstfall gewährleistet ist. Auf eine Videoüberwachung müssten die Bürgerinnen und Bürger deutlich öffentlich hingewiesen werden. Videokameras würden nur im Zusammenwirken mit den Kommunen aufgestellt. Der Wortlaut der beabsichtigten Regelungen spricht jedoch eine andere Sprache:

– Der Begriff des Kriminalitätsbrennpunktes zieht sich zwar wie ein roter Faden durch die Entwurfsbegründung und die darin enthaltenen Ausführungen zur Rechtfertigung des Gesetzesvorhabens. Im Gesetzestext wird dieser Begriff aber nicht erwähnt, geschweige denn definiert. Der Entwurf verweist vielmehr auf die im geltenden Polizeigesetz bereits enthaltene Definition der sog. verrufenen Orte. Das sind Orte, an denen sich erfahrungsgemäß Straftäter verbergen, Personen Straftaten verabreden, vorbereiten oder verüben, sich ohne erforderliche Aufenthaltserlaubnis treffen oder der Prostitution nachgehen. Eine solche Regelung ginge zu weit. Die Videoüberwachung soll – wie ihre Befürworter betonen – in erster Linie der vorbeugenden Bekämpfung der typischen Straßenkriminalität dienen. Deshalb sollte sie wenigstens auf solche Straßen und öffentliche Plätze beschränkt werden, an denen wiederholt Straftaten von nicht unerheblicher Bedeutung begangen worden sind und bei denen Tatsachen die Annahme rechtfertigen, dass dort weitere Straftaten zu erwarten sind. Es kann nicht angehen, dass eine solche Maßnahme bereits dann möglich sein soll, wenn sich Personen an einem Ort ohne die erforderliche Aufenthaltserlaubnis treffen oder dort der Prostitution nachgehen. Damit die in der Begründung des Gesetzesentwurfs enthaltene Zusicherung, dass sich die Videoüberwachung auf wenige Orte in Baden-Württemberg beschränken wird, wirklich zum Tragen kommt, ist eine gesetzliche Definition des Begriffs des Kriminalitätsbrennpunktes im Polizeigesetz unerlässlich. Der nicht unerkleckliche Betrag, der derzeit noch für eine Videoüberwachungsanlage ausgegeben werden muss, eignet sich nun wirklich nicht als Regulativ für die mit einer Videoüberwachung einhergehenden Eingriffe in das Persönlichkeitsrecht der davon betroffenen Personen.

– Die beabsichtigte Regelung schreibt weder vor, dass Polizeibeamte die Videobilder ständig live am Überwachungsmonitor verfolgen müssen, noch verlangt sie, dass eine ständige Einsatzbereitschaft der Polizei garantiert ist. Mit ihrem Wortlaut wäre eine Aufzeichnung der am Überwachungsmonitor aufgelaufenen Videobilder durchaus vereinbar, ohne dass jemand einen Blick auf sie geworfen hat. Dass solches nicht aus der Luft gegriffen ist, zeigt nicht nur der Verlauf der Debatte, die der Landtag von Baden-Württemberg am 5. Okt. 2000 über die Einsatzkonzeption für die offene Videoüberwachung an öffentlichen Straßen und Plätzen geführt hat (vgl. Plenarprotokoll, S. 7421 [7424]). Dafür spricht vor allem auch, dass nach dem Entwurf außer dem Polizeivollzugsdienst auch die Ortspolizeibehörden eine Videoüberwachung anordnen können. Dass beide Stellen dabei zusammenwirken müssen, steht nirgends. Die beabsichtigte Regelung ließe ihrem Wortlaut zufolge deshalb durchaus zu, dass Ortspolizeibehörden Videoüberwachungen in eigener Regie durchführen. Da sie aber gar kein Personal haben, das für die vorbeu-

gende Bekämpfung und für die Verfolgung der Straßenkriminalität eingesetzt werden kann, sollte den Ortspolizeibehörden erst gar nicht die Befugnis für eine Videoüberwachung eingeräumt werden.

– Dürfen die Videokameras nur laufen, wenn – wie die Gesetzesbegründung betont – tatsächlich Polizeibeamte am Überwachungsmonitor sitzen und die Geschehnisse vor Ort im Blick haben, besteht für eine unterschiedslose, permanente Aufzeichnung der Videobilder rund um die Uhr keine Notwendigkeit. Eine solche lückenlose Aufzeichnung will der Gesetzentwurf aber für die Dauer von 48 Stunden ermöglichen. Im Klartext hieße dies, dass ganz überwiegend völlig unverdächtige Personen mit all ihren individuellen Verhaltensweisen, die sie an den überwachten Örtlichkeiten fremden Personen oder ihren Begleitern gegenüber an den Tag gelegt haben, aufgezeichnet würden. Sie und nicht die Personen, denen die Polizei zur Bekämpfung der Straßenkriminalität erklärtermaßen mit der Videoüberwachung auf den Leib rücken will, würden zu Hauptdarstellern auf den polizeilichen Videofilmen avancieren. Mit einer solchen Aufzeichnung würde ein noch gravierenderer Eingriff in das Recht auf informationelle Selbstbestimmung der vielen unbescholtenen Personen bewerkstelligt als mit dem „bloßen“ Verfolgen der Videobilder am Überwachungsmonitor. Eine Aufzeichnung sollte deshalb nur zugelassen werden, wenn der Polizeibeamte am Überwachungsmonitor ein Geschehen sieht, das ihm Veranlassung für die Annahme des Verdachts einer Straftat gibt. So wird bei der nach Angaben der Polizei mit gutem Erfolg praktizierten Videoüberwachung am Leipziger Hauptbahnhof verfahren. Dies sollten all diejenigen, die bei der Frage, ob eine Videoüberwachung etwas bringt, gerne auf Leipzig verweisen, nicht vergessen, wenn zur Debatte steht, wie bei der Aufzeichnung von Videobildern eine übermäßige Datenspeicherung über völlig unverdächtige Personen vermieden werden kann.

– Wird die im Entwurf vorgesehene Regelung Gesetz, ist keineswegs gewährleistet, dass allen Personen klipp und klar vor Betreten eines überwachten Ortes vor Augen geführt wird, dass sie dort einer Videoüberwachung ausgesetzt sind. Der Wortlaut der beabsichtigten Regelung verlangt lediglich, dass die Videoüberwachung offen erfolgen muss. Dies bedeutet aber nur, dass die Kameras nicht versteckt installiert werden dürfen. Um dieses Manko zu beheben, muss im Gesetzestext klargestellt werden, dass die Videoüberwachung durch geeignete Maßnahmen an Ort und Stelle erkennbar zu machen ist.

– Im Gesetz sollte vorgeschrieben werden, dass eine polizeiliche Videoüberwachung nur gestartet werden darf, wenn sie zuvor eine sog. Vorabkontrolle absolviert hat. Dazu hat die Stelle, die eine solche Maßnahme ergreifen will, eine Risikoanalyse zu erstellen und festzulegen, welche Maßnahmen zum Schutz des Persönlichkeitsrechts der betroffenen Personen zu ergreifen sind. Das Ergebnis dieser Untersuchung ist dem zuständigen Datenschutzbeauftragten zur Revision zuzuleiten. Eine solche Prozedur verlangt §12 LDSG bei automatisierten Datenverarbeitungsverfahren, mit denen besondere Gefahren für das Persönlichkeitsrecht verbunden sein können. Dass dies gerade bei der polizeilichen Videoüberwachung der Fall ist, sollte eigentlich keine Frage sein. Die Gesetzesverfasser sehen dies offenbar anders.

Ob meine Vorschläge im Gesetzgebungsverfahren Berücksichtigung finden, muss sich zeigen. Die Landesregierung drückt offenbar aufs Tempo. Sie will die Regelung über die polizeiliche Videoüberwachung noch in dieser Legislaturperiode, die sich bereits ihrem Ende zuneigt, im Gesetzblatt stehen sehen.

2. Aussonderungsprüffristen für polizeiliche personenbezogene Sammlungen

Wer es nicht mit eigenen Augen gesehen hat, kann sich schwerlich eine Vorstellung darüber machen, wo bei der Polizei überall personenbezogene Daten gespeichert sein können. Außer Akten über Ermittlungsverfahren und der Personenauskunftsdatei, in der die Polizei Personen registriert, die mutmaßlich oder tatsächlich eine Straftat begangen haben, gibt es – um nur

einige Beispiele zu nennen – Unterlagen und Dateien über Ordnungswidrigkeitenverfahren, Abschiebeberichte, Ermittlungsersuchen anderer Stellen, Sachverständigengutachten, Fahrradbücher, Betäubungsmittelbücher, Arbeitsdateien und diverse Meldedienste. So unterschiedlich all dies erscheinen mag, eine Gemeinsamkeit gibt es: Seit die Polizeidienststellen üppig mit Computern ausgestattet sind, führen sie solche Dateien, Bücher, Verzeichnisse und Meldedienste immer häufiger automatisiert. Dabei verarbeiten sie in aller Regel personenbezogene Daten. In Akten und Dateien über Ordnungswidrigkeitenverfahren kann die Polizei nachschauen, gegen wen sie etwa wegen einer Tempoüberschreitung oder wegen welcher Ordnungswidrigkeit sonst ermittelt hat. In Abschiebeberichten ist beispielsweise zu lesen, wen sie nach Ablehnung seines Asylantrags zum Flughafen gefahren hat, damit er in sein Heimatland abgeschoben werden kann. Im Fahrradbuch wird festgehalten, wem wann wo welches Fahrrad gestohlen oder abhanden gekommen ist und wer ein gefundenes Fahrrad bei der Polizei abgeliefert hat. Arbeitsdateien richtet sie in umfangreichen Ermittlungsverfahren ein; darin registriert sie eine Vielzahl von Personen, angefangen von den Beschuldigten über Tatverdächtige bis hin zu sog. Kontakt- und Begleitpersonen. Dass die Polizei solche Unterlagen, Dateien, Bücher und Verzeichnisse deshalb nicht bis zum Sankt-Nimmerleins-Tag aufbewahren darf, ist dem Kenner der Materie klar. Er weiß auch, dass Maßstab dafür, wann sie sich davon wieder trennen muss, das Erforderlichkeitsprinzip ist. Danach ist sie gehalten, gespeicherte personenbezogene Daten zu löschen und die der Speicherung zugrunde liegenden Akten und Unterlagen auszusondern, wenn ihre Kenntnis zur Wahrnehmung polizeilicher Aufgaben nicht mehr erforderlich ist. Um der Polizei dabei wegen des massenhaften Geschäftsanfalls die Arbeit zu erleichtern, erlaubt ihr das Polizeigesetz, Aussonderungsprüffristen zu bestimmen, nach deren Ablauf sie sich mit der Frage der Datenlöschung und der Aussonderung der Unterlagen befassen muss. Für die Bestimmung solcher Fristen ist wiederum das Erforderlichkeitsprinzip maßgebend.

