Datenschutz für unsere Bürger

2007

28. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

28. Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz
in Baden-Württemberg
2007

Herausgegeben
vom Landesbeauftragten für den Datenschutz
Peter Zimmermann
Urbanstraße 32 · 70182 Stuttgart
Telefon 07 11/61 55 41-0
http://www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfd.bwl.de
PGP Fingerprint: A5A5 6EC4 47B2 6287 E36C 5D5A 43B7 29B6 4411 E1E4
Veröffentlicht als Landtags-Drucksache Nr. 14/2050

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven
lediglich das bestimmende Geschlecht genannt. Selbstverständlich richtet sich
dieser Bericht an die Angehörigen beider Geschlechter.

Das Papier dieser Broschüre wurde
aus chlorfrei gebleichtem Zellstoff hergestellt.

INHALTSVERZEICHNIS

1. Teil: Zur Situation

Das Spannungsverhältnis von Freiheit und Sicherheit war auch im ablaufenden Berichtsjahr ein den Datenschutz beherrschendes Thema. Die Tendenz – einerlei ob auf Europa-, Bundes- oder Landesebene – bleibt unverkennbar: Insbesondere die Furcht vor dem Terrorismus animiert immer mehr dazu, staatliche Überwachungszuständigkeiten weit ins Vorfeld konkreter Gefahren zu verlagern. Dabei ist durchaus zuzugeben, dass für viele Bürger des Landes die Verheißung einer größtmöglichen Sicherheit eine attraktive Perspektive darstellt. Beunruhigend – und dies nicht nur aus der Sicht eines von Berufs wegen mit Datenschutz Befassten – ist es jedoch, wenn mit der Installierung immer weiter gehender Sicherheitsmaßnahmen die verfassungsrechtlich gebotene Balance zwischen möglicher Freiheit und notwendiger Sicherheit verloren zu gehen droht. Anzeichen hierfür gibt es genügend. Nicht zu Unrecht wird das Bundesverfassungsgericht schon vielfach als „Reparaturbetrieb der Legislative“ bezeichnet. Dabei ist es zunächst als völlig normal, ja geradezu als Beleg für einen gefestigten Rechtsstaat anzusehen, wenn das Bundesverfassungsgericht da und dort korrigierend in die Gesetzgebungsarbeit eingreift. Derzeit erfolgen solche Korrekturen jedoch in außergewöhnlich dichter Abfolge. Zu nennen sind hier die Entscheidungen zur akustischen Wohnraumüberwachung, zum Zollfahndungsgesetz, zur Rasterfahndung, zur präventiven Telekommunikationsüberwachung und zum Luftsicherheitsgesetz – und man muss kein großer Prophet sein, um vorauszusagen, dass demnächst auch dem nordrhein-westfälischen Landesverfassungsschutzgesetz zum Thema Online-Durchsuchung in Karlsruhe deutliche verfassungsrechtliche Korrekturen beschieden sein werden.

Begleitet werden diese ausgetragenen oder noch laufenden verfassungsrechtlichen Auseinandersetzungen von einer Fülle weiterer staatlicher Maßnahmen, die die Datenerfassung der Bürger immer engmaschiger werden lassen und vereinzelt wohl zu weiteren Befassungen des Bundesverfassungsgerichts führen dürften. Die Vorratsspeicherung von Telekommunikationsdaten, die Einführung einer Steuer-Identifikationsnummer, der Kontenabruf, eine breitere Anwendung der Videoüberwachung, die mögliche Ausweitung der Nutzung der Mautdaten und eine über das nordrhein-westfälische Landesverfassungsschutzgesetz hinausgehende Anwendung der Online-Durchsuchung auf Bundes- und Länderebene sind einige Beispiele, die den Trend einer stetig zunehmenden Sammlung und Kontrolle von Bürgerdaten belegen. Hinzu kommt die eigene Dynamik, die mit dem weiteren – an sich durchaus positiv zu wertenden – Zusammenwachsen der Mitgliedstaaten der Europäischen Union verbunden ist. Dass es notwendig ist, auch im Sicherheitsbereich zu einer besseren Zusammenarbeit der national zuständigen Behörden zu gelangen, steht außer Frage. Allerdings sollten auch hier die Aspekte des Datenschutzes eine frühzeitige und angemessene Berücksichtigung finden. Hiervon kann man nicht ohne weiteres überzeugt sein, wenn – wie kürzlich bekannt wurde – die EG-Kommission beabsichtigt, den Austausch von Flugpassagierdaten allgemein für Flüge aus der Europäischen Union und in die Europäische Union am Beispiel der mit den USA getroffenen Vereinbarung zu orientieren. Diese war – so erinnert man sich – auch in der Europäischen Union auf große datenschutzrechtliche Vorbehalte gestoßen. Jetzt scheinen diese Bedenken verflogen zu sein und man will das von den USA initiierte Flugpassagierabkommen praktisch eins zu eins insgesamt auf Europa übertragen, das heißt als Muster für Vereinbarungen der Europäischen Union mit anderen Staaten nutzen. Ein Fortschritt in Sachen Datenschutz sieht anders aus.

Wohl als Folge der geschilderten Gesamtentwicklung in Europa, im Bund und im Land werde ich immer häufiger gefragt, ob wir bei uns denn nicht schon von einem Überwachungsstaat reden müssten. Meine Haltung hierzu ist klar: Von einem Überwachungsstaat im heutigen Deutschland kann keine Rede sein, denn die rechtsstaatlichen Mechanismen, die vor allem unser Grundgesetz eingebaut hat, funktionieren durchaus. Die technische Infrastruktur für eine umfassende Überwachung der Bürger ist allerdings schon heute vorhanden und eine stetig fortschreitende Entwicklung zu einem noch dichter werdenden Erfassungsnetz ist unverkennbar. Dies gilt in wachsendem Maße – wenn man etwa an den Einsatz von Payback-Karten oder an die zunehmende Verbreitung der RFID-Technologie denkt – für den nicht-öffentlichen, aber eben auch und insbesondere für den staatlichen Bereich. Deshalb bereits heute

von einem Überwachungsstaat zu reden, halte ich gleichwohl für überzogen. Allerdings befinden wir uns offensichtlich in einer Phase, in der die Entscheidungen der Bürger über ihr eigenes Verhalten nicht mehr so frei getroffen werden, wie es sein sollte. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil von 1983 die Gefahren einer solchen Entwicklung eindrucksvoll beschrieben: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“ Der gefühlte Zwang oder auch nur die wachsende Unsicherheit kann zu vorauseilendem Gehorsam und letztlich in so etwas wie eine Anpassungsgesellschaft führen. Da und dort ist ein solches Anpassungsverhalten bereits zu spüren. Oder ist es wirklich „normal“, wenn Bürger Flüge in die USA – wenn sie denn die Wahl haben – deshalb meiden, weil sie nicht einschätzen können, was mit ihren anzugebenden Flugpassagierdaten geschieht? Und ist es nicht ein Zeichen von höchster Verunsicherung, wenn Bundesbürger die Ausstellung von Reisepässen teilweise nur deshalb zeitlich vorziehen, weil sie noch einen Reisepass der alten Generation erhalten wollen und nicht einen Reisepass mit von wem auch immer auslesbaren biometrischen Daten?

Für die Gesetzgebungsarbeit auf Landesebene hatte ich im vorangegangenen Tätigkeitsbericht prognostiziert, dass die Novelle zum Polizeigesetz eine Nagelprobe für die Frage sein werde, wie es das Land mit der Beachtung der bürgerlichen Freiheitsrechte hält. Diese Aussage gilt auch weiterhin. Ein ausformulierter Gesetzentwurf ist mir im Rahmen meiner nach § 31 Abs. 3 des Landesdatenschutzgesetzes (LDSG) vorgeschriebenen Beteiligung bislang noch nicht zugeleitet worden. In der Öffentlichkeit wurden mögliche Inhalte der Novelle allerdings bereits heftig diskutiert. Bewegte zunächst vor allem die Ausdehnung der polizeilichen Videoüberwachung die Gemüter, wurde im Laufe dieses Jahres die mögliche Einführung der Online-Durchsuchung zum beherrschenden Thema. Dem Vernehmen nach soll letztere keinen Eingang in den Gesetzentwurf finden – aufgrund der jedenfalls mir zugänglichen Erkenntnisse über die technischen Probleme der Online-Durchsuchung und der sehr diffizilen rechtlichen Fragestellungen dürfte dies kein Fehler sein. Die oben bereits angesprochene zu erwartende Entscheidung des Bundesverfassungsgerichts zum nordrhein-westfälischen Landesverfassungsschutzgesetz wird hier weitere Fingerzeige geben (vgl. zur Online-Durchsuchung auch die Entschließungen der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März und vom 25./26. Oktober 2007, Anhang 3 und 4). Wegen des Fehlens eines ausformulierten Gesetzentwurfs ist mir eine datenschutzrechtliche Bewertung der beabsichtigten Regelungen zur Änderung des Polizeigesetzes nicht möglich. Es besteht aus meiner Sicht für die Novellierungsarbeiten auch kein Grund zur Eile, denn die dem Gesetzgeber obliegende Pflichtaufgabe, die verfassungsgerichtlichen Vorgaben zur Rasterfahndung in das Polizeigesetz einzuarbeiten, ist deshalb nicht besonders dringlich, weil davon auszugehen ist, dass das Land diese Vorgaben in der Praxis auch im Vorgriff auf eine neue gesetzliche Regelung beachten wird. Ansonsten gilt, dass es sicher lohnen würde, sich die notwendige Zeit für eine sowohl die Sicherheitsbelange wie auch die Freiheitsrechte der Bürger angemessen berücksichtigende Regelung zu nehmen.

Zum Stichwort Videoüberwachung ist eine in der Öffentlichkeit weithin unbemerkt gebliebene, aber für die Praxis gleichwohl bedeutsame Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2007, 1 BvR 2368/06, zu erwähnen. In der Entscheidung ging es nicht um die polizeiliche Videoüberwachung, sondern um eine Videoüberwachungsmaßnahme durch die Stadt Regensburg. Die Stadt wollte ein Gelände, auf dem ein Bodenrelief über den Resten einer ehemaligen mittelalterlichen Synagoge errichtet worden war, per Video einschließlich Aufzeichnung überwachen. Sie wollte sich dabei auf die allgemeinen Datenerhebungsregelungen des bayerischen Landesdatenschutzgeset-

zes stützen. Das Bundesverfassungsgericht hat klargestellt, dass eine Videoüberwachung öffentlich zugänglicher Orte und Einrichtungen – jedenfalls mit Aufzeichnung des gewonnenen Bildmaterials – nicht auf allgemeine datenschutzgesetzliche Regelungen gestützt werden kann. Wegen des mit einer solchen Überwachung verbundenen erheblichen Eingriffs in das Recht auf informationelle Selbstbestimmung seien vielmehr spezielle gesetzliche Regelungen erforderlich, die Anlass, Zweck und Grenzen des Eingriffs präzise und normenklar festlegen. Wegen der Vergleichbarkeit der bayerischen und baden-württembergischen Gesetzeslage hat die Entscheidung auch Bedeutung für unser Land. Sie bedeutet, dass für alle von öffentlichen Stellen beabsichtigten Videoüberwachungen von allgemein zugänglichen Orten und Einrichtungen – jedenfalls soweit die Videoüberwachungen mit einer Aufzeichnung verbunden sind – eine spezielle gesetzliche Grundlage vorhanden sein muss, wie dies etwa für den Polizeibereich in § 21 PolG der Fall ist. Meine Beratungs- und Kontrollpraxis richtet sich an diesen vom Bundesverfassungsgericht formulierten Anforderungen aus.

Das bereits vor zwei Jahren an dieser Stelle angesprochene, von der EG-Kommission gegen die Bundesrepublik Deutschland eingeleitete Vertragsverletzungsverfahren in Sachen Unabhängigkeit datenschutzrechtlicher Kontrollstellen für den nicht-öffentlichen Bereich hat einen neuen Stand erreicht. Nachdem sich EG-Kommission und Bundesrepublik nicht auf eine gemeinsame Rechtsauffassung verständigen konnten, hat dem Vernehmen nach die EG-Kommission beim Europäischen Gerichtshof mittlerweile Klage gegen die Bundesrepublik eingereicht, um die Beachtung der EG-Datenschutzrichtlinie durchzusetzen. Ein Erfolg dieser Klage dürfte auch rechtliche Auswirkungen auf die Stellung der Landesbeauftragten für den Datenschutz als Kontrollstellen für den öffentlichen Bereich haben. Bemerkenswert jedenfalls ist, dass mit Rheinland-Pfalz ein weiteres Bundesland die öffentliche und die nicht-öffentliche Datenschutzaufsicht zusammenzulegen beabsichtigt, ohne die Entscheidung des Europäischen Gerichtshofs abzuwarten. Ein Beispiel, das zeigt, dass man auch bei uns im Land schon heute modernere und effizientere Strukturen im Datenschutz schaffen könnte – wenn man nur wollte.

2. Teil: Öffentliche Sicherheit und Justiz

1. Abschnitt: Öffentliche Sicherheit

1. Ein Härtetest für das Trennungsgebot – die Einführung der Antiterrordatei in Baden-Württemberg

1.1 Die Vorgeschichte

Kaum ein anderes sicherheitspolitisches Thema – mal abgesehen von der immer noch umkämpften Online-Durchsuchung – war in letzter Zeit so umstritten wie die Errichtung gemeinsamer Dateien von Polizeien und Nachrichtendiensten durch das entsprechende Artikelgesetz vom 22. Dezember 2006 (BGBl. I S. 3409), auf dessen Grundlage inzwischen beim Bundeskriminalamt u. a. eine zentrale Datei zur Aufklärung und Bekämpfung des internationalen Terrorismus eingerichtet wurde (Antiterrordatei/ATD). Bereits im Oktober 2006 hatten die Datenschutzbeauftragten des Bundes und der Länder – durchaus in Anerkennung der hohen Bedrohung durch den internationalen Terrorismus und der Notwendigkeit zur Optimierung des Informationsaustauschs zwischen den Sicherheitsbehörden – auf schwerwiegende verfassungs- und datenschutzrechtliche Risiken des Vorhabens hingewiesen; diese Probleme hatte ich auch in meinem letzten Tätigkeitsbericht angesprochen (vgl. 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650). Die nach wie vor bestehenden Bedenken richten sich insbesondere gegen den mangels Normenbestimmtheit kaum eingrenzbaren Kreis der Betroffenen (vgl. § 2 des Antiterrordateigesetzes/ATDG), die Verwendung von Freitextfeldern (vgl. § 3 Abs. 1 Nr. 1, Buchst. b, Unterbuchst. rr ATDG) und den sich abzeichnenden Zugriff von Polizeidienststellen auf die „weichen“ Vorfelderkenntnisse des Verfassungsschutzes. In Anbetracht der abweichenden Zielrichtungen von Nachrichtendiensten und Polizeien war außerdem die Frage spannend, wie vor allem die Verfassungsschutzbehörden mit der im Gesetz verankerten Pflicht zur Einspeicherung umgehen würden, konnten sie doch bisher eher nach Opportunitätsgesichtspunkten entscheiden, welche Personen sie unter Beobachtung nehmen. Zwar wurden nach einer Expertenanhörung im Innenausschuss des Deutschen Bundestags im Laufe des Gesetzgebungsverfahrens noch einige Details nachgebessert, insbesondere die Definition der einzuspeichernden „Kontaktpersonen“ präzisiert, an der Gesamtkonzeption änderte sich aber nichts mehr.

Inzwischen ist die Antiterrordatei durch den Bundesinnenminister Ende März 2007 feierlich in Betrieb genommen worden. Angeschlossen waren zu diesem Zeitpunkt bundesweit 38 Sicherheitsbehörden von Bund und Ländern, darunter das Landesamt für Verfassungsschutz und das Landeskriminalamt mit der Abteilung Staatsschutz; beabsichtigt ist, noch einige Staatsschutzdienststellen bei ausgewählten Polizeidirektionen im Land anzuschließen. Die angeschlossenen Dienststellen sind jetzt in der Lage, in der Datei online sog. Grunddaten einer Person einzusehen (Familienname, Vornamen, frühere Namen, Aliaspersonalien, Geschlecht, Geburtsdatum und -ort, aktuelle und frühere Staatsangehörigkeiten, Lichtbilder). Daneben können auf Nachfrage – oder im Eilfall durch die anfragende Behörde selbst – sog. erweiterte Grunddaten zur Einsicht freigeschaltet werden; hierzu zählen Telekommunikationsanschlüsse, E-Mail-Adressen, Bankverbindungen, genutzte Fahrzeuge, Familienstand, Angaben zur Gefährlichkeit (z. B. Waffenbesitzer, Sprengstoffexperte usw.), Fahr- und Flugerlaubnisse sowie – sofern im Einzelfall erforderlich – Angaben zur Religionszugehörigkeit.

Im Unterschied zu den sonst üblichen Dateien bei Verfassungsschutz und Polizei ist bei der Antiterrordatei zu beachten, dass die teilnehmenden Behörden nach § 2 Abs. 1 ATDG nicht nur berechtigt, sondern sogar verpflichtet waren, Personen der im Gesetz näher genannten Kategorien einzuspeichern, sofern deren Daten bereits auf der für sie jeweils geltenden gesetzlichen Grundlage zulässigerweise gespeichert worden waren. Bei den angeschlossenen Dienststellen mussten also be-

reits Ausgangsdateien vorhanden sein, aus denen heraus dann personenbezogene Daten an die neu aufgebaute Antiterrordatei beim Bundeskriminalamt zu exportieren waren. Ausgangsdateien in diesem Sinn waren insbesondere bei den Verfassungsschutzbehörden das Nachrichtendienstliche Informationssystem (NADIS) und bei den Polizeien u. a. die Datei INPOL-Fall „Innere Sicherheit“ (IFIS).

Was den in der Antiterrordatei auf diese Weise zu erfassenden Personenkreis angeht, so ist Folgendes zu sagen: Da sich § 2 ATDG, in dem die Kategorien der einzuspeichernden Personen genannt sind, im Vorfeld der Abwehr konkreter Gefahren bzw. der Verfolgung bereits begangener Straftaten bewegt, sind die gesetzlichen Bestimmungen, welche Personen einzuspeichern sind, ausgesprochen unscharf; sie beziehen nämlich – zumindest nach dem Gesetzeswortlaut – auch solche Personen mit ein, die nur mittelbar einen Bezug zu terroristischen Bestrebungen oder Terrorverdächtigen haben. Dies betrifft weniger die Personen, die selbst einer in- oder ausländischen terroristischen Vereinigung nach § 129 a und § 129 b des Strafgesetzbuchs (StGB) angehören oder eine solche unterstützen (Fallgruppen 1 und 2; § 2 Satz 1 Nr. 1 a ATDG); diese Personen hätten sich nach den genannten Vorschriften ohnehin bereits strafbar gemacht und stünden vermutlich auf den Fahndungslisten. Aber in die Antiterrordatei müssen auch Daten von Personen eingestellt werden, die einer Gruppierung angehören oder eine solche unterstützen, die ihrerseits wiederum eine der vorgenannten terroristischen Vereinigungen unterstützt (§ 2 Satz 1 Nr. 1 b ATDG); bei dieser dritten Kategorie reicht demnach bereits eine Unterstützung „um zwei Ecken“ aus. Vollends vage wird der Bezug zum Terrorismus in der vierten Fallgruppe nach § 2 Satz 1 Nr. 2 ATDG, weil die Einspeicherung hier schon dann vorzunehmen ist, wenn eine Person „rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange“ anwendet oder eine solche Gewaltanwendung „unterstützt, vorbereitet, befürwortet oder durch ihre Tätigkeit vorsätzlich hervorruft“. Weder bezieht sich der verwendete Gewaltbegriff auf den Terrorismus noch ergibt sich aus dem Gesetz (und auch nicht aus der Gesetzesbegründung), wo die Grenze zwischen dem verwerflichen „Befürworten“ und einer grundrechtlich unter Umständen geschützten Meinungsäußerung verlaufen soll. Die Befürwortung militärischer „Befreiungskriege“ im Heimatland eines Betroffenen könnte demnach gegebenenfalls zur Aufnahme in die Antiterrordatei ausreichen.

Auch die Kategorie der sog. Kontaktpersonen (§ 2 Abs. 1 Satz 1 Nr. 3 ATDG) kann nach dem Gesetzeswortlaut leicht ausufern und ist deshalb verfassungsrechtlich nicht unproblematisch. Danach sind Personen einzuspeichern, bei denen lediglich tatsächliche Anhaltspunkte für einen nicht nur flüchtigen oder zufälligen Kontakt zu einer „Hauptperson“ (im Sinne der zuvor genannten Fallgruppen) vorliegen; auf die Kenntnis der Kontaktperson über den – möglicherweise nur auf vagen Indizien beruhenden – Verdacht eines speicherungsrelevanten Hintergrunds der Hauptperson soll es zumindest hinsichtlich der Grunddaten nicht ankommen. Damit wäre es nach dem Gesetzeswortlaut sogar geboten, die Grunddaten nachweislich argloser Kontaktpersonen einzuspeichern; für eingeweihte („dolose“) Kontaktpersonen müssten hingegen erweiterte Grunddaten eingestellt werden. Die Möglichkeit, Personen in die Antiterrordatei aufzunehmen, wird zudem dadurch erweitert, dass die beteiligten Behörden zur Einspeicherung bereits erhobener Daten verpflichtet sind, wenn sie über polizeiliche oder nachrichtendienstliche Erkenntnisse verfügen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass die Daten sich auf Personen aus einer der vorgenannten vier Fallgruppen beziehen. Da nicht entscheidend ist, in welchem Zusammenhang die besagten Erkenntnisse gewonnen wurden, könnten auf diese Weise sogar Personen als Kontaktpersonen erfasst werden, die gemeinsam mit einem Verdächtigen auf der Teilnehmerliste einer Veranstaltung aufgeführt sind. Zwar gilt für alle Fallgruppen generell die weitere Voraussetzung, dass die Kenntnis der Daten für die Aufklärung des internationalen Terrorismus mit Bezug zur Bundesrepu-

blik Deutschland erforderlich sein muss (§ 2 Satz 1, Halbsatz 2 ATDG); diese Voraussetzung ist angesichts des Zwecks der Datei aber ohnehin selbstverständlich und trägt insgesamt nicht zu einer klareren Eingrenzung des betroffenen Personenkreises bei.

Da wir wissen wollten, wie sich die politisch zunächst heftig umstrittene Datei im Alltag bewährt, haben meine Mitarbeiter in mehrtägigen Kontrollbesuchen beim Landeskriminalamt (Abteilung Staatsschutz) und beim Landesamt für Verfassungsschutz im Sommer 2007 die technischen Rahmenbedingungen vor Ort und vor allem die durch beide Behörden veranlassten Datenspeicherungen in der Antiterrordatei näher unter die Lupe genommen. Dabei waren wir insbesondere gespannt zu erfahren, welche Kriterien im Einzelnen für die Einspeicherung maßgeblich waren. Wer jetzt aufsehenerregende Einzelheiten von der vordersten Front der Terroristenjäger im Land zu erfahren hofft, den müssen wir leider enttäuschen, denn das Landeskriminalamt wies uns in seiner Stellungnahme zu unserem Kontrollbericht darauf hin, dass die in der Antiterrordatei gespeicherten Daten „in ihrer Gesamtheit“ als geheim zu haltende Verschlusssache (VS-geheim) eingestuft seien; dies beziehe sich nach bundesweiter Absprache auch auf statistische Daten wie die Anzahl eingespeicherter Personendaten oder auch auf die Aufschlüsselung von gespeicherten Personen nach den im Antiterrordateigesetz (§ 2) genannten Fallgruppen. Da auch die uns übergebenen Unterlagen zu den technischen Besonderheiten der Datei und zu organisatorischen Aspekten der Zusammenarbeit als Verschlusssachen eingestuft waren, müssen wir uns an dieser Stelle auf einige allgemeine Hinweise beschränken. Die Geheimhaltung rund um die Antiterrordatei ist allerdings nur teilweise nachvollziehbar, hat doch der Bundesinnenminister selbst anlässlich der Inbetriebnahme der Antiterrordatei am 30. März 2007 in seiner Pressemitteilung interessante Details preisgegeben: Dort war zu lesen, dass in die Antiterrordatei mit Betriebsbeginn 15 000 Datensätze eingestellt waren; weil aber zahlreiche Personen durch jeweils unterschiedliche Behörden gespeichert worden seien, liege die Zahl der gespeicherten Personen bei rd. 13 000. In einem ersten Schritt seien Grunddaten aus dem Bereich des islamistischen Terrorismus vollständig eingegeben worden, in einem nächsten Schritt würden hierzu die erweiterten Grunddaten folgen. In Bezug auf die genannte Zahl der gespeicherten Personen und den zunächst einzuspeichernden Personenkreis sei außerdem zu beachten, dass der ganz überwiegende Teil nicht in Deutschland lebe, sondern radikalen islamistischen Organisationen im Ausland angehöre, die wiederum Verbindungen zu Deutschland haben. Die Zahl der in Deutschland lebenden gespeicherten Personen mache daher weniger als ein Viertel der Gesamtmenge aus. Nur ein kleiner Teil dieser Personen werde akut als Gefährder im polizeilichen Sinn eingestuft. Die Antiterrordatei habe aber den Zweck, über diese Personen hinaus auch das gewaltgeneigte extremistische Umfeld zu erfassen, um in der Zukunft weitere Gefährder und mögliche neue Netzwerkstrukturen möglichst schnell und frühzeitig zu erkennen.

1.2 Was die Kontrollbesuche ergaben

Um das Ergebnis unserer Kontrollbesuche vorwegzunehmen: Skandalöse Zustände haben wir nicht angetroffen. Die technischen und organisatorischen Vorkehrungen zum Schutz der in die Datei eingespeicherten personenbezogenen Daten sind sowohl beim Landesamt für Verfassungsschutz als auch beim Landeskriminalamt hochwertig. Die technische Einrichtung der Antiterrordatei beim Bundeskriminalamt und deren Vernetzung insbesondere im Polizeibereich war aber – wie der Bundesinnenminister in der genannten Pressemitteilung erklärte – ein gewaltiger Kraftakt. Eine der größten Herausforderungen sei dabei der Aufbau eines sog. Verschlusssachen-Netzes gewesen, das es ermöglicht, auch bis zum Geheimhaltungsgrad „VS-geheim“ eingestufte Daten in der Antiterrordatei sicher zu verarbeiten; der Verfassungsschutz verfügte bundesweit bereits über ein solches Netz. Es war bei unseren Gesprächen in den beiden Dienststellen deutlich erkennbar,

dass der Aufbau der Antiterrordatei von Beginn an unter einem hohen Zeitdruck und unter engen inhaltlichen Vorgaben erfolgte und der Termin der Inbetriebnahme nur durch ein straffes Projektmanagement des Bundeskriminalamts gehalten werden konnte. Das Bundeskriminalamt hatte auch das Datenbankgerüst vorgegeben, woraus sich einige Unzulänglichkeiten in der praktischen Anwendung erklärten, die hier nicht weiter ausgebreitet werden können; wie wir erfuhren, werde über den Umstieg auf eine andere technische Plattform nachgedacht. Unter dem Zeitdruck scheint – um es vorsichtig unter Beachtung der erbetenen Geheimhaltung anzudeuten – insbesondere beim Landeskriminalamt gelegentlich die Qualität bei der Auswahl der einzuspeichernden Personen gelitten zu haben. In einigen Fällen schien uns die Zuordnung der eingespeicherten Personen zu einer der im Antiterrordateigesetz genannten Kategorien zu schematisch bzw. zu großzügig erfolgt zu sein. In seiner Stellungnahme zu unserem Prüfungsbericht hat das Landeskriminalamt denn auch eingeräumt, dass die rechtlichen Voraussetzungen für die Einspeicherung aufgrund des hohen Zeitdrucks in einigen Fällen zu weit ausgelegt worden sein könnten. Wir haben deshalb an beide Behörden appelliert, bei allen weiteren Schritten zur Befüllung der Antiterrordatei, namentlich bei der Eingabe der erweiterten Grunddaten für den im ersten Anlauf ausgewählten Personenkreis, auf eine (erneute) sorgfältige Prüfung der gesetzlichen Voraussetzungen zu achten. Da bereits die Eingabe der Grunddaten der Betroffenen einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, kann die gebotene inhaltliche Überprüfung der gesetzlichen Voraussetzungen eigentlich nicht auf diese spätere Phase verschoben werden. Da der Meldetermin für die zweite Stufe aber vor der Tür stand, hielten wir es für vertretbar, die gebotene Überprüfung mit der Eingabe der erweiterten Grunddaten zu verbinden. Uns wurde zugesichert, die erforderliche inhaltliche Überprüfung bei jedem weiteren Bearbeitungsschritt sorgfältig vorzunehmen und dabei auch die von uns festgestellten Kritikpunkte zu beachten.