Das Innenministerium informierte uns im Sommer über seine Arbeiten zur Bereinigung der polizeilichen Aussonderungsprüffristen und schickte uns eine umfangreiche Auflistung darüber ins Haus, für welche Akten, Bücher, Dateien und Verzeichnisse nach seinen Vorstellungen welche Aussonderungsprüffrist vorgesehen werden soll. Die vorgeschlagenen Fristen gingen im Großen und Ganzen in Ordnung. Dass sie sich im Rahmen dessen halten, was zur polizeilichen Aufgabenerledigung notwendig ist, ließ sich nicht von der Hand weisen. Folgende Punkte mussten wir jedoch aufgreifen:

- Das Innenministerium hatte für Unterlagen, Karteien und Dateien im Zusammenhang mit Ordnungswidrigkeitenverfahren eine dreijährige Aussonderungsprüffrist vorgesehen. Dies erschien uns zu lang. Die Polizei wird im Ordnungswidrigkeitenverfahren als Ermittlungsorgan für die Bußgeldbehörde oder die Staatsanwaltschaft tätig. Diesen Stellen hat sie die Ermittlungsakte sobald wie möglich vorzulegen, damit sie entscheiden können, ob die Ordnungswidrigkeit verfolgt und zur Ahndung gebracht oder das Verfahren eingestellt wird. Mit der Vorlage der Akten ist erfahrungsgemäß die Tätigkeit der Polizei im Ordnungswidrigkeitenverfahren beendet. Dass sie hin und wieder in Nachermittlungen eintreten muss oder ein Polizeibeamter in Bußgeldverfahren als Zeuge geladen und vernommen wird, mag die Aufbewahrung der Ermittlungsakte bei der Polizei für eine gewisse Zeit rechtfertigen, eine dreijährige Frist jedoch nicht. Dies sah das Innenministerium am Ende auch so und verkürzte die Frist auf ein Jahr.
- Dass ein Sachverständigengutachten zur Ermittlungsakte genommen und darin so lange aufbewahrt werden kann, wie die gesamte Ermittlungsakte der Polizei zur Erfüllung ihrer Aufgaben zur Verfügung stehen muss, leuchtet ohne weiteres ein. Zur Erfüllung welcher Aufgaben der Polizei es aber notwendig sein soll, dass eine mit der Erstellung eines Gutachtens beauftragte Untersuchungsstelle wie z. B. das Kriminaltechnische Institut des Landeskriminalamts eine Mehrfertigung des Gutachtens genauso lange und damit im Klartext drei, fünf, zehn Jahre oder gar noch länger mit all den personenbezogenen Daten, die darin vor allem über Opfer von Straftaten stehen können, aufbewahrt, erläuterte uns das

Innenministerium bisher nicht. In diesem Punkt ist deshalb die Diskussion ebenso wenig abgeschlossen wie bei der Frage, wie lange die Polizei ihre Geschäftstagebücher, in denen sie alle ihre Geschäftsvorfälle oftmals mit Angaben zum Anzeigeerstatter, Geschädigten oder Tatverdächtigen registriert, eigentlich braucht.

3. Einzelfälle

Nach wie vor wenden sich viele Personen an mein Amt, weil sie befürchten oder genau wissen, dass die Polizei Daten über sie speichert und dies überprüft haben wollen. Manchem konnten wir helfen.

3.1 Ein Schwachpunkt des Schengener Informationssystems und seine Notlösung

Im Sommer 1985 unterzeichneten Belgien, die Niederlande, Luxemburg, Frankreich und Deutschland im luxemburgischen Schengen das Übereinkommen zum schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen. Darin vereinbarten sie u. a. den vollständigen Abbau der Grenzkontrollen im Personenverkehr und deren Verlagerung an die Außengrenzen der Vertragsstaaten möglichst bis Anfang 1990. Die Schlagbäume an ihren gemeinsamen Grenzen gingen freilich noch lange nicht hoch. Erst Mitte 1990 einigten sich die fünf Vertragsstaaten auf das Schengener Durchführungsübereinkommen, dem mittlerweile Italien, Spanien, Portugal, Griechenland, Österreich, Dänemark, Schweden und Finnland beigetreten sind und dessen Kernstück das sog. Schengener Informationssystem (SIS) ist. Der Sache nach handelt es sich um eine praktisch europaweite Fahndungsdatei, in der vor allem Personen, die aus Gründen der Strafverfolgung oder Strafvollstreckung zum Zweck der Auslieferung festgenommen werden sollen, und unerwünschte Ausländer aus Drittstaaten registriert werden können, denen die Einreise an den Außengrenzen der Vertragsstaaten verweigert werden soll. Wie man sich im SIS verheddern kann, zeigte sich im Falle eines Mannes aus der Türkei, der seit 1987 in Deutschland lebt und hier eine Aufenthaltsberechtigung besitzt. Er wollte – wie er uns schrieb – nach einem Urlaub von der Türkei über Griechenland nach Deutschland zurückfahren. Die griechischen Grenzschutzbehörden hätten ihn ohne Angabe von Gründen zurückgewiesen. Er habe deshalb in die Türkei zurückfahren müssen. Schließlich sei er mit der Fähre via Brindisi nach Deutschland gekommen. Hier sei er von der Polizei kontrolliert worden. Weil die Kontrolle gedauert habe, habe er nach dem Grund dafür gefragt. Der Polizeibeamte habe ihm erklärt, dass jemand mit gleichem Namen wie er sowohl in INPOL – also dem Fahndungscomputer der Polizeien des Bundes und der Länder – als auch im SIS zur Fahndung ausgeschrieben sei und dass es eben seine Zeit gedauert habe, bis geklärt gewesen sei, dass er nicht der Gesuchte sei. Weil der Mann befürchtete, dass er künftig wieder mit dem tatsächlich gesuchten Mann verwechselt wird und weil er eine so beschwerliche Rückreise aus der Türkei nicht noch einmal erleben wollte, wandte er sich an uns mit der Frage, was tun.

Seine Befürchtung war nicht aus der Luft gegriffen. Tatsächlich war, wie sich bei unseren Recherchen zeigte, im INPOL-Fahndungscomputer, der auf dem Rechner des Bundeskriminalamts läuft und den jeder deutsche Polizeibeamte rund um die Uhr in Sekundenschnelle online abfragen kann, und im SIS jemand zur Festnahme ausgeschrieben, der genau gleich hieß wie der Mann und am selben Tag geboren war wie dieser. Die INPOL-Ausschreibung stammte von einer hiesigen Polizeidienststelle; diejenige im SIS von der italienischen Polizei, was die Sache noch komplizierter machte, als sie eh schon war. Zu lösen war sie im INPOL-Fahndungscomputer einfacher als im SIS. Das ging so:

Die hiesige Polizei speicherte in den INPOL-Datensatz der gesuchten Person einen Warnhinweis ein, dass der Mann nicht mit der ausgeschriebenen Person identisch ist und sich mit dem Reisepass mit der Nummer so und so ausweist. Weil sie dabei auf Nummer sicher gehen wollte, musste er sich erkennungsdienstlich behandeln, also Fingerabdrücke abnehmen und fotografieren lassen, damit sie die Fingerabdrücke und

Fotos mit denjenigen des Gesuchten vergleichen konnte. Ändert sich die Reisepassnummer des Mannes, muss er daran denken, die hiesige Polizei zu informieren, damit sie den Warnhinweis entsprechend ändert. Achtet er darauf, dürfte er bei einer Abfrage des INPOL-Fahndungscomputers im Zuge einer Personenkontrolle vor einer Verwechslung mit der dort zur Festnahme ausgeschriebenen Person gefeit sein, weil dem abfragenden Polizeibeamten der Warnhinweis sofort am Bildschirm angezeigt wird.

Beim SIS ist die Zuspeicherung eines entsprechenden Warnhinweises aus technischen Gründen nicht möglich. Gibt die hiesige Polizei oder diejenige eines Staates, der an das SIS angeschlossen ist, den Namen des Mannes am SIS-Abfrageterminal ein, zeigt der SIS-Computer den Fahndungsdatensatz der namensgleichen, zur Festnahme ausgeschriebenen Person an und schon können die Schwierigkeiten für den Mann beginnen. Weil dieser Konstruktionsfehler des SIS sich offenbar auf die Schnelle nicht beheben lässt und der Mann nicht der Erste war, der ihm zum Opfer fiel, hatte das Bundeskriminalamt, das in Deutschland die zuständige Stelle für den Betrieb des SIS ist, schon vor geraumer Zeit eine Notlösung gefunden. Dazu musste sich der Mann noch einmal erkennungsdienstlich behandeln lassen. Seine Fingerabdrücke und Fotos wurden unter Vermittlung des Bundeskriminalamtes der italienischen Polizei zugeleitet. Sobald diese dem Bundeskriminalamt bestätigt, dass der Mann mit der ausgeschriebenen Person nicht identisch ist, stellt es ihm eine Bescheinigung aus, die er der Polizei im In- und Ausland vorlegen kann. Nicht vergessen darf er auch hier, jede Änderung seiner Reisepassnummer dem Bundeskriminalamt mitzuteilen, damit dieses die Bescheinigung entsprechend ändern kann. Bei der anstehenden Überarbeitung des SIS soll – wie zu hören ist – Platz für einen solchen Warnhinweis geschaffen werden, wie er im INPOL-Fahndungscomputer schon heute möglich ist. Bis dahin kann man dem Mann nur raten, die Bescheinigung immer in der Tasche zu tragen.

3.2 In der PAD gelöscht

Oftmals werden wir in Eingaben ganz gezielt auf Datenspeicherungen in der Personenauskunftsdatei (PAD) angesprochen und gebeten, zu prüfen, ob diese in Ordnung gehen. Mancher ist danach gar nicht mehr in der PAD registriert, bei anderen ist das PAD-Konto bereinigt, anderen müssen wir sagen, dass an ihrer PAD-Speicherung nicht zu kritteln ist.

– Kein Exhibitionist

  Ein pensionierter Lehrer war 1996 so in ein Ermittlungsverfahren geraten: Eine Frau hatte bei der Polizei Anzeige erstattet, sie sei von einem Mann auf offener Straße exhibitionistisch belästigt worden. Beschreiben konnte sie den Täter nur äußerst vage. Die Polizei fuhr die Gegend ab und sah ein paar Straßenzüge weiter den Pensionär. Sie stellte ihn der Frau gegenüber. Diese meinte in ihm den Täter wieder zu erkennen. Der Pensionär verwahrte sich ganz entschieden dagegen. Er konnte belegen, dass er zur Tatzeit in einer Gaststätte zu Mittag gegessen hatte. Die Staatsanwaltschaft stellte das Ermittlungsverfahren umgehend mangels hinreichendem Tatverdacht ein. Weil ihre Mitteilung darüber bei der Polizei nicht angekommen oder dort versandet war, war damals die gebotene Löschung des PAD-Datensatzes unterblieben, der ja nun wirklich geeignet war, ein schiefes Licht auf den Pensionär zu werfen. Als dieser uns bat, der Sache nachzugehen, löschte die Polizei umgehend.

– Vom Saulus zum Paulus

  Ein Abiturient schrieb mir, er sei als 17-jähriger mit dem Betäubungsmittelgesetz (BtMG) in Konflikt geraten. Er habe von einem jugendlichen Dealer mehrmals Amphetamin gekauft. Der Dealer sei aufgeflogen und habe bei der Polizei über seine Abnehmer ausgesagt. Der Jugendrichter habe ihn wegen seiner Drogenkäufe zu 20 Stunden gemeinnütziger Arbeit verurteilt. Er wisse, dass er wegen dieser Vorfälle in der PAD und in der bundesweiten Falldatei Rauschgift

registriert sei, in der die Polizeien des Bundes und der Länder Daten über Personen speichern, die mutmaßlich oder tatsächlich eine Rauschgiftstraftat begangen haben. Die Verurteilung durch den Jugendrichter sei aus heutiger Sicht für ihn ein Segen gewesen. Sie habe ihm die Augen geöffnet. Er habe danach sein Leben grundlegend geändert. Mit Drogen habe er seither nichts mehr zu tun gehabt. Inzwischen sei er Schulsprecher an seinem Gymnasium und stelle mit seinem Verbindungslehrer ein Projekt zur Drogenprävention auf die Beine. Dabei wolle er seinen Mitschülern aus eigenem Erleben berichten, dass es sich lohnt, clean zu werden und clean zu bleiben. Er hoffe, dass seine Umkehr auch von der Polizei honoriert werde. Da stieß er beim Landeskriminalamt auf offene Ohren. Als wir dort seinen Fall vorbrachten, löschte es seine alten Btm-Speicherungen in der PAD und in der Falldatei Rauschgift; neue waren seit damals nicht dazu gekommen.