Was die Zahl der von beiden Behörden eingespeicherten Hauptpersonen und Kontaktpersonen angeht, dürfen wir – wie gesagt – keine Auskunft geben. Wir haben bei beiden Dienststellen jeweils ca. zehn Prozent der eingespeicherten Datensätze (sowohl Haupt- als auch Kontaktpersonen) anhand der vorhandenen Unterlagen überprüft. Dabei haben wir festgestellt – was auch der Pressemitteilung des Bundesinnenministers zu entnehmen und im Grunde zu erwarten war –, dass etliche Personen in der Antiterrordatei von beiden Behörden (und vermutlich auch von weiteren teilnehmenden Stellen auf Bundesebene oder in anderen Bundesländern) eingegeben worden waren. Hierzu wurde uns erklärt, dass das Bundeskriminalamt sich in nächster Zeit um die erforderliche Konsolidierung der Daten bemühen wolle.

Inhaltlich hat unsere Prüfung ergeben, dass die gesetzlichen Voraussetzungen bei einigen Personen nicht vorlagen bzw. aus den vorhandenen Unterlagen nicht zweifelsfrei hervorgingen. Bei einem als „Hauptperson“ eingespeicherten Betroffenen war beispielsweise einem in den Akten befindlichen Strafurteil zu entnehmen, dass er selbst nach Meinung des polizeilichen Sachbearbeiters „keineswegs in irgendwelchen islamistischen Hintergrund verstrickt“ war; das Gericht schloss sich dieser Auffassung an. Auch einem anderen Vermerk in derselben Akte war zu entnehmen, dass nach Meinung der Polizei „ein staatsschutzrelevanter, namentlich islamistischer Hintergrund nicht erkennbar“ war. Wie der Mann dennoch in die Antiterrordatei geraten konnte, ist kaum nachvollziehbar. Den einzigen Kontakt zu einer mutmaßlich islamistischen Person hatte der im Strafprozess Mitangeklagte. Das Landeskriminalamt hat den Betroffenen inzwischen in der Antiterrordatei gelöscht.

Bei zwei weiteren „Hauptpersonen“ war im Zusammenhang mit einer bestimmten Straftat ein früheres Ermittlungsverfahren wegen des Verdachts der Mitgliedschaft in einer terroristischen Vereinigung vor einigen Jahren eingestellt worden; ein politisch motivierter Hintergrund wurde ausweislich der Akten danach in Frage gestellt. Nachdem wir das

Landeskriminalamt um Überprüfung gebeten hatten, wurde einer der beiden zur Kontaktperson „abgestuft“, der andere gelöscht.

Bei der Prüfung der vom Landeskriminalamt eingespeicherten „Kontaktpersonen“ trafen wir auf das Problem, dass zu diesem Personenkreis keine gesonderten Akten geführt wurden, sondern die Daten zunächst umständlich in der Akte einer dazu gehörigen „Hauptperson“ gesucht werden mussten, wobei erschwerend hinzukam, dass die jeweiligen „Kontaktpersonen“ nicht immer auf dem für die „Hauptperson“ angelegten Datenblatt (sog. Personagramm) mit Fundstelle verzeichnet waren, obwohl es dort extra eine Rubrik für „Kontaktpersonen“ gab. Häufig fanden wir dann Angaben zu einer mutmaßlichen „Kontaktperson“ versteckt auf Antreffensmeldungen, die in der Akte der „Hauptperson“ enthalten waren. Solche Meldungen fallen bekanntlich an, wenn eine Zielperson z. B. nach § 25 des Polizeigesetzes (PolG) zur polizeilichen Beobachtung ausgeschrieben und im Rahmen einer Routinekontrolle im Straßenverkehr oder beim Grenzübertritt etwa zur Schweiz festgestellt wird. Die kontrollierende Polizeidienststelle meldet dann an die ausschreibende Dienststelle, wann, wo und in wessen Begleitung sie die jeweilige Zielperson angetroffen hat. Dementsprechend waren in den Akten einer als Islamist in der Antiterrordatei eingespeicherten Hauptperson auch Meldungen über Fahrzeuginsassen enthalten, die im Fahrzeug der Hauptperson bei einer Kontrolle angetroffen worden waren und die vom Landeskriminalamt deshalb als Kontaktpersonen angesehen und ebenfalls eingespeichert wurden. Dabei fiel in einigen Fällen auf, dass den Akten keine weiteren Belege für den Inhalt und die Intensität der Beziehung zwischen Haupt- und Kontaktperson zu entnehmen waren. Bereits der Umstand, dass beide in demselben Fahrzeug unterwegs waren, hatte demnach für die Einspeicherung als Kontaktperson ausgereicht. Aus unserer Sicht ist das zu wenig. Wir haben dem Landeskriminalamt mitgeteilt, dass eine sorgfältigere Prüfung der gesetzlichen Voraussetzungen gerade bei Kontaktpersonen dringend geboten sei. Das Landeskriminalamt hat eingeräumt, dass es in einzelnen Fällen schwierig sei, die Intensität der bestehenden Kontakte zu bewerten; gerade im Bereich des Terrorismus seien die Übergänge zwischen normalen sozialen Kontakten und einvernehmlichem Zusammenwirken fließend. Aufgrund unserer Prüfungsbemerkungen hat das Landeskriminalamt inzwischen drei Kontaktpersonen gelöscht und zu den übrigen überprüften Datenspeicherungen weitere Erläuterungen gegeben, die die Aufnahme in die Antiterrordatei – vor allem in Anbetracht der großzügigen gesetzlichen Voraussetzungen hierfür – als vertretbar erscheinen lassen. Das Landeskriminalamt hat auch zugesagt, die Aktenführung zu verbessern.

Die stichprobenartige Überprüfung der vom Landesamt für Verfassungsschutz in die Antiterrordatei eingespeicherten Datensätze ergab keine Mängel; die Einspeicherungen waren jeweils fachlich nachvollziehbar und inhaltlich gründlich dokumentiert.

Praktische Erfahrungen der beiden Behörden mit Dateizugriffen anderer Dienststellen bestanden zum Zeitpunkt der Überprüfung kaum. Als ausgesprochen ärgerlich ist aus unserer Sicht in diesem Zusammenhang der Umstand zu werten, dass eine Überprüfung der Datenabrufe aus der Antiterrordatei anhand der Protokolldaten lediglich beim Bundeskriminalamt erfolgen kann (§ 9 ATDG). Wir werden daher, wenn die Antiterrordatei im Wirkbetrieb einige Zeit läuft, in Abstimmung mit dem Bundesdatenschutzbeauftragten die Möglichkeiten zur Überprüfung der Protokolldaten aus Baden-Württemberg ausloten.

1.3 Wie geht es weiter?

In Anbetracht der geschilderten Einführungssituation konnte unser Kontrollbesuch nur eine Momentaufnahme liefern. Die Antiterrordatei ist auch derzeit noch im Aufbau begriffen. Manche Schwachpunkte, auch hinsichtlich der Datenqualität, werden im Zuge des praktischen Umgangs und mit zunehmender Erfahrung voraussichtlich abgestellt werden. Die Antiterrordatei wird daher uns und die an ihr beteiligten

Dienststellen in den nächsten Jahren weiter beschäftigen. Weitere Kontrollen der Speicher- und Abfragepraxis haben wir uns deshalb ausdrücklich vorbehalten.

Nach dem politischen Schlachtenlärm, der rund um die Einführung der Antiterrordatei geherrscht hat, ist der Betrieb dieser Datei mittlerweile in ein etwas ruhigeres Fahrwasser geraten. Inwieweit die hohen Erwartungen, die mit der Einführung der Datei verbunden waren, erfüllt werden (können), muss die Zukunft zeigen. Insgesamt haben wir den Eindruck gewonnen, dass infolge des bestehenden Informationsverbunds unter den Verfassungsschutzbehörden von Bund und Ländern (Stichwort: NADIS) der Zusatznutzen durch die Antiterrordatei beim Landesamt für Verfassungsschutz eher gering ist. Dies ist in Anbetracht des Umstands, dass die eingespeicherten Daten zuvor schon vorhanden sein mussten, auch nachvollziehbar. Jedenfalls wird diese Datei eine gründliche Analyse jeder einzelnen Zielperson nicht ersetzen können. Ohne eine vertiefte Bewertung der persönlichen und ideologischen Hintergründe und Motive der einzuspeichernden Personen wird die Antiterrordatei allenfalls ein formales Hilfsmittel bleiben, um einen Informationsaustausch zwischen den Sicherheitsbehörden anzuregen.

Inzwischen ist eine Verfassungsbeschwerde gegen das Antiterrordateigesetz anhängig; der Beschwerdeführer ist übrigens derselbe, der bereits vor einigen Jahren die präventive Telekommunikationsüberwachung im niedersächsischen Polizeigesetz durch eine Verfassungsbeschwerde zu Fall gebracht hat. Die Landesbeauftragten für den Datenschutz haben in einer gemeinsamen Stellungnahme noch einmal auf die verfassungsrechtlichen Kritikpunkte, insbesondere auf den zu weit gezogenen Personenkreis in § 2 ATDG und die Lockerung des Trennungsgebots, hingewiesen. Es wird sich daher in absehbarer Zeit auf dem Prüfstand des Bundesverfassungsgerichts zeigen, ob die Antiterrordatei in der bisherigen Form eine Zukunft hat.

2. Der Staatsschutz und die Demokratie – Neues von der Arbeitsdatei „Politisch motivierte Kriminalität“ (AD PMK)

2.1 Die Vorgeschichte

Die Arbeitsdatei „Politisch motivierte Kriminalität“ (AD PMK) ist seit dem Jahr 2003 für alle polizeilichen Staatsschutzdienststellen im Land online verfügbar und soll – wie der Name schon sagt – der Bekämpfung der politisch motivierten Kriminalität dienen. Bereits im Jahr 2005 hatten wir grundsätzliche datenschutzrechtliche Mängel festgestellt: Teilweise gab es für die Speicherungen keinen ausreichenden Aktenrückhalt, teilweise keinen Beleg für eine politische Motivation, teilweise erfolgten sie zu lange, außerdem in der Mehrzahl in einer Kategorie („andere Personen“), die in der Errichtungsanordnung für diese Datei gar nicht vorgesehen war und die wohl als Auffangtatbestand für die Speicherung von anderweitig nicht zuzuordnenden Betroffenen gewählt worden war (vgl. 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910). Die geplanten Abhilfemaßnahmen haben wir in unserem 27. Tätigkeitsbericht für das Jahr 2006 (LT-Drucksache 14/650) geschildert. Dazu zählte vor allem eine Anleitung des Landeskriminalamts („Orientierungshilfen“), mit deren Hilfe die Staatsschutzdienststellen insbesondere die Speicherung der „anderen Personen“ kritisch überprüfen und diese gegebenenfalls den Fallgruppen „potenzieller Straftäter“ (§ 20 Abs. 3 Nr. 1 PolG) und „Kontakt- und Begleitpersonen“ (§ 20 Abs. 3 Nr. 2 PolG) zuordnen sollten. Immerhin wurde im Zuge dieser Überprüfung die Zahl der Datenspeicherungen nicht unerheblich verringert: Die AD PMK wies mit Stand vom 26. November 2007 insgesamt noch knapp 29 000 (von ursprünglich ca. 40 500) Personen auf; davon waren nur noch 338 als „andere Personen“ gespeichert (ursprünglich ca. 24 000). Zumindest in dieser Hinsicht sei die Überprüfung der AD PMK abgeschlossen, erklärte das Landeskriminalamt.

Außer der Zuordnung einzelner Personen zu bestimmten Fallgruppen war vor allem umstritten, welche Arten von Informationen zu den jeweiligen Personen erhoben und in der AD PMK gespeichert werden dürfen. Aus meiner Sicht müssen die gesetzlichen Anforderungen für jedes personenbezogene Datum, das gespeichert werden soll, gesondert vorliegen; zwar politisch motivierte, jedoch für sich betrachtet strafrechtlich nicht relevante Handlungen haben daher in der AD PMK – in der es ja um „Kriminalität" gehen soll – in der Regel nichts zu suchen, schon gar nicht die zulässige Wahrnehmung von Grundrechten, wie z. B. die Teilnahme an nicht verbotenen (politischen) Versammlungen, die Verteilung von Flugblättern, das Betreiben von Informationsständen, das Abhalten von Mahnwachen usw. Dies gilt auch, wenn die betreffende Person wegen anderer, politisch motivierter und strafrechtlich relevanter Vorkommnisse dort zulässigerweise gespeichert sein mag. In der Stellungnahme zu meinem letzten Bericht (LT-Drucksache 14/1269) hat die Landesregierung darauf eher ausweichend reagiert; im Kern hielt sie es nämlich weiterhin nicht für schlechthin unzulässig, dass – sofern eine Person aufgrund tatsächlicher Anhaltspunkte zutreffend als potenzieller Straftäter anzusehen sei – auch die sonstigen Informationen über dieselbe Person gespeichert werden dürfen. Maßstab sei (allein) die Erforderlichkeit des Datums zur vorbeugenden Bekämpfung von Straftaten. Diese Auslegung wurde u. a. mit der Notwendigkeit gerechtfertigt, angesichts der Terrorgefahr durch islamistische Attentäter müssten bereits unscheinbare, für sich betrachtet strafrechtlich nicht relevante Indizien für typische Verhaltensmuster dieses Personenkreises zusammengetragen und ausgewertet werden dürfen. Mögen diese Argumente bei Terrorverdächtigen noch nachvollziehbar sein, so zeigen die nachstehend genannten Beispiele, was eine derart autorisierte Speicherpraxis für seltsame Blüten treiben kann. Sie sollen zugleich illustrieren, mit welcher Akribie der Staatsschutz auch nebensächliche Details erfasst – ungeachtet der hohen Arbeitsbelastung des Polizeivollzugsdienstes im Übrigen.

2.2 Von Tierversuchsgegnern und Umweltschützern – Was den Staatsschutz interessierte

Um die Speicherpraxis des polizeilichen Staatsschutzes in den beiden folgenden Fällen zu begreifen, muss man sich vor Augen halten, dass es aus Sicht der Landesregierung zulässig sein soll, auch Informationen über „legale" Verhaltensweisen in der AD PMK hinzuzuspeichern. Ich stelle nicht in Abrede, dass die beiden jungen Frauen, um die es in den folgenden Beispielen geht, zunächst strafrechtlich relevant aufgefallen sind. Insoweit ist gegen die Datenspeicherungen auch nichts zu sagen, wenngleich die Zuordnung zu einer Kategorie der „politisch motivierten Kriminalität" mitunter diskussionswürdig erschien. Nicht erwartet hatte ich jedoch, in der AD PMK auf zahlreiche Vorgänge aus dem „demokratischen Alltag" der Bevölkerung zu stoßen.

Fall 1:

Eine junge Frau aus der Nähe von Karlsruhe, nennen wir sie A, engagierte sich vor allem – die Grenzen des geltenden Rechts gelegentlich überschreitend – gegen Tierversuche. Sie wird in der AD PMK und in anderen Dateien des Landeskriminalamts als „potenzielle Straftäterin" geführt. Außerdem ist A in den polizeilichen Verbunddateien INPOL-Z und INPOL-Fall „Innere Sicherheit" (IFIS) von der Polizei des Landes Nordrhein-Westfalen als „Straftäterin, linksmotiviert" im Zusammenhang mit einem strafrechtlichen Ermittlungsverfahren wegen Nötigung und Hausfriedensbruchs bei einer Demonstration gegen Tierversuche in Münster im Jahr 2004 erfasst worden. Datensätze hierüber und über weitere Vorkommnisse wurden in der AD PMK unterschiedlichen Kategorien („links" und „Sonstige") zugeordnet. Während einige Datenspeicherungen in der AD PMK zulässig bis vertretbar erschienen, weil daraus mögliche Straftaten oder zumindest Ordnungsverstöße hervorgingen, ließ sich das für rd. zwölf Datenspeicherungen nicht behaupten; sie werden hier in der Diktion des Landeskriminalamts bzw. der AD PMK auszugsweise wiedergegeben:

– Am ... (im Januar 2004) findet eine von der ... (Name einer Tierschutzorganisation), vertreten durch A, bei ... angemeldete Kundgebung statt, bei der „4 Teilnehmer mit Trillerpfeifen ihren Unmut gegen Tierversuche ausdrücken“. (Hinweis: In der AD PMK wird ausdrücklich festgehalten, dass es zu keinen Störungen kam.)

– An einem anderen Tag im Januar 2004 findet eine ordnungsgemäß von A angemeldete Demonstration derselben Organisation vor dem Gebäude einer Pharmafirma in ... statt. Laut AD PMK haben dabei „5 Teilnehmer Flugblätter verteilt und themenbezogene Transparente gezeigt“. (Hinweis: Auch hier wurden keine Störungen gemeldet.)

– A wird zusammen mit einem Verein in der AD PMK jeweils als Anmelder einer „Protestkundgebung und Infostand für Informationsfreiheit, Datenschutz, Meinungsfreiheit usw.“ in ... für zwei Termine im April 2004 erfasst. (Hinweis: Aus dieser und einigen anderen Formulierungen ist zu schließen, dass in der AD PMK vielfach aus der Anmeldung bei der Versammlungsbehörde zitiert wird.)

– Im Mai 2004 wird über einen von A betriebenen Infostand in derselben Stadt berichtet. Diesmal lautet nach dem Eintrag in der AD PMK das Motto: „Informationsfreiheit, Meinungsfreiheit, Datenschutz, das Recht auf Privatsphäre und informationelle Selbstbestimmung“.

– Bereits für den nächsten Tag hat A bei der Versammlungsbehörde in ... „eine Kundgebung/einen Infostand“ angemeldet. Das Thema lautet „Tierschutz, Tierrechte“. Erwartet werden „5 bis 8 Teilnehmer“.

– Im Juli 2004 meldet A eine öffentliche Versammlung in ... zum Thema „Ethik und Tierrechte“ an.

– Im Februar 2005 meldet die bereits erwähnte Tierschutzorganisation, vertreten durch A, in ... eine öffentliche Versammlung mit 5 bis 8 erwarteten Teilnehmern an, bei der Passanten über das Thema Tierrecht „mit Schwerpunkt Pelzhandel“ informiert werden sollen.

Weitere Datenspeicherungen betrafen andere Infostände und Versammlungen zu vergleichbaren Themen, vereinzelt war auch die Anmeldung einer Versammlung erfasst worden, ohne dass das Thema dem Datensatz zu entnehmen war. Wie die Informationen über diese Veranstaltungen in diesem und in vergleichbaren Fällen an die jeweiligen Polizeidienststellen gelangt sind, wird noch gesondert zu untersuchen sein.

Fall 2:

Eine andere junge Frau – nennen wir sie B – ist in ihrer Heimatstadt engagierte Aktivistin einer weltweit agierenden Umweltschutzorganisation, deren Akteure bei ihren öffentlichkeitswirksamen Aktionen Gesetzesverstöße mitunter in Kauf zu nehmen pflegen. Über sie speichert die Polizei in ihren polizeilichen Informationssystemen (u. a. in der Verbunddatei INPOL-Fall „Innere Sicherheit“ [IFIS]) Informationen über ein strafrechtliches Ermittlungsverfahren wegen Nötigung im Jahre 2002, das zu einer Verurteilung von B zu einer geringen Geldstrafe auf ein Jahr Bewährung führte. Zugrunde lag eine Blockadeaktion mehrerer Aktivisten der Umweltschutzorganisation vor der Einfahrt einer großen Automobilfirma, bei der sich die Akteure, darunter B, an mitgebrachte Krankenhausbetten anketteten und auf Transparenten auf das mögliche Krebsrisiko durch Dieselruß hinwiesen. Die zuständige Polizeidienststelle hatte den Vorfall auch in der AD PMK erfasst. Gegen diese Datenspeicherung bestehen aus meiner Sicht – zumindest außerhalb der AD PMK – keine grundsätzlichen datenschutzrechtlichen Bedenken. Dies gilt auch hinsichtlich anderer Vorfälle, die über B im Rahmen des bundesweiten Kriminalpolizeilichen Meldedienstes Staatsschutz von anderen Bundesländern gemeldet wurden; dabei ging es um mögliche Straftaten der jungen Frau bei Protestaktionen wegen Sachbeschädigung, Nötigung und/oder Hausfriedensbruch usw. Teilweise waren die Verfahrensausgänge aber noch zu klären.

Daneben hatten Polizeidienststellen des Landes in der AD PMK Informationen über rd. 15 weitere „Vorkommnisse“ gespeichert, die – wie im ers-

ten Fall – keine erkennbare strafrechtliche Relevanz aufwiesen: In seiner Index-Datei (Aktenverwaltungssystem) hat das Landeskriminalamt z. B. vermerkt, dass B im Oktober 2006 eine Kundgebung mit Infostand in ihrer Heimatstadt angemeldet hatte, durch die auf „das fortschreitende Verschwinden der Fische aus dem Meer“ aufmerksam gemacht werden sollte. Weitere typische Beispiele werden hier auszugsweise in der Diktion des Landeskriminalamts bzw. der AD PMK wiedergegeben:

- Im August 2002 ist ... (B) Versammlungsleiterin bei einer Aktion der ... (Name der Umweltschutzorganisation) vor der ... – Tankstelle in ... zum Thema „Globale Klimaerwärmung“.
- Im Januar 2004 fand vor der Zufahrt des ... (Name eines Kernkraftwerks in Baden-Württemberg) eine Demonstration von einer Gruppe von Aktivisten der ... (Name der Umweltschutzorganisation) statt. Die Demonstration richtete sich gegen einen Excellox-Transport aus dem Kernkraftwerk in das Wiederaufbereitungslager Sellafield. B war Teilnehmerin.
- Im Mai 2004 fand in ... (der Heimatstadt von B) eine Spontan-Demo mit Aktivisten der ... (Name der Umweltschutzorganisation) zum Thema „Urwaldzerstörung“ statt. Es wurden Flugblätter an Passanten verteilt und ein Plakat mit der Aufschrift „Recycling statt Kahlschlag“ aufgehängt. B wird als Veranstalterin verzeichnet.
- Im November 2004 fand in der ... Innenstadt vor mehreren Objekten (meist Kaufhäuser) eine Aktion der ... wegen dort angeblich verkauften genmanipulierten Lebensmittel statt. Die Versammlungen waren nicht angemeldet. Es wurden Flugblätter verteilt und mindestens ein Stofftransparent gezeigt. B war Teilnehmerin der Aktion.
- Anlässlich des 60. Jahrestags des Atombombenabwurfs auf die Stadt Hiroshima hielten ca. 10 Personen der ... (Ortsgruppe der Umweltschutzorganisation) im August 2005 eine Mahnwache in ... ab und erinnerten mit einem aus Kerzen gebildeten Atomzeichen an die Opfer des ersten Atombomben-Abwurfs. ... Verantwortliche dieser Veranstaltung war B.
- Die Protestaktion der ... im März 2006 zum Thema „Gegen die Verwendung von Gen-Pflanzen in Lebens- und Futtermitteln“ in ... wurde von ... (B) angemeldet und geleitet. Mit einem Banner, einem ca. 2 m hohen Joghurtglas (Durchmesser von ca. 1,50 m) sowie einer ca. 3 m hohen Milchflasche wurde auf die Versammlung aufmerksam gemacht. Außerdem wurde eine themenbezogene Umfrage durchgeführt und Flugblätter von ... verteilt, auf denen u. a. Gründe gegen Gentechnik aufgeführt waren. ... Außerdem werden die Leser der Flugblätter aufgefordert, ihren Supermarkt zu bitten, nur noch Milchprodukte zu verkaufen, die garantiert ohne Gen-Pflanzen im Tierfutter erzeugt werden ...

Weitere in der AD PMK über B gespeicherte Vorkommnisse betrafen andere Protestaktionen zu vergleichbaren Themen; von Straftaten oder Ordnungsstörungen ist nichts zu lesen. Stattdessen werden geradezu liebevoll – vermutlich durch Observation gewonnene – Details wiedergegeben, so z. B., dass bei von B angemeldeten Versammlungen im Februar und im Juli 2006 auf die „Zerstörung des Amazonas-Regenwaldes durch Soja-Anbau“ durch „Papp-Pflanzen/-Bäume“, „Stoffkuscheltiere“ und „Verkleidungsmaterial“ sowie durch einen „überdimensionalen aufblasbaren Jaguar“ hingewiesen wurde. Wohl nicht nur mir stellt sich da die Frage: Sind derartige Nebensächlichkeiten für den Staatsschutz wirklich von Belang?

2.3 Warum alles geheim bleiben soll

Besonders schwer fällt ins Gewicht, dass das Landeskriminalamt den jungen Frauen – mit Ausnahme des Verfahrens wegen Nötigung im Jahr 2002 bei B – die Auskunft über die in der AD PMK gespeicherten Informationen verweigert hat. Das Landeskriminalamt verfährt häufig

auch in anderen vergleichbaren Fällen so, hier wie dort zumeist mit der pauschalen Begründung, durch die Auskunftserteilung könne die polizeiliche Aufgabenerfüllung gefährdet werden (§ 21 Abs. 5 Nr. 1 LDSG). Gegenüber den Betroffenen wird die Auskunftsverweigerung üblicherweise nicht weiter begründet, sondern diese werden nur an meine Dienststelle verwiesen (§ 21 Abs. 6 LDSG). Bedauerlicherweise wird dann auch mir in vielen Fällen – so auch bei den beiden jungen Frauen – nicht erlaubt, die Betroffenen zu informieren (§ 27 Abs. 2 Satz 1 LDSG). Weil die Weigerung der speichernden Stelle ein formales Hindernis darstellt, sind mir damit zunächst die Hände gebunden. Als ich im Fall von A um eine genauere Begründung für die Geheimhaltung bat, hat mir das Landeskriminalamt unter Verweis auf §§ 37, 20 Abs. 3 Nr. 1 PolG Folgendes erklärt:

> „Dazu (Anmerkung: gemeint sind die zur polizeilichen Aufgabenwahrnehmung erforderlichen Daten) gehören auch Ereignisse, die aus polizeilicher Erfahrung auf einen künftigen Sachverhalt oder eine Entwicklung schließen lassen und somit als Indizien zu werten sind, die die Prognose der tatsächlichen Anhaltspunkte stützen. Solche Indizien sind u. a. Demonstrationen, Verteilen von Flugblättern, Mahnwachen und andere Aktionen, die belegen, dass die Einstellung des Betroffenen auch weiterhin dem Ziel dient, Einfluss auf den demokratischen Willensbildungsprozess zu nehmen. Die Speicherung solcher Erkenntnisse – die keine Straftaten oder polizeirechtswidrige Störungen darstellen – sind somit für die polizeiliche Aufgabenwahrnehmung erforderlich und somit zulässig."