– Aus dem Blick des Staatsschutzes

  Einem studierten Mann mit einem ehrbaren Beruf hatte die Polizei seines Wohnortes auf seinen Auskunftsantrag mitgeteilt, ihr Dezernat Staatsschutz speichere Daten über ihn. Um was es dabei im Einzelnen gehe, werde sie ihm nicht offen legen. Wenn er wolle, könne er deswegen den Datenschutzbeauftragten anrufen. Darauf müsse sie ihn hinweisen; das schreibe das Landesdatenschutzgesetz bei einer Auskunftsverweigerung vor. Als der Mann sich an uns wandte und wir bei der Polizeidienststelle nachfragten, listete diese uns alle Datenspeicherungen – so wie es sich gegenüber der unabhängigen Datenschutzkontrolle gehört – fein säuberlich auf. Weil diese Sammlung nicht den Schluss rechtfertigte, bei dem Mann handle es sich um jemanden, der künftig womöglich eine Straftat begeht, baten wir die Polizeidienststelle ihre Datenspeicherungen zu löschen, was sie auch tat. Beim Staatsschutz gibt es jetzt nichts mehr über den Mann.

– Eine kompromittierende Verkehrskontrolle

  Eine junge Frau schrieb uns, die Polizeibeamten hätten sie bei einer Verkehrskontrolle eingehend danach befragt, ob sie Drogen dabei habe. Auf ihre Frage, wie sie zu einer solchen Annahme kämen, hätten ihr die Polizeibeamten gesagt, sie sei im Polizeicomputer wegen Btm-Delikten registriert. Weil ihr Beifahrer alles mitbekommen habe, sei ihr die Angelegenheit mehr als peinlich, zumal der Btm-Vorwurf schon so lange zurückliege, dass sie sich daran kaum mehr erinnern könne. Als wir der Sache nachgingen, zeigte sich rasch, dass die Auskunft der Polizeibeamten schon richtig gewesen war. In der PAD war ein sog. personengebundener Hinweis gespeichert, der die Frau als Betäubungsmittelkonsumentin hinstellte. In der bereits erwähnten Falldatei Rauschgift gab es einen fast 10 Jahre alten Eintrag über Btm-Erwerb. Was diesen beiden Speicherungen im Einzelnen zugrunde lag, ließ sich nicht mehr rekonstruieren, weil die Polizei die Akten über diesen Fall schon vernichtet hatte. Dabei hatte sie offenbar versäumt, den personengebundenen Hinweis in der PAD und den Btm-Eintrag in der Falldatei-Rauschgift zu löschen. Dies holte sie jetzt umgehend nach. Weil der Btm-Eintrag der hiesigen Polizei die Löschung eines noch älteren Eintrags der Polizei eines anderen Bundeslandes in der Falldatei Rauschgift blockiert hatte und dieser Eintrag jetzt alleine dastand, schalteten wir unsere Kollegen ein, die uns kurz darauf mitteilen konnten, dass ihre Polizei den in der Falldatei Rauschgift übrig gebliebenen Eintrag umgehend gelöscht hat. Vorhaltungen wie bei der Verkehrskontrolle muss sich die Frau jetzt nicht mehr anhören.

– „Alte Kunden“

  Hin und wieder haben wir es mit Eingaben von Personen zu tun, die ein langes Register in der PAD haben. Auch sie haben Anspruch darauf, dass sich mein Amt genau so akribisch mit ihrem Anliegen, die PAD-Speicherungen zu überprüfen, befasst wie mit den Eingaben aller anderen Personen, die befürchten, durch die Verarbeitung ihrer

Daten in ihren Datenschutzrechten verletzt worden zu sein. Das Recht, die unabhängige Datenschutzkontrolle anzurufen, steht nämlich jedem zu, ganz gleich ob und wie oft er sich schon etwas zu Schulden kommen lassen hat, auch wenn dies der eine oder andere hin und wieder nicht so recht wahrhaben will. Dass ein solcher Schritt keine verlorene Mühe ist, zeigen folgende beide Fälle exemplarisch:

- Ein Mann, dem – wie er uns schrieb – bei einer Verkehrskontrolle ein 8 Jahre zurückliegendes Ermittlungsverfahren wegen eines angeblichen Btm-Delikts vorgehalten worden war, hatte uns gebeten zu überprüfen, was die Polizei alles sonst noch über ihn speichert. Beinahe 40 Einträge in der PAD waren es; dazu kam noch der Btm-Eintrag in der Falldatei Rauschgift, auf den die Polizeibeamten den Mann bei der Verkehrskontrolle offenbar angesprochen hatten. Das Ergebnis unserer Arbeit war: Jede zweite PAD-Speicherung und der Eintrag in der Falldatei Rauschgift sind gelöscht. Die übrigen Datenspeicherungen waren nicht zu kritisieren.
- Weil ihn ein Polizeibeamter bei einer Kontrolle als alten Kunden tituliert hatte, bat uns ein anderer Mann zu prüfen, was dahinter steckt. Schon klar: Er hatte insgesamt 18 Einträge in der PAD wegen mutmaßlich oder tatsächlich begangener Straftaten. Sein PAD-Konto konnten wir um drei Einträge reduzieren. Immerhin steht er jetzt nicht mehr in der PAD als jemand, der Betrügereien begeht. Weil er wegen der verbliebenen Straftaten meistens zu Geld- oder gar Freiheitsstrafe auf Bewährung verurteilt worden war, hielt die Polizei zu Recht an diesen PAD-Speicherungen fest.

5. Teil: Andere Bereiche

1. Abschnitt: Kommunales

1. Meldewesen

Das Melderegister zu führen ist eine wichtige Aufgabe der Gemeinden und Städte. Es dient nicht nur dazu, die Einwohner zu registrieren, damit deren Identität und Wohnung festgehalten wird, sondern ist auch Ziel vieler Auskunftswünsche. Obwohl die Voraussetzungen, unter denen die Meldebehörde Auskünfte erteilen darf oder muss, im Meldegesetz detailliert geregelt sind, gibt es in diesem Bereich Jahr für Jahr Kontroversen.

1.1 Adressen von Wahlberechtigten – Begehrte Objekte

Im vergangenen Jahr hatte ich mich mit der Frage zu befassen, ob die Meldebehörden der Christlich-Demokratischen Union Deutschlands (CDU) Anschriften von Seniorenwählern geben dürfen, damit deren Bundesvorsitzender ihnen den sog. „Rentenbrief“ zuschicken kann (vgl. 20. Tätigkeitsbericht 1999, LT-Drs. 12/4600, S. 95). Jetzt wirft die Landtagswahl am 25. März 2001 ihre Schatten voraus und weckt neuen Hunger nach Adressen von Wahlberechtigten.

Ein Kreisverband einer Partei im Schwarzwald wollte möglichst alle in seinem Bezirk bei der Landtagswahl Wahlberechtigten persönlich anschreiben. Ihm war aber offenbar bekannt, dass das Meldegesetz nur erlaubt, Parteien eine sog. Gruppenauskunft zu erteilen, bei der für die Zusammensetzung der Gruppe das Alter der Wahlberechtigten maßgebend ist. Die Auskunft darf also nur Wahlberechtigte einzelner Altersgruppen umfassen. Weil der Kreisverband folglich die Städte und Gemeinden nicht einfach um die Herausgabe der Adressen aller Wahlberechtigten ohne Altersangabe bitten konnte, probierte er es bei einer Stadt mit einem Trick: Er bat kurzerhand um Übersendung von Name und Anschrift der am 25. März 2001 Wahlberechtigten „in den Altersgruppen 18 – 24, 25 – 44, 45 – 64, 65 und älter“, und damit eben doch von allen Wahlberechtigten. Die Stadt ließ sich freilich dadurch nicht irritieren und beabsichtigte, das Auskunftsersuchen abzulehnen. Um aber ganz sicher zu gehen, bat

sie mich um Bestätigung ihrer Rechtsauffassung. Dass die Stadt in ihrer rechtlichen Beurteilung richtig lag und eine Umgehung des Gesetzes auf diese Weise nicht möglich ist, versteht sich eigentlich von selbst. Offenbar hat auch schon das Innenministerium mit solchen Winkelzügen von Parteien und anderen Trägern von Wahlvorschlägen gerechnet, denn es führt in der Allgemeinen Verwaltungsvorschrift zum Meldegesetz aus: „Durch die Worte 'von Gruppen' von Wahl- oder Stimmberechtigten wird klargestellt, dass nicht über die Daten aller Wahl- oder Stimmberechtigten verfügt werden darf, sondern nur eingeschränkt und nicht umfassend. Hierdurch soll den Parteien etc. eine altersspezifische Ansprache (z. B. Jungwählerlisten) ermöglicht werden. Soweit alle Wahl- oder Stimmberechtigten angesprochen werden sollen, ist auf anderweitige Möglichkeiten, z. B. Postwurfsendungen, zu verweisen." Dem ist nichts hinzuzufügen.

Welche Bedeutung Parteien Melderegisterauskünften über Wählergruppen beimessen, hat die Stadt Baden-Baden erfahren. Sie hatte dem dortigen CDU-Kreisverband im Vorfeld der letztjährigen Kommunalwahl die Namen und Anschriften der Erstwähler und der Seniorenwähler mit der Begründung verweigert, sie gebe keiner Partei solche Gruppenauskünfte, weil sonst auch extremistische Parteien dies fordern und dann verfassungsfeindliche Materialien versenden könnten. Die Stadt berief sich dabei auf den Wortlaut der Bestimmung des Meldegesetzes, der ihr durch das Wörtchen „kann" das Ermessen einräumt, selbst zu entscheiden, ob sie Parteien Melderegisterauskünfte erteilen will oder nicht. Auch das Regierungspräsidium sah keinen Grund, warum die Stadt die Auskunft hätte erteilen müssen. Damit wollte sich der CDU-Kreisverband aber nicht abfinden und zog vor Gericht. Das Verwaltungsgericht Karlsruhe gab ihm unlängst in erster Instanz Recht. Es meint offenbar (die Begründung der Entscheidung lag bei der Erstellung des Berichts noch nicht vor), die Stadt habe ihr Ermessen nicht zweckentsprechend ausgeübt, weil Zweck der in Rede stehenden Vorschrift des Meldegesetzes sei, dem legitimen Informationsbedürfnis der Parteien Rechnung zu tragen. Dass Parteien, denen nach Art. 21 Abs. 1 des Grundgesetzes eine besondere Stellung zukommt, ein berechtigtes Interesse an den Anschriften von Wahlberechtigten haben, ist schon richtig. Das bedeutet aber nicht zwangsläufig, dass das Ermessen der Meldebehörde quasi auf null reduziert ist und dass Parteien grundsätzlich Anspruch auf Auskunft aus dem Melderegister haben. Dem Interesse der Parteien, sich unmittelbar an den einzelnen Wahlberechtigten wenden zu können, steht nämlich das Grundrecht des Einzelnen auf informationelle Selbstbestimmung gegenüber. Ob sich das Verwaltungsgericht mit der Abwägung beider Rechtspositionen auseinander gesetzt hat, ist bislang nicht bekannt. Das Oberverwaltungsgericht Sachsen-Anhalt hat es jedenfalls in einer Entscheidung vom 24. März 1998 getan und ist aus gutem Grund zum Ergebnis gekommen, dass die Meldebehörde bei ihrer Ermessensentscheidung sehr wohl dem Datenschutz den Vorrang einräumen darf, weil sie damit auch die Bürger zu schützen vermag, die aus Unkenntnis der Rechtslage keinen Widerspruch gegen eine Gruppenauskunft haben eintragen lassen. Ich hoffe, der Verwaltungsgerichtshof in Mannheim erhält die Gelegenheit, diesen Grundsätzen auch hier im Land Geltung zu verschaffen.