Mit dieser Erläuterung bezieht sich das Landeskriminalamt auf das bundesweit geltende „Definitionssystem Politisch motivierte Kriminalität" des Bundeskriminalamts, wonach politisch motivierte Straftaten vorlägen, wenn „in Würdigung der Umstände der Tat und/oder der Einstellung des Täters Anhaltspunkte dafür vorliegen, dass sie den demokratischen Willensbildungsprozess beeinflussen sollen, der Erreichung oder Verhinderung politischer Ziele oder sich gegen die Realisierung politischer Entscheidungen richten." Im Fall von A wurde mir außerdem erklärt, es ginge nicht darum, „taktisches Vorgehen der Polizei vor Ort geheim zu halten, sondern nicht offen darzulegen, dass solche Erkenntnisse als Indizien gespeichert werden". Die „Erfahrung in den einzelnen Szenen" belege, dass die Betroffenen nach Kenntnis der „polizeilichen Vorgehensweise" ihr Verhalten ändern würden und dadurch die „polizeiliche Aufgabenwahrnehmung erschweren bzw. unmöglich machen".

Auf einen Nenner gebracht sollte das wohl heißen: Die Registrierung legaler oder sogar grundrechtlich besonders geschützter politischer Aktivitäten der Betroffenen durch den polizeilichen Staatsschutz muss geheim bleiben, weil die Betroffenen nicht wissen dürfen, dass die Polizei diese Aktivitäten erfasst und speichert, denn wenn sie es wüssten, würden sie ihr Verhalten ändern. Aus meiner Sicht offenbart diese Erklärung ein geradezu erschreckendes Verständnis von den Aufgaben der Polizei im demokratischen Rechtsstaat.

Datenschutzrechtlich halte ich die Auskunftsverweigerung in beiden Fällen jedenfalls für unzulässig, ja sogar für rechtsmissbräuchlich, da die Datenspeicherung über strafrechtlich nicht relevante Vorkommnisse in der AD PMK nicht zulässig ist und daher auch nicht der ordnungsgemäßen Aufgabenerfüllung der Polizei dienen kann. Die Auskunftserteilung kann nur ausnahmsweise unter gewissen Voraussetzungen unterbleiben, wozu insbesondere der Vorrang der polizeilichen Geheimhaltungserfordernisse gegenüber den Interessen des Betroffenen an der Bekanntgabe gehört (§ 21 Abs. 5 LDSG). Eine Auskunftsverweigerung erfordert daher eine gründliche Abwägung und Begründung (zumindest mir gegenüber), warum die Interessen des Betroffenen an einer Auskunft im konkreten Fall entgegen der Regel weniger gewichtig sind als die der Polizei an einer heimlichen Arbeitsweise. Dieser Abwägungsprozess war überhaupt nicht zu erkennen. Soweit die Auskunftsverweigerung bei „legalen" Verhaltensweisen des Betroffenen lediglich damit

begründet wird, der Betroffene dürfe nicht erfahren, dass (auch) diese Verhaltensweisen von der Polizei registriert werden, stellt dies geradezu einen absurden Zirkelschluss dar.

Die junge Frau im ersten Fall hat uns übrigens ein Schreiben des Landeskriminalamts Nordrhein-Westfalen zugeleitet, an das sie sich wegen einer Auskunftserteilung gewandt hatte. In seiner Antwort teilt ihr dieses Einzelheiten zu zwei Datenspeicherungen in „einer bundesweit abfragbaren Verbunddatei" aufgrund des Kriminalpolizeilichen Meldedienstes „Politisch motivierte Kriminalität" (KPMD-PMK) mit; die Informationen betrafen zwei strafrechtlich relevante Vorkommnisse in den Jahren 2003 und 2004. Es ist nicht nachvollziehbar, dass A über die Speicherung strafrechtlich relevanter Informationen zu politisch motivierten Vorgängen von der Polizei des Landes Nordrhein-Westfalen in Kenntnis gesetzt wird, während sich die Polizei des Landes Baden-Württemberg zu Datenspeicherungen, die politisch motivierte, aber strafrechtlich nicht relevante Vorfälle betreffen, ausschweigen will. Es drängt sich insofern der Eindruck auf, dass das Landeskriminalamt sich der Zweifelhaftigkeit seiner Speicherpraxis durchaus bewusst ist und unbedingt vermeiden will, dass diese den Betroffenen bekannt wird.

Dass es im Hinblick auf die AD PMK selbst in Baden-Württemberg auch anders geht, hat uns ein mit dem ersten Beispiel völlig vergleichbarer Fall aus dem Regierungsbezirk Karlsruhe gezeigt. Auch hier ging es um einen engagierten Tierversuchsgegner, der ins Visier des Staatsschutzes geraten war. Als wir das Regierungspräsidium Karlsruhe, Landespolizeidirektion, um eine Stellungnahme baten, erfuhren wir, dass der Petent als „Straftäter, linksmotiviert" wegen desselben Vorfalls wie A in INPOL gespeichert war, außerdem mit zwei anderen Vorkommnissen in der AD PMK. Die Stellungnahme endete mit dem datenschutzfreundlichen Satz: „Gegen die Bekanntgabe der Datenspeicherung an Herrn ... bestehen aus polizeitaktischer Sicht keine Bedenken." Bleibt zu hoffen, dass diese mustergültige Einstellung nicht nur ein vorübergehender Anflug badischer Liberalität war, sondern sich auch auf die obersten Staatsschützer im württembergischen Landesteil übertragen möge. Aufgrund unserer Intervention wurden übrigens die beiden Datenspeicherungen dieses Petenten in der AD PMK inzwischen gelöscht und die hierauf bezogenen Unterlagen vernichtet.

2.4 Warum die Vorfälle den Staatsschutz nichts angingen

Die Brisanz der geschilderten – aus der Sicht des unbefangenen Lesers vielleicht unbedeutenden – Datenspeicherungen und der Auskunftsverweigerungen wird deutlicher, wenn man sich einige Kernaussagen des sog. Volkszählungsurteils des Bundesverfassungsgerichts vor Augen führt (Urteil vom 15. Dezember 1983, 1 BvR 209/83). Darin hat das Gericht erläutert, warum das Grundrecht des Einzelnen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen („informationelle Selbstbestimmung"), auch eine klare gesellschaftspolitische Komponente hat, die für das Funktionieren unserer Demokratie wesentlich ist:

> „... Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. *Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.* Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Es bedarf keiner weiteren Begründung, dass die Registrierung der Teilnahme der beiden jungen Frauen A und B an den geschilderten Aktionen verhaltenssteuernd im Sinne der Warnung des Bundesverfassungsgerichts sein kann. Wer nicht weiß, ob seine Teilnahme an Anti-AKW-Demonstrationen oder seine Mitwirkung in Bürgerinitiativen zugunsten des Erhalts des Regenwalds behördlich registriert werden, wird möglicherweise auf ein entsprechendes Engagement verzichten. Im Klartext: Die Polizei unterliegt einem grundlegenden Irrtum, wenn sie es für ihre Aufgabe hält, derartige Aktivitäten zu registrieren, nur um festzustellen (um das Landeskriminalamt zu zitieren), ob „die Einstellung des Betroffenen auch weiterhin dem Ziel dient, Einfluss auf den demokratischen Willensbildungsprozess zu nehmen". Die Lektüre des Volkszählungsurteils hätte hier vielleicht weitergeholfen. Aber auch die bundesweit gültigen Richtlinien für den Kriminalpolizeilichen Meldedienst „Politisch motivierte Kriminalität" (KPMD-PMK) sind meines Erachtens eindeutig; danach sind durch die Polizei (Staatsschutzdienststellen) politisch motivierte Straftaten zu melden und zu speichern. Nur auf Straftaten, nicht auf Personen bezieht sich auch das in den Richtlinien genannte und vom Landeskriminalamt zitierte Kriterium der „politischen Einflussnahme". Aufgabe der Polizei ist es daher nicht, jegliche politische Aktivitäten zu registrieren, auch nicht bei (politisch motivierten) potenziellen Straftätern, sondern nur solche mit strafrechtlicher Relevanz (dazu möglicherweise einschlägige Ordnungsstörungen wie Verstöße gegen das Versammlungsrecht).

Selbst wenn man mit der Landesregierung als Maßstab und damit Begrenzung für die Speicherung weiterer Daten die Erforderlichkeit des Datums zur vorbeugenden Bekämpfung von Straftaten annimmt, so fehlt es schon an der Eignung der Informationen hierfür. Ich vermag nicht zu erkennen, welche Schlussfolgerungen die Polizei aus den geschilderten – geradezu demokratietypischen – Vorkommnissen im Hinblick auf künftige Straftaten ziehen will. Die Aktionen ließen kein bestimmtes Muster erkennen, wonach aus friedlichen Versammlungen, Mahnwachen und Flugblattverteilaktionen der Organisationen, für die sich A oder B betätigten, auf drohende Straftaten geschlossen werden konnte. Aus den einzelnen Aktionen konnte auch nicht auf eine sich steigernde Entwicklung geschlossen werden, die zwangsläufig in eine Straftat mündet. Der Staatsschutz konnte daraus allenfalls ersehen – um die Argumentation des Landeskriminalamts zu wiederholen –, ob A oder B politisch noch aktiv sind. Dies zu registrieren und zu speichern, ist indessen nicht Aufgabe der Polizei, die die Grenzen des Polizeigesetzes und der Strafprozessordnung zu beachten hat.

Um keine Missverständnisse aufkommen zu lassen: Beide junge Frauen waren mehrfach mit dem Gesetz in Konflikt gekommen. Die Speicherung ihrer strafrechtlichen Ermittlungsverfahren (z. B. bei A das in Nordrhein-Westfalen) war daher datenschutzrechtlich nicht zu beanstanden. Diese Informationen reichen zur vorbeugenden Straftatenbekämpfung und zur Abwehr konkreter Gefahren aber auch aus; die Speicherung der zeitlich dazwischen liegenden „legalen" Aktivitäten war insofern schlicht überflüssig.

Welche weiteren Organisationen oder Gruppierungen bzw. deren Mitglieder oder Aktivisten sich der besonderen Aufmerksamkeit des Staatsschutzes erfreuen und in der AD PMK erfasst sind, wissen wir im Moment noch nicht. Vorstellen lässt sich nach den genannten Beispielen vieles: Angefangen von Umweltschützern über Aktivisten der Friedensbewegung bis hin zu Atomkraft- oder Globalisierungsgegnern. Vom Landeskriminalamt wissen wir inzwischen, dass Straftaten von „Tierrechtsaktionisten" bundesweit der politisch motivierten Kriminalität unter dem Phänomenbereich „Sonstige" zugerechnet werden. Hierzu muss man wissen, dass das bereits erwähnte „Definitionssystem Politisch motivierte Kriminalität" des Bundeskriminalamts zwischen den Bereichen „Politisch motivierte Kriminalität – links", „Politisch motivierte Kriminalität – rechts" und „Politisch motivierte Ausländerkriminalität" unterscheidet. Alle politisch motivierten Straftaten und Ereignisse, die sich nicht diesen Bereichen zuordnen lassen, werden unter

dem (Auffang-)Bereich „Sonstige bzw. nicht zuzuordnen“ erfasst. Mangels einer „Zuordnungsliste“ für diesen Bereich konnte uns das Landeskriminalamt auch nicht abschließend angeben, welche relevanten Straftaten oder Ereignisse hierzu zählten. Im Grunde könnten hierunter alle politisch motivierten Straftaten bzw. strafrechtlich relevanten Ereignisse im Zusammenhang mit den Themenfeldern Kerntechnik, Gentechnik oder Tierschutz bzw. Jagd fallen. Mit Stand 12. September 2007 seien insgesamt 463 Personen unter der Kategorie „Sonstige“ in der AD PMK gespeichert. Eine detaillierte Recherche nach den Zuordnungsgründen sei aber aufgrund der Datenstruktur der AD PMK technisch nicht machbar und manuell nicht leistbar. Mit dieser Auskunft des Landeskriminalamts werden wir uns sicher nicht zufrieden geben.

2.5 Wie das Landeskriminalamt reagierte

Als Reaktion auf unsere deutliche Kritik zu den beiden oben genannten Fällen, die mit der Androhung einer förmlichen Beanstandung verbunden war, trat das Landeskriminalamt den geordneten Rückzug bzw. die Flucht nach vorne an. Unumwunden gestand es ein, dass die Speicherpraxis von den in den Orientierungshilfen getroffenen Regelungen offenbar teilweise abweichen würde bzw. der Grund der Speicherung nicht ausreichend ersichtlich sei. In den Orientierungshilfen sei nämlich „unmissverständlich“ geregelt, dass eine Speicherung personenbezogener Daten „grundsätzlich“ nicht rechtmäßig ist, wenn Personen „zulässig“ Grundrechte wahrnehmen. Über die bereits erfolgte „datenschutzrechtliche Sensibilisierung“ hinaus werde das Landeskriminalamt daher durch „weitergehende Maßnahmen“ auf die Einhaltung datenschutzrechtlicher Bestimmungen auch im Hinblick auf künftige Datenspeicherungen hinweisen und zudem folgende Maßnahmen ergreifen:

– Spezifische Schulung der Sachbearbeiter bei den Staatsschutzdienststellen ... insbesondere über die datenschutzrechtlichen Belange bei der Erfassung und Speicherung personenbezogener Daten in polizeilichen Auskunftssystemen,

– Sensibilisierung der Führungsebene für die Speicherproblematik im Bereich Staatsschutz,

– Fortsetzung der Prüfung und gegebenenfalls Bereinigung der gespeicherten Datensätze in der AD PMK,

– Erarbeitung von Maßnahmen zur wirksamen Qualitätssicherung.

Die Umsetzung dieser Maßnahmen sei ab November/Dezember 2007 geplant. Grundsätzlich sei vorgesehen, alle in der AD PMK gespeicherten Daten auf die Zulässigkeit der Speicherung durch die eingebenden Dienststellen überprüfen und gegebenenfalls bereinigen zu lassen. Dies erfordere nicht nur eine vorherige Aufbereitung der zu überprüfenden Datensätze, sondern zuvor auch die entsprechende Sensibilisierung und Schulung der Sachbearbeiter, um die Prüfung „sachgerecht und kompetent“ durchführen zu können. Nach Durchführung der Fortbildungs- und Sensibilisierungsmaßnahmen werde die Überprüfung durch die örtlichen Dienststellen „im Rahmen der laufenden Sachbearbeitung“ erfolgen. Offenbar um den Umfang der dabei zu bewältigenden Arbeiten deutlich zu machen, vergaß das Landeskriminalamt nicht zu erwähnen, dass in der AD PMK derzeit (Stand: Anfang Oktober 2007) ca. 129 000 Datensätze, davon ca. 30 000 Personendatensätze, gespeichert sind, von denen bis dato lediglich die Datensätze der beiden Petentinnen A und B überprüft worden seien. Bis wann die Überprüfung abgeschlossen sein werde, könne noch nicht abgeschätzt werden.

Zu den beiden konkreten Fällen teilte uns das Landeskriminalamt nach Beteiligung der örtlich zuständigen Polizeidienststellen mit, dass bei B sämtliche der von uns kritisierten Speicherungen über „legale“ Aktivitäten gelöscht worden seien; bei A sei das mit zwei Ausnahmen, die noch vertieft von uns zu prüfen sind, ebenfalls geschehen.

Zu dem im Zusammenhang mit A in der AD PMK erwähnten Verein, der sich für Datenschutz und informationelle Selbstbestimmung einsetzt, hat das Landeskriminalamt übrigens klargestellt, dass der Name dieses (der Polizei) zuvor unbekannten Vereins nur deshalb „als Kontaktstelle“ erfasst worden sei, weil A im Namen des Vereins eine öffentliche Veranstaltung angemeldet habe. Weitere Mitglieder des Vereins, der nach seinen Vereinszielen „als Beobachtungsobjekt“ ausscheide, seien nicht erfasst und der Eintrag inzwischen gelöscht worden. Daraus ist offenbar der auch für mich beruhigende Schluss zu ziehen, dass das Engagement für die informationelle Selbstbestimmung nicht als politisch motivierte Kriminalität bewertet wird.

2.6 Was noch zu sagen ist

Die AD PMK hat sich mittlerweile zu einem datenschutzrechtlichen „Dauerbrenner“ entwickelt: Je tiefer man gräbt, desto mehr Fragen und Mängel tauchen auf. So erfreulich die weitgehende Bereinigung und Löschung der zu den beiden jungen Frauen gespeicherten Datensätze ist, so ernüchternd ist doch bei näherer Betrachtung die Reaktion des Landeskriminalamts: Wenn als Gegenmaßnahme in Aussicht gestellt wird, die Mitarbeiter des polizeilichen Staatsschutzes und deren Vorgesetzte im Hinblick auf datenschutzrechtliche Anforderungen sensibilisieren und fortbilden zu wollen, dann ist das nicht nur selbstverständlich, es kann in Bezug auf die Datenqualität der AD PMK bis dato nur als Offenbarungseid verstanden werden. Offenbar wurde diese Datei trotz bundes- und landesweiter Richtlinien, Orientierungshilfen usw. viel zu leichtfertig befüllt. Im zentralen Punkt vermisse ich zudem eine klare Aussage: Was soll es heißen, dass eine Speicherung personenbezogener Daten (nur) „grundsätzlich“ nicht rechtmäßig ist, wenn Personen „zulässig“ Grundrechte wahrnehmen? Was heißt „grundsätzlich“, was soll „zulässig“ bedeuten? Es war nie fraglich, dass die Polizei personenbezogene Daten speichern darf, wenn es bei Demonstrationen zu Krawallen kommt und Straftaten begangen werden. Wie steht der Staatsschutz aber zu unserer Forderung, „legale“ Verhaltensweisen gar nicht erst in der AD PMK zu erfassen? Aus meiner Sicht besteht daher weiterhin die Gefahr, dass bei – aus Sicht des Staatsschutzes – einschlägig verdächtigen Personen auch unverfängliche Verhaltensweisen gespeichert werden. Und wenn es heißt, die Überprüfung werde im Rahmen der „laufenden Sachbearbeitung“ vorgenommen, dann hört sich das so an, als hänge es vom Zufall ab, wann ein Vorgang zwecks Überprüfung in die Hand genommen wird. De facto wird die dringende Revision der Datei damit auf die lange Bank geschoben.

Bleibt noch das leidige Thema Auskunft: Hierzu hat mir das Landeskriminalamt „im Einvernehmen mit dem Innenministerium“ lapidar erklärt, dass einer Auskunftserteilung an die beiden Petentinnen „aus den bereits genannten Gründen“ nicht zugestimmt werde; die Möglichkeit der verwaltungsgerichtlichen Überprüfung stehe (den Petentinnen) offen. Der angemahnte Abwägungsprozess ist bei dieser Verweigerung nicht zu erkennen. Ich habe daher inzwischen die Auskunftsverweigerung in beiden Fällen förmlich beanstandet. Möglicherweise hat das Landeskriminalamt mittlerweile gemerkt, dass es sich für die Begründung einer Auskunftsverweigerung mehr einfallen lassen muss; in einer jüngeren Stellungnahme wurden jedenfalls längere Ausführungen dazu gemacht, warum die Beobachtung einer in die „linke Szene“ verstrickten Frau weiterhin verheimlicht werden müsse. Dass im Zweifel das Auskunftsrecht der Betroffenen Vorrang hat, war dieser Stellungnahme allerdings immer noch nicht anzumerken.

Zu welchen Ergebnissen die abermals angekündigte Revision der AD PMK führen wird, bleibt abzuwarten. In mindestens zwei weiteren Fällen (ein ähnlich engagierter Tierversuchsgegner wie A und ein Gegner der CASTOR-Transporte) warten die Petenten und ich seit Wochen auf habhafte Informationen, weil vom Landeskriminalamt lediglich die Auskunft zu hören ist, dass es sich jeweils um einen „gleich gelagerten“ Fall (wie bei A und B) handle, der zur Zeit einer „sensibleren Überprüfung“ unterzogen werde.

3. Gelöscht und vielleicht doch nicht? Die Verarbeitung erkennungsdienstlicher Unterlagen beim Bundeskriminalamt

Dass die Polizei zur Identitätsfeststellung, also z. B. für die Überprüfung von Fingerabdrücken, die am Tatort gefunden wurden, oder für Zwecke des Erkennungsdienstes, also zur vorbeugenden Straftatenbekämpfung, Personen nach den Vorschriften der Strafprozessordnung (vgl. § 81 b StPO) bzw. des Polizeigesetzes (vgl. § 36 PolG) erkennungsdienstlich behandeln darf, ist hinlänglich bekannt. Weniger bekannt ist, wie mit den so gewonnenen erkennungsdienstlichen Daten anschließend verfahren wird, insbesondere wie lange diese Daten aufbewahrt und von wem sie schließlich gelöscht werden. Die Aufgabenverteilung zwischen den Polizeien von Bund und Ländern sorgt hier nämlich für datenschutzrechtlich nicht immer einwandfreie Zustände, denen wir im Rahmen einer konzertierten Aktion der Datenschutzbeauftragten von Bund und Ländern nachgingen.

Um das Verfahren kurz zu schildern: Wenn eine Polizeidienststelle in Baden-Württemberg die erkennungsdienstliche Behandlung einer Person durchgeführt hat – beispielsweise die Abnahme von Fingerabdrücken –, dann legt sie einen Datensatz – eine sog. E-Gruppe – an und erstellt ein Fingerabdruckblatt. Zu dem Datensatz, den sie zunächst in ihrem landeseigenen polizeilichen Auskunftssystem (POLAS-BW) speichert, vergibt sie eine Aussonderungsprüffrist, das heißt sie legt einen Zeitpunkt fest, an dem der Datensatz darauf zu überprüfen ist, ob er weiter aufbewahrt oder eben ausgesondert (gelöscht) werden soll. Die Dauer dieser Frist bestimmt sich nach der Speicherdauer für den zugrunde liegenden Tatvorwurf und beträgt in Baden-Württemberg in der Regel fünf Jahre (vgl. § 5 Abs. 1 Nr. 1 der Durchführungsverordnung zum Polizeigesetz, DVO PolG). Datensatz und Fingerabdruckblatt werden anschließend dem Bundeskriminalamt in seiner Funktion als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen zur Speicherung bzw. Aufbewahrung übersandt. Dort wird die E-Gruppe im informationstechnischen Verbundsystem der Polizeien von Bund und Ländern (INPOL-Zentral, hier in den Dateien „Erkennungsdienst“ und „Automatisches Fingerabdruck-Identifizierungssystem – AFIS“) gespeichert, wobei das Bundeskriminalamt aber unabhängig vom Aussonderungsprüfdatum der erhebenden Stelle eine eigene Aussonderungsprüffrist vergibt, die in der Regel zehn Jahre beträgt. Das Bundeskriminalamt begründet diese Verfahrensweise damit, dass es nach Bearbeitung des übersandten Fingerabdruckblatts den (verwaltungstechnischen) „Besitz“ an den angelieferten Daten der E-Gruppe übernehme und die anliefernde Stelle daran lediglich „Mitbesitz“ behalte. Dementsprechend wird in INPOL-Zentral der ursprüngliche Besitzer im Feld „Ehemaliger Besitzer“ (Feld E 36) eingetragen. Löscht nun die Stelle, die ursprünglich die erkennungsdienstlichen Daten erhoben hat, den Datensatz nach Ablauf der dort vergebenen – wie gesagt: häufig kürzeren – Aussonderungsprüffrist in ihrem System (in Baden-Württemberg also POLAS-BW), dann wird automatisch eine Nachricht an das Bundeskriminalamt geschickt, die zur Löschung des Eintrags im Feld E 36 führt. Die übrigen Daten des Datensatzes in INPOL-Zentral bleiben stehen. Nach Auffassung des Bundeskriminalamts gibt nämlich die erhebende Stelle damit lediglich ihren „Mitbesitz“ auf. Deshalb bleibt der Datensatz beim Bundeskriminalamt bis zum Ablauf der dort vergebenen Frist gespeichert. Auf diese Daten kann dann auch im Rahmen des bundesweit verfügbaren Informationssystems INPOL-Zentral zugegriffen werden.

Um die geschilderte Verfahrensweise in Bezug auf die in Baden-Württemberg angelegten E-Gruppen zu überprüfen, haben wir beim Landeskriminalamt im Juni 2006 eine Stichprobe von 30 Datensätzen erhoben, die zum 31. Juli 2006 zur Löschung im Landessystem (POLAS-BW) anstanden. Das Landeskriminalamt erklärte in diesem Zusammenhang, dass es durch die Löschung im Landessystem und den automatisierten Versand einer Löschanzeige an das Bundeskriminalamt das auf Landesebene Erforderliche veranlasse, um beim Bundeskriminalamt die Voraussetzungen für die Löschung der gesamten E-Gruppe auch in INPOL-Zentral herbeizuführen. Einige Monate später haben wir bei einer anderen Datenstation der Polizei in den polizeilichen Informationssystemen INPOL-Zentral und POLAS-BW nachgeschaut, was mit den 30 Datensätzen passiert ist. Von den 30 Da-

tensätzen waren zum Zeitpunkt der Nachschau im Januar 2007 elf Datensätze in beiden Systemen gelöscht. 18 Datensätze waren nicht mehr in POLAS-BW, sondern nur noch in INPOL-Zentral gespeichert. Ein Datensatz war noch sowohl in INPOL-Zentral als auch in POLAS-BW gespeichert, was durch ein neues Ermittlungsverfahren und die hierbei verlängerte Aussonderungsprüffrist zu erklären war. Soweit die Speicherung in POLAS-BW inzwischen gelöscht war, konnte durch Einblick in INPOL-Zentral festgestellt werden, dass Baden-Württemberg als „Mitbesitzer" in dem Feld E 36 tatsächlich gelöscht war; die automatisierte Anzeige der „Mitbesitzaufgabe" an das Bundeskriminalamt aus dem Landessystem heraus scheint insoweit zu funktionieren. In einigen (wenigen) Fällen, in denen nur noch eine Speicherung in INPOL-Zentral festzustellen war, waren inzwischen Einträge von Polizeidienststellen anderer Bundesländer hinzugekommen, für die die Aussonderungsprüffrist in den dortigen Landessystemen offenkundig noch lief. Insoweit bestanden gegen die fortlaufenden Datenspeicherungen keine durchgreifenden Bedenken. Problematisch sind indessen die Fälle, in denen keine Vorkommnisse aus anderen Bundesländern festzustellen waren und die E-Gruppe in INPOL-Zentral lediglich infolge der Meldung aus Baden-Württemberg angelegt worden war. In diesen Fällen bleibt der Datensatz unverändert in INPOL-Zentral gespeichert, also auch mit dem Hinweis, aus welchem Grund, wann und von welcher baden-württembergischen Polizeidienststelle eine erkennungsdienstliche Behandlung veranlasst worden war.