1.2 Der Widerspruch gegen die Veröffentlichung im Adressbuch – formlos, fristlos und manchmal fruchtlos

Unisono teilten die Mitglieder einer Familie bereits im Jahre 1987 der Stadt Bad Friedrichshall mit, sie wünschten nicht, im örtlichen Adressbuch genannt zu werden. Was die Stadt daraufhin veranlasste, konnte sie nicht sagen. Klar ist nur, was sie nicht tat, nämlich – wie es ihre Pflicht gewesen wäre – den Widerspruch gegen die Adressbuch-Veröffentlichung im Melderegister zu vermerken. So kam es wie es kommen musste. Prompt wurden in drei Ausgaben

von Adressbüchern der Stadt alle Familienmitglieder aufgeführt. Von meinem Amt um Stellungnahme gebeten, gab die Stadt anstelle eines Wortes des Bedauerns lieber ihrer Verwunderung darüber Ausdruck, „dass die genannten Personen sich nicht schon bei den früheren Veröffentlichungen gemeldet haben." Inzwischen hat die Stadt das Versäumte nachgeholt.

1.3 Melderegisterauskünfte an der Meldebehörde vorbei – genial oder rechtswidrig?

Ein Unternehmen in Heidelberg, das sich als hundertprozentige Tochter der Deutschen Telekom AG vorstellte, wandte sich an Städte und Gemeinden im Land und teilte ihnen Folgendes mit:

> „Wir haben ein Programm entwickelt, durch das Daten zur Einwohnermeldeamtsanfrage in einer Datei gespeichert werden. Diese Datei kann per DFÜ oder per Datenträger an die entsprechende Stadt verschickt werden. ... Wir bereiten Daten säumiger Schuldner zur Bearbeitung durch den Rechtsanwalt auf. Bei Städten, die Melderegisterauskünfte per Datenträger ermöglichen, wollen wir gerne auf diesen Service zurückgreifen. Sie können sich sicher vorstellen, dass bei uns täglich Anfragen anfallen, so dass Ihnen und auch uns durch eine solche Lösung geholfen ist."

Zudem wies die Firma darauf hin, die Stadt Stuttgart habe sich bereits diesem Verfahren angeschlossen.

Es bedurfte schon ein wenig Fantasie herauszufinden, welches Anliegen sich hinter diesen Sätzen verbarg und was das Unternehmen mit seinem Vorstoß eigentlich bezweckte. Um sich mühsame Recherchen bei den einzelnen Meldebehörden zu ersparen, wollte es seine Auskunftsersuchen jeweils bezogen auf das Einzugsgebiet eines Rechenzentrums diesem in elektronischer Form zuleiten und die Melderegisterauskünfte auf gleichem Wege zurückbekommen. Dass dieses Verfahren nicht dem entspricht, wie sich der Gesetzgeber die Auskunft aus dem Melderegister vorstellt, war dem Unternehmen wohl klar. Offenbar war es jedoch der Meinung, es genüge, wenn die einzelnen Meldebehörden dem Verfahren kurzerhand zustimmen würden. Der schöpferische Vorschlag konnte freilich vor dem Gesetz keinen Bestand haben, denn er hätte bedeutet, dass in Wirklichkeit nicht die Meldebehörde die Auskunft erteilt, sondern das Rechenzentrum, das ja nur im Auftrag der Gemeinde tätig werden darf. So kann es natürlich nicht gehen. Nach den Regelungen des Meldegesetzes muss die Meldebehörde nämlich eine Ermessensentscheidung darüber treffen, ob und in welcher Weise sie Auskünfte aus dem Melderegister erteilt. Dabei hat sie auch bei den sog. einfachen Melderegisterauskünften, bei denen nur Vor- und Nachname, Doktorgrad und Anschriften mitgeteilt werden, darauf zu achten, dass die schutzwürdigen Interessen der Betroffenen nicht beeinträchtigt werden. Würde die Meldebehörde aber, wie von dem Unternehmen gewünscht, das Rechenzentrum pauschal beauftragen die Auskünfte zu erteilen, hätte sie keine Kontrolle mehr darüber, wer die Auskunft einholt und ob hierdurch evtl. schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Nachdem sich das Innenministerium in gleicher Weise geäußert hatte, hat das Unternehmen wohl den Rückzug angetreten. Dass die Stadt Stuttgart eine andere Meinung zur Zulässigkeit dieses Verfahrens vertreten würde, konnte ich mir kaum vorstellen, und ich sollte Recht behalten. Die Behauptung des Unternehmens, die Stadt habe bereits die Zustimmung erteilt, war schlicht frei erfunden.

2. Umgang mit Abbuchungsermächtigungen fehlerhaft

Eine Ermächtigung zur Abbuchung vom Konto ist eine nützliche Sache. Fast jeder von uns erlaubt dem einen oder anderen Gläubiger, Beträge von seinem Konto einzuziehen, z. B. zur Bezahlung des Zeitungs- oder Theaterabonnements, der Monatsfahrkarte, von Warenlieferungen oder

auch zur Begleichung der Kfz-Steuer oder von Grundbesitzabgaben. Gegenüber dem Dauerauftrag hat das Lastschriftverfahren den Vorteil, dass der Schuldner nicht bei jeder Änderung des zu zahlenden Betrags den Bankauftrag ändern muss. Der Nachteil ist, dass der Gläubiger auch dann in den Besitz des Geldes kommt, wenn im Einzelfall Streit über die Höhe des Zahlungsbetrags besteht. Deshalb will es gut überlegt sein, wem man für welche Forderungen eine Abbuchungsermächtigung erteilt. Diese Vorsicht nützt freilich nichts, wenn von ihr nicht korrekt Gebrauch gemacht wird, wie folgende Beispiele zeigen:

Im ersten Fall bezog ein Bürger seit langem das Amtliche Mitteilungsblatt von seiner Gemeinde. Weil er diese für zuverlässig hielt, hatte er ihr zum Einzug der fälligen Gebühren eine Abbuchungsermächtigung erteilt. Als dann im Lauf der Zeit die Herausgabe des Mitteilungsblatts defizitär wurde, beauftragte die Gemeinde einen Verlag damit, das Blatt zu publizieren. Dies hatte zur Folge, dass der Bezugspreis nunmehr an den Verlag zu zahlen war. Gemeinde und Verlag waren sich jedoch einig, den Herausgeberwechsel „unbürokratisch“ über die Bühne gehen zu lassen. Deshalb gab die Gemeinde an den Verlag nicht nur die Namen und Anschriften der bisherigen Abonnenten weiter, sondern auch die von diesen erteilten Abbuchungsermächtigungen. Eines Tages stellte besagter Bürger bei der Lektüre seines Kontoauszugs zu seinem Erstaunen fest, dass anstelle der Gemeinde der Verlag die Gebühren von seinem Konto abgebucht hatte, ohne dass er um sein Einverständnis dazu gefragt worden war. Auf Nachfrage erhielt er vom Bürgermeister die lapidare Antwort, es habe schon alles seine Richtigkeit. Dem war jedoch nicht so. Zwar war nicht zu kritisieren, dass die Gemeinde Namen und Anschriften der Abonnenten an den Verlag weitergegeben hatte. Denn für einen Bürger, der das Mitteilungsblatt beziehen will, kommt es im Regelfall nur darauf an, dass er das Amtsblatt erhält, nicht aber von wem. Anders verhält es sich dagegen mit der Weitergabe der Abbuchungsermächtigungen. Hier macht es schon einen Unterschied, ob ein Abonnent die Abbuchungsermächtigung seiner Gemeinde erteilt, also einer ihm als zuverlässig bekannten öffentlichen Stelle, oder einem Verlag, den er überhaupt nicht kennt. Die Gemeinde hätte deshalb nach den Vorschriften des Landesdatenschutzgesetzes genau genommen das Einverständnis der Abonnenten zur Weitergabe der Abbuchungsermächtigungen einholen, zumindest aber ihnen die Möglichkeit einräumen müssen, der Weitergabe zu widersprechen. Weil die Gemeinde und der Verlag sich ohnehin im Mitteilungsblatt an die Abonnenten wenden und sie über den neuen Herausgeber unterrichten mussten, wäre dies auch mit keinerlei Mehraufwand verbunden und zudem bürgerfreundlich gewesen.

Im zweiten Beispiel war ein Grundstücksbesitzer bass erstaunt, als er bei der Lektüre seines Kontoauszugs entdeckte, dass ihm die Gemeinde nicht nur die Wasser- und Abwassergebühren, sondern auch die Abfallgebühren per Lastschrift von seinem Konto eingezogen hatte. Für letztere hatte der Bürger nämlich nie eine Abbuchungsermächtigung erteilt. Deshalb bat er mich, den Fall aufzuklären. Die Recherchen ergaben, dass hier keine böse Absicht oder „aufgedrängte Verwaltungsvereinfachung“ im Spiel war, sondern offenbar nur das von der Gemeinde beauftragte Rechenzentrum geschludert hatte. Denn der Fehler passierte, als für die Abrechnung der Abfallgebühren ein neues EDV-Verfahren eingeführt wurde. Aus technischen Gründen konnte das Rechenzentrum die Umstellung aber nur so bewerkstelligen, dass es den Grunddatenbestand aus dem für die Erhebung der Wasser- und Abwassergebühren verwendeten Verfahren in das neue Computerprogramm übernahm. Dabei sollte allerdings das Merkmal „Abbuchungsermächtigung“ und die Kontoverbindung ausgespart bleiben. Dies war aber, so musste das Rechenzentrum einräumen, aus welchen Gründen auch immer missglückt. Weil jedoch die Gemeinde für die ordnungsgemäße Verarbeitung der Daten verantwortlich ist, konnte ich ihr den Vorwurf mangelnder Kontrolle nicht ersparen.

3. Nachdenken!

Ein Immobilienmakler lag mit einem Landratsamt heftig im Clinch, weil es ihm die Maklererlaubnis entzogen hatte. Da er sich dies nicht gefallen

lassen wollte, nahm er Einsicht in die über diesen Vorgang entstandenen Verfahrensakten um prüfen zu können, ob dabei alles mit rechten Dingen zugegangen war. Dabei stellte er fest, dass das Landratsamt ein Schreiben, in dem er sich gegen den angekündigten Widerruf der Erlaubnis gewandt hatte, und den Bescheid über den Widerruf selbst der Industrie- und Handelskammer (IHK) übersandt hatte. Weil aus seiner Sicht keinerlei Anlass für die Übersendung dieser Unterlagen bestand, bat er uns, der Sache auf den Grund zu gehen. Vom Landratsamt und von der IHK wollten wir wissen, auf wessen Betreiben die Übersendung der Unterlagen erfolgte, ob die IHK am Verfahren des Widerrufs der Maklererlaubnis beteiligt war und warum sich das Landratsamt, sofern die Voraussetzungen für eine Unterrichtung der IHK vorlagen, nicht darauf beschränkte, dieser den Widerruf der Maklererlaubnis mitzuteilen. Das Landratsamt konnte oder wollte nur wenig zur Sachverhaltsaufklärung beitragen. Es teilte wortkarg mit, die zuständige Sachbearbeiterin könne sich an die Gründe, warum vor 10 Monaten die Unterlagen übersandt wurden, nicht erinnern. Es könne auch nicht sagen, ob die IHK beim Widerrufsverfahren überhaupt beteiligt war. Zur Frage, warum es der IHK nicht lediglich mitgeteilt hatte, dass es die Maklererlaubnis widerrufen hat, fiel ihm als Begründung nur ein: Das machen wir schon immer so. Mehr Erinnerungsvermögen besaß die IHK. Durch ihre Antwort konnte der Sachverhalt weitgehend aufgeklärt werden. Es stellte sich heraus, dass der Makler die IHK im Februar 1999 gefragt hatte, welche Daten sie über ihn im Zusammenhang mit dem Verfahren zum Widerruf der Maklererlaubnis speichert. Weil die IHK vom Landratsamt jedoch in diesem Verfahren gar nicht beteiligt worden war, konnte sie auch keinen Vorgang finden. Deshalb erkundigte sie sich telefonisch beim Landratsamt, um was für eine Angelegenheit es sich handelt. Dabei erfuhr sie, dass die IHK „wegen Eindeutigkeit des Falles wahrscheinlich nicht angehört worden sei“. Nicht mehr klären ließ sich, ob die IHK um Übersendung der Unterlagen gebeten hatte oder ob das Landratsamt dies von sich aus veranlasst hatte. Für die datenschutzrechtliche Beurteilung spielt das aber auch keine Rolle. Nach der Gewerbeordnung hätte das Landratsamt die IHK nur dann informieren dürfen, wenn es diese, was zulässig gewesen wäre, hier aber nicht der Fall war, am Verfahren beteiligt hätte. Selbstverständlich hätte es – so schreibt es das Gesetz explizit vor – der IHK auch dann nur das Ergebnis des Widerrufsverfahrens mitteilen dürfen, soweit die IHK diese Information für ihre Aufgaben benötigt. Geht es wirklich zu weit, wenn man von Behördenmitarbeitern fordert, dass sie sich vor einer Weitergabe von Unterlagen über einzelne Personen wenigstens Gedanken über die Erforderlichkeit machen sollen? Ich meine nein und habe deshalb den Datenschutzverstoß beanstandet.