Der gegenwärtige Zustand ist aus datenschutzrechtlicher Sicht sehr unbefriedigend. Denn was für einen Zweck hat die Löschung im Landessystem, wenn dieselben Daten zum Abruf im bundesweit verfügbaren Polizeisystem INPOL-Zentral selbst dann weiter vorgehalten werden, wenn offenkundig nur die von dem betreffenden Bundesland eingegebenen Daten Anlass für die Speicherung in INPOL-Zentral waren? Hinzu kommt, dass die polizeilichen Datenstationen unter einer einheitlichen Benutzeroberfläche praktisch gleichzeitig auf das Schengener Informationssystem (SIS), das Bund-Länder-System INPOL-Zentral und das Landessystem POLAS-BW zugreifen können und dass es insofern eigentlich sekundär ist, aus welcher der drei Datenbanken der angezeigte „Treffer" stammt. Wenn INPOL-Zentral also „Treffer" wie in POLAS-BW anzeigt, stellt es de facto ein polizeiliches „Reservesystem" für die Vorhaltung auch solcher Daten dar, die nach Landesrecht längst zu löschen sind. Zur rechtlichen Seite der Angelegenheit ist auf § 12 Abs. 2 des Gesetzes über das Bundeskriminalamt (BKAG) hinzuweisen, wonach im Rahmen des polizeilichen Informationssystems (INPOL-Zentral) die datenschutzrechtliche Verantwortung für die beim Bundeskriminalamt gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit oder Aktualität der Daten den Stellen obliegt, die die Daten unmittelbar eingeben, also eigentlich den Dienststellen der Länder. Der Hinweis auf die „Besitzübernahme" durch das Bundeskriminalamt infolge der Eingabe des Datensatzes in das Verbundsystem INPOL-Zentral stellt sich vor diesem Hintergrund als datenschutzrechtlich nicht hinzunehmende Spitzfindigkeit dar. Klar ist vielmehr, auch nach Ansicht des Bundesdatenschutzbeauftragten: Erkennungsdienstliches Material ist Bestandteil der kriminalpolizeilichen personenbezogenen Sammlungen, die das Bundeskriminalamt gemäß § 2 Abs. 4 BKAG zur Erfüllung seiner Aufgaben als Zentralstelle der Polizeien des Bundes und der Länder führt. Die Regelungen der §§ 11 ff. BKAG enthalten keine Rechtsgrundlage für eine „Besitzübernahme" durch das Bundeskriminalamt hinsichtlich der Daten, die durch einen Verbundteilnehmer in das System eingegeben werden. Damit ist auch die Vergabe einer eigenen Aussonderungsprüffrist durch das Bundeskriminalamt für die von den Verbundteilnehmern zur Speicherung in dem Zentralsystem übermittelten Daten unzulässig. Nur die ursprünglich einspeichernde Stelle hat die dem Datensatz zugrunde liegenden Akten, nur sie kennt die Einzelheiten des Falles, nur sie kennt den Tatverdächtigen und kann die Gefahr neuer Straftaten einschätzen und dementsprechend die Speicherfrist bestimmen. Nur sie hat daher nach § 12 Abs. 2 BKAG über die Veränderung oder Löschung eines Datensatzes zu entscheiden. Werden die Daten von der verantwortlichen Stelle gelöscht, kann die betreffende erkennungsdienstliche Speicherung in INPOL-Zentral nur dann aufrechterhalten werden, wenn zu

dem Betroffenen eigene Erkenntnisse des Bundeskriminalamts oder einer anderen Landespolizei vorliegen, die eine weitere Speicherung rechtfertigen. Ansonsten ist es nicht erforderlich, diese Daten beim Bundeskriminalamt weiter vorzuhalten.

Wie geht es weiter? Das Bundeskriminalamt hat gegenüber dem Bundesdatenschutzbeauftragten zwar eingeräumt, die Datensätze nicht weiter aufbewahren zu wollen, wenn die zugrunde liegenden Erkenntnisse bei der ursprünglich speichernden Stelle gelöscht worden sind. Solange das Bundeskriminalamt jedoch eine eigene Aussonderungsprüffrist vergibt, die von der der Länder abweicht, und solange die Löschung im Landessystem nicht automatisch zur Löschung im Verbundsystem führt, wird sich an dem gegenwärtigen Zustand nur wenig ändern. Das Landeskriminalamt hat uns gegenüber – gewissermaßen achselzuckend – erklärt, dass es auch nicht verstehe, nach welcher Systematik das Bundeskriminalamt manche Datensätze lösche, andere hingegen nicht. Im Übrigen hält es das Landeskriminalamt – wie wir – zur Zeit für nicht hinreichend gewährleistet, dass E-Gruppen in INPOL-Zentral zuverlässig gelöscht werden, wenn der ursprüngliche Datenbesitzer den „Mitbesitz“ aufgegeben hat. Es sieht allerdings (offenbar „nur“) das Bundeskriminalamt in der Pflicht, für eine zuverlässige Löschung der Datensätze zu sorgen. Wir meinen, dies greift zu kurz. Hier stehen alle Polizeien des Bundes und der Länder gemeinsam in der Pflicht, ihr informationstechnisches Verbundsystem auf Vordermann zu bringen. Denn die Polizeien der Länder bleiben nach § 12 Abs. 2 BKAG weiterhin für „ihre“ Datensätze verantwortlich und können sich nicht aus der Verantwortung stehlen. Aus Sicht eines Betroffenen, der in eine Polizeikontrolle gerät, spielt es nämlich keine Rolle, in welcher polizeilichen Datenbank er gespeichert ist.

Ein Blick in die Zukunft zeigt, dass hinsichtlich einer datenschutzkonformen Verarbeitung erkennungsdienstlicher Daten der Länder im Bundeskriminalamt dringend etwas geschehen muss: Der polizeiliche Informationsaustausch mit anderen europäischen Staaten wird in den nächsten Jahren nämlich erheblich ausgebaut. So räumen sich beispielsweise die Unterzeichnerstaaten des „Prümer Vertrags“ gegenseitig einen beschränkten automatisierten Zugriff auf die jeweiligen nationalen Sammlungen erkennungsdienstlicher Daten ein. Dass auf diese Weise erkennungsdienstliche Daten, die nicht länger für die Aufgabenerfüllung der Polizeien des Bundes und der Länder erforderlich sind und damit längst hätten gelöscht werden müssen, europaweite Verbreitung finden, ist aus meiner Sicht nicht hinnehmbar. Der Bundesdatenschutzbeauftragte hat sich in diesem Sinne inzwischen an den Bundesinnenminister gewandt; die Prüfung sei dort aber noch im Gang.

4. Bereinigung des Datenbestands der DNA-Analyse-Datei

In unserem letzten Tätigkeitsbericht hatten wir über Auffälligkeiten bezüglich der beim Bundeskriminalamt geführten DNA-Analyse-Datei berichtet. Dort werden die nach § 81 g StPO erhobenen Identifizierungsmuster aus molekulargenetischen Untersuchungen von Personen gespeichert, die verdächtigt werden, bestimmte Straftaten begangen zu haben, und von denen angenommen wird, sie könnten wieder entsprechende Straftaten begehen. Dabei muss es sich um Straftaten von erheblicher Bedeutung oder um Straftaten gegen die sexuelle Selbstbestimmung handeln; infolge der Novellierung dieser Vorschrift im Jahr 2005 reicht mittlerweile auch die wiederholte Begehung sonstiger Straftaten aus, wenn dies im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichkommt. Festgestellt worden war nun, dass etliche der Datenspeicherungen nicht den gesetzlichen Anforderungen für die Aufnahme in die DNA-Analyse-Datei zu entsprechen schienen, weil die im jeweiligen Deliktsdatenfeld eingetragenen Straftaten eher der minderschweren Kriminalität zuzuordnen waren (z. B. Sachbeschädigung, strafbarer Eigennutz, falsche Verdächtigung, Widerstand gegen die Staatsgewalt usw.). Das von uns im letzten Jahr um Stellungnahme gebetene Innenministerium hat daraufhin eine Stichprobenerhebung und -auswertung durch das Landeskriminalamt veranlasst, die aber wegen dessen Arbeitsbelastung erst nach Vorlage unseres letzten Tätigkeitsberichts abge-

schlossen werden konnte. Das Landeskriminalamt sollte im Zuge der Überprüfung auch unrichtige Datensätze berichtigen und ohne ausreichende Rechtsgrundlage gespeicherte Daten löschen.

Inzwischen liegen die Ergebnisse der relativ aufwendigen Einzelfallprüfung vor, über die wir in Ergänzung des letzten Tätigkeitsberichts berichten wollen. Danach hat das Landeskriminalamt insgesamt 493 Datensätze der DNA-Analyse-Datei aus folgenden Deliktsbereichen überprüft:

- Sachbeschädigung (161 Datensätze),
- strafbarer Eigennutz (17 Datensätze),
- Widerstand gegen die Staatsgewalt (216 Datensätze),
- falsche Verdächtigung (12 Datensätze),
- Diebstahl und Unterschlagung geringwertiger Sachen (1 Datensatz),
- Entziehung elektrischer Energie (1 Datensatz),
- unbefugter Gebrauch eines Fahrzeugs (7 Datensätze),
- Unterschlagung (78 Datensätze).

Bei einem Teil der Datensätze (83) war offenbar das Anlassdelikt lediglich aus Versehen falsch eingetragen worden und in Wirklichkeit erheblich; hier wurden die entsprechenden Datenfelder korrigiert. Bei 80 Datensätzen ergab die Überprüfung des konkreten Falls, dass das Delikt – ungeachtet der zunächst „harmlos“ klingenden Deliktsgruppe – erheblich war; hier wurde der Datensatz unverändert belassen. In 33 Fällen ergab die Überprüfung ein vorangegangenes erhebliches Delikt; hier erfolgte eine entsprechende „Umwidmung“ des Datensatzes. In 89 Fällen reichte die der molekulargenetischen Untersuchung zugrunde liegende Einwilligungserklärung des Betroffenen bzw. der alternativ erforderliche gerichtliche Beschluss nicht aus und wurde in korrigierter Form nachgeholt.

In sage und schreibe 208 Fällen (rd. 42 %) musste der Datensatz in der DNA-Analyse-Datei aber aufgrund der Einzelfallprüfung des Landeskriminalamts gelöscht werden. Was dieser hohe Prozentsatz über die Qualität des Datenbestands in dieser Datei aussagt, kann man nur ahnen. Zwar betraf die Überprüfung nur solche Datensätze, die schon infolge der Bezeichnung der Anlassstraftat auf mögliche Fehler hindeuteten. Andererseits gibt es in der DNA-Analyse-Datei sicher auch zahlreiche Datensätze, bei denen die jeweilige Anlassstraftat zunächst gravierend klingt, sich bei näherer Prüfung aber doch nicht als so erheblich herausstellt. Es liegt jedenfalls auf der Hand, dass die rechtlichen Voraussetzungen für die Speicherung von Tatverdächtigen in dieser sensiblen Datei vielfach nicht ausreichend geprüft wurden. Ob dies in Zukunft geschieht, bleibt offen. Insbesondere die schwierige Frage, wann eine wiederholte Begehung minderschwerer Straftaten der Begehung einer Straftat von erheblicher Bedeutung im Unrechtsgehalt gleichsteht (§ 81 g Abs. 1 Satz 2 StPO), bietet einen erheblichen Interpretationsspielraum, der in der polizeilichen Praxis zu einer eher großzügigen Anwendung führen dürfte. Die festgestellten Mängel sind nämlich auch vor dem Hintergrund zu sehen, dass – wie wir in anderem Zusammenhang vom Innenministerium erfuhren – DNA-Proben in über 90 % der Fälle aufgrund der schriftlichen Einwilligung des Betroffenen entnommen werden und nur in einem geradezu verschwindend geringen Ausmaß die relativ differenzierte Prüfung der Voraussetzungen nach § 81 g Abs. 3 StPO durch ein Gericht erfolgt. Um den Unterschied zu verdeutlichen: Nach § 81 g Abs. 3 Satz 5 StPO ist in der schriftlichen Begründung des Gerichts einzelfallbezogen (!) darzulegen, welche Tatsachen die Erheblichkeit der Anlassstraftat ausmachen, welche Erkenntnisse für die Gefahr erneuter Straftaten des Beschuldigten sprechen und wie die jeweils maßgeblichen Umstände abgewogen werden. Zwar wird ein Beschuldigter von der Polizei formularmäßig korrekt darüber belehrt, welche gesetzlichen Voraussetzungen für die DNA-Probe vorliegen müssen. Allerdings wird er als juristischer Laie meistens nicht in der Lage sein, einen ähnlich differenzierten Abwägungsprozess wie das Gericht vorzunehmen, zumal er dabei schwierige Rechtsfragen (Beispiel: Unrechtsgehalt mehrerer Ladendiebstähle) be-

antworten und sich selbst zu allem Überfluss eine Negativprognose hinsichtlich künftiger Straftaten ausstellen muss. Hinzu kommt sicher vielfach der Druck in einer Vernehmungssituation. Die Prüfung der Voraussetzungen für die Vornahme einer DNA-Probe wird von der Polizei – wenn die Einwilligung des Betroffenen vorliegt – überdies nicht im gleichen Umfang dokumentiert, wie dies in der schriftlichen gerichtlichen Anordnung geschieht. Die Einwilligung des Betroffenen kann jedoch nicht die nach § 81 g Abs. 1 StPO erforderlichen Voraussetzungen für eine molekulargenetische Untersuchung ersetzen. Jedenfalls ist nicht auszuschließen, dass insbesondere die auf der Grundlage von Einwilligungen des Beschuldigten vorgenommenen Datenspeicherungen in der DNA-Analyse-Datei eine hohe Fehlerquote aufweisen. Es bleibt zu hoffen, dass die alarmierenden Ergebnisse der Stichprobe zu einer verbesserten polizeiinternen Qualitätskontrolle führen werden. Wir werden uns bei Gelegenheit erlauben, mal wieder nachzuschauen, wie es um die Datenqualität der DNA-Analyse-Datei bestellt ist. Bis auf weiteres können wir den Betroffenen angesichts der geschilderten Überprüfungsergebnisse nur raten, sich die Unterschrift unter eine schriftliche Einwilligungserklärung für die DNA-Analyse gut zu überlegen und im Zweifelsfall lieber darauf zu bestehen, dass eine richterliche Anordnung eingeholt wird.

5. Sicherheitsüberprüfungen in der Grauzone – „Zuverlässigkeitsüberprüfungen“ durch die Polizei auf der Grundlage informierter Einwilligungen der Betroffenen

Im vergangenen Jahr haben wir uns – wie sich vielleicht der eine oder andere Leser meiner Tätigkeitsberichte erinnern wird – ausführlich mit dem Akkreditierungsverfahren zur Fußballweltmeisterschaft befasst, bei dem knapp 150 000 Personen auf Vorerkenntnisse bei Polizei und Nachrichtendiensten abgeklopft wurden, bevor sie in offizieller Funktion die Stadien betreten durften (vgl. 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650). Nach den Ablehnungskriterien konnten dabei nicht etwa nur rechtskräftige strafrechtliche Verurteilungen, sondern gegebenenfalls auch eingestellte Ermittlungsverfahren und vage Erkenntnisse des Verfassungsschutzes zum Stolperstein werden. Grundlage der Überprüfungsverfahren waren jeweils ausführliche formularmäßige Einwilligungserklärungen, die vom Betroffenen online auszufüllen waren. Technisch und organisatorisch wurde das Verfahren über eine zentrale Kontaktstelle beim Bundeskriminalamt abgewickelt. Trotz erheblicher datenschutzrechtlicher Bauchschmerzen hatten wir das Verfahren damals notgedrungen hingenommen, da die Verantwortlichen auf die erhebliche Gefahr terroristischer Anschläge, zwingende Zusagen gegenüber der FIFA und insbesondere auf den einmaligen Ausnahmecharakter des Verfahrens hinwiesen; schließlich sollte das weltweit beachtete Sport- und Medienereignis Fußball-WM nicht am Datenschutz scheitern.

Mittlerweile beobachte ich mit Sorge, dass die im vergangenen Jahr anlässlich der Fußballweltmeisterschaft noch als angeblich singulär bezeichneten Sicherheitsüberprüfungen im Rahmen eines Akkreditierungsverfahrens für Funktionsträger offenbar zum polizeilichen Standardinstrument aus unterschiedlichen Anlässen werden. Dabei geht es nicht mehr nur um große Sportveranstaltungen, wie z. B. vor kurzem die Radweltmeisterschaft in Stuttgart, bei der in bestimmten Sicherheitszonen eingesetzte Ordner und andere Helfer überprüft wurden; für die Turn-WM in Stuttgart konnte ein ähnliches Verfahren nur aus Zeitgründen nicht mehr realisiert werden. Zunehmend werden auch weitere Anwendungsbereiche bekannt, bei denen Bürger mit Hilfe einer Einwilligung auf polizeiliche Vorerkenntnisse überprüft werden sollen. So erfuhren wir vor einiger Zeit aufgrund eines Hinweises des Bundesdatenschutzbeauftragten davon, dass es bereits seit Oktober 2004 eine – uns bis dato unbekannte – Vereinbarung zwischen der Deutschen Bundesbank und dem Landeskriminalamt Baden-Württemberg gibt, wonach das bei der Deutschen Bundesbank, Hauptverwaltung Stuttgart, eingesetzte Fremdpersonal (vermutlich Handwerker, Reinigungspersonal, Wartungspersonal für technische Geräte usw.) einer Zuverlässigkeitsüberprüfung im Hinblick auf kriminalpolizeiliche und staatsschutzrelevante Erkenntnisse – allerdings wohl ohne Beteiligung der Nachrichtendienste – unterzogen wird.

Im Zusammenhang mit der deutschen EU-Ratspräsidentschaft und dem G 8-Vorsitz wurde ferner bekannt, dass Personen, die bei Ministertreffen in Baden-Württemberg in sicherheitsempfindlichen Bereichen der entsprechenden Veranstaltungsorte (z. B. Hotels) tätig waren, einer Zuverlässigkeitsüberprüfung im Rahmen eines Akkreditierungsverfahrens unterzogen wurden; allerdings lagen diese Verfahren in der Verantwortung der Bundesregierung bzw. des Bundeskriminalamts. Die Rechtslage dürfte sich bei dieser Fallkonstellation aufgrund der Verantwortung des Bundeskriminalamts, für den Schutz der Mitglieder der Bundesregierung zu sorgen, auch von jener bei einem Tätigwerden im Auftrag privater Sportveranstalter unterscheiden.

Die vom Innenministerium bereits anlässlich der Fußball-WM zu dieser Problematik vertretene Auffassung, dass datenschutzrechtlich die erforderliche gesetzliche Grundlage durch die Einwilligung des Betroffenen ersetzt werde, kann nicht unwidersprochen bleiben. Ich möchte daher meinen Standpunkt auch an dieser Stelle noch einmal kurz erläutern:

- Bei Zuverlässigkeitsüberprüfungen wird in das Grundrecht auf informationelle Selbstbestimmung eingegriffen. Solche Eingriffe sind nur zulässig, wenn sie durch ein Gesetz, das den verfassungsrechtlichen Anforderungen genügt und insbesondere den Grundsatz der Verhältnismäßigkeit beachtet, erlaubt sind oder der Betroffene einwilligt.
- In speziellen grundrechtsrelevanten Bereichen muss der Gesetzgeber nach der Wesentlichkeitstheorie die Eingriffsvoraussetzungen selbst regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsüberprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.
- Polizeiliche und nachrichtendienstliche Zuverlässigkeitsüberprüfungen können durch „informierte Einwilligungen“ alleine nicht legitimiert werden. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Zuverlässigkeitsüberprüfungen sind hoheitliche Verfahren, die der Gesetzgeber ausdrücklich und abschließend geregelt hat. Zu nennen sind z. B. die Sicherheitsüberprüfungsgesetze, das Atomgesetz oder das Luftsicherheitsgesetz. Diese Normen verlangen zusätzlich zu materiellen und verfahrensrechtlichen Regelungen die Mitwirkung in Form einer schriftlichen Erklärung der betroffenen Personen bei der Einleitung einer solchen Überprüfung durch die Sicherheitsbehörden. Außerdem gewährleisten sie ein transparentes Verfahren, in dem u. a. die Rechte Betroffener, wie z. B. das Recht auf Auskunft und Anhörung vor negativer Entscheidung, geregelt sind. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich. Die Einwilligung kann eine fehlende Rechtsgrundlage daher nicht ersetzen.
- Die Polizei kann nur die durch ein Gesetz zugewiesenen Aufgaben wahrnehmen. Wenn eine gesetzliche Grundlage besteht, bedarf es keiner Einwilligung des Betroffenen zur Datenerhebung und -übermittlung. Wenn keine Rechtsgrundlage für die Wahrnehmung einer Aufgabe vorliegt, kann sie auch nicht durch die Einwilligung des Betroffenen geschaffen werden.
- Sollten Zuverlässigkeitsüberprüfungen in der zunehmend praktizierten Form wirklich als unerlässlich angesehen werden, so bedarf es für deren Durchführung daher einer gesetzlichen Grundlage, die den Anforderungen an Normenklarheit genügt, verfahrensrechtliche Sicherungen enthält und dem Verhältnismäßigkeitsgrundsatz Rechnung trägt.
- Nicht zuletzt ist auch daran zu erinnern, dass insbesondere in denjenigen Fällen, in denen es um die Überprüfung von Firmenmitarbeitern im Interesse von privatrechtlichen Auftraggebern (z. B. Sportveranstaltern) geht, der Gesetzgeber mit dem aus dem Bundeszentralregister erstellten Führungszeugnis ein geeignetes Instrument zur Verfügung stellt, um sich über die Unbedenklichkeit eines Vertragspartners bzw. Mitarbeiters zu informieren. Damit hat er eine Bewertung zum Ausdruck gebracht, in

welchem Umfang strafrechtlich relevante Verhaltensweisen bekannt und gegebenenfalls gegen den Betroffenen verwendet werden können. § 51 des Bundeszentralregistergesetzes (BZRG) stellt klar, dass eine im Register getilgte Tat und die Verurteilung – vorbehaltlich der in § 52 BZRG genannten Ausnahmen – dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden dürfen. Selbst ein Verurteilter ist nicht unter allen Umständen verpflichtet, eine frühere Verurteilung zu offenbaren (vgl. § 53 BZRG). Demgegenüber erstreckt sich die von der Polizei – gegebenenfalls auch von den Nachrichtendiensten – vorzunehmende Sicherheitsüberprüfung auf alle in den polizeilichen (und gegebenenfalls nachrichtendienstlichen) Informationssystemen gespeicherten Informationen über den Betroffenen. Darunter befinden sich in der Regel auch Informationen über eingestellte strafrechtliche Ermittlungsverfahren, die auf diese Weise dem Betroffenen beruflich zum Nachteil gereichen können, obwohl sie im Bundeszentralregister nicht einzutragen sind. In Bezug auf die Nachrichtendienste geht es zudem vielfach um schwer fassbare Bewertungen und um Erkenntnisse, die u. U. mit Hilfe nachrichtendienstlicher Mittel gewonnen wurden und die deshalb für den Betroffenen kaum nachvollziehbar sind. Damit ergibt sich außerhalb des Anwendungsbereichs des Bundeszentralregistergesetzes und der Regelungen über Sicherheitsüberprüfungen in den einschlägigen Gesetzen zunehmend eine Grauzone, die schon aus Gründen der Normenklarheit zu vermeiden ist. Aus meiner Sicht sollte es genügen, dass ein Auftraggeber den beauftragten Firmen auferlegt, von ihren Mitarbeitern die Vorlage eines Führungszeugnisses zu verlangen.

Abschließend ist zu erwähnen, dass die rasche Bereitschaft des Landeskriminalamts Baden-Württemberg, im Auftrag der Deutschen Bundesbank deren Vertragspartner zu durchleuchten, andernorts offenbar nicht geteilt wird. So wissen wir inzwischen aus einigen anderen Bundesländern, dass vergleichbare Ansinnen der Bundesbank durch die dortigen Landeskriminalämter unter Verweis auf die fehlende Rechtsgrundlage kühl zurückgewiesen wurden.

Im Hinblick auf den zunehmenden Wildwuchs von Zuverlässigkeitsüberprüfungen im Rahmen sportlicher und anderer Großveranstaltungen haben auch die Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz am 25./26. Oktober 2007 nachdrücklich auf die vorgenannten Bedenken hingewiesen (vgl. Anhang 6).

6. Die Ausschreibung zur verdeckten Registrierung nach Artikel 99 des Schengener Durchführungsübereinkommens (SDÜ)

Im letzten Jahr hatten wir uns im Rahmen einer konzertierten Kontrollaktion der Datenschutzbeauftragten eingehend mit der Ausschreibung von Personen zur verdeckten Registrierung – von der Polizei vielfach auch als polizeiliche Beobachtung bezeichnet – im Schengener Informationssystem (SIS) befasst (vgl. 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650). Über die zwischenzeitlich eingetretenen Veränderungen wollen wir nun berichten.

Zur Erinnerung: Rechtsgrundlage für die Ausschreibung ist das Schengener Durchführungsübereinkommen (SDÜ), namentlich dessen Artikel 99. Vergleichbare Befugnisse finden sich in den nationalen Polizeigesetzen, so auch in § 25 PolG, wobei hier an die Ausschreibung etwas geringere Anforderungen als auf internationaler Ebene gestellt werden: Während im Schengen-Raum der Betroffene im Verdacht stehen muss, außergewöhnlich schwere Straftaten zu planen oder zu begehen, fordert das Polizeigesetz eine ähnliche Prognose „nur“ hinsichtlich Straftaten mit erheblicher Bedeutung. Hier wie dort geht es aber darum, heimlich zu registrieren, wann, wo und mit wem die Zielperson angetroffen wird. Auf diese Weise lassen sich – wenn auch mehr oder weniger nur zufällig aus Anlass von Polizeikontrollen im Verkehr oder beim Grenzübertritt – Bewegungs- und Verhaltensprofile der Betroffenen anlegen. Der Vollständigkeit halber ist noch zu erwähnen, dass entsprechende Ausschreibungen auch von den Justizbehörden auf der Grundlage von § 163 e StPO angeordnet werden können, die wir bei un-

serer Prüfung jedoch ausklammerten. Unser Kontrollbesuch beim Landeskriminalamt im Jahr 2006 hatte zu Tage gefördert, dass Baden-Württemberg zum damaligen Zeitpunkt im Bundesvergleich die meisten Ausschreibungen nach Artikel 99 SDÜ, nämlich 376, vorgenommen hatte. Dies hing mit einigen „Sammelverfahren" gegen Tätergruppen, aber auch – so das Landeskriminalamt – mit polizeiinternen Vorgaben zusammen, wonach im Hinblick auf die Grenzlage des Landes Ausschreibungen zur polizeilichen Beobachtung nur ausnahmsweise regional begrenzt werden sollten. Bei unserer Überprüfung hatten wir zunächst die „Altfälle" herausgesucht, die schon länger als zwei Jahre ausgeschrieben waren; die dabei herausgefilterten 67 Fälle stammten samt und sonders aus dem Staatsschutzbereich (PB-07-Fälle). Weitere 56 Fälle aus anderen Deliktsbereichen wurden ebenfalls anhand der vorhandenen Unterlagen auf ihre rechtliche Tragfähigkeit hin überprüft. Wie seinerzeit berichtet, stießen wir bei näherer Durchsicht auf eine Reihe von Fehlern: So hatte das Landeskriminalamt beispielsweise „Kontakt- und Begleitpersonen" zur polizeilichen Beobachtung (auf nationaler wie auf internationaler Ebene) ausgeschrieben, obwohl diese Möglichkeit rechtlich nicht vorgesehen ist. Vielfach wurden Ausschreibungen ohne allzu kritische Prüfung von Jahr zu Jahr verlängert, ohne dass eine außergewöhnlich schwere Straftat in Sicht kam. Generell wurde – wie sich an den verwendeten Ausschreibungsformularen zeigte – auch nicht hinreichend beachtet, dass die Ausschreibungen nach Artikel 99 SDÜ strengeren Anforderungen unterliegen als diejenigen nach § 25 PolG.

Das Landeskriminalamt hat damals auf die Kritikpunkte reagiert, die groben Fehler abgestellt und einige Verbesserungen in den Ausschreibungsformularen vorgenommen. Im Zuge der erforderlichen Überprüfung der Datenspeicherungen wurden etliche Ausschreibungen gelöscht, sodass zum Stichtag 16. Oktober 2006 noch 315 Personen in den nationalen Systemen und im Schengener Informationssystem ausgeschrieben waren, davon 66 nur in den nationalen Systemen. Von den ursprünglich im Staatsschutzbereich gespeicherten 118 Personen wurden bis dato 67 Personen gelöscht. In einigen Punkten wollte das Landeskriminalamt zunächst nicht nachgeben: So hatten wir gefordert, dass alle Ausschreibungen im Schengener Informationssystem gezielt darauf überprüft werden müssten, ob die ausgeschriebene Person tatsächlich eine außergewöhnlich schwere Straftat begangen hat oder plant. Das Landeskriminalamt wollte damit zuwarten, weil sich abzeichnete, dass die strengen Anforderungen des Schengener Durchführungsübereinkommens im Zuge der Erweiterung des Schengen-Raums und in Verbindung mit der Weiterentwicklung des Schengener Informationssystems zu einem SIS II möglicherweise abgesenkt werden könnten. Nachdem SIS II weiter auf sich warten lässt und voraussichtlich nicht vor Ende 2008 eingeführt werden wird, hat das Landeskriminalamt nach einigem Hin und Her nun offenbar die gewünschte Einzelfallprüfung vorgenommen. Denn es hat uns zum Stichtag 20. Juli 2007 schließlich bestätigt, dass sämtliche Ausschreibungen nach Artikel 99 SDÜ mittlerweile die strengeren Anforderungen dieser Vorschrift erfüllten. Außerdem wurde eine weitere deutliche Reduzierung der Zahl der Ausschreibungen vermeldet: Danach waren zu dem genannten Datum insgesamt noch 74 Personen zur verdeckten Registrierung im Schengener Informationssystem gespeichert, davon wurden 22 Anordnungen durch Justizbehörden nach § 163 e StPO veranlasst, die übrigen aus präventiv-polizeilichen Gründen durch das Landeskriminalamt. Im Staatsschutzbereich gab es mittlerweile keine polizeilichen Ausschreibungen nach Artikel 99 SDÜ mehr, sondern ausschließlich nur noch solche, die durch die Justiz veranlasst worden waren. Insgesamt – so lässt sich konstatieren – hat unser Kontrollbesuch im Jahr 2006 damit zu einer nicht unerheblichen Bereinigung der Ausschreibungspraxis baden-württembergischer Polizeidienststellen geführt.

7. Einzelfälle

7.1 Mausklick mit Folgen – Vertrauliche Informationen zur Terrorbekämpfung landen bei der Presse

Risiko und Nutzen liegen nur in wenigen Bereichen so dicht beisammen wie bei der Benutzung eines Computers, wovon auch jeder Laie

ein Lied singen kann. Einerseits ist der Computer zum unentbehrlichen Hilfsmittel bei der täglichen Korrespondenz, bei der Erstellung von Schriftstücken und bei der Recherche im Internet geworden. Andererseits ist die Gefahr der Fehlbedienung mit unter Umständen fatalen Folgen stets präsent. Wie oft werden in mühevoller Arbeit erstellte Dokumente durch einen unbeabsichtigten Klick auf die Tastatur oder die Computermaus gelöscht, wie leicht erfolgt der vorzeitige Versand von im Postausgang vergessenen Entwürfen per E-Mail. Das mag im Privatbereich manchmal ärgerlich bis peinlich sein. Im öffentlichen oder geschäftlichen Bereich können die Folgen gravierender sein, wie folgender Zwischenfall zeigt.

Aus der Presse erfuhren wir, dass ein Dienstgruppenführer eines Polizeireviers am 7. September 2007 Informationen, die für Zwecke der Terrorbekämpfung an andere Dienstgruppenangehörige übermittelt werden sollten und zum Teil als vertraulich eingestuft waren, offenbar aus Versehen an rd. 60 Empfänger des Presseverteilers der Polizeidirektion verschickt hatte. Unter den versandten Dokumenten sollten sich nach den Zeitungsmeldungen eine aktuelle Lagebeurteilung (unter Nennung von terrorverdächtigen Personen), eine 16-seitige Liste gefährdeter Einrichtungen, Informationen über laufende Observationen sowie Einsatzpläne befunden haben. Obwohl die Presse fairerweise die vertraulichen Einzelheiten für sich behielt, führten die Andeutungen über die brisanten Inhalte zu einem bundesweiten Medienecho. Auch bei der Polizei löste der Vorfall hektische Betriebsamkeit aus. Die Polizeidirektion kündigte umgehend eine umfassende interne Untersuchung des Vorfalls an, und das Innenministerium beauftragte noch am selben Tag das zuständige Regierungspräsidium, Landespolizeidirektion, straf- und disziplinarrechtliche Ermittlungen gegen den verantwortlichen Beamten aufzunehmen. Es war auch zu hören, dass eine polizeiinterne Arbeitsgruppe eingerichtet worden sei, um künftig ähnliche Missgeschicke zu verhindern.

Da nach den Presseberichten davon auszugehen war, dass die versandten Dokumente auch personenbezogene Daten enthielten, baten wir die Polizeidirektion um eine Auskunft über den genauen Ablauf der folgenreichen Panne. Die Stellungnahme machte deutlich, dass die verhängnisvolle Fehlbedienung auch systembedingte Ursachen hatte und deshalb kein Einzelfall bleiben muss. Was war geschehen? Der besagte Dienstgruppenführer – nennen wir ihn D – sichtete zu Beginn seiner Schicht im Dienstgruppenleiterzimmer des Polizeireviers zunächst die in seinem dienstlichen E-Mail-Postkorb seit dem letzten Dienst (Nachtdienst am 4. September 2007) eingegangenen E-Mails. Darunter befanden sich u. a. als „VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD) eingestufte E-Mails bzw. E-Mail-Anhänge wie eine Lagebeurteilung einer gemeinsamen Ermittlungsgruppe von Bund und Ländern beim Bundeskriminalamt nach der Festnahme mutmaßlicher islamistischer Terroristen im Sauerland am 4. September 2007 (mit den Personalien der Tatverdächtigen), der hieraus resultierende Einsatzbefehl mit einer Liste anschlagsgefährdeter US-Objekte in Baden-Württemberg sowie eine Information zum Besuch des Ministerpräsidenten bei einer Firma am 8. September 2007 in Immenstaad. Auch die übrigen, nicht als vertraulich eingestuften Mitteilungen enthielten etliche personenbezogene Informationen, z. B. über Tatverdächtige, Beschuldigte und vermisste Personen. D wollte nun eine Auswahl der vorgefundenen E-Mails, darunter auch die als Verschlusssache eingestuften Nachrichten, per E-Mail an die dienstlich-persönlichen E-Mail-Adressen der übrigen Mitarbeiter seiner Dienstgruppe weiterleiten. Zu diesem Zweck beabsichtigte er, einen entsprechenden E-Mail-Verteiler aus dem Adressbuch des auf seinem Rechner für die E-Mail-Funktionen installierten Programms (Microsoft Office Outlook 2003) zu verwenden. In diesem Outlook-Adressbuch des Computers waren seinerzeit insgesamt 83 E-Mail-Verteiler der Polizeidirektion, u. a. bis auf die Ebene der Dienstgruppen, eingerichtet. Die E-Mail-Adresse des gewünschten Verteilers der Dienstgruppe lautete dabei „VT VN Prev FN Dgr A (pers)“; hinter dieser Adresse sind die E-Mail-Adressen aller

dienstlich-persönlichen Postkörbe aller Angehörigen der Dienstgruppe A des Polizeireviers hinterlegt. Da D diesen Verteiler in der Vergangenheit regelmäßig nutzte, reichte es nach Angaben der Polizeidirektion aus, im Anschriftenfeld der zu versendenden E-Mail nur den Buchstaben „V“ einzugeben, woraufhin MS-Outlook in einem aufklappenden Fenster umgehend mehrere, von D bereits benutzte E-Mail-Adressen anzeigte, die u. a. den Buchstaben „V“ enthielten. Diese oft nützliche „Auto-Vervollständigen-Funktion“ von MS-Outlook entwickelte in diesem Fall allerdings eine verhängnisvolle Wirkung. Denn unter den angezeigten E-Mail-Verteilern befand sich auch der von D gelegentlich genutzte „Presseverteiler“ der Polizeidirektion mit der Kurzbezeichnung „ZZZ VT FN PD Presse täglich“. Im Unterschied zu allen anderen E-Mail-Verteilern war für diesen Verteiler bewusst die Anfangskennung „ZZZ“ gewählt worden, um Verwechslungen mit anderen E-Mail-Verteilern im Outlook-Adressbuch der Polizeidirektion auszuschließen. D wählte nun – offenbar versehentlich und möglicherweise durch den Dienstbetrieb in dem danebenliegenden Wachraum abgelenkt – aus den angebotenen Verteileradressen statt der Adresse seines Dienstgruppenverteilers den Verteiler für die Presse aus; es bedurfte lediglich eines kurzen Mausklicks auf den Schaltknopf „Senden“ und schon beförderte er die E-Mail mit den brisanten Dokumenten ungehindert an 67 in- und ausländische Medien (inkl. zwölf österreichische und zwei Schweizer Medien), die im E-Mail-Presseverteiler enthalten waren. D bemerkte das Versehen auch nach Versand zunächst nicht. Erst als sich kurz darauf die ersten Empfänger bei der Polizeidirektion meldeten, wurde ihm die verhängnisvolle Fehlbedienung bewusst.

Die Polizeidirektion hat in ihrer umfangreichen Stellungnahme, die auch eine Dokumentation der an die Presse verschickten E-Mails einschloss, ein vorsätzliches Fehlverhalten von D ausgeschlossen. Sie hat die Gründe dargelegt, warum D zur Verwendung des Presseverteilers grundsätzlich berechtigt war und warum derartige Nachrichten an die übrigen Mitarbeiter der Dienstgruppe zu gehen haben: D habe als Dienstgruppenführer im sog. „Leitrevier“ der Polizeidirektion den Auftrag gehabt, an Wochenenden und Feiertagen den Pressebericht der Polizeidirektion an die Adressen des Presseverteilers zu versenden. Deshalb hatte ihm auch MS-Outlook diesen Verteiler mit Hilfe der „Auto-Vervollständigen-Funktion“ angeboten. Die Information aller Dienstgruppenangehörigen über die zuvor von der Polizeidirektion an alle Revierleitungen verschickten Nachrichten habe den Zweck verfolgt, alle Mitarbeiter auf den gleichen Informationsstand zu bringen, und der Führungsverantwortung von D entsprochen. Ob wirklich alle Dienstgruppenangehörigen alle der verschickten Informationen benötigt hätten, kann letztlich dahingestellt bleiben, denn man wird den polizeilichen Vorgesetzten einen fachlichen Beurteilungsspielraum zubilligen müssen, welche Informationen sie an ihre Mitarbeiter weiterleiten und welche nicht.

Aus meiner Sicht ist zu dem Vorfall zunächst festzuhalten, dass es sich um einen gravierenden datenschutzrechtlichen Verstoß gehandelt hat. Von einer Beanstandung habe ich jedoch abgesehen, da D nicht vorsätzlich handelte und die Polizei umgehend Gegenmaßnahmen ergriff. Nachdem das Kind bereits in den Brunnen gefallen war, hat uns naturgemäß mehr interessiert, wie die Polizeidirektion auf die Tücken des E-Mail-Programms MS-Outlook reagierte, weil die von diesem Programm angebotenen Funktionen auch auf den anderen Polizeicomputern zur Verfügung stehen und zu ähnlichen Fehlbedienungen führen können. Zunächst wurde auf Weisung der zuständigen Landespolizeidirektion der benutzte Computer von D umgehend vom Netz genommen und für weitere Untersuchungen sichergestellt, wobei zu bemerken ist, dass den Sachverhalt aufhellende Tatsachen eher auf dem E-Mail-Server als auf dem Arbeitsplatzrechner zu finden sein dürften. Noch in den Abendstunden des 7. September 2007 wurde beim bisherigen E-Mail-Presseverteiler der Polizeidirektion im Outlook-Adressbuch die Funktion „Adresse nicht in Exchange-Adresslisten anzeigen“ aktiviert, sodass dieser Verteiler bei der Erstellung von E-Mails nicht mehr ange-

zeigt und daher auch nicht mehr angewählt werden konnte. Schließlich regelte die Polizeidirektion einige Tage später in einer Dienstanweisung das Versenden von Nachrichten an die Medien; danach sollte der Versand von Presseberichten nur noch von vier PCs möglich sein. Neben den für „Öffentlichkeitsarbeit/Prävention“ zuständigen Mitarbeitern war allerdings auch weiterhin der jeweilige Dienstgruppenleiter von dem PC in seinem Dienstraum aus zum Versand an die Presse berechtigt. Die bisher auf den Rechnern angelegten Profile der Nutzer wurden außerdem gelöscht, sodass die früher verwendeten E-Mail-Verteiler nicht mehr angezeigt wurden. Die Benutzer wurden ferner angewiesen, die Outlook-Funktion „Vorschlag ähnlicher Adressfelder“ unverzüglich abzuschalten. Schließlich wurde der Presseverteiler komplett neu erstellt und erhielt auch eine neue Kennung namens „ZZZ FN Medienverteiler“, die aufgrund der oben geschilderten Maßnahme nicht mehr automatisch im Adressbuch von Outlook angezeigt wurde; vielmehr war die E-Mail-Adresse des Verteilers vollständig von Hand einzugeben. Zusätzlich wurde die Nutzung des Verteilers an eine Berechtigung gebunden. Der Versand durch einen nicht berechtigten Benutzer wird mit einer Fehlermeldung quittiert. Nach den unliebsamen Erfahrungen war es der Polizeidirektion nicht zu verdenken, dass sie die betroffenen Mitarbeiter dringlich ermahnte, vor dem Versenden eines Presseberichts noch einmal die Richtigkeit der im Adressfeld ausgewiesenen E-Mail-Adresse zu kontrollieren.

Ist nun alles in Ordnung? Was den konkreten Fall angeht, ist der Polizeidirektion zuzugestehen, dass sie rasch und zielgerichtet reagiert und die naheliegendsten Fehlerquellen abgestellt hat. Inwieweit Konsequenzen auch für andere Polizeidienststellen zu ziehen sind, würde sich – so hofften wir – aus dem angekündigten Bericht der vom Innenministerium eingesetzten polizeiinternen Arbeitsgruppe ergeben. Dieser Bericht, der uns kurz vor Redaktionsschluss unseres Tätigkeitsberichts erreichte, enthält – kurz gesagt – aber leider keine neuen Erkenntnisse, wie die falsche Adressierung zuverlässig verhindert werden kann. Lapidar wird vielmehr festgestellt, dass die Fehladressierung von E-Mails weder durch organisatorische noch durch technische Maßnahmen gänzlich verhindert werden könne. Ein Risikofaktor bleibe der die Kommunikationssysteme bedienende Mitarbeiter. Diese Feststellung ist zwar nicht falsch – aber genügt sie, um den im System liegenden Fehlerquellen beizukommen? Jedenfalls hat der Bericht die Frage, was softwareergonomisch unternommen werden kann oder könnte, damit es nicht zu Fehladressierungen kommt, nur sporadisch abgehandelt. Und damit bleibt der Bericht hinter den bei der Polizeidirektion getroffenen Maßnahmen zurück. Weder wird empfohlen, wenigstens bei besonders „gefährdeten“ Benutzern die „Auto-Vervollständigen-Funktion“ beim Ausfüllen von Adressfeldern zu deaktivieren, noch wird vorgeschlagen, besonders kritische Verteiler an Berechtigungen zu knüpfen. Die bestenfalls theoretische Maßnahme der Plausibilitätsprüfung bzw. des Abgleichs von Inhalt und Empfänger dürften die am Markt verfügbaren E-Mail-Server auf absehbare Zeit nicht unterstützen. Und ob ein Ausweichen auf andere Informationsplattformen eine Lösung ist, muss sich erst noch zeigen.

Immerhin hat der Bericht in Erinnerung gerufen, dass es bei der Polizei des Landes eigentlich zwei E-Mail-Systeme gibt: Ein „formelles“ („EPOST810“) zur Abwicklung der formellen Kommunikation nach der Polizeidienstvorschrift (PDV) 810.1, also nach bundesweit einheitlichen Standards bis auf die Ebene der Reviere. Dieses besondere Nachrichtensystem ist für die Übertragung von Nachrichten zwischen allen Behörden und Einrichtungen der Polizei zu nutzen. Selbstverständlich ist in der genannten Dienstvorschrift auch geregelt, dass in anderen Nachrichtensystemen (z. B. der Bürokommunikation) keine Daten von besonderer Schutzwürdigkeit oder Nachrichten an private Empfänger übertragen werden dürfen. Daneben besteht auch ein „nicht formelles“ E-Mail-System als Bestandteil der polizeilichen Bürokommunikation, das landesweit an jedem Computerarbeitsplatz der Polizei verfügbar ist. Hierdurch kann von jedem Arbeitsplatz via Intranet jeder landesinterne

und via Internet jeder E-Mail-Empfänger adressiert werden. Natürlich ist auch für die Benutzung der „nicht formellen“ Kommunikation geregelt, dass Daten mit besonderer Schutzwürdigkeit nicht an externe Adressen, also in Richtung des Internets, übertragen werden dürfen. Für einen Fehler wie den geschilderten ist die technische Realisierung des Mailtransports aber irrelevant, weil der Ablauf des Mailversands aus Benutzersicht bei der formellen und bei der nicht formellen Kommunikation grundsätzlich identisch ist. Außerdem können hier wie dort die (zentral oder dezentral) vorgegebenen E-Mail-Adressen und -Verteiler praktisch beliebig durch weitere interne und externe Adressen und Verteiler ergänzt werden. Dass auch zentral vergebene Namenskonventionen oder abweichende Namenskonventionen für „sensible“ Verteiler („ZZZ“) keine Fehlbedienung ausschließen können, hat der Fall hinreichend deutlich gemacht. Dass interne und externe Adressen und Verteiler in den von dem E-Mail-Programm angebotenen Adressverzeichnissen strikt zu trennen sind, sollte eigentlich selbstverständlich sein, ist es aber offenbar nicht. Möglicherweise scheut sich auch das Innenministerium, restriktiv in die umfassenden und bequemen Nutzungsmöglichkeiten des Arbeitsplatzcomputers einzugreifen. Immerhin wäre es ja denkbar, dass der Versand von E-Mails an externe Adressen technisch über eine zentrale Stelle der jeweiligen Dienststelle gesteuert wird, die den Versand freizugeben hat („Vier-Augen-Prinzip“). Der Bericht der polizeiinternen Arbeitsgruppe schließt mit der Empfehlung, zum einen die Schulung und Sensibilisierung der Mitarbeiter zu intensivieren, und zum andern, die in dem Bericht lediglich angerissenen technisch-organisatorischen Maßnahmen vom Landeskriminalamt umsetzen zu lassen. Wir sind auf das Ergebnis gespannt. Bis auf weiteres ist aber nicht auszuschließen, dass auf etlichen der von Polizeibeamten genutzten Computern trotz interner Bestimmungen auch E-Mail-Adressen, vielleicht sogar E-Mail-Verteiler ohne unmittelbaren dienstlichen Bezug existieren. Dann bedarf es nur einer kurzen Ablenkung und einer fehlenden Kontrolle dessen, was im Adressfeld steht, und schon reicht ein Mausklick, um dienstlich geheim zu haltende Daten an unerwünschte Empfänger zu versenden.

7.2 Staatsbürgerkunde mit Risiken – der geplante Besuch beim Karlsruher Verfassungsgespräch und die unerwarteten Nebenwirkungen

„Vor Risiken und Nebenwirkungen wird gewarnt“ – mit diesem Hinweis sollten vielleicht das Bundesverfassungsgericht und die Stadt Karlsruhe die seit einigen Jahren gemeinsam durchgeführte Veranstaltungsreihe „Karlsruher Verfassungsgespräch“ versehen. Diese unerwartete Erkenntnis vermittelte uns jedenfalls die Eingabe eines jungen Mannes türkischer Abstammung – nennen wir ihn A –, die uns im Sommer 2007 auf den Tisch kam. Zugleich wurde erneut unsere Erfahrung bestätigt, dass das wirkliche Leben mitunter datenschutzrechtliche Fallkonstellationen bietet, die man sich trotz aller Fantasie nicht vorstellen kann. Was war geschehen? Gewissermaßen aus Anlass des Geburtstags unseres Grundgesetzes findet seit einigen Jahren im Gebäude des Bundesverfassungsgerichts eine auch für Bürger zugängliche Veranstaltungsreihe statt, bei der die Stadt Karlsruhe als Mitveranstalter auftritt. In diesem Jahr, am 22. Mai 2007, stand die öffentliche Veranstaltung, an der neben dem Präsidenten des Bundesverfassungsgerichts, dem Ministerpräsidenten, dem Bundesinnenminister und dem Oberbürgermeister eine Reihe hochkarätiger Wissenschaftler und Verbandsvertreter teilnehmen sollten, unter dem Motto „Privatisierung öffentlicher Aufgaben – Gefahren für die Steuerungsfähigkeit des Staates und für das Gemeinwohl“. Im Internet wurde auf der Homepage der Stadt – vermutlich auch in den örtlichen Zeitungen – darauf hingewiesen, dass („maximal zwei“) Einlasskarten für Bürger (sog. Bürgerkarte) am 18. Mai, ab 8 Uhr, an der Rathauspforte gegen Vorlage des Personalausweises zu beantragen seien. Dies tat auch A, der sich zum damaligen Zeitpunkt in der Ausbildung für den mittleren Verwaltungsdienst bei der Stadt Karlsruhe befand, unter Vorlage seines Ausweises; seine Daten und die anderer Bewerber wurden dabei offenbar auf einer Liste erfasst. Ob und in welcher Form die Bewerber darauf hingewiesen wurden, dass im Zusammen-

hang mit der Vergabe der Eintrittskarten eine Überprüfung in Bezug auf „Sicherheitsbedenken“ stattfinden würde, ist nicht eindeutig geklärt. Der junge Mann erklärte uns gegenüber, er habe einen derartigen Hinweis nicht wahrgenommen, sondern sei der Meinung gewesen, dass im Hinblick auf die begrenzte Anzahl der Zuschauerplätze eine namentliche Erfassung der Veranstaltungsbesucher erforderlich sei. Das von uns später um Stellungnahme gebetene Landeskriminalamt erklärte hingegen, die Interessenten seien auf eine Überprüfung hingewiesen worden. Fest steht jedenfalls, dass die personenbezogenen Daten der Interessenten von der Bundespolizeiinspektion Karlsruhe (Einsatzabschnitt Bundesverfassungsgericht) auf polizeiliche Erkenntnisse hin überprüft wurden. Beim Abgleich der Besucherdaten mit dem Datenbestand des gemeinsamen Informationssystems der Polizeien von Bund und Ländern (INPOL-Zentral) ergab sich für A, dass er dort mit einem Falldatum registriert war. Die Bundespolizei holte nun eine Auskunft beim Polizeipräsidium Karlsruhe ein, die weitere „Treffer“ im polizeilichen Informationssystem des Landes (POLAS-BW) zu Tage förderte. Die polizeilichen Datenspeicherungen über A standen im Zusammenhang mit früheren – samt und sonders eingestellten – strafrechtlichen Ermittlungsverfahren. Die Bundespolizei äußerte daraufhin – im Rahmen eines Abstimmungsgesprächs mit zwei Mitarbeiterinnen der Stadt (Hauptamt) und des Bundesverfassungsgerichts – zunächst generelle „Sicherheitsbedenken“ gegen die Teilnahme von A an dem Verfassungsgespräch, ohne jedoch Einzelheiten offenzulegen. Die anwesende Vertreterin des Hauptamts glaubte sich daran zu erinnern, dass der junge Mann bei der Stadt beschäftigt ist, und ließ sich dies bei einem Telefongespräch mit dem Personalamt bestätigen. Dabei teilte sie dem Personalamt auch mit, dass die Bundespolizei „Sicherheitsbedenken“ gegen die Teilnahme des städtischen Mitarbeiters A an dem Verfassungsgespräch geltend gemacht habe.

Dass A bei der Stadt beschäftigt war, ließ sie dann die Bundespolizei wissen, was dort offenbar zu einem Meinungsumschwung führte, denn das Landeskriminalamt teilte uns später mit, dass „nach erneuter Würdigung der Gesamtumstände“ seitens der Bundespolizei keine Sicherheitsbedenken mehr gegen die Teilnahme von A an dem 7. Karlsruher Verfassungsgespräch erhoben worden seien. Ob die Bundespolizei dies tat, weil sie ahnte, dass es nun Ärger für den jungen Mann geben könnte, oder ob sie die Beschäftigung bei der Stadt als Beleg für seine Harmlosigkeit ansah, wissen wir nicht. Weitere Nachforschungen bei der Bundespolizei sind uns verwehrt, denn diese unterliegt bekanntlich der datenschutzrechtlichen Aufsicht des Bundesdatenschutzbeauftragten; wir haben A daher empfohlen, sich gegebenenfalls dorthin zu wenden. Wir kennen auch die Kriterien nicht, nach denen die Bundespolizei Besuchern den Zugang zum Bundesverfassungsgericht verwehrt. Soweit aus den von uns beigezogenen polizeilichen Ermittlungsakten ersichtlich, betraf das einzige „Gewaltdelikt“, das die Polizei über A gespeichert hatte und das möglicherweise Anlass für die „Sicherheitsbedenken“ war, eine nachbarschaftliche Auseinandersetzung im August 2001, also vor fast sechs Jahren, als der damals 18-jährige A von einer Nachbarin angezeigt wurde. A hatte einem anderen Nachbarn geholfen, im Hof eines Mehrfamilienhauses Altpapier zu entsorgen und zu diesem Zweck eine Tüte mit Altpapier aus einem Fenster im Obergeschoss geworfen, die die im Hof stehende Anzeigeerstatterin offenbar knapp verfehlte. Jedenfalls glaubte die Nachbarin, die mit A schon öfter Streit hatte, seinerzeit eine Absicht von A zu erkennen und zeigte den jungen Mann wegen gefährlicher Körperverletzung an. Die Staatsanwaltschaft stellte das Verfahren denn auch umgehend nach § 170 Abs. 2 StPO ein, da eine versuchte gefährliche Körperverletzung nicht nachzuweisen war. Der Bundespolizei ist zugute zu halten, dass der tatsächliche Geschehensablauf aus den dürren Zeilen der polizeilichen Datenbanken nicht ohne weiteres ersichtlich ist.

Die alarmierende Meldung, dass gegen A „Sicherheitsbedenken“ bestehen, entfaltete bei der Stadt jedenfalls eine fast schon tragisch zu nennende Wirkung. Zwar erhielt A Anfang August noch eine schrift-

liche Auskunft von der Bundespolizei, in der ihm die Umstände und Hintergründe der Sicherheitsprüfung erläutert wurden. Auf Wunsch von A teilte die Bundespolizei der Stadt telefonisch auch mit, dass die vorhandenen polizeilichen Erkenntnisse geringfügig und die Sicherheitsbedenken deshalb zurückgezogen worden seien. Die bei der Stadt bekannt gewordenen „Sicherheitsbedenken" ließen sich aber so nicht mehr aus der Welt schaffen und für A wurde nun – wie sich denken lässt – nicht mehr die Bundespolizei, sondern das Personalamt der Stadt zum Stolperstein. Denn dieses, einmal bösgläubig gemacht, wollte nun von A die Hintergründe wissen, weshalb die Bundespolizei gegen seine Teilnahme an dem Verfassungsgespräch „Sicherheitsbedenken" erhoben hatte. Im Personalgespräch wies A darauf hin, dass es sich bei den polizeilichen Erkenntnissen im Wesentlichen um Strafanzeigen im Zusammenhang mit Nachbarschaftsstreitigkeiten gehandelt habe und sämtliche Verfahren eingestellt worden seien. Mündlich sei von A – so die Stadt – bei dieser Gelegenheit zugesagt worden, einer Übermittlung der polizeilichen Daten an die Stadt bzw. einer Akteneinsicht bei den Strafverfolgungsbehörden zuzustimmen. Nachdem eine entsprechende schriftliche Einverständniserklärung nicht einging, erklärte das Personalamt Anfang September 2007 in einem Schreiben an den Anwalt des jungen Mannes, dass dieser nicht weiterbeschäftigt werden könne. Der Dienstherr habe nämlich u. a. zu prüfen, ob ein Bewerber (auf Übernahme in das Beamtenverhältnis) die Gewähr dafür bietet, dass er jederzeit für die freiheitlich-demokratische Grundordnung eintritt und die Befähigung zur Bekleidung öffentlicher Ämter besitzt. Das lasse sich ohne Kenntnis der Gründe für die besagten „Sicherheitsbedenken" der Bundespolizei nicht abschließend beurteilen. Die Stadt sei als Arbeitgeber befugt, sich im Zusammenhang mit der Übernahme in ein Beschäftigungsverhältnis ein eigenes umfassendes Bild über einen Bewerber zu verschaffen. Die Öffentlichkeit messe das Verhalten der städtischen Mitarbeiter mit einem strengeren Maßstab als das anderer Staatsbürger. Die Stadt erwarte deshalb von allen städtischen Mitarbeitern ein einwandfreies inner- und außerdienstliches Verhalten. Da A die entstandenen Bedenken nicht ausgeräumt und die erbetene Einverständniserklärung zur Einsicht in die Polizeiunterlagen nicht erteilt habe, bestehe seitens der Stadt auch keine Verpflichtung, ihn nach Ende der Ausbildung zu übernehmen. Das Ausbildungsverhältnis ende daher mit dem letzten Prüfungstag am 19. September 2007. Da A bis dahin das Verhältnis zu seinem Arbeitgeber nicht unnötig belasten wollte, hatte er uns zunächst gebeten, von uns aus nicht auf die Stadt zuzugehen. Erst als er den besagten „blauen Brief" erhielt, stimmte er zu, dass wir endlich eine Stellungnahme der Stadt einholen. Anlass zu kritischen datenschutzrechtlichen Fragen und Anmerkungen bietet der Fall nämlich reichlich:

– Vorab ist klarzustellen: Dass die Polizei befugt ist, Informationen über strafrechtliche Ermittlungsverfahren – auch über eingestellte Verfahren – zu speichern, wenn ein Tatverdacht und eine Wiederholungsgefahr anzunehmen sind, ist unstreitig und ergibt sich aus dem Polizeirecht (vgl. § 38 PolG). Mit Ausnahme eines Vorfalls, der nach unserer Intervention aus dem polizeilichen Datenbestand gelöscht wurde, waren die Datenspeicherungen über A – nicht zuletzt in Folge der großzügigen gesetzlichen Voraussetzungen der polizeilichen Speicherpraxis – datenschutzrechtlich zulässig. Sie sind, obwohl Auslöser der Ereignisse, für die im Mittelpunkt stehenden Fragen der Datenübermittlung zwischen den Beteiligten jedoch nur am Rande von Bedeutung.