2. Abschnitt: Personalwesen

1. Die aufgeblähte Personalnebenakte

Mit Personaldaten gehen nicht nur die Behörden um, die Personal auszuwählen, einzustellen und die Personalgrundakte zu führen haben. Auch die ihnen nachgeordneten Stellen, denen Aufgaben der Personalverwaltung übertragen sind, benötigen bestimmte Informationen über ihre Mitarbeiter und führen deshalb sog. Personalnebenakten. So stellt z. B. das Oberschulamt zwar alle Lehrer ein und führt ihre Personalgrundakte. Bei den Grund-, Haupt-, Real- und Sonderschullehrern nimmt jedoch auch das Staatliche Schulamt Personalverwaltungsaufgaben wahr, indem es u. a. bestimmt, wo und mit welchem Lehrauftrag die seinem Bezirk zugewiesenen Lehrkräfte eingesetzt werden. Mitunter ist eine Personalnebenakte sogar deutlich dicker als die Personalgrundakte, was aber oft nur daran liegt, dass sie vieles enthält, was dort gar nicht hinein gehört. Wiederholt hatten wir in Tätigkeitsberichten (vgl. 15. Tätigkeitsbericht 1994, LT-Drs. 11/5000, S. 85 ff.; 18. Tätigkeitsbericht 1997, LT-Drs. 12/2242, S. 82 ff.) versucht deutlich zu machen, was in die Personalnebenakten aufzunehmen ist und was nicht und wie mit ihnen umzugehen ist. Verinnerlicht haben viele Behörden diese Grundsätze offenbar noch nicht. Dies zeigte sich einmal mehr, als mich ein Lehrer – nennen wir ihn Herrn Maier – bat, ich möge doch einmal seine immerhin

zweibändige, beim Staatlichen Schulamt geführte Personalnebenakte unter die Lupe nehmen. Dabei hätte gerade die Kultusverwaltung Anlass genug gehabt, mit gutem Beispiel voranzugehen und dafür zu sorgen, dass die ihr nachgeordneten Stellen den Anforderungen eines datenschutzgerechten Umgangs mit Personalnebenakten entsprechen. Bereits 1994 hatten wir nämlich dem Kultusministerium einige grundsätzliche Mängel in diesem Bereich, die wir bei einem Kontrollbesuch beim Staatlichen Schulamt Ludwigsburg festgestellt hatten, aufgezeigt und es gebeten, Abhilfe zu schaffen (vgl. 15. Tätigkeitsbericht 1994, a.a.O.). Damals ließ uns das Ministerium wissen, es wolle erst dann konkret tätig werden, wenn die Regelungen über Personalakten im Landesbeamtengesetz in Kraft getreten seien. Das war im Januar 1996 der Fall, doch auch danach rührte sich nichts.

Bei der Personalnebenakte des Herrn Maier gab es hauptsächlich Folgendes zu bemängeln:

1.1 Das alte Lied und Leid mit dem Personalbogen

Bisher ist es Usus, dass die Staatlichen Schulämter einfach ein Doppel des vom Oberschulamt für seine Zwecke verwendeten Personalbogens zur Personalnebenakte nehmen. Weil Herr Maier schon einige Dienstjahre auf dem Buckel hat, befand sich in seiner Personalnebenakte derselbe Personalbogen, den wir seinerzeit beim Staatlichen Schulamt Ludwigsburg angetroffen hatten. Abgesehen davon, dass dieser alte Personalbogen etliche Fragen aufweist, die seit jeher einem Stellenbewerber überhaupt nicht gestellt werden dürfen, wird darin nach einigen Angaben wie z. B. nach Wehr-/Zivildienst, früheren Berufstätigkeiten oder nach dem laufbahnrechtlichen Werdegang gefragt, die zwar für das Oberschulamt als Einstellungsbehörde relevant sind, das Staatliche Schulamt jedoch nichts angehen. Das Kultusministerium wird nicht umhin können, den Staatlichen Schulämtern genau zu sagen, welche Angaben über die Lehrkräfte sie in einem Personalbogen festhalten dürfen.

1.2 Der Lebenslauf – gebräuchlich, aber fehl am Platz

Die Personalnebenakte von Herrn Maier enthielt – wie dies auch bei anderen Personalnebenakten anzutreffen ist – einen handgeschriebenen Lebenslauf. Auch der hat dort nichts zu suchen. Durch die Vorlage eines Lebenslaufs offenbart der Betroffene eine nach Umfang und Inhalt nicht begrenzte Vielzahl personenbezogener Daten, die dem Empfänger durch ihre Zusammenfassung auf engem Raum ein ebenso prägnantes wie schnell überschaubares und abgerundetes Persönlichkeitsbild des Betroffenen liefert. Zudem wird der Betroffene häufig veranlasst, mehr über sich preiszugeben, als der Empfänger des Lebenslaufs an personenbezogenen Daten über ihn erheben dürfte, weil es in der Regel an klaren Vorgaben für den Inhalt des geforderten Lebenslaufs fehlt. Die Erhebung personenbezogener Daten in Form eines Lebenslaufs stellt deshalb einen besonders starken Eingriff in das Recht auf informationelle Selbstbestimmung dar. Vor diesem Hintergrund stellt sich bei Lehramtsbewerbern schon die Frage, ob die Anforderung eines Lebenslaufs überhaupt Sinn macht. Selbst wenn man diese Frage bejahen wollte, hätte nur das Oberschulamt als Einstellungsbehörde das Recht, einen solchen Lebenslauf zu fordern. In die beim Staatlichen Schulamt geführte Personalnebenakte einer Lehrkraft gehört ein Lebenslauf keinesfalls.

1.3 Ärztliche Zeugnisse

Immer wieder finden sich in Personalnebenakten der Staatlichen Schulämter vom Oberschulamt übersandte ärztliche Gutachten. Die Akte des Herrn Maier machte da keine Ausnahme; in ihr waren mehrere ärztliche Zeugnisse – teils sogar Originale – offen abgelegt. Meist übersenden Oberschulämter ihren nachgeordneten Behörden die Kopie eines ärztlichen Zeugnisses aus Bequemlichkeit, obwohl

es ihnen dadurch lediglich mitteilen will, von wann bis wann diese mit der Dienstunfähigkeit einer Lehrkraft zu rechnen haben. Ärztliche Atteste sind jedoch nur für die Personal verwaltende Behörde, also das Oberschulamt, von Bedeutung und dort nur im verschlossenen Umschlag zur Personalgrundakte zu nehmen. Obwohl wir diese datenschutzwidrige Praxis bereits 1996 beanstandet hatten (vgl. 17. Tätigkeitsbericht 1996, LT-Drs. 12/750, S. 72) fällt es den Oberschulämtern offenbar schwer, von dieser lieb gewordenen Gewohnheit Abschied zu nehmen.

Die Personalnebenakte des Herrn Maier enthielt noch viele andere Unterlagen, die dort nicht hinein gehören. Die gravierendsten Mängel habe ich gegenüber dem Kultusministerium beanstandet. Diese wären freilich gar nicht ans Tageslicht gekommen, wenn das Staatliche Schulamt die Akte rechtzeitig ausgesondert hätte. Dazu wäre es nämlich schon längst verpflichtet gewesen, weil Herr Maier seit mehr als 7 Jahren nicht mehr im Dienst des Staatlichen Schulamts stand und klar war, dass er auch nicht mehr dorthin zurückkehren würde. Auch dies beanstandete ich Ende Juli gegenüber dem Kultusministerium. Eine Stellungnahme zu meinem Schreiben erhielt ich noch nicht. Vielmehr teilte es mir mit, eine Arbeitsgruppe werde jetzt klären, welche personenbezogenen Daten der Lehrkräfte die Staatlichen Schulämter zur rechtmäßigen Aufgabenerledigung benötigen, das Ministerium sei aber bemüht, bis Ende November Stellung zu nehmen. Im Klartext heißt das: Bis sich bei der Führung der Personalnebenakten der Lehrer in der Praxis etwas ändert, wird noch einige Zeit ins Land gehen. Geduld ist eben nicht nur, wie Rosa Luxemburg meinte, die Tugend der Revolutionäre, sondern auch der Lehrer.

2. Suchtprobleme coram publico?

Seit vielen Jahren besteht zwischen der Verwaltung und dem Gesamtpersonalrat einer Stadt eine Dienstvereinbarung über „Suchtprävention und Suchtkrankenhilfe“. Diese sieht u. a. vor, dass mit Mitarbeitern, die „infolge von missbräuchlichem Umgang mit potenziell Sucht auslösenden Stoffen eine Sicherheitsgefahr darstellen“, Gespräche zu führen sind. Zu diesen sollen je nach Lage der Dinge außer den direkten Vorgesetzten und Bediensteten der Personalverwaltung der Sozialdienst für Mitarbeiter, der Personalrat, Familienangehörige und Freunde hinzugezogen werden können. Bisher geschehe dies – wie uns die Stadt früher einmal wissen ließ – nur mit Einverständnis des Betroffenen. Bei der anstehenden Überarbeitung der Dienstvereinbarung wollten sich Personalverwaltung und Gesamtpersonalrat die Arbeit erleichtern und auf die Einwilligung verzichten. Sie hatten das neue Landesdatenschutzgesetz aufmerksam gelesen und dabei entdeckt, dass danach personenbezogene Daten von Beschäftigten u. a. verarbeitet werden dürfen, wenn eine Dienst- oder Betriebsvereinbarung dies vorsieht. Nur der Datenschutzbeauftragte der Stadt hatte Zweifel, ob der Dienstherr wirklich berechtigt ist, Suchtprobleme von Bediensteten ohne deren Einverständnis vor dem Personalrat, Kollegen, Familienangehörigen und Freunden auszubreiten und wollte dies von uns geklärt wissen. Mit seinen Bedenken lag er durchaus richtig, denn eine Dienstvereinbarung kann kein Freibrief für Eingriffe in das Persönlichkeitsrecht von Bediensteten sein. Zwar gibt es unterschiedliche Auffassungen darüber, ob durch einen Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung stärker in das Persönlichkeitsrecht eines Bediensteten eingegriffen werden darf, als dies nach allgemeinem Datenschutzrecht zulässig wäre. Während das Bundesarbeitsgericht dies grundsätzlich bejaht, halten namhafte Stimmen in der Literatur dies für unmöglich. Im Ergebnis laufen beide Ansichten jedoch weitgehend auf dasselbe hinaus. Denn auch das Bundesarbeitsgericht weist darauf hin, dass datenschutzrechtliche Regelungen in Tarifverträgen oder Betriebsvereinbarungen nicht einen beliebigen Inhalt haben können. Sie müssten sich vielmehr an den grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den sich aus allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen orientieren. Deshalb können Dienstvereinbarungen im Wesentlichen nur das allgemeine Datenschutzrecht konkretisieren.