– Unstreitig ist ebenfalls, dass die Bundespolizei bzw. das Bundeskriminalamt den Personen- und Objektschutz für die Verfassungsorgane (also auch das Bundesverfassungsgericht) zu gewährleisten haben und dabei gegebenenfalls auch Besucher der Gebäude auf sicherheitsrelevante Vorerkenntnisse überprüfen dürfen. Ob Taschenkontrollen und Sicherheitsschleusen – wie etwa für den Zugang zur Besuchertribüne des Deutschen Bundestags – reichen oder ob man auch das Vorleben der Besucher erforschen muss, unterliegt der fachlichen

Beurteilung der Bundespolizei. Generell ist hierzu noch zu sagen, dass der Abgleich personenbezogener Daten mit dem Inhalt von Dateien, die das Bundeskriminalamt (bzw. die Bundespolizei zu dessen Unterstützung) zur Aufgabenerledigung benötigt (z. B. INPOL), in § 28 Abs. 1 des Gesetzes über das Bundeskriminalamt (BKAG) geregelt ist; zur Wahrnehmung seiner Aufgaben nach § 5 BKAG können die Polizeidienststellen des Bundes selbstverständlich auch Anfragen an Polizeidienststellen der Länder richten und sich personenbezogene Daten aus den dortigen Dateien übermitteln lassen (vgl. § 24 BKAG).

– Inwieweit die Übermittlung von „Sicherheitsbedenken“ bezüglich bestimmter Besucher durch die Bundespolizei an die Vertreterin der Stadt zulässig war, ist von uns mangels Zuständigkeit nicht zu prüfen. Generell darf das Bundeskriminalamt unter gewissen Voraussetzungen – u. a. zur Erfüllung seiner Aufgaben oder zum Zweck der Gefahrenabwehr (vgl. § 10 Abs. 2 Nr. 1 und 3 BKAG) – personenbezogene Daten nicht nur an die Polizeien der Länder, sondern auch an andere öffentliche Stellen – hierzu würde auch die Stadtverwaltung Karlsruhe gehören – übermitteln. Da die Stadt Mitveranstalterin war und offenkundig die Zulassung von Besuchern (mit) zu organisieren hatte, ist nicht auszuschließen, dass die Datenübermittlung Zwecken der Gefahrenabwehr dienen sollte. Die Stadt hat uns gegenüber inzwischen erklärt, sie habe sich nur nach den Vorgaben der Bundespolizei gerichtet. Offen bleibt, ob die Bundespolizei nicht auch ohne Benachrichtigung der Stadt in der Lage gewesen wäre, „bedenkliche“ Besucher zurückzuweisen. Zumindest wäre es datenschutzrechtlich vorteilhafter gewesen, wenn die Bundespolizei den Betroffenen selbst – wie später auch geschehen – über die vorhandenen Bedenken im Wege der Anhörung unterrichtet und ihm auf diese Weise sogar Gelegenheit gegeben hätte, diese auszuräumen.

– Das Landeskriminalamt hat besonders hervorgehoben, dass der Stadt keine Einzelheiten zu den polizeilichen Vorerkenntnissen über A mitgeteilt worden seien, sondern generell (nur) von „Sicherheitsbedenken“ die Rede gewesen sei. Damit sollte offenbar der Eindruck erweckt werden, es seien keine spezifischen personenbezogenen Daten übermittelt worden und die datenschutzrechtliche Relevanz sei dementsprechend zu vernachlässigen. Falls das gemeint sein sollte, so ist dem deutlich zu widersprechen: Auch die (allgemeine) Mitteilung, dass bezüglich einer bestimmten Person „Sicherheitsbedenken“ bestehen, stellt die Übermittlung eines personenbezogenen Datums dar. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (jeweils § 3 Abs. 1 LDSG und BDSG). Die Bundespolizei hat offenkundig der Vertreterin der Stadt zumindest den Namen, verbunden mit der Aussage, dass in Bezug auf A „Sicherheitsbedenken“ bestünden, genannt. In Bezug auf den Namen geht es eindeutig um personenbezogene Daten, aber ebenso bei der hiermit verknüpften Aussage hinsichtlich angeblicher „Sicherheitsbedenken“. Ob der Begriff „Sicherheitsbedenken“ eine Tatsachenbehauptung oder ein Werturteil darstellt, kann letztlich dahingestellt bleiben. Personenbezogene Daten lassen sich nämlich nicht nur auf Informationen tatsächlicher Art verengen; auch Werturteile dienen der Darstellung persönlicher und sachlicher Verhältnisse einer Person und gehören daher zu den „Angaben“ im Sinne der gesetzlichen Definition. Dass ein Werturteil die einzelnen tatsächlichen Elemente, auf denen es aufbaut, nicht erkennen lässt, ändert nichts daran, dass es etwas über die „Verhältnisse“ des Betroffenen „angibt“. Der schlichte Hinweis, dass in Bezug auf A „Sicherheitsbedenken“ bestehen, war daher datenschutzrechtlich durchaus relevant, wegen der lapidaren Formulierung, die gerade deshalb Anlass zu Spekulationen geben konnte, vielleicht sogar mehr, als es eine detaillierte Auflistung der eingestellten Ermittlungsverfahren je gewesen wäre.

– Unterstellt, das Hauptamt wäre befugt gewesen, die durch die Bundespolizei erhaltene Information aus Gründen der Gefahrenabwehr bei

der Besucherzulassung zum „Verfassungsgespräch“ zu verwenden, schließt sich die Frage an, ob diese Information innerhalb der Stadtverwaltung für andere Zwecke weitergegeben werden durfte. In diesem Zusammenhang ist daran zu erinnern, dass das Datenschutzrecht grundsätzlich von einer strikten Zweckbindung der Datenverarbeitung geprägt ist. Diese Zweckbindung gilt auch in funktionaler Hinsicht innerhalb derselben Körperschaft, sodass die Informationserhebung und -nutzung auch innerhalb einer Stadtverwaltung nach dem jeweiligen Zweck der Aufgabenerfüllung strikt zu trennen ist. Dies bedeutet: Eine Weitergabe der personenbezogenen Daten an eine andere Stelle innerhalb derselben Organisation ist nur zulässig, soweit eine gesetzliche Vorschrift dies erlaubt oder der Betroffene einwilligt. Eine Einwilligung von A lag erkennbar nicht vor, eine gesetzliche Befugnis vermögen wir ebenfalls nicht zu erkennen.

– An dieser Stelle sei der Hinweis gestattet, dass dem Dienstherrn eines Beamten Informationen aus (eingestellten) strafrechtlichen Ermittlungsverfahren nicht unbekannt bleiben müssen, weil sie ihm unter gewissen Voraussetzungen, insbesondere nach Maßgabe der §§ 12, 14 des Einführungsgesetzes zum Gerichtsverfassungsgesetz (EGGVG) in Verbindung mit Nr. 15 der Anordnung über Mitteilungen in Strafsachen (MiStra) durch einen Richter oder Staatsanwalt mitzuteilen sind (Nr. 15 Abs. 3 Satz 4 MiStra). Danach unterbleibt bei eingestellten strafrechtlichen Ermittlungsverfahren die Übermittlung, soweit nicht besondere Umstände des Einzelfalls die Übermittlung erfordern; dies ist insbesondere dann der Fall, wenn die Tat bereits ihrer Art nach geeignet ist, Zweifel an der Zuverlässigkeit oder Eignung des Betroffenen für die gerade von ihm ausgeübte berufliche Tätigkeit hervorzurufen (§ 14 Abs. 2 EGGVG). Nr. 15 Abs. 3 Satz 1 MiStra konkretisiert diese Übermittlungspflicht hinsichtlich der Beamten. Danach sollen Informationen über Verfahrenseinstellungen übermittelt werden, wenn die Kenntnis der Daten aufgrund der Umstände des Einzelfalls erforderlich ist, um zu prüfen, ob dienstrechtliche Maßnahmen zu ergreifen sind; dabei ist zu berücksichtigen, wie gesichert die zu übermittelnden Erkenntnisse sind. Zwei Aspekte sprechen allerdings gegen die Anwendbarkeit dieser Vorschriften im vorliegenden Fall: Zum einen geht es bei den genannten Vorschriften um die Übermittlung aktueller Informationen aus einem gerade abgeschlossenen Ermittlungsverfahren und nicht um längere Zeit zurückliegende Verfahren. Zum andern ist eine entsprechende Mitteilung von einem Richter oder Staatsanwalt anzuordnen (vgl. Nr. 15 Abs. 3 Satz 4 MiStra). Dass die Polizei (von sich aus) den Dienstherrn eines Beamten in gleicher Weise über eingestellte Strafverfahren unterrichten darf, vermögen wir nicht zu erkennen. Dementsprechend dürfte auch die „Umwidmung“ der von der Bundespolizei erhaltenen Informationen in Form der Weiterleitung an das Personalamt der Stadt datenschutzrechtlich bedenklich gewesen sein.

– Zu dem Auskunftsverlangen der Stadt gegenüber A ist zu sagen: Üblicherweise geht ein öffentlicher Arbeitgeber anders vor. Er pflegt ein Führungszeugnis einzuholen und mit Hilfe eines Personalfragebogens den Bewerber nach laufenden strafrechtlichen Ermittlungsverfahren zu befragen. Diese Datenerhebung hatte bei A jedoch keine Erkenntnisse geliefert, da weder laufende Ermittlungsverfahren anhängig waren noch sein Führungszeugnis einen Eintrag aufwies. Inwieweit A um weitere Informationen über die eingestellten Ermittlungsverfahren gebeten werden durfte, ist zweifelhaft. Einerseits braucht sich der Dienstherr nicht künstlich „dumm“ zu stellen und darf Informationen nachgehen, die Zweifel an der Eignung und Befähigung eines Bewerbers wecken könnten. Auf der anderen Seite hat der Gesetzgeber mit der Regelung in § 53 des Bundeszentralregistergesetzes eine gewisse Wertung getroffen, in welchem Umfang strafrechtlich relevante Vorkommnisse Einfluss im Rechtsverkehr haben dürfen. Nach dieser Vorschrift kann sogar ein Verurteilter nicht gezwungen werden, getilgte oder nicht in das Führungszeugnis aufzunehmende Straftaten zu offenbaren; was hinsichtlich

rechtskräftiger Strafurteile gilt, wird erst recht für eingestellte Ermittlungsverfahren zu gelten haben. Letztlich ist die Frage, was ein Bewerber offenbaren muss, jedoch nach den Maßstäben des Beamtenrechts zu prüfen. Der entscheidende Gesichtspunkt des vorliegenden Falls ist jedoch, dass A die Stadt nicht zwingen kann, die einmal erlangte Information als nichtexistent zu betrachten und ihn in ein Beschäftigungsverhältnis zu übernehmen.

Wie geht es weiter? Mittlerweile hat sich das Regierungspräsidium Karlsruhe, das wir ebenfalls über unsere datenschutzrechtliche Bewertung informiert haben, als Rechtsaufsichtsbehörde eingeschaltet. Die Stadt hat uns gegenüber inzwischen eingeräumt, dass es für die Mitteilung der „Sicherheitsbedenken" an das Personalamt in der Tat keine Rechtsgrundlage gegeben habe. Die Mitarbeiterin habe A auf diese Weise die Teilnahme an dem Verfassungsgespräch ermöglichen wollen. Dies habe auch geklappt, denn die Bundespolizei habe die Sicherheitsbedenken zurückgezogen, als sie erfuhr, wer der Arbeitgeber des jungen Mannes ist. Logisch ist das nicht. Selbst dann, wenn die Mitarbeiterin des Hauptamts sich nur beim Personalamt hätte vergewissern wollen, ob A bei der Stadt beschäftigt ist (was sie nach A's Meinung ohnehin schon wusste), wäre es nicht erforderlich gewesen, das Personalamt über die „Sicherheitsbedenken" der Bundespolizei zu unterrichten. Hinzu kommt, dass es für die Vergabe der „Bürgerkarten" natürlich nicht darauf ankam, ob ein Bewerber bei der Stadt tätig war oder nicht. Ob es hinsichtlich der Berufsaussichten des jungen Mannes bei der Stadt Karlsruhe doch noch zu einem Happy End kommen wird, ist aus unserer Sicht zweifelhaft, denn die Stadt hat uns wissen lassen, dass die Nichtübernahme von A primär (!) „aufgrund mangelnder fachlicher Leistungen und persönlicher Eignung" erfolgte und weil A gegebene Zusagen nicht einhielt. Über das, was sich „sekundär" im Hinterkopf der Entscheidungsträger abspielte, kann man nur spekulieren. Jedenfalls fällt mir bei dieser Erklärung der Stadt nur ein bekanntes französisches Sprichwort ein: Honi soit qui mal y pense.

7.3 Die voreilige Fehlerbeseitigung

Dass die Behörden auf unsere Anfragen reagieren, vorhandene Datenspeicherungen selbstkritisch prüfen und Fehler umgehend abstellen, sollte eigentlich eine Selbstverständlichkeit sein, ist es aber nicht immer. Leider allzu oft zieht sich die argumentative Auseinandersetzung um die Berechtigung einer Datenspeicherung über Wochen und Monate hin. Manchmal kann es aber auch unerwartet schnell gehen, ja sogar zu schnell, wie wir im Juli 2007 im Zusammenhang mit einer Eingabe aus dem Enzkreis erleben mussten. Ein junger Mann hatte sich an unsere Dienststelle mit der Bitte um Prüfung gewandt, ob und welche Daten über ihn von der Polizei gespeichert werden. Er werde bei Verkehrskontrollen immer wieder angehalten und auf frühere Rauschgiftdelikte angesprochen. Gelegentlich müsse er dabei sogar Urinproben abliefern, selbst wenn er sich in der Begleitung von Verwandten und Bekannten befinde. Dabei habe er sich nichts zuschulden kommen lassen; auch sei gegen ihn nie ein strafrechtliches Ermittlungsverfahren angestrengt worden.

Nun darf die Polizei zwar die ihr aus strafrechtlichen Ermittlungsverfahren bekannt gewordenen Daten nach § 38 PolG speichern, wenn ein Tatverdacht und die Gefahr der Wiederholung besteht. Für den Tatverdacht muss dabei keine rechtskräftige Verurteilung vorliegen, sondern es reicht gegebenenfalls sogar aus, wenn das Ermittlungsverfahren gegen den Betroffenen eingestellt und der Tatverdacht dabei nicht völlig ausgeräumt worden ist. Aber dass personenbezogene Daten ohne ein Ermittlungsverfahren gespeichert und zum Anlass für verschärfte Kontrollen gemacht werden, ist gewiss atypisch. Umso mehr waren wir gespannt zu erfahren, ob und aus welchem Grund die zuständige Polizeidirektion den jungen Mann im polizeilichen Auskunftssystem des Landes (POLAS-BW) erfasst hatte. Leider blieb uns diese Erkenntnis verwehrt, denn die um Auskunft gebetene Polizeidirektion teilte uns in

ihrer Antwort nur lapidar mit, dass die POLAS-Daten des jungen Mannes zwischenzeitlich gelöscht und die zugehörigen Akten vernichtet worden seien. Vermutlich war erst aufgrund unserer Anfrage festgestellt worden, dass die Datenspeicherung fehlerhaft war. Angesichts vollendeter Tatsachen blieb uns nichts anderes übrig, als dem jungen Mann das – für ihn positive – Ergebnis mitzuteilen.

So löblich es jedoch ist, einen offenbar rechtswidrigen Zustand umgehend zu beenden, so misslich ist die rasche Datenlöschung und Aktenvernichtung sowohl für die Auskunftsrechte des Betroffenen als auch für unser Kontrollrecht gewesen. Immerhin wäre es interessant gewesen zu erfahren, wie und auf welcher Rechtsgrundlage es überhaupt zu der Datenspeicherung gekommen war. Dies haben wir auch die Polizeidirektion wissen lassen und außerdem das Innenministerium gebeten, dafür zu sorgen, dass die Polizeidienststellen künftig unzulässig gespeicherte Daten bis zum Abschluss unserer Ermittlungen allenfalls sperren und erst anschließend die Unterlagen in Absprache mit uns vernichten. Das Innenministerium hat erfreulich rasch reagiert und die nachgeordneten Dienststellen entsprechend angewiesen. Es bleibt abzuwarten, ob im polizeilichen Alltag auch so verfahren wird oder ob nicht ab und an der Wunsch stärker ist, Fehler sofort zu beseitigen, bevor es zur kritischen Nachschau durch uns kommt.

7.4 Leibesvisitation wegen der Verletzung von Dienstgeheimnissen

Wenn die Polizei an einem Tatort Spuren (z. B. Fingerabdrücke) findet, dann darf sie beim Tatverdächtigen zur Identitätsfeststellung eine erkennungsdienstliche Behandlung durchführen, um ihn überführen oder den Tatverdacht ausschließen zu können. Diese allgemein bekannte Befugnis ergibt sich aus § 81 b der Strafprozessordnung (StPO). In demselben Paragrafen ist aber noch eine weitere Alternative geregelt, wonach eine erkennungsdienstliche Behandlung des Beschuldigten auch für Zwecke des Erkennungsdienstes, das heißt zur vorbeugenden Verbrechensbekämpfung, zulässig ist. Die entsprechenden Daten des Beschuldigten bleiben dann eine Weile zentral gespeichert, um Spuren, die bei künftigen Delikten aufgefunden werden, rasch mit den erkennungsdienstlichen Daten des Betroffenen abgleichen zu können; die Ermittlungstätigkeit der Strafverfolgungsbehörden wird so wesentlich erleichtert. Diese Regelung stellt eigentlich materielles Polizeirecht dar und bildet einen Fremdkörper in der Strafprozessordnung. Es liegt auf der Hand, dass die prophylaktische Speicherung von Lichtbildern und Fingerabdrücken im Vergleich zu der Identifizierung eines konkreten Tatverdächtigen strengeren Voraussetzungen unterliegt. Erkennungsdienstliche Behandlungen zu präventiv-polizeilichen Zwecken kommen in Betracht, wenn – unter Berücksichtigung aller Umstände des Einzelfalls, also insbesondere von Art, Schwere und Begehungsweise der zur Last gelegten Straftat – Anhaltspunkte dafür vorliegen, dass der Beschuldigte in ähnlicher oder anderer Weise erneut straffällig werden könnte; dies wird in erster Linie bei Gewohnheitstätern der Fall sein. Ferner müssen die erkennungsdienstlichen Unterlagen zur Förderung der dann zu führenden Ermittlungen geeignet erscheinen. Außerdem muss eine erkennungsdienstliche Behandlung verhältnismäßig sein, das heißt sie darf zum Anlassdelikt nicht außer Verhältnis stehen. Die Polizeigesetze enthalten ähnliche Regelungen, die erkennungsdienstliche Behandlungen für einen größeren Personenkreis – z. B. auch für Schuldunfähige und Strafunmündige – zulassen (vgl. § 36 PolG). Die Anordnung einer erkennungsdienstlichen Behandlung stellt übrigens einen Verwaltungsakt dar, gegen den sich der Betroffene mit den Mitteln des Widerspruchs oder der verwaltungsgerichtlichen Klage zur Wehr setzen kann. Viele Betroffene bringen allerdings nicht den Mut auf, von der Polizei zunächst einmal eine schriftliche Anordnung zu verlangen, wenn sie zu einer erkennungsdienstlichen Behandlung vorgeladen werden. Manchmal wäre etwas mehr Widerstand durchaus angebracht, wie der folgende Fall zeigt.

Eine Polizeidirektion hatte gegen eine Frau seit 2005 ein strafrechtliches Ermittlungsverfahren u. a. wegen des Vorwurfs der Verletzung

von Dienstgeheimnissen durchgeführt. Die Beschuldigte wurde verdächtigt, als Angestellte einer sozialtherapeutischen Anstalt an einen in Sicherungsverwahrung befindlichen Gefangenen und an andere Personen etwa dreißig anonyme Postkarten – zum Teil beleidigenden Inhalts – geschickt und darauf geheime Informationen aus der Akte des Gefangenen (Daten seiner Taten und Opfer) preisgegeben zu haben. Hintergrund waren möglicherweise Rachemotive, weil der Gefangene früher ein Verhältnis zu der Beschuldigten unterhalten und dieses gegen den Willen der Frau beendet hatte. Letztlich blieb unklar, ob sie wirklich die Täterin war. Zuvor war die Frau, die die Vorwürfe im Übrigen bestritt, strafrechtlich nicht in Erscheinung getreten. Im Rahmen des Ermittlungsverfahrens wurde die Beschuldigte im April 2005 umfassend erkennungsdienstlich behandelt. Dabei wurden auch körperliche Merkmale, insbesondere Narben im Bereich des Bauchs, in Augenschein genommen und im Protokoll festgehalten. Im polizeilichen Auskunftssystem (POLAS-BW) wurden indessen diese Angaben nicht gespeichert. Das strafrechtliche Ermittlungsverfahren wurde von der zuständigen Staatsanwaltschaft Ende August 2006 nach § 170 Abs. 2 StPO eingestellt; in der Begründung hieß es, dass bereits die objektive Verwirklichung der Straftatbestände der Verletzung von Dienstgeheimnissen nach § 353 b des Strafgesetzbuchs (StGB) oder der Verletzung von Privatgeheimnissen nach § 203 StGB fraglich sei. Jedenfalls sei der Tatnachweis nicht mit der erforderlichen Sicherheit zu führen. Hinsichtlich einer etwaigen Beleidigung fehle es außerdem an dem erforderlichen Strafantrag. Mit der Einstellungsverfügung der Staatsanwaltschaft in Händen wandte sich die anwaltlich vertretene Frau nun an die Polizeidirektion und verlangte die Löschung ihrer erkennungsdienstlichen Daten, außerdem legte sie eine Dienstaufsichtsbeschwerde gegen die polizeiliche Sachbearbeiterin ein, die bei ihr die erkennungsdienstliche Behandlung vorgenommen hatte. Beide Anliegen wurden von der Polizeidirektion im Dezember 2006 zurückgewiesen; weder sei der Tatverdacht gegen die Betroffene ausgeräumt noch sei die Wiederholungsgefahr gebannt. Auch sei die Anfertigung erkennungsdienstlicher Unterlagen verhältnismäßig gewesen. Die Betroffene, die sich mit dieser Entscheidung nicht abfinden wollte, legte hiergegen Widerspruch ein und wandte sich parallel dazu an unsere Dienststelle. Das mit dem Widerspruch befasste Regierungspräsidium, Landespolizeidirektion, kam im Ergebnis zu einer ähnlichen rechtlichen Beurteilung wie wir: Die fortgesetzte Datenspeicherung war angesichts der Zweifel der Staatsanwaltschaft am tatbestandsmäßigen Handeln der Beschuldigten nicht in Ordnung; damit waren auch die erkennungsdienstlichen Daten zu vernichten. Besonders abwegig war aber der Umfang der erkennungsdienstlichen Behandlung im April 2005. Die polizeiliche Sachbearbeiterin hatte im Protokoll damals säuberlich festgehalten: „Rumpf: Narbe, 10 cm, links; Bauch: Narbe, 15 cm, Mitte; Bauch: Narbe, 15 cm, rechts“. Was die Beschreibung und Vermessung nicht (ohne weiteres) sichtbarer Narben am Körper zur Aufklärung späterer Straftaten aus dem Bereich der Verletzung von Dienst- oder Privatgeheimnissen oder möglicher Beleidigungsdelikte hätten beisteuern können, wird ihr Geheimnis bleiben. Mag es noch theoretisch vorstellbar sein, dass für die spätere Überführung eines Tatverdächtigen, der anonyme Drohbriefe verfasst, die Erhebung der Fingerabdrücke hilfreich sein kann, so fehlt der logische Zusammenhang zwischen Art und Umfang der Narbenvermessung und den in Rede stehenden Deliktsarten völlig.

Eigentlich hätte die Polizeidirektion gewarnt sein müssen. Hatte doch der Verwaltungsgerichtshof Baden-Württemberg mit Urteil vom 18. Dezember 2003, 1 S 2211/02, eine von einer anderen Polizeidienststelle im Bereich der Polizeidirektion angeordnete erkennungsdienstliche Behandlung aufgehoben, bei der im Zuge einer Leibesvisitation Narben vermessen und protokolliert worden waren. Auch die seinerzeit betroffene Tatverdächtige (die allerdings bereits häufig polizeilich in Erscheinung getreten war) stand im Verdacht, Drohbriefe verfasst zu haben. Der Verwaltungsgerichtshof hatte damals zwar die erkennungsdienstliche Behandlung dem Grunde nach für zulässig erklärt, jedoch zugleich klargestellt, dass der gegen die Betroffene bestehende Tatver-

dacht nicht das Erheben von Daten zu äußerlich nicht ohne weiteres erkennbaren, unveränderlichen besonderen körperlichen Merkmalen durch Leibesvisitation rechtfertigte. Dies ergebe sich bereits aus dem Wortlaut des § 81 b 2. Alternative StPO, wonach die Maßnahmen nur zulässig sind, „soweit“ dies für die Zwecke des Erkennungsdienstes „notwendig“ ist. Bei dieser Begrenzung erkennungsdienstlicher Maßnahmen auf das notwendige Maß handle es sich um eine (einfachgesetzliche) Ausprägung des Grundsatzes der Verhältnismäßigkeit, dem der mit der Datenerhebung verbundene Eingriff in grundrechtlich geschützte Belange des Betroffenen, insbesondere in dessen Recht auf informationelle Selbstbestimmung genügen muss (vgl. bereits Bundesverwaltungsgericht, Urteil vom 9. Februar 1967, BVerwGE 26, 169, 172). Bei keinem der durchgeführten Ermittlungs- und Strafverfahren (gegen die damalige Beschuldigte) sei es jedoch von Bedeutung gewesen, ob bzw. welche unveränderlichen körperlichen Merkmale die Klägerin besitzt.

So war es aber auch in dem neuen Fall unserer Petentin, sodass das Regierungspräsidium dem Widerspruch stattgab und die Löschung veranlasste: Für die Aufklärung künftiger Straftaten der Betroffenen aus den einschlägigen Deliktsbereichen waren die Narben am Körper schlicht irrelevant. Die Polizeidirektion räumte dies uns gegenüber schließlich ebenfalls ein und erklärte, beim Landeskriminalamt auf eine Änderung der entsprechenden Vordrucke für die Anordnung der erkennungsdienstlichen Behandlung hinwirken zu wollen, damit im Feld für die Personenbeschreibung künftig deutlicher auf den Zusammenhang mit dem konkreten Delikt, dessen Wiederholung befürchtet wird, hingewiesen wird. Außerdem seien die Mitarbeiter der Polizeidirektion im Hinblick auf die rechtlichen Anforderungen bei der Durchführung erkennungsdienstlicher Behandlungen nochmals schriftlich und mündlich sensibilisiert worden. Wir haben uns inzwischen die im November 2006 vom Landeskriminalamt herausgegebenen, überarbeiteten „Erkennungsdienstlichen Richtlinien“ (ED-Richtlinien) und das angesprochene Formular besorgt, um nachzuschauen, welche Hinweise den polizeilichen Sachbearbeitern für vergleichbare Fälle an die Hand gegeben werden. Die ED-Richtlinien gelten bundesweit, werden jedoch durch landesspezifische Regelungen ergänzt. In der ergänzenden Regelung des hiesigen Landeskriminalamts wird unter Hinweis auf die oben genannte Entscheidung des VGH Baden-Württemberg mit erfreulicher Deutlichkeit betont, dass die erkennungsdienstlichen Maßnahmen auch in ihrem Umfang in jedem Einzelfall auf ihre Verhältnismäßigkeit zu prüfen sind und dass ein hinreichender Zusammenhang zwischen der Art der erhobenen Daten und der Art und Begehungsweise der vom Betroffenen künftig zu erwartenden Straftaten bestehen muss. Leider ist dem oben genannten Formular „Auftrag zur Durchführung einer erkennungsdienstlichen Behandlung/DNA-Probe“ nicht zu entnehmen, dass die Anregung der betroffenen Polizeidirektion aufgegriffen wurde: Die Rubrik „Angeordnete Maßnahme“ enthält weiterhin nur ein einziges Ankreuzfeld für die Maßnahme „Personenbeschreibung“; ein weiteres Feld kann für ein zusätzliches Lichtbild im Fall von Tätowierungen und Narben angekreuzt werden. Ein ausdrücklicher Hinweis, welchen Umfang die Personenbeschreibung haben darf, fehlt demnach. Ob die polizeilichen Sachbearbeiter im hektischen Polizeialltag beim Ausfüllen des Formulars dann jedes Mal an die ergänzenden rechtlichen Hinweise der ED-Richtlinien denken, darf bezweifelt werden.

2. Abschnitt: Justiz

1. Neue gesetzliche Bestimmungen für den Datenschutz im Strafvollzug

Mit Urteil vom 31. Mai 2006 hatte das Bundesverfassungsgericht entschieden, dass der Jugendstrafvollzug eigenständiger, auf die besonderen Anforderungen an den Strafvollzug an Jugendlichen zugeschnittener und auf das Vollzugsziel der Resozialisierung ausgerichteter Regeln bedürfe. Es müsse der Tatsache Rechnung getragen werden, dass sich Jugendliche biologisch,

psychisch und sozial in einem Stadium des Übergangs befinden. Da die gesetzgeberische Zuständigkeit im Bereich des Strafvollzugs im Zuge der ersten Stufe der Föderalismusreform zwischenzeitlich vom Bund auf die Länder übergegangen ist, standen die Landesgesetzgeber in der Pflicht, ein entsprechendes Gesetz zu schaffen, ehe die vom Bundesverfassungsgericht gesetzte Übergangsfrist am 31. Dezember 2007 abläuft. Diese Aufgabe hat das Land mit dem Erlass eines Jugendstrafvollzugsgesetzes erfüllt. Doch hat der Landesgesetzgeber noch ein Übriges getan und der landesrechtlichen Neuregelung des Jugendstrafvollzugs überdies ein „Justizvollzugsdatenschutzgesetz“ an die Seite gestellt, das auch den Datenschutz im baden-württembergischen Justizvollzug auf eine neue rechtliche Grundlage stellt.

1.1 Jugendstrafvollzugsgesetz (JStVollzG)

Der vom Justizministerium erarbeitete Entwurf eines Jugendstrafvollzugsgesetzes wurde während des Gesetzgebungsverfahrens im Landtag parteiübergreifend als grundsätzlich gelungen gelobt. Auf Kritik stießen freilich die in § 22 Abs. 2 des Entwurfs formulierten überaus ambitionierten „Behandlungs- und Erziehungsgrundsätze“ sowie die Tatsache, dass zahlreiche zentrale Bestimmungen zu den Haftbedingungen der jungen Gefangenen und zur Gestaltung des Alltags im Vollzug bewusst als bloße Ermessens- und Sollvorschriften ausgestaltet worden sind. Aus unserer dem Datenschutz verpflichteten Perspektive mussten demgegenüber andere Aspekte des Gesetzentwurfs im Vordergrund stehen. Anlass zu kritischen Anmerkungen bot dieser auch zunächst genug, denn ungeachtet des parallel konzipierten, grundsätzlich auch für den Jugendstrafvollzug einschlägigen Justizvollzugsdatenschutzgesetzes enthält das Jugendstrafvollzugsgesetz nicht wenige eigenständige datenschutzrechtliche Bestimmungen, die in ihrer ursprünglichen Fassung nicht durchweg gelungen erschienen.

Wir haben jedoch im Anhörungsverfahren mit zahlreichen Einwänden und Anregungen Gehör gefunden, sodass aus der Rückschau konstatiert werden kann, dass sich die schließlich am 27. Juni 2007 vom Landtag verabschiedete Fassung aus datenschutzrechtlicher Sicht positiv vom ersten Entwurf abhebt. Sah dieser beispielsweise noch vor, dass im Aufnahme- und Diagnoseverfahren, das bei der Neuaufnahme eines Gefangenen durchgeführt wird, alle Umstände erhoben werden dürfen, deren Kenntnis für die Erfüllung des Erziehungsauftrags und die Eingliederung nach der Entlassung „hilfreich“ sein könnten, so wird in der verabschiedeten Fassung des Gesetzes die entsprechende Datenerhebungsbefugnis der Vollzugsbehörde, wie datenschutzrechtlich geboten, auf die insoweit „erforderlichen“ Umstände beschränkt (§ 24 Abs. 2 Satz 1 JStVollzG). § 41 Abs. 3 Satz 3 JStVollzG stellt nunmehr klar, dass die vom Verteidiger des Gefangenen mitgeführten Schriftstücke und Unterlagen inhaltlich nicht überprüft werden dürfen. § 42 Abs. 1 JStVollzG trägt den verfassungsmäßigen Anforderungen an die Wahrung des Briefgeheimnisses besser als der Erstentwurf Rechnung, indem er die Überwachung des Schriftverkehrs des „jungen Gefangenen“ auf die Fälle beschränkt, in denen eine solche Maßnahme „zur Erreichung des Erziehungsauftrags (...) oder aus Gründen der Sicherheit und Ordnung der Jugendstrafanstalt erforderlich ist“. Die Aufzählung der im Detail erreichten datenschutzrechtlichen Verbesserungen ließe sich noch fortsetzen.

Allerdings fanden nicht alle unsere Einwände Berücksichtigung. Bedenken haben wir beispielsweise nach wie vor gegen eine Regelung in § 56 JStVollzG, wonach dem Gefangenen als „Bezugsperson“ anstelle eines haupt- oder ehrenamtlichen Vollzugsmitarbeiters gegebenenfalls ein „geeigneter“ junger Mitgefangener zugewiesen werden kann, der als solcher unweigerlich Kenntnis teils sensibler personenbezogener Daten des neuen Gefangenen erlangen wird. Ob ein Mitgefangener tatsächlich die notwendige Eignung als Bezugsperson besitzt, scheint doch fraglich zu sein. Dennoch wird man, alles in allem, aus datenschutzrechtlicher Sicht mit dem Jugendstrafvollzugsgesetz voraussichtlich gut leben können.

1.2 Justizvollzugsdatenschutzgesetz (JVollzDSG)

Das „Gesetz über den Datenschutz im Justizvollzug in Baden-Württemberg“, das am 27. Juni 2007 vom baden-württembergischen Landtag verabschiedet worden ist, ist am 1. August dieses Jahres in Kraft getreten. Seine Bestimmungen sollen gemäß § 1 Abs. 2 JVollzDSG für alle Arten gerichtlich angeordneten Freiheitsentzugs in den Justizvollzugsbehörden des Landes und für den Jugendarrest gelten und treten in Baden-Württemberg nach Maßgabe des Artikels 125 a des Grundgesetzes an die Stelle der bisher einschlägigen §§ 179 ff. des Strafvollzugsgesetzes.

Erklärte Absicht des Landesgesetzgebers war es, ein einheitliches Regelwerk für die Verarbeitung personenbezogener Daten im Justizvollzug des Landes zu schaffen, das „unter Wahrung des Rechts des Betroffenen auf informationelle Selbstbestimmung den Anforderungen und Bedürfnissen eines modernen, sicherheitsorientierten und kostenbewussten Informationsmanagements entspricht“. Ob die schlussendlich in Kraft getretene Gesetzesfassung diesem Anspruch in jeder Hinsicht gerecht wird, soll dahingestellt bleiben. Jedenfalls regelt das Justizvollzugsdatenschutzgesetz ungeachtet seines Namens den Datenschutz im Justizvollzug nicht wirklich umfassend, sondern klammert wichtige Bereiche, wie die Überwachung des Brief- und Besucherverkehrs, aus. Überdies ist nicht zu verkennen, dass das Justizvollzugsdatenschutzgesetz der Effizienz des Strafvollzugs meist Vorrang vor dem Recht der Gefangenen auf informationelle Selbstbestimmung einräumt, ohne dass die verschiedenen Weiterungen der Datenverarbeitungsbefugnisse der Vollzugsbehörden durchweg überzeugend begründet erscheinen. Rechtstechnisch lehnt sich das Justizvollzugsdatenschutzgesetz zum einen an die §§ 179 ff. des Strafvollzugsgesetzes des Bundes (StVollzG) an, zum anderen – so etwa im Hinblick auf die von der bundesdatenschutzrechtlichen Terminologie abweichenden Begrifflichkeiten des Gesetzes – auch an das Landesdatenschutzgesetz, dessen Normen teils im Wortlaut übernommen wurden, teils über Einzelverweisungen für direkt anwendbar erklärt wurden.

Inhaltlich wird der bisher in Gestalt der §§ 179 ff. StVollzG vorhandene Bestand an bereichsspezifischen datenschutzrechtlichen Regelungen um neue Befugnisse der Justizvollzugsanstalten zur Verarbeitung biometrischer Daten sowie erkennungsdienstlicher Unterlagen (z. B. Lichtbilder, Fingerabdrücke) erweitert, wobei auch letztere künftig vom datenschutzrechtlich grundlegenden Begriff des personenbezogenen Datums mit umfasst werden sollen. Als weiteres neues Instrument der Datenverarbeitung wird in § 7 JVollzDSG die Radio-Frequenz-Identifikation eingeführt – eine Technik, bei der ein Lesegerät per Funk Daten aus einem beispielsweise an der Kleidung des Gefangenen angebrachten Datenträger, dem sog. Transponder, ausliest. Sie soll zum Einsatz kommen können, um eine automatisierte Erhebung von Daten über den jeweiligen Aufenthaltsort des betroffenen Gefangenen innerhalb der Anstalt zu ermöglichen. Ebenfalls erstmals explizit geregelt wurde ferner die Befugnis der Vollzugsanstalten, das Anstaltsgelände und das Innere der Anstaltsgebäude mit Videotechnik zu überwachen und dabei im erforderlichen Maße auch Videoaufzeichnungen anzufertigen. Schließlich findet sich in § 27 JVollzDSG nunmehr eine Rechtsgrundlage für die Auftragsdatenverarbeitung im Justizvollzug.

Die meisten Bestimmungen des Justizvollzugsdatenschutzgesetzes verbleiben demgegenüber grundsätzlich im bisher bereits vom Strafvollzugsgesetz des Bundes vorgegebenen Regelungsrahmen, erweitern aber tendenziell die datenschutzrechtlichen Handlungsspielräume des Justizvollzugs. Viele der Änderungen gegenüber der bisherigen Rechtslage mögen bei oberflächlicher Lektüre des Gesetzes unspektakulär anmuten, dennoch dürfen ihre Konsequenzen für die Betroffenen nicht unterschätzt werden. Beispielsweise werden die schon bisher nach Maßgabe des § 180 Abs. 2 und Abs. 4 StVollzG bestehenden Übermittlungsbefugnisse der Strafvollzugsbehörden in § 12 Abs. 1 Nr. 4 JVollzDSG um einen neuen bzw. zumindest neu gefassten Übermittlungstatbestand er-

gänzt, welcher zur Datenweitergabe an die „zuständigen öffentlichen Stellen“ ermächtigt, soweit dies für „sozialrechtliche Maßnahmen“ erforderlich sei. Der Gesetzgeber hat diese Übermittlungsbefugnis ausweislich der amtlichen Begründung des Gesetzes bewusst weit formuliert und hat offensichtlich keine Bedenken bezüglich der Normenklarheit; denn aufgrund der weitgehenden Durchnormierung des Sozialrechts in den Sozialgesetzbüchern I bis XII sei der gewählte Anknüpfungspunkt ungeachtet der „Vielzahl von Lebensbereichen“, die vom Sozialrecht als Querschnittsmaterie erfasst würden, noch hinreichend konkret und normenklar. Der Gefangene, zumal wenn er kein ausgewiesener Experte des Sozialrechts ist, wird gleichwohl künftig noch weniger als schon bisher überschauen und kontrollieren können, welche Stelle zu welchem Zeitpunkt über welche Informationen über ihn verfügt.

Kritik nicht nur von unserer Seite haben des Weiteren die Ausweitungen der Offenbarungspflichten der in den Vollzugsanstalten beschäftigten Berufsgeheimnisträger (im Sinne des § 203 Abs. 1 Nr. 1, Nr. 2 und Nr. 5 StGB: Ärzte, Berufspsychologen, Sozialarbeiter, Sozialpädagogen etc.) durch § 21 Abs. 2 JVollzDSG erfahren. Betroffen sind insbesondere die Anstaltsärzte. War dem Arzt nach alter Rechtslage lediglich eine Befugnis eingeräumt, Privatgeheimnisse der Gefangenen, die ihm im Zuge seiner Tätigkeit auf dem Gebiet der Gesundheitsfürsorge bekannt geworden waren, dem Anstaltsleiter zu offenbaren, soweit dies für die Aufgabenerfüllung der Vollzugsbehörde „unerlässlich“ oder zur Abwehr erheblicher Gefahren für Leib und Leben des Gefangenen oder Dritter erforderlich war, so soll er jetzt zur Offenbarung solchen Wissens in gleicher Weise und in demselben Umfang verpflichtet sein wie die übrigen Berufsgeheimnisträger (mit Ausnahme der privilegierten Seelsorge). Es steht zu befürchten, dass diese Offenbarungspflicht das Vertrauensverhältnis zwischen dem Arzt und seinen Patienten belasten wird, ohne dass mit der Neuregelung notwendig ein echter Gewinn an Sicherheit verbunden sein muss. Denn auch nach bisherigem Recht waren dem verantwortungsbewussten Arzt in Fällen schwerster Gefährdungen für die Gesundheit oder das Leben von Personen ja keinesfalls die Hände gebunden. Bedauerlicherweise sind wir mit unserer Anregung, eine differenziertere Regelung zu treffen, im Anhörungsverfahren nicht durchgedrungen.

In anderer Hinsicht konnten wir durchaus einige Verbesserungen des ersten Entwurfs bewirken. Die auf unsere Initiative zurückgehenden Änderungen reichen von bloßen Ergänzungen der amtlichen Begründung über zahlreiche für die Lesbarkeit und Verständlichkeit des Gesetzestextes nicht unwichtige redaktionelle Korrekturen bis hin zur Nachbesserung einzelner zunächst unzulänglicher Vorschriften. So hat sich der Gesetzgeber erst auf unsere Kritik dazu entschließen können, zum Schutze der in Akten und Dateien gespeicherten Gefangenendaten vor unbefugtem Zugriff neben rein organisatorischen wenigstens nachrangig auch technische Vorkehrungen einzufordern, „wenn durch organisatorische Maßnahmen die Rechte der Betroffenen nicht ausreichend geschützt werden können“ (§ 20 Abs. 3 JVollzDSG). Trotz solcher datenschutzrechtlicher Gewinne im Detail ist aus der Perspektive unserer Dienststelle gleichwohl zu konstatieren, dass der Landesgesetzgeber von seinem erkennbaren Grundkonzept, der Effizienz des Justizvollzugs im Konfliktfall Vorrang vor dem informationellen Selbstbestimmungsrecht der Gefangenen und anderer Betroffener einzuräumen, insgesamt kaum abgerückt ist.

2. Die ominöse Gerichtspost

Wie dem regelmäßigen Leser unserer Tätigkeitsberichte vielleicht noch erinnerlich sein wird, hatten sich bereits in der Vergangenheit mehrere Petenten an unsere Dienststelle gewandt, weil sie Justizpost erhalten hatten, deren Sichtfensterbriefumschlag auch ungeöffnet mehr über den Inhalt des jeweiligen Schreibens verriet, als den Empfängern recht sein konnte. Wir haben in unserem 25. Tätigkeitsbericht für das Jahr 2004 (LT-Drucksache

13/3800) sowie nochmals in unserem 26. Tätigkeitsbericht für das Jahr 2005 (LT-Drucksache 13/4910) hierüber berichtet. Ging es seinerzeit jedoch „nur“ darum, dass im Sichtfenster der einkuvertierten Schreiben nebst Namen und Anschrift des Adressaten einmal der vergleichsweise harmlose Hinweis auf einen vom Gerichtsvollzieher festgesetzten Termin, ein andermal ein gerichtliches Aktenzeichen zu lesen war, das gewisse Rückschlüsse auf die Art des Verfahrens erlaubte, so sahen wir uns im Berichtszeitraum mit einem neuerlichen Fall allzu transparenter Gerichtspost befasst, der die genannten „Präzedenzfälle“ gewissermaßen noch überbot. Nicht genug damit, dass das Sichtfenster des auch diesmal verwendeten Fensterbriefumschlags besonders brisante Daten aus dem Inhalt des Schreibens preisgab, geriet dieses zudem auch noch an den falschen Empfänger.

Unfreiwillige Beteiligte im aktuellen Fall war die Landeshauptstadt Stuttgart. Dort ging eines Tages ein offenkundig amtliches Schreiben ein, mit dem die Stadt begreiflicherweise wenig anzufangen wusste. Im Fensterfeld des – wie sich schließlich herausstellte, amtsgerichtlichen – Briefs standen außer dem Namen des Betroffenen das Wort „Personenfahndung“ sowie die Angabe zu lesen, dass der Adressat des Schreibens eine gewisse „Datenstation Stuttgart II in Stuttgart“ sei. Da diese Adressangabe augenscheinlich unvollständig war, der Briefumschlag aber auch keinen Aufschluss über den Absender des Schreibens gab, sah sich die Stadt gezwungen, die ominöse Postsendung zu öffnen, um zu ermitteln, ob diese möglicherweise von einer städtischen Dienststelle herrühre. Da dies nicht der Fall war, leitete der behördliche Datenschutzbeauftragte der Stadt den offenkundigen Irrläufer kurzerhand zur weiteren Veranlassung an unsere Dienststelle weiter.

Von uns um eine Stellungnahme gebeten, hat uns das betreffende Amtsgericht überzeugend darlegen können, dass die ganze Angelegenheit auf einem nicht mehr restlos aufklärbaren Versehen des Postversands beruhe. Für die Personenfahndung gebe die vom Gericht eingesetzte IuK-Fachanwendung Formulare vor, die zunächst von den zuständigen Mitarbeitern des amtsgerichtlichen Serviceteams um die erforderlichen Daten ergänzt und alsdann über den Behördenaustausch, das heißt direkt von Dienststelle zu Dienststelle, zur Erfassung an die Datenstation der Landespolizeidirektion versandt würden. Nur versehentlich sei im gegebenen Fall für diesen Versand statt eines fensterlosen Kuverts ein Fensterumschlag verwendet worden. In welcher Verteilerstelle der Brief fehlgeleitet worden sei, lasse sich nicht mehr nachvollziehen.

Da uns der Präsident des Amtsgerichts im Übrigen versicherte, er habe den Vorfall zum Anlass genommen, alle mit dem Postversand betrauten Mitarbeiter der Behörde nochmals darauf hinzuweisen, dass in Fensterkuverts keinerlei personenbezogene Daten sichtbar sein dürften und der Adressat des Schreibens eindeutig zu bezeichnen sei, konnten wir die Angelegenheit letztlich auf sich beruhen lassen.

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

Für den Gesundheitsbereich könnte man frei nach Schopenhauer sagen: „Gesundheit ist nicht alles, aber ohne Gesundheit ist alles nichts“. Dieser Aussage dürften sich die meisten Bürgerinnen und Bürger ohne weiteres anschließen, wenn man sie dazu befragen würde. Es verwundert deshalb nicht, dass es in kaum einem anderen Bereich in so rascher Zeitfolge vergleichbar viele Aktivitäten mit Veränderungen und Weiterentwicklungen in EDV-technischer, medizinischer und pharmakologischer Hinsicht gibt. Der Gesundheitsmarkt ist in Baden-Württemberg Branchenprimus – zumindest was die Zahl der Beschäftigten anbelangt – mit einer Wertschöpfung von fast 30 Milliarden Euro im Jahr. Es gibt allein im Land rd. 300 Krankenhäuser, 61 000 Betten, fast zwei Millionen Patienten jährlich und rd. 140 000 dort tätige Mitarbeiter. Für die Kosten einzutreten haben dabei in der Regel die private bzw. überwiegend die gesetzliche Krankenversicherung.

Dass dieser Teil des sozialen Sicherungssystems trotz weiterer Verbesserungen im Leistungs- und Behandlungsangebot und zum Teil darauf zurückzuführender Teuerungen auch noch weiter von der Solidargemeinschaft der Versicherten finanziert werden kann, ist ein schwer zu lösendes Problem. Intensivere und von den Versicherten oft als zu weitgehend und zu bürokratisch empfundene Einzelfallprüfungen, Rückfragen und Recherchen ihrer Krankenkassen führten auch im Berichtsjahr wieder zu einer steigenden Zahl von Eingaben und Beratungen durch meine Dienststelle. Dies kann angesichts eines selbst für Fachleute nur noch sehr schwer zu durchdringenden Geflechts an Regelungen vor allem in den Sozialgesetzbüchern, verbunden mit Gesetzesänderungen in rascher Folge und ebensolchen Entwicklungen im IT-Bereich, nicht verwundern.

Sehr anspruchsvoll und beratungsintensiv für meine Dienststelle waren auch verschiedene Forschungsvorhaben, mit denen sich baden-württembergische Universitätskliniken auf nationaler und internationaler Ebene befassen wollten. Gleiches lässt sich auch über unsere Beratungstätigkeit im Rahmen von Modellprojekten zur integrierten Versorgung nach § 140 a des Fünften Buchs des Sozialgesetzbuchs – SGB V – und solchen Vorhaben, die sich dafür ausgaben, berichten. Beratung Suchende waren hierbei in erster Linie gesetzliche Krankenkassen und das Ministerium für Arbeit und Soziales. Eine wichtige (Teil-) Aufgabe meines Amts ist auch die Durchführung von Außenkontrollen. Diese können anlassbezogen sein oder auch aus anderen Erwägungen stattfinden. In diesem Jahr haben wir uns schwerpunktmäßig für die Prüfung eines Zentrums für Psychiatrie entschieden, über dessen Ergebnis später berichtet wird.

1. Die elektronische Gesundheitskarte

Mit der vom Bundesgesetzgeber im Fünften Buch des Sozialgesetzbuchs – SGB V – (vgl. § 291 a Abs. 1 SGB V) als Erweiterung der bisherigen Krankenversichertenkarte allgemein verbindlich eingeführten elektronischen Gesundheitskarte soll in verschiedenen Ausbaustufen das Gesundheitswesen elektronisch vernetzt werden. Im Rahmen eines der umfangreichsten und teuersten IT-Projekte Deutschlands sollen ca. 80 Millionen neue Karten an Versicherte der gesetzlichen und privaten Krankenversicherung ausgegeben werden und bundesweit u. a. rd. 21 000 Apotheken, 123 000 niedergelassene Ärzte, 65 000 Zahnärzte, 2 200 Krankenhäuser sowie 300 gesetzliche und private Krankenkassen mit der neuen Karte arbeiten.

Bereits im 26. Tätigkeitsbericht für das Jahr 2005 (LT-Drucksache 13/4910) und im 27. Tätigkeitsbericht für das Jahr 2006 (LT-Drucksache 14/650) hatten wir uns sehr ausführlich mit dieser Thematik befasst. Vorliegend möchten wir daher über in der Zwischenzeit eingetretene Weiterentwicklungen des IT-Projekts berichten und nochmals die Position des Datenschutzes verdeutlichen.

Nach dem Willen des Gesetzgebers sollte bekanntlich die elektronische Gesundheitskarte die heutige Krankenversichertenkarte zum 1. Januar 2006 ablösen. Dieses Ziel wurde – was angesichts der Komplexität des Vorha-

bens nicht verwundert – deutlich verfehlt. Bis zum Ende des Berichtszeitraums wurden die vom Bundesministerium für Gesundheit förmlich festgeschriebenen verschiedenen Phasen der Testung für die Einführung der elektronischen Gesundheitskarte (vgl. Rechtsverordnung vom 5. Oktober 2005, zuletzt geändert am 2. Oktober 2006, Bundesgesetzblatt I, Nr. 45, S. 2189 ff.) nicht einmal in der ersten Teststufe (sog. Zehntausendertest) verwirklicht. In weiteren Phasen sollen sich daran sog. Hunderttausendertests anschließen.

Das Verfehlen des zeitlichen „Klassenziels“ möchten wir nur als Information verstanden wissen und nicht als Forderung, um den Preis mangelnder Sorgfalt die elektronische Gesundheitskarte nunmehr voreilig einzuführen. Im Gegenteil: Zum einen ist der Wunsch, mit Hilfe der neuen Krankenversichertenkarte die Wirtschaftlichkeit, Qualität und Transparenz der Behandlung zu verbessern, ein politisches Ziel, das aufgrund der zahlreichen Schwierigkeiten, die reale Welt im Gesundheitswesen in einem IT-Projekt abzubilden, von Seiten des Datenschutzes durchaus kritisch gesehen wird. Geht es doch letztlich um sensible Gesundheits- bzw. Sozialdaten von Betroffenen. Zum anderen verstehen wir unsere Forderung, dass Sorgfalt vor Schnelligkeit gehen müsse, nicht als den Versuch von datenschutzrechtlichen Bedenkenträgern, ein Projekt verzögern zu wollen, sondern als einen konstruktiven (Teil-)Beitrag zum Gelingen des Vorhabens. Die Überzeugung von der Sinnhaftigkeit des Projekts kann bei sämtlichen Beteiligten nur dann erreicht werden, wenn diese auch darauf vertrauen können, dass mit ihren Daten im Rahmen des IT-Projekts verantwortungsvoll umgegangen wird. Aus verschiedenen Anfragen und Eingaben von Bürgerinnen und Bürgern hören wir immer wieder von deren ernster Sorge, dass sie nunmehr wegen der elektronischen Gesundheitskarte zum „Gläsernen Patienten“ werden könnten.