Für die Mitwirkung der genannten Personen bedeutet das:

Soweit es zu den Aufgaben des betrieblichen Sozialdienstes gehört, beim Umgang mit solchen „Problemfällen“ mitzuwirken, nimmt er Personalverwaltungsaufgaben wahr, so dass die Teilnahme an einem Gespräch mit dem Betroffenen auch ohne dessen Zustimmung zulässig ist. Bei der Mitwirkung des Personalrats liegen die Dinge dagegen anders. Den Bestimmungen des Landespersonalvertretungsgesetzes ist zu entnehmen, dass der Personalrat grundsätzlich nicht gegen den Willen des Bediensteten bei individuellen Personalmaßnahmen tätig werden darf. Die Ausnahmen von diesem Grundsatz sind im Gesetz selbst dezidiert und abschließend geregelt. Eine Teilnahme von Personalratsmitgliedern an einem Gespräch mit dem Betroffenen ohne dessen Einverständnis ist deshalb nicht möglich. Erst recht dürfen Kollegen, Angehörige und Freunde nicht ohne Einverständnis des Betroffenen am Gespräch teilnehmen. Eine gegenteilige Regelung wäre in der Dienstvereinbarung nur möglich, wenn die Datenweitergabe an den genannten Personenkreis im überwiegenden Allgemeininteresse geboten wäre. Davon kann jedoch keine Rede sein. Wie es mit der Überarbeitung der Dienstvereinbarung weitergeht, ist noch offen.

3. Kein Datenschutz in der Familie?

Immer wieder erreichen mich Briefe, in denen so oder ähnlich zu lesen ist:

> „Ich lebe seit einigen Monaten von meinem Noch-Ehemann getrennt. Meine Beihilfeanträge muss ich über meinen Mann an das Landesamt für Besoldung und Versorgung einreichen. Eine Vollmacht, damit ich die Anträge selbst einreichen kann, unterschreibt er mir nicht. Diese Praxis bedeutet eine grobe Verletzung meiner Persönlichkeitsrechte. Hier gelangt eine Person, meiner Meinung nach widerrechtlich, an Informationen (meine Krankengeschichte), die er (im Scheidungsverfahren) zu seinen Gunsten ausnutzen kann. Das darf doch wohl nicht wahr sein!“

Recht hat die Dame, doch helfen konnte ich ihr dennoch nicht, denn die Rechtslage ist eindeutig. Regelmäßig muss ich in meiner Antwort konstatieren, dass der Datenschutz der Familienangehörigen bei der Gewährung der beamtenrechtlichen Beihilfe auf der Strecke bleibt. Während nämlich bei der gesetzlichen Krankenversicherung jedes Familienmitglied einen eigenen Anspruch auf Versicherungsleistungen hat, ist das bei der Bewilligung von Beihilfe anders. Dort hat lediglich der Beamte oder Richter selbst einen Erstattungsanspruch. Nur er kann die Aufwendungen, die einem Familienangehörigen durch eine ambulante oder stationäre Behandlung entstanden sind, geltend machen; einen eigenen Beihilfeanspruch haben die Familienangehörigen nicht. Auch der Beihilfebescheid muss dem Beihilfeberechtigten selbst zugesandt werden, damit er wirksam wird. Die gewährte Beihilfe wird ihm überwiesen. Auf diese Weise erfährt er stets die Krankheitsdaten seiner Angehörigen und kann dieses Wissen zu seinen Gunsten verwenden. Das ist aber gerade dann besonders problematisch, wenn das Partnerschaftsverhältnis oder die Eltern-Kind-Beziehung gestört ist. Schon seit langem fordern die Datenschutzbeauftragten des Bundes und der Länder einen eigenen Beihilfeanspruch für Angehörige. Erfolg bislang gleich Null, denn nicht einmal ein erster Schritt in Richtung einer Rechtsänderung ist getan. Das Finanzministerium hat bisher lediglich akzeptiert, dass der Beihilfeberechtigte seinen Ehegatten bevollmächtigen kann, einen Beihilfeantrag für sich und die bei ihm lebenden Kinder zu stellen und die gewährte Beihilfe entgegenzunehmen. Nicht nur aus meiner Sicht ein unmöglicher Zustand!

3. Abschnitt: Schulen und Hochschulen

1. Antworten der Schüler sind gefragt

Manche Datenschutzprobleme sind quasi Eintagsfliegen – einmal abgehandelt, kehren sie nicht wieder. Andere sind gewissermaßen Dauer-

brenner. Dazu gehört die datenschutzkonforme Befragung bei Forschungsvorhaben und anderen Untersuchungen. Weil dabei der Datenschutz immer wieder ignoriert wird, habe ich die Materie im letzten Tätigkeitsbericht am Beispiel der Befragung von Schülern zum wiederholten Mal eingehend behandelt. Das Resultat stimmt nachdenklich, denn es gibt nicht nur Positives zu vermelden – auch in diesem Jahr musste ich wieder Schülerbefragungen kritisieren, bei denen der Datenschutz missachtet wurde.

1.1 IGLU mit kleinen Mängeln

Nachdem das Kultusministerium im letzten Jahr bei drei Schülerbefragungen datenschutzrechtlich Schiffbruch erlitten hatte (vgl. 20. Tätigkeitsbericht 1999, LT-Drs. 12/4600), ging es in diesem Jahr vorsichtiger zu Werke. Sofort nachdem es die Unterlagen zur „Internationalen Grundschul-Lese-Untersuchung (IGLU)“, an der sich das Land beteiligt, erhalten hatte, bat es mein Amt um eine datenschutzrechtliche Beurteilung. Mit dieser Studie wird untersucht, wie Kinder lesen lernen. Dabei sollen die Grundschüler Angaben zu ihren Lese- und Fernsehgewohnheiten, ihrer Einstellung zum Lesen und Lernen, der Unterstützung des Lesens durch die Eltern und zum soziodemografischen Hintergrund machen. Die Eltern der teilnehmenden Kinder werden zu ihren Erfahrung beim Lesenlernen ihres Kindes und den familiären Rahmenbedingungen gefragt. Bei der Prüfung des Vorhabens zeigte sich schnell, dass das IEA Data Processing Center in Hamburg, das uns von der Durchführung der im letzten Jahr beurteilten Untersuchungen „PISA“ und „Civic Education“ bekannt ist, seine Lektion gelernt hatte. Zwar musste es hinsichtlich der Information von Eltern und Schülern sowie bei den Schüler- und Eltern-Fragebogen vor allem im Hinblick auf die Einwilligung etwas nachbessern, ansonsten war die Konzeption aber datenschutzrechtlich in Ordnung.

1.2 Runde Tische ecken an

Ausgelöst durch einige Vorfälle, bei denen Schüler gegenüber Lehrern, Mitschülern oder anderen Personen gewalttätig geworden waren, haben sich in vielen Städten und Gemeinden sog. „Runde Tische“ gebildet. Sie dienen dazu, Maßnahmen zu planen und durchzuführen, die Kriminalität, insbesondere Gewalt von Jugendlichen, vorbeugen und vermeiden helfen. Mitglieder dieser Arbeitskreise sind regelmäßig die Schulen und/oder Elternbeiräte, die Polizei, Träger von Jugendeinrichtungen und last not least Städte und Gemeinden, die dabei Regie führen. So weit, so gut. Als eine der ersten Maßnahme steht dann oft die Durchführung einer Schülerbefragung zum Thema „Jugend und Gewalt“ oder „Gewaltprävention in der Stadt“ auf der Tagesordnung. Erboste Eltern machten uns mehrfach auf solche Schülerbefragungen aufmerksam und meinten zu Recht, es könne doch nicht sein, dass ihr Kind befragt werden darf, ohne dass sie dazu ihr Einverständnis erklärt hätten. Die Initiatoren machten genau die gleichen Fehler, wie wir sie von den früheren Schülerbefragungen her kannten. Kardinalfehler war, dass sie die Befragung als „anonym“ bezeichneten, obwohl die Schüler u. a. nach ihrem Alter, ihrem Geschlecht und ihrer Staatsangehörigkeit, ihrer Schule und Klassenstufe und ihrem Ortsteil gefragt wurden und dadurch viele von ihnen mühelos zu identifizieren waren mit der Folge, dass die Vorschriften des Landesdatenschutzgesetzes anzuwenden gewesen wären.

Am Beispiel einer Befragung im Oberschwäbischen will ich die wesentlichen Mängel nochmals darstellen:

– Im Elternanschreiben beschränkte sich die Unterrichtung darüber, was Gegenstand der Schülerbefragung sein soll, darauf, dass Angaben zur körperlichen, seelischen und sexuellen Gewalt in der Schule erbeten werden. Darüber, dass die Kinder in erheblichem Umfang auch nach dem häuslichen Umfeld und dem

Umgang mit den Eltern gefragt werden, ließ man diese im Unklaren. Zudem fehlte jede Aufklärung darüber, nach welchen Kriterien und mit welchem Ziel die Fragebogen ausgewertet und wo und wie lange die erhobenen Angaben aufbewahrt werden sowie welche Stelle dafür letztendlich verantwortlich ist.

- Im Elternanschreiben und im Fragebogen fehlte der nötige Hinweis darauf, dass durch die Nichtteilnahme an der Befragung keinerlei Nachteile entstehen.
- Im Gegensatz zum Anschreiben an die Eltern fehlten im Fragebogen selbst die Hinweise darauf, dass die Teilnahme an der Befragung freiwillig ist. Dies wäre aber erforderlich gewesen, weil die Schülerinnen und Schüler an der Befragung auch dann nicht teilnehmen müssen, wenn ihre Eltern der Teilnahme zugestimmt haben.
- Die Eltern hätten der Teilnahme ihrer Kinder an der Befragung ausdrücklich und schriftlich zustimmen müssen. Dies ist unterblieben. Eine konkludente Einwilligung durch Nichtäußerung, wie sie die Konzeption der Befragung vorsah, kennt das Landesdatenschutzgesetz nicht.
- Es dürfte für die Schülerinnen und Schüler zudem unzumutbar gewesen sein, sich durch ihre Antworten auf bestimmte Fragen ggf. eines strafbaren Verhaltens zu bezichtigen, zumal die Strafverfolgungsbehörden nicht gehindert wären, Fragebogen zur Strafverfolgung zu beschlagnahmen.

In zwei Fällen habe ich die datenschutzwidrige Durchführung der Schülerbefragung gegenüber den betroffenen Städten förmlich beanstandet und diese gebeten, die rechtswidrig erhobenen Daten zu löschen. Dem sind beide Städte auch ohne weiteres nachgekommen.

Die Durchführung von Schülerbefragungen hat aber noch einen anderen Aspekt: Nach einer Verwaltungsvorschrift des Kultusministeriums müssen solche Befragungen vom Oberschulamt genehmigt werden. Sinn dieser Regelung ist es, dass an höherer Stelle geprüft werden soll, ob eine Befragung pädagogisch sinnvoll und nach Art und Umfang mit dem Erziehungs- und Bildungsauftrag der Schule vereinbar ist. Weil dem so ist, bedürfen Schülerbefragungen auch dann der Genehmigung, wenn die Stadt oder Gemeinde, die Trägerin der Schule ist, für sie verantwortlich zeichnet. Die in der Verwaltungsvorschrift vorgesehene Genehmigungsfreiheit für den Schulträger ist demgegenüber nur dann gegeben, wenn dieser eine Erhebung durchführt, deren Ergebnisse er benötigt, um gerade seine Aufgabe als Schulträger besser erfüllen zu können.

Damit verhielt es sich in den mir bekannt gewordenen Fällen so:

- In zwei Fällen ersuchten die Schulen das Oberschulamt tatsächlich um Genehmigung. Dieses kam dem Wunsch nach und verzichtete ausdrücklich „unter Zurückstellung von Bedenken“ darauf, dass sie die Einwilligung der Eltern einholen.
- Im dritten Fall hielt sich das Staatliche Schulamt für kompetent genug und genehmigte die Befragung kurzerhand selbst.
- Bei der vierten Schülerbefragung verzichteten die Schulen lieber von vornherein darauf, das Oberschulamt um Genehmigung zu bitten.

Der letzte Fall muss wohl auch für das Kultusministerium ärgerlich gewesen sein, weil es zuvor bereits in einem Erlass an die Oberschulämter auf die datenschutzrechtlichen Voraussetzungen bei der Genehmigung von wissenschaftlichen Erhebungen in Schulen hingewiesen hatte. Dieser Ukas kam aber entweder bei den Schulen nicht an oder er wurde schlicht missachtet. Deshalb will das Kultusministerium nun meinem Vorschlag nachkommen und die datenschutzrechtlichen Anforderungen nochmals durch Veröffentlichung in seinem Amtsblatt, im Internet und im „Info-Dienst Schulleitung“

veröffentlichen. Ich hoffe, dass dann endlich die nötige Breitenwirkung erzielt wird und künftig auch die Schulen ihre Sache besser machen.

2. Prüfungsergebnisse via Internet

Mitunter ist es nicht nur zulässig, sondern sogar datenschutzfreundlicher, traditionelle Vorgehensweisen durch elektronische Angebote zu ersetzen. Ein Beispiel dafür ist die Bekanntgabe von Prüfungsergebnissen an Hochschulen. Diese werden bislang oft, durch Verwendung der Matrikelnummer anstelle des Namens des Prüflings mehr schlecht als recht anonymisiert, an einem „Schwarzen Brett" ausgehängt. Dort kann jeder, der zufällig die Matrikelnummer eines Kommilitonen kennt, dessen Leistung in der Prüfung in Erfahrung bringen. In einer Zeit, in der fast jeder Student an der Alma Mater oder privat über einen Internet-Zugang verfügt, halten dies manche Hochschulen und Studierende gleichermaßen nicht mehr für zeitgemäß. Sie wollen den Aushang der Noten durch eine Abrufmöglichkeit per Internet ersetzen. Verschiedentlich wurde ich gefragt, wie ich ein solches Verfahren bewerte. Aus Sicht des Datenschutzes, so meine Antwort, kann der Notenabruf via Internet einen besseren Schutz vor unberechtigter Kenntnisnahme bieten als ein Aushang am Schwarzen Brett. Voraussetzung dafür ist allerdings, dass die notwendigen Sicherheitsvorkehrungen getroffen werden.

Zum einen muss gewährleistet sein, dass nur der Prüfling und sonst niemand auf seine Prüfungsdaten zugreifen kann. Würden z. B. die Prüfungsergebnisse zusammen mit den Matrikelnummern in einer frei zugänglichen Web-Seite im Internet eingestellt, so könnte jeder, dem die Matrikelnummer eines Studierenden bekannt ist, mit einer im Internet verfügbaren Suchmaschine gezielt nach dessen Benotung suchen. Dies wäre wesentlich leichter ins Werk zu setzen als wenn derjenige, der sich für die Benotungen interessiert, dazu in die Hochschule gehen und dort mit einigem Aufwand an Zeit und Spürsinn das richtige Schwarze Brett und die Prüfungsergebnisse suchen müsste. Deshalb muss das Verfahren so gestaltet sein, dass jeder Prüfling zweifelsfrei identifiziert wird, bevor er sich sein Prüfungsergebnis anzeigen lassen kann. Das wäre in herkömmlicher Manier durch Eingabe einer individuellen Benutzerkennung und eines Passworts zu bewerkstelligen. Eine sicherere Variante, wenngleich aufwendiger, wäre die Verwendung einer digitalen Signatur. Zum andern sind die Daten zu verschlüsseln um auszuschließen, dass sie ein Dritter während der Übertragung im Internet lesen kann.

4. Abschnitt: Die Archive

1. Die Zwangsarbeiter

Ein trauriges Kapitel unserer Geschichte, nämlich die Beschäftigung von Zwangsarbeitern in der NS-Zeit, hat im Zuge der Auseinandersetzung über die Entschädigungszahlungen durch die Stiftung „Erinnerung, Verantwortung und Zukunft" und deren Finanzierung eine besondere Aktualität erhalten. Das wirkte sich auch auf die Arbeit meines Amtes aus:

1.1 Wohin mit den Unterlagen?

Was viele vielleicht nicht wissen: Auch die während der NS-Zeit zur Zwangsarbeit eingesetzten Fremdarbeiter waren – unfreiwillig – Mitglied in der gesetzlichen Krankenversicherung. Unterlagen, die dies dokumentieren, lagern heute noch zuhauf in Altregistraturen von Krankenkassen. Gehören diese nicht in die Archive, deren Aufgabe es ja ist, die Unterlagen aufzubewahren, denen historischer Wert zukommt und die es auch der Nachwelt ermöglichen sollen, sich ein Bild darüber zu verschaffen, wie unser Gemeinwesen sich früher darstellte? Danach gefragt, habe ich folgende Auffassung vertreten:

Das Landesarchivgesetz verpflichtet die Krankenkassen im Lande, alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen, dem für sie zuständigen Staatsarchiv anzubieten, es sei denn, sie ver-

fügen über ein eigenes, archivfachlichen Ansprüchen genügendes Archiv. Letzteres ist aber, soweit ich weiß, nirgendwo der Fall. Nun benötigt aber eine Krankenkasse die in ihrem Besitz befindlichen Unterlagen über die Zwangsarbeiter ganz sicher nicht mehr zur Gewährung von Leistungen, so dass der Fall auf den ersten Blick eigentlich klar sein müsste. Geht man der Fragestellung aber genauer auf den Grund, zeigt sich, dass sich die Krankenkassen dieser Unterlagen keineswegs so ohne weiteres, sei es durch Abgabe an das Archiv oder aber durch ihre Vernichtung, entledigen dürfen. Denn das Sozialgesetzbuch geht davon aus, dass Angaben über Versicherte, auch wenn die Krankenkasse sie zur Erbringung von Versicherungsleistungen nicht mehr benötigt, dann nicht gelöscht werden dürfen, wenn Grund zur Annahme besteht, dass durch die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Genau dies wäre aber bei einer Vernichtung der Unterlagen über Zwangsarbeiter der Fall: Sie könnten nämlich bei einer Vernichtung unter Umständen nicht mehr nachweisen, dass sie in der NS-Zeit zur Zwangsarbeit eingesetzt worden waren. Hat diese Regelung zur Folge, dass die Unterlagen bis zum Sankt-Nimmerleins-Tag oder jedenfalls so lange, bis angenommen werden kann, dass alle ehemaligen Zwangsarbeiter gestorben sind, bei den Krankenkassen gelagert werden müssen? Mitnichten. Eine Abgabe an das Staatsarchiv kann vielmehr dann erfolgen, wenn dieses sich jeweils gegenüber der Krankenkasse verpflichtet, Auskunftsersuchen von Zwangsarbeitern in der gleichen Weise zu entsprechen, wie dies die Krankenkasse selbst tun würde. Ist das der Fall, gibt es nämlich für die Krankenkassen keinen Grund mehr anzunehmen, durch einen Verzicht auf die Speicherung im eigenen Haus würden schutzwürdige Interessen der Zwangsarbeiter beeinträchtigt.

1.2 Die Arbeitgeber

Die Stiftungsinitiative der Deutschen Wirtschaft tut sich erkennbar schwer, die Mittel aufzubringen, die sie für die Stiftung „Erinnerung, Verantwortung und Zukunft“ bereitstellen will. Offensichtlich ist die Bereitschaft von Unternehmen, zu diesem Zweck einen Beitrag zu leisten, nicht so ausgeprägt, wie sich viele dies erhofft hatten. In gewisser Weise nachvollziehbar ist deshalb der Wunsch mancher Personen und Organisationen, die Unternehmen, die in der NS-Zeit Zwangsarbeiter beschäftigt haben, in Erfahrung zu bringen, um auf sie einwirken zu können. Mit einem solchen Ansinnen konfrontiert, wollte eine Stadt von mir wissen, wie ich die Rechtslage beurteile. In ihrem Archiv bewahrt sie unmittelbar nach Kriegsende erstellte Listen mit den Namen von Zwangsarbeitern und Landwirten auf, denen diese in der NS-Zeit zugeteilt waren. Für die in diesen Listen enthaltenen Angaben legt das Landesarchivgesetz eine Nutzungssperre fest, die frühestens 10 Jahre nach dem Tod der einzelnen Personen endet. Kann der Todeszeitpunkt nicht oder nur mit unvertretbarem Aufwand festgestellt werden, endet die Frist erst 90 Jahre nach der Geburt. Das bedeutet, dass die Sperrfrist bei vielen der in den Listen aufgeführten Personen noch nicht abgelaufen war. Das Landesarchivgesetz sieht zwar auch die Möglichkeit einer Verkürzung der Sperrfrist vor, so z. B. dann, wenn die Nutzung zur Wahrnehmung berechtigter Belange, die im überwiegenden Interesse einer anderen Person oder Stelle liegen, unerlässlich ist und durch eine Anonymisierung oder durch andere Maßnahmen die schutzwürdigen Belange der Betroffenen angemessen berücksichtigt werden. Diese Voraussetzungen waren nun aber in dem von der Stadt geschilderten Fall ganz sicher nicht gegeben, so dass eine komplette Überlassung der Zwangsarbeiter- und Arbeitgeberlisten nicht in Frage kam.

2. Das Archiv als Hilfsregistratur

Es gibt Dinge auf dieser Welt, die sind für die Ewigkeit bestimmt. Einbürgerungsakten gehören offenbar auch dazu. Stellt ein Ausländer einen Antrag, um die deutsche Staatsangehörigkeit zu erwerben, legt die Einbürgerungsbehörde eine Akte an, in die sie alle Unterlagen aufnimmt, die in diesem Verfahren anfallen. Dabei handelt es sich um teilweise recht sensible Informationen wenn man bedenkt, dass die einbürgerungswilligen Ausländer u. a.

ausreichende Einkünfte und ihre Loyalität zum deutschen Staat belegen müssen. Diese Akten halten zwei von meinem Amt kontrollierte Einbürgerungsbehörden für so wichtig, dass sie sie für unbestimmte Zeit aufbewahren wollen. Es könnten ja in ferner Zukunft irgendwann einmal Zweifel daran aufkommen, ob man den Großvater eines Mitbürgers seinerzeit zu Recht eingebürgert hat!

Die Folge ist klar: Der Aktenbestand nimmt immer größere Ausmaße an. Er wird in absehbarer Zeit sogar noch umfangreicher werden, weil der Gesetzgeber die Voraussetzungen für den Erwerb der deutschen Staatsbürgerschaft erleichtert hat und deswegen die Zahl der Einbürgerungsanträge steigen wird. Die beiden Einbürgerungsbehörden erkannten diese Misere. Sie behelfen sich damit, dass sie einfach alle Aktenvorgänge, die vor einem bestimmten Zeitpunkt entstanden sind, an das Archiv ihrer Stadt oder ihres Landkreises abgeben. Natürlich haben sie sich den weiteren Zugriff auf dieses Schriftgut dort vorbehalten, denn diese Akten sollen ja – wie gesagt – stets und ewig zur Erfüllung ihrer Aufgaben notwendig sein.