Aus Sicht des Datenschutzes soll deshalb nochmals zur Verdeutlichung gesagt werden, dass der Gesetzgeber in § 291 a SGB V nur eine schrittweise Verwirklichung verschiedener Funktionen und als Pflichtteil der elektronischen Gesundheitskarte neben den administrativen Daten auf der Krankenversichertenkarte (Name, Anschrift, Geburtsdatum, Krankenkasse, Versichertenstatus, Versichertennummer und [neu] Lichtbild) lediglich die Nutzung als elektronisches Rezept vorgesehen hat. Mit anderen Worten: Die elektronische Gesundheitskarte stellt (zunächst nur) ein papierloses Rezept im „Scheckkartenformat“ dar. Darüber hinaus muss nach dem Willen des Gesetzgebers die Gesundheitskarte auch geeignet sein, in einem freiwilligen Teil medizinische Daten (z. B. für die Notfallvorsorge, Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte, Impfungen, Blutgruppe etc.) aufzunehmen. Darüber hinaus können – ebenfalls freiwillig – von Versicherten selbst zur Verfügung gestellte weitere Gesundheitsdaten auf der elektronischen Gesundheitskarte gespeichert werden. Der vorgesehene kleinere Pflichtteil entspricht demzufolge dem vom Bundesverfassungsgericht in seinem sog. Volkszählungsurteil vom 15. Dezember 1983 formulierten Grundsatz der informationellen Selbstbestimmung insoweit, als der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten im Rahmen der Einführung der elektronischen Gesundheitskarte (ausgenommen der Pflichtteil) bestimmen darf. Der allgemein geltende datenschutzrechtliche Grundsatz, dass die Gefahr einer Datenschutzverletzung umso geringer ist, je weniger Daten ein Betroffener von sich preisgibt, gilt selbstverständlich auch hier. Skeptische Bürger werden die Nutzung der Versichertenkarte daher zunächst auf das elektronische Rezept beschränken.

Hiervon unabhängig möchten wir noch einmal die Grundsatzposition des Datenschutzes zur Einführung der elektronischen Gesundheitskarte in Erinnerung rufen, wie sie in einer gemeinsamen Entschließung der Datenschutzbeauftragten von Bund und Ländern vom 18./11. März 2005 (siehe 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910) zum Ausdruck kam. Folgende Aspekte zum Schutz der Patientenrechte wurden dabei als wesentlich angesehen:

– Die über die Karte erfolgende Datenverarbeitung muss nach den gesetzlichen Vorgaben weitgehend aufgrund der Einwilligung der Versicherten erfolgen.

– Um die hierfür nötige Akzeptanz bei den Versicherten zu erhalten, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen dafür zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und Übermittlung gewahrt sind.

– Die Versicherten müssen auch darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben.

– Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt.

– Die Verfügungsbefugnis der Versicherten über ihre Daten muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen zu gewährleisten.

– Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen.

– Die Test- und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben. Vorgesehene Einführungstermine dürfen, so die Datenschutzkonferenz weiter, kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Aus Sicht des Datenschutzes wird es deshalb ganz wesentlich darauf ankommen, die vom Gesetzgeber in § 291 a SGB V gemachten Vorgaben, die vom Ansatz her als durchaus datenschutzfreundlich bezeichnet werden können, auch in die praktische Realität umzusetzen. Erste Voraussetzung dafür wäre, dass die Gematik GmbH (Anmerkung: Es handelt sich um eine eigens auf Bundesebene für die Einführung der elektronischen Gesundheitskarte geschaffene Gesellschaft, der Krankenkassen und Verbände der Leistungserbringer angehören) endlich ihrem gesetzlichen Auftrag nachkommt und ein umfassendes und primär mit dem Bundesdatenschutzbeauftragten abgestimmtes Datenschutzkonzept vorlegt.

Der Stand der Einführung der elektronischen Gesundheitskarte ist gegenwärtig folgender:

Nachdem Ende vergangenen Jahres die ebenfalls vorgesehene Testregion Bremen ihre Teilnahme an dem Zehntausendertest aufgekündigt hat, wird dieser nunmehr noch in sieben Testregionen in verschiedenen Bundesländern durchgeführt, darunter im Stadt- und im Landkreis Heilbronn (Testregion Heilbronn).

Die Suche nach 10 000 Patienten, 25 Ärzten, zehn Apotheken und einem Krankenhaus, die auf freiwilliger Basis am Test teilzunehmen bereit sind, gestaltete sich in der Testregion schwieriger als zunächst angenommen. Insbesondere die Ärzteschaft und die ärztlichen Berufsverbände – und dies nicht nur in dieser Testregion – zeigten sich skeptisch, weil sie zusätzliche Kosten und Zeitaufwand durch die elektronische Gesundheitskarte auf sich zukommen sehen und auch datenschutzrechtliche Bedenken geltend machten, ohne diese allerdings näher benennen zu können. Von Seiten des Ministeriums für Arbeit und Soziales gab es, nachdem sich Mediziner aus dem Unterland im Ministerium darüber beschwert hatten, dass sie angeblich von ihrer Standesvertretung unter Druck gesetzt worden seien, die Testung zu boykottieren, harsche Worte. Die Ministerin teilte dem Medi-Verbund im Unterland, dem 430 der 620 niedergelassenen Ärzte aus dem Stadt- und dem Landkreis Heilbronn angehören, mit, dass sie im Hinblick auf die Beschwerden und die möglichen negativen Auswirkungen auf den Testlauf die weitere „konstruktive Zusammenarbeit mit den Medi-Verbund als gefährdet“ ansehe.

Tatsache ist, dass in der Testregion Heilbronn in der ersten Testphase im sog. Offline-Betrieb zunächst lediglich 7 500 Versicherte, 14 niedergelassene Ärzte und zehn Apotheken teilnehmen; ein Krankenhaus soll noch später hinzukommen. Im ersten Schritt soll dabei das Zusammenspiel zwischen der elektronischen Gesundheitskarte und dem Heilberufeausweis des Arztes und des Apothekers mit den technischen Komponenten, also Lesegerät, Konnektor und der jeweiligen Systemsoftware, und die Nutzung des elektronischen Rezepts getestet werden. Anzumerken ist ferner, dass die freiwillig teilnehmenden Tester in dieser Testphase sowohl über ihre bereits vorhandene Versicherungskarte als auch über die neue elektronische Gesundheitskarte verfügen und sie in dieser Zeit die Rezepte sowohl auf der elektronischen Karte als auch noch in Papierform für die Einlösung in der Apotheke erhalten. Das elektronische Rezept wird dabei mittels Lesegerät und persönlicher fünfstelliger PIN vom behandelnden Arzt auf der elektronischen Gesundheitskarte gespeichert. In den Apotheken, die am Test teilnehmen, kann das elektronische Rezept ebenfalls nur mittels eines Lesegeräts eingelesen werden. Auch hierfür muss der Apotheker seinen Heilberufeausweis mit persönlicher PIN nutzen. Am 10. Oktober 2007 erhielten wir von einer unserer Kontrolle unterliegenden Krankenkasse die „Jubelmeldung“, dass um „10.58 Uhr die erste elektronische Gesundheitskarte eines echten Patienten“ in einer Arztpraxis in der Testregion Heilbronn eingelesen und mit einer E-Verordnung beschrieben worden sei. Der Vorgang – so die Krankenkasse weiter – sei reibungslos und ohne technische Probleme abgelaufen.

Kritisch anzumerken ist jedoch, dass sich diese frohe Botschaft lediglich darauf bezog, dass in der allerersten Teilteststufe ein kleiner Mosaikstein eines insgesamt komplexen IT-Projekts funktioniert hat. Wie sich das Ganze weiterentwickeln wird, wenn es in weiteren Testphasen in den viel schwierigeren Online-Betrieb geht und komplexe Anwendungen hinzukommen, bleibt abzuwarten. Aussagen in der Presse, wonach die Datenschützer im Land grünes Licht für die Testung im Unterland gegeben haben, können sich deshalb auch nur auf diese Teiltestungen im Offline-Betrieb beziehen.

Zu gewissen Irritationen führten auch Aussagen der Bundesregierung, wonach mit einem bundesweiten Rollout der Komponenten bereits im zweiten Quartal 2008 begonnen werden soll. Im Ergebnis käme dadurch die elektronische Gesundheitskarte doch noch früher auf den Markt, als man aufgrund der eingetretenen Verzögerungen eigentlich erwarten konnte. Befürchtet wird in diesem Zusammenhang nicht nur von Datenschützern, dass damit z. B. auf die verordnungsmäßig vorgegebenen weiteren wichtigen Testabschnitte (z. B. sog. Hunderttausendertests) verzichtet werden könnte.

Eine besorgte Nachfrage des Bundesdatenschutzbeauftragten im Bundesministerium für Gesundheit brachte die Auskunft, dass zu dem genannten Zeitpunkt zwar elektronische Gesundheitskarten ausgegeben werden sollen, allerdings ohne jegliche Funktion und Anwendung – was immer dies auch für einen Sinn ergeben mag. Einen Verzicht auf etwaige Testungen soll es jedenfalls nicht geben. Meine Kolleginnen und Kollegen im Bund und in den anderen Ländern sehen es daher als wichtige Aufgabe an, bei der Einführung der elektronischen Gesundheitskarte weiter darauf zu achten, dass der in vier Teststufen in der oben genannten Verordnung präzise vorgegebene Migrationsplan zur Einführung dieses IT-Projekts auch entsprechend der dort normierten Schritte unter Wahrung der Belange des Datenschutzes erfolgt. Auf Landesebene wurde im Februar 2005 für die Einführung der elektronischen Gesundheitskarte in Baden-Württemberg und zur Durchführung der Testung in der Region Heilbronn eine Arbeitsgemeinschaft (ARGE eGK) gegründet, deren Arbeit wir u. a. in einem eigens dafür gebildeten Beirat und in einer Unterarbeitsgruppe „Datenschutz“ konstruktiv begleiten. In diesem Zusammenhang möchten wir ausdrücklich die fachlich wie atmosphärisch reibungslose Zusammenarbeit in diesen Gremien loben. Eine gute Idee ist dabei, im Internet-Portal der ARGE eGK (http://www.gesundheitskarte-bw.de) die am häufigsten gestellten Fragen und ihre Antworten zur elektronischen Gesundheitskarte einzustellen. Gleiches gilt im Übrigen für die Telefonaktion einer Regionalzeitung. Diese Aktion bot einem Mitarbeiter meiner Dienststelle die Gelegenheit, auf Fragen des Datenschutzes am Expertentelefon einzugehen, wobei interessant war, dass sich die meisten Anrufe

auf das Thema Datenschutz und nicht auf andere, die elektronische Gesundheitskarte betreffende Fragestellungen bezogen.

2. Datenschutz im Zentrum für Psychiatrie – Ein Kontrollbesuch

Die Kernversorgung der Bevölkerung im stationären Bereich nehmen bei psychischen Erkrankungen in Baden-Württemberg neun Zentren für Psychiatrie wahr. Sie unterliegen als Anstalten des öffentlichen Rechts unserer datenschutzrechtlichen Kontrolle und haben sich aus den ursprünglichen Heil- und Pflegeanstalten sowie den psychiatrischen Landeskliniken (ab dem Jahr 1953) entwickelt. Je nach Versorgungsregion kooperieren jeweils drei Zentren für Psychiatrie insbesondere auf der Verwaltungsebene miteinander bzw. bilden einen sog. Organisationsverbund. Im Rahmen eines anlassunabhängigen Kontrollbesuchs vor Ort führte uns in diesem Jahr der Weg nach Südwürttemberg, wo drei Kliniken in Verbundform organisiert sind. Die nachstehenden Ausführungen sind somit auch unmittelbar auf die beiden anderen Verbundklinken übertragbar; sie dürften aber auch ganz generell für die anderen Kliniken im Land wichtige datenschutzrechtliche Hilfestellungen geben.

Bereits anlässlich früherer Außenprüfungen in Kliniken mit gänzlich anderen Aufgabenstellungen hatten wir Verständnis dafür geäußert, dass es im Spannungsbogen des täglichen Klinikbetriebs einerseits und der reinen Lehre des Datenschutzes andererseits nicht immer einfach ist, das richtige Maß zu finden. Dies gilt insbesondere für stationäre Einrichtungen, wie sie die Zentren für Psychiatrie darstellen. Umso erfreulicher war, dass wir anlässlich unseres Kontrollbesuchs feststellen konnten, dass der „Datenschutz“ in der von uns geprüften Einrichtung ein Thema ist, für das sich nicht nur der behördliche Datenschutzbeauftragte des Zentren-Verbunds, sondern auch die Geschäftsführung und die ärztliche Leitung sehr aufgeschlossen zeigten. Dieser Eindruck spiegelte sich auch in der Stellungnahme des Zentrums zu unserem Prüfbericht wieder. Der Kontrollbesuch wird darin als konstruktiv sowie problem- und beratungsorientiert bezeichnet. Wie man uns weiter mitgeteilt hat, sollen unsere Anregungen und Forderungen vollständig aufgegriffen und auch umgesetzt werden. Der vom Zentrum geäußerten Bitte, dieses im Rahmen der Beratungstätigkeit meines Amts gemäß § 31 Abs. 3 LDSG auch bei der konkreten Umsetzung der Vorschläge zu unterstützen, werden wir im Rahmen unserer Möglichkeiten gerne nachkommen.

Von dem Kontrollbesuch meiner Dienststelle ist Folgendes berichtenswert:

2.1 Patientenaufnahme

Erste Anlaufstelle bei einem geplanten Krankenhausaufenthalt ist regelmäßig eine speziell für diese Zwecke eingerichtete zentrale Anlaufstelle der Krankenhausverwaltung. Hier werden erstmals sensible Patientendaten erhoben, gespeichert und an weitere Organisationseinheiten des Krankenhauses übermittelt. Daraus ergeben sich unterschiedliche datenschutzrechtliche Fragestellungen, die wir bereits in früheren Tätigkeitsberichten ausführlich behandelt haben (vgl. u. a. 25. Tätigkeitsbericht für das Jahr 2004, LT-Drucksache 13/3800).

Wie wir anlässlich unserer Prüfung vor Ort feststellen konnten, erfolgt die reguläre Aufnahme neuer Patienten des Zentrums nicht in Zentraleinrichtungen des Krankenhauses, sondern unmittelbar auf den Stationen. Die für die Aufnahme benötigten Informationen werden dabei im Dialog zwischen Patient und Aufnahmekraft erfragt und direkt in das im Zentrum verwendete EDV-System eingegeben. Grundsätzlich zu unterscheiden ist dabei zwischen der administrativen und der medizinischen Aufnahme. Während die administrative Aufnahme im Wesentlichen den Abschluss des Behandlungsvertrags sowie Angelegenheiten der Unterbringung im Krankenhaus beinhaltet, dient die medizinische Aufnahme der Vorbereitung der Behandlung.

Eine stichprobenweise Prüfung ergab, dass im Zentrum – soweit wir feststellen konnten – nur Daten erhoben werden, die für die oben ge-

nannten Zwecke erforderlich sind. Mit dem verwendeten EDV-System besteht auch die Möglichkeit, in der Aufnahmemaske eine Auskunftssperre vermerken zu lassen. Dies ist für den Bereich eines Zentrums deshalb wichtig, weil Patienten teilweise verhindern wollen, dass ihre Aufnahme in das Krankenhaus bei der Pforte oder auf anderem Weg von Dritten erfragt werden kann. Ein wesentlicher Grund dafür ist die leider auch heute noch teilweise festzustellende Neigung zur Vorverurteilung, wenn aufgrund einer psychischen Erkrankung eine stationäre Behandlung in einem Zentrum erforderlich wird.

Im Zusammenhang mit der Patientenaufnahme ist aus datenschutzrechtlicher Sicht die Erfassung der Religionszugehörigkeit nach wie vor ein Thema, zu dem uns immer wieder Anfragen erreichen. Anlässlich eines früheren Kontrollbesuchs im Jahr 2004 hat sich meine Dienststelle hierzu bereits geäußert (vgl. 25. Tätigkeitsbericht für das Jahr 2004, LT-Drucksache 13/3800). Unter Beachtung des in § 45 Abs. 2 des Landeskrankenhausgesetzes geschaffenen Regelwerks dürfen personenbezogene Daten für Zwecke der Krankenhausseelsorge grundsätzlich erhoben werden. Da die beiden beim Zentrum tätigen Krankenhauspfarrer ihr Betreuungsangebot aber nur im Rahmen von Andachten, Gottesdiensten oder auf ausdrücklichen Wunsch der Patienten wahrnehmen, ist es datenschutzrechtlich korrekt, dass beim Zentrum im Rahmen der Aufnahme keine entsprechenden Daten erhoben werden.

Ein anderes Thema, das bei Anfragen öfters eine Rolle spielt, ist die Nutzung von Telefax-Geräten. Auf den von uns besuchten Stationen gab es – was wir ausdrücklich begrüßen – keine Telefaxgeräte, mit denen sensible Patientendaten versandt bzw. empfangen werden können. Diese Geräte befinden sich vielmehr zentral jeweils im Büro der Abteilungssekretärin, die auch die Verteilung eingehender Post an die Ärzte in die dafür vorgesehenen Postfächer vornimmt.

2.2 Behandlung

Ein Kontrollbesuch bedarf für meine Mitarbeiter einer gründlichen Vorbereitung. Hierzu lassen wir uns regelmäßig Organisationspläne der Einrichtung, Verfahrensverzeichnisse nach § 11 LDSG, evtl. vorhandene Zugriffs-, Sperr- und Löschkonzeptionen, Verträge mit Dritten (Datenverarbeitung im Auftrag) sowie vorhandene Vordrucke vorlegen. Bereits im Vorfeld der Außenprüfung mussten wir feststellen, dass die vom Zentrum aktuell verwendeten Behandlungsverträge einer Überarbeitung bedürfen. Einer der gravierendsten Mängel in dem dafür vorgesehenen Vordruck war, dass der Patient in der Einwilligungserklärung – wenn man die gewählte Überschrift als Maßstab nimmt – unter Hinweis auf § 73 Abs. 1 b SGB V (nur) in eine „Datenübermittlung an den Hausarzt“ einwilligt, während er bei vollständiger Betrachtung des Vertragstextes mit seiner Unterschrift zugleich auch darin einwilligt, dass seine beim Hausarzt vorliegenden Behandlungsdaten, soweit diese für die Behandlung im Zentrum für erforderlich angesehen werden, durch die Klinik angefordert werden dürfen. Beiden Formen der Datenübermittlung muss bereits in der Überschrift oder auf anderem Weg hinreichend deutlich Rechnung getragen werden. Das Zentrum hat zugesagt, diese Anregung im Rahmen der Neufassung der Behandlungsverträge umzusetzen und dabei im Rahmen der Neugestaltung auch deutlicher als bisher darauf hinzuweisen, dass bestimmte Erklärungen „freiwillig“ sind. Ein solcher Hinweis erfolgt gegenwärtig nur neben anderen Informationen im laufenden Vordrucktext und wird im Übrigen auch nicht durch entsprechende Textgestaltung (z. B. Fettdruck) gegenüber anderen Passagen besonders hervorgehoben. Dies entspricht nicht den in § 4 Abs. 3 LDSG enthaltenen Anforderungen.

Ein anderes datenschutzrechtliches Thema, dessen sich meine Mitarbeiter vor Ort angenommen haben, betrifft die Türbeschriftung der Patientenzimmer. Bei einem Besuch auf zwei Krankenstationen (Geriatrie, Suchtabteilung) fiel auf, dass neben den Zimmertüren die Namen der Patienten angebracht waren. Eine Rückfrage ergab, dass es bisher keine schriftliche Dienstanweisung dafür gibt, nach welchen Kriterien die Na-

mensschilder angebracht werden dürfen (oder besser nicht). Es bleibt vielmehr dem Pflegedienst der einzelnen Stationen selbst überlassen, auf welche Art und Weise diese die Beschriftung an den Zimmertüren vornehmen. Unbestritten stellen Namensschilder für Besucher und Patienten an den Zimmertüren eine Orientierungshilfe dar. Man kann auch davon ausgehen, dass Patienten den Besuch am Krankenbett wünschen und damit (möglicherweise) sogar konkludent in entsprechende Türinformationen einwilligen. Dies gilt jedoch dann nicht, wenn Anhaltspunkte für einen gegenteiligen Willen vorliegen. Hiervon ist grundsätzlich bei Patienten in einem Zentrum und hier insbesondere für bestimmte Krankenstationen auszugehen. Es lässt sich nämlich nicht ausschließen, dass über die Zimmerbeschriftung Besucher, Nachbarn, Firmenvertreter, Pflegedienste etc. – bewusst oder unbewusst – etwas über die Anwesenheit bestimmter Personen im Zentrum und – in Verbindung mit der Abteilungsbezeichnung – sogar etwas über die Art der Erkrankungen erfahren, obwohl die Patienten diese Informationen aus nachvollziehbaren Gründen gerade nicht weiter verbreitet sehen möchten. Möchte man zur Vermeidung von Nachfragen durch Besucher – aber auch zur Erleichterung des Arbeitsablaufs für die ärztlichen und nichtärztlichen Mitarbeiter im Krankenhaus – auf die Beschriftung der Zimmertüren nicht gänzlich verzichten, bietet sich aus Sicht des Datenschutzes als Lösung an, die Patienten selbst entscheiden zu lassen, ob sie eine Namensbeschriftung möchten oder nicht. Dies kann z. B. – soweit möglich – durch die Aushändigung eines unbeschrifteten Türschilds mit der Möglichkeit, dieses selbst auszufüllen, erfolgen oder durch eine ausdrückliche Erklärung gegenüber dem Pflegepersonal auf der Station (z. B. direkt bei der Aufnahme oder zu einem späteren Zeitpunkt). Im wohlverstandenen Eigeninteresse des Krankenhauses empfehlen wir zusätzlich noch eine schriftliche Dokumentation eines solchen Patientenwunsches. Das Zentrum hat zugesagt, in Kürze eine Dienstanweisung mit entsprechendem Inhalt zu erlassen.

2.3 Krankenhausverwaltung

Im Fokus unserer Prüf- und Beratungstätigkeit vor Ort stand auch der Pfortenbereich und dort insbesondere die Frage, ob durch technisch-organisatorische Maßnahmen sichergestellt wird, dass Auskünfte über Patienten an private Stellen (z. B. Besucher, Angehörige, Firmenvertreter, Versicherungen) nur in dem vom jeweiligen Patienten gewünschten Umfang erteilt werden und dass Auskünfte an öffentliche Stellen (z. B. Polizei) nur in dem gesetzlich erlaubten Umfang erfolgen.

Für die im Pfortendienst eingesetzten Teilzeitkräfte gibt es bisher keine schriftliche Anweisung, wie im Einzelfall telefonische oder persönliche Anfragen an der Pforte zu erledigen sind. Dies hat zur Folge, dass die Auskunftspraxis uneinheitlich sein dürfte und nach „bestem Wissen und Gewissen“ situativ durch das Pfortenpersonal erledigt wird. Ein meiner Dienststelle im Nachgang zu dem Kontrollbesuch übermitteltes Papier, das möglicherweise als Dienstanweisung hinsichtlich der Erteilung von Auskünften an externe Stellen generell für das Zentrum gelten soll, ist für die konkrete Aufgabenerledigung eines Pfortendienstes zu umfangreich, um für die dort eingesetzten Teilzeitkräfte eine echte Hilfestellung zu geben. Eine knapp gehaltene Positivliste – wem darf die Pforte was mitteilen? – würde hier wesentlich weiterhelfen.

Wie wir weiter feststellen konnten, bietet das Patientenmanagementverfahren die Möglichkeit, auf Wunsch die Namen bestimmter Patienten aus dem allgemeinen Patientenverzeichnis, das an der Pforte aufgerufen werden kann, herauszunehmen. Gleichwohl war es für uns möglich, an der Pforte eine eigene Liste aufzurufen, welcher sich Namen, Vornamen und Geburtsdaten auch solcher Patienten entnehmen ließen, für die eine diesbezügliche Sperre extra dafür eingerichtet worden war. Wozu die Pforte solche brisanten Informationen über „gesperrte“ Patienten überhaupt benötigt, ließ sich vor Ort nicht klären. Des Weiteren mussten wir feststellen, dass Stammdaten von entlassenen Patienten noch sechs Wochen nach deren Entlassung an der Pforte eingesehen werden können, obwohl uns von den Mitarbeitern erklärt wurde, dass Anfragen,

für die diese Daten tatsächlich benötigt werden, in der Praxis relativ selten seien. Über die Rechtslage gibt § 23 Abs. 1 LDSG Auskunft: Danach sind personenbezogene Daten in Dateien immer dann zu löschen, wenn die speichernde Stelle diese zur Aufgabenerfüllung nicht mehr benötigt. Aus Sicht des Datenschutzes sollte deshalb eine deutlich reduzierte Speicherdauer Eingang in eine schriftliche Dienstanweisung (Löschkonzeption) finden.

Es gibt – so wurde uns berichtet – auch immer wieder fernmündliche Anfragen der Polizei. Sie erkundigt sich beim Pfortendienst, ob sich eine von ihr gesuchte Person im Zentrum in der stationären Behandlung befindet. Auf unsere Nachfrage, ob und wie der Pfortendienst am Telefon überhaupt nachprüfen könne, ob es sich bei dem Anfragenden um eine auskunftsberechtigte Person handelt, wurde erklärt, dass man sich in erster Linie von Sekundärmerkmalen (z. B. Polizeifunkverkehr im Hintergrund, Art und Weise des „Auftretens“ des Anfragers) orientiere, nachdem es hierfür keine schriftlichen Handlungsanleitungen gebe. Zur Wahrung der Patientenrechte haben wir deshalb in unserem Prüfbericht das Zentrum gebeten, das Verfahren der Pfortenauskunft in einer einfach gestalteten schriftlichen Anweisung speziell für die dort eingesetzten Beschäftigten datenschutzkonform zu vereinheitlichen.

Das Zentrum hat unsere diesbezüglichen Vorschläge aufgegriffen und wird in Kürze eine entsprechende „Positivliste“ für die Pforte erstellen, in der auch der Teilbereich der Erteilung von Auskünften bei Anfragen der Polizei geregelt sein wird. Die Möglichkeit, die Speicherdauer von Stammdaten entlassener Patienten im Bereich des Pfortendienstes zu reduzieren, wird nach Aussagen des Zentrums aktuell von einer dafür eingerichteten Arbeitsgruppe sowohl technisch als auch organisatorisch mit dem Ziel geprüft, das Verfahren entsprechend der Empfehlungen meiner Dienststelle umzugestalten.

2.4 Dokumentation der Behandlung

Nach der standesrechtlichen Berufsordnung für Ärzte (vgl. § 10 der [Muster-]Berufsordnung für die deutschen Ärztinnen und Ärzte (MBO-Ä) mit inhaltsgleicher Landesregelung), aber auch unter haftungsrechtlichen Aspekten, sind Ärzte und Pflegepersonal verpflichtet, die Behandlung von Patienten vollständig zu dokumentieren. Die ärztliche Leitung des Krankenhauses trägt dabei die Gesamtverantwortung für die Dokumentation der Krankenhausbehandlung. Diese erfolgt in den drei dem Zentren-Verbund angehörenden Krankenhäusern EDV-unterstützt durch die für den Zentrums-Bereich speziell entwickelte Patientenmanagement-Software. Seit ca. sechs Jahren kommt diese einheitlich in allen dem Verbund der Südwürttembergischen Zentren für Psychiatrie angeschlossenen Einrichtungen zur Anwendung, sodass konventionelle Krankenakten nur noch als Teilakten für solche Bereiche (ergänzend) geführt werden, die nicht mit Hilfe der vorgenannten Software dokumentiert werden können (z. B. Röntgenaufnahmen, externe Anfragen und Unterlagen).

Im Rahmen unserer Außenprüfung sind wir auch der Frage nachgegangen, welche Personen Patientenakten führen dürfen, wer und auf welche Weise Krankenakten von früheren Aufenthalten desselben Patienten im Zentrum beigezogen werden dürfen und wie mit diesen Dokumenten auf den von uns besuchten Stationen durch die Mitarbeiter umgegangen wird. Zu diesem Themenkomplex haben wir im Rahmen der bei einem solchen Kontrollbesuch immer nur möglichen stichprobenweisen Überprüfung erfreulicherweise keine gravierenden Defizite feststellen können.

2.5 Archivierung von Patientenunterlagen

Die oben genannte (Muster-)Berufsordnung für die deutschen Ärztinnen und Ärzte, die inhaltsgleich in Landesrecht umgesetzt wurde, enthält korrespondierend zur Dokumentationspflicht über vorgenommene Behandlungen auch Regelungen, wonach ärztliche Aufzeichnungen für die Dauer von (mindestens) zehn Jahren nach Abschluss der Behand-

lung aufzubewahren sind (vgl