Dass die Einbürgerungsbehörden einen Teil ihrer Akten dem Archiv übergeben, obwohl diese noch gar nicht abgeschlossen sind, ist nicht zu kritisieren. Zwar schreibt das Landesarchivgesetz vor, dass einmal an die Archive abgegebene Unterlagen grundsätzlich erst nach Ablauf von bestimmten Sperrfristen genutzt werden dürfen. Von diesem Nutzungsverbot sind jedoch die Stellen ausgenommen, bei denen das Aktenmaterial entstanden ist. Sie können im Archiv in ihren Akten auch dann noch blättern, wenn sie sie diesem sozusagen vorzeitig überlassen haben, der Zeitpunkt, zu dem der jeweilige Vorgang ausgesondert werden muss, also noch gar nicht gekommen ist.

Da aber liegt das eigentliche Problem. Einen solchen Zeitpunkt, zu dem sie die Einbürgerungsakten endgültig schließen und sich von ihnen verabschieden müssen, haben die beiden kontrollierten Einbürgerungsbehörden ja gerade nicht vorgesehen. Da es sich dabei um eine Frage handelt, die alle Einbürgerungsbehörden betrifft, habe ich das Innenministerium aufgefordert, landeseinheitliche Regelungen für die Aufbewahrungsdauer von Einbürgerungsakten zu schaffen. Dort hat man einen Grund gefunden, die Sache auf die lange Bank schieben zu können: Man glaubt daran, dass es irgendwann in der Zukunft eine „Gesamtreform des deutschen Staatsangehörigkeitsrechts“ geben wird. Und erst mit dieser zusammen wolle man auch die Frage der Aufbewahrungsdauer von Einbürgerungsakten wieder aufgreifen. Bis dahin bleibt es jedenfalls beim bisherigen Zustand: Einbürgerungsakten sind für die Ewigkeit bestimmt.

5. Abschnitt: Das Finanzamt

1. Fair zum Steuerbürger!

Trotz aller Beteuerungen, man wolle ein bürgerfreundliches „Service-Unternehmen“ sein, scheint Fairness gegenüber der „Kundschaft“ bei manchen Finanzämtern noch kein ausgeprägter Wesenszug zu sein. Dass zeigte der Fall eines Eigenheimerwerbers. Er hatte bei seinem Finanzamt einen Antrag auf Gewährung einer sog. Eigenheimzulage, ein staatlicher Geldsegen für die Anschaffung selbstgenutzten Wohnraums, gestellt. Alsbald erhielt er einen vom Finanzamt für solche Fälle eingesetzten Fragebogen, auf dem es u. a. eine Zusammenstellung der Anschaffungskosten für das erworbene Objekt und eine Finanzierungsaufstellung erbat. Unmissverständlich brachte das Finanzamt auf diesem Formular zum Ausdruck, dass diese Unterlagen erforderlich seien, um den Antrag rasch bearbeiten zu können. Unserem Mann kamen jedoch Zweifel, ob es denn für die Gewährung der Zulage tatsächlich notwendig sein soll, dem Finanzamt im Einzelnen darzulegen, wo das Geld für seine Immobilie herstammt. Er fragte deswegen dort nach und erhielt zur Antwort: „Die Frage der Finanzierung der Anschaffungskosten spielt für die Bearbeitung des Antrags auf Eigenheimzulage keine Rolle!“ Aber wenn man schon – so die Erklärung des Finanzamts weiter – in diesem Verfahren eine Reihe von Unterlagen anfordere, dann solle der Antragsteller auch gleich die Finanzierungsaufstellung mit vorlegen. Diese

benötige man nämlich im nächsten Jahr für seine Einkommensteuerveranlagung. Doch auch diese Auskunft war unzutreffend. Für diesen Zweck hätte sich das Finanzamt allenfalls danach erkundigen können, ob dem Steuerpflichtigen durch den Erwerb der Immobilie Verluste entstanden oder Einkünfte zugeflossen sind, nicht aber danach, wie er sie finanziert hat. Da er offensichtlich keine Lust mehr hatte, sich immer neue Versionen des Finanzamts anzuhören, wandte er sich an mein Amt.

Ich musste ihm mitteilen, dass das Finanzamt durchaus berechtigt ist, diese Fragen zu stellen und, um seine Auskünfte nachvollziehen zu können, entsprechende Unterlagen anzufordern. Denn dass es solche Anträge sorgfältig prüft und der Betroffene dazu eine Reihe von Angaben machen muss, etwa wie hoch seine Anschaffungskosten waren und ob er dieses Wohnobjekt selbst nutzt, ist datenschutzrechtlich keineswegs zu kritisieren. Auch dürfen die Finanzämter hellhörig werden, wenn sie von derart kapitalintensiven Anschaffungen Kenntnis erhalten. Denn sie mussten immer wieder die Erfahrung machen, dass es manche Steuerpflichtige mit dem Abführen von Kapitalertrags- und Schenkungssteuern nicht besonders genau nehmen. Deswegen nehmen sie solche Gelegenheiten zum Anlass, sich danach zu erkundigen, ob der Steuerpflichtige die eingesetzten Gelder in der Vergangenheit auch ordnungsgemäß versteuert hat. Wenn die Finanzämter dazu eine Finanzierungsaufstellung für das Kaufobjekt anfordern, ist dies durchaus zulässig.

Das eigentliche Problem dieses Falles ist ein anderes: Das Finanzamt hätte den Steuerpflichtigen korrekt darüber belehren müssen, welche seiner Angaben für die Bearbeitung des Antrags erforderlich sind und welche Kontrollzwecken dienen bzw. welche Angaben er im eigenen Interesse für die Gewährung der begehrten Zulagen machen sollte und welche er machen muss, um sich nicht dem Verdacht der Steuerhinterziehung auszusetzen. Denn Erhebungsformulare – das gilt auch für die der Steuerverwaltung – müssen die Rechtsgrundlage und den Zweck, für den die Daten erhoben werden, eindeutig erkennen lassen. Dieser Verpflichtung wurde das Finanzamt in doppelter Weise nicht gerecht: Zum einen erweckte es mit seinem Formular den unzutreffenden Eindruck, sämtliche darauf erfragten Angaben des Steuerpflichtigen seien ausschließlich für die Bearbeitung seines Antrags erforderlich. Zum anderen steigerte es die Verwirrung beim Bürger noch dadurch, dass es dessen Rückfragen falsch beantwortete.

Auf meine Kritik an dieser rechtswidrigen Praxis reagierte die zuständige Oberfinanzdirektion rasch: Sie wies die Finanzämter an, künftig die Angaben für diese beiden Verfahren mittels verschiedener Formulare zu erheben, auf denen sie jeweils auf den tatsächlichen Datenverarbeitungszweck hinweisen.

2. Und sie bewegt sich doch!

An diesen berühmt gewordenen Ausspruch von Galileo Galilei erinnerte ich mich, als mir das Finanzministerium im Frühjahr dieses Jahres mitteilte, künftig würde bei allen Einkommensteuer-Erstattungen auf dem Überweisungsträger als Verwendungszweck lediglich die Steuernummer sowie der zusammengefasste Grund der Erstattung angegeben werden. Auf die bis dahin übliche Angabe zu den Annexsteuern, also insbesondere zur Kirchensteuer, wolle man verzichten. Damit fand eine lange Auseinandersetzung mit der Steuerverwaltung ein gutes Ende. Erstmals im Jahr 1988 hatte mein Amt das Finanzministerium aufgefordert dafür Sorge zu tragen, dass die Banken bei der Überweisung von Steuerrückerstattungen nicht erkennen können, ob jemand Kirchensteuerzahler ist oder nicht. Eine solche Unterrichtung der Bank sei zur Durchführung von Erstattungen nicht notwendig (vgl. 9. Tätigkeitsbericht 1988, LT-Drs. 10/950, S. 44). Zahlreiche Schreiben gingen daraufhin hin und her. Das Bundesfinanzministerium veranstaltete eine Länderumfrage. Die Bundessteuerberaterkammer, der Deutsche Steuerberaterverband und der Bundesverband der Steuerberater votierten unterschiedlich. Dazwischen erreichten uns immer wieder Beschwerden von Bürgern, die mit der Vorgehensweise der Finanzämter nicht einverstanden waren. Lange schien es, als ob sich nichts bewegen würde. Dann, zu Anfang des Jahres 1998, gab es erstmals einen Ruck. Das Finanzministerium ordnete

an, dass in den sog. Arbeitnehmerfällen, das sind die Fälle, in denen lediglich ein Lohnsteuerjahresausgleich durchgeführt wird, eine „detaillierte Erläuterung und Aufgliederung des Steuerbetrags auf den Überweisungsträgern unterbleibt“. Das war zwar ein Schritt in die richtige Richtung, eine endgültige Lösung war es noch nicht. Dazu konnte sich das Finanzministerium erst jetzt durchringen. Aber immerhin, es sprang jetzt über seinen Schatten.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Anhang 1: Risiken und Grenzen der Videoüberwachung

Anhang 2: Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Anhang 3: Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

Anhang 4: Für eine freie Telekommunikation in einer freien Gesellschaft

Anhang 5: Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Anhang 6: Data Warehouse, Data Mining und Datenschutz

Anhang 7: Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Anhang 8: Auftragsdatenverarbeitung durch das Bundeskriminalamt

Anhang 9: Entschließung zur Novellierung des BDSG

Anhang 10: Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung

Anhang 11: Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Anhang 12: Datensparsamkeit bei der Rundfunkfinanzierung

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 2000

Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

– eine strenge Zweckbindung,

– eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,

– die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,

– die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten

sowie

– die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozeßrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener – insbesondere biometrischer – Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

   – Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen – **soweit nicht***

überwiegende schutzwürdige Belange von Betroffenen entgegenstehen – *unter anderem in Betracht[1]:*

- *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.*
- *für die Verkehrslenkung nur Übersichtsaufnahmen,*
- *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*

– Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.

– Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.

– Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im Einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.

– Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.

– Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

[1] Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 2000

Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 2000

Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu“ eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere“ jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereitgehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung“. Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten“, nicht die einzelne Person und auch nicht das „Gesamtbild einer Person“. Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 2000

Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- Erhebliche Zunahme der Telekommunikationsvorgänge

  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mailboxen sowie das Internet genutzt.

- Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten

  – Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.

  – Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.

  – Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.

  – Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.

  – Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

- Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten

  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

- Entwicklung des Internets zum Massenkommunikationsmittel

  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

- Schwer durchschaubare Rechtslage

  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802

- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der

Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.
- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen „ENFOPOL“ , befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.
- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.
- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.
- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.
- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.
- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.
- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhält-

nismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.
- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.
- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 2000

Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o. Ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen haben, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.
- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind – es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann – zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden – nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.

  Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o. g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum – ausschließlich zum Zweck der Sicherung des Rechtsschutzes – aufzubewahren.
- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).

  Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.

  Damit sind Regelungen z. B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmelde-

geheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.

Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.

- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.
- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.
- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung – bei Datenübermittlungen auch bei den Datenempfängern – erstrecken.
- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.
- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.
- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 2000

Data Warehouse, Data Mining und Datenschutz

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse“ werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining“ bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus“ gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden sind. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern“ rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining“ ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse“ - und „Data Mining“-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26. Juni 2000

Effektive parlamentarische Kontrolle von Lauschangriffen
durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe“ zu unterrichten. § 100 e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahmen zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100 e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem „Großen Lauschangriff“ ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z. B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn – wie in den „Wire-tap-Reports“ der USA – die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100 c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe“.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 10. Oktober 2000

Auftragsdatenverarbeitung durch das Bundeskriminalamt

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Die Datenschutzbeauftragten warnen vor einer solchen Entwicklung und fordern dazu auf, die für die Datenverarbeitung beim BKA gesetzlich gezogenen Grenzen strikt zu beachten.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 12./13. Oktober 2000

Entschließung zur Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz – § 3 a E-BDSG) und die Einführung des Datenschutzaudit (§ 9 a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Anhang 10

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 12./13. Oktober 2000

Vom Bürgerbüro zum Internet
– Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung –

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Anhang 11

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 12./13. Oktober 2000

Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen, zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.
4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur – wie bisher – Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

Anhang 12

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 12./13. Oktober 2000

Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes“ anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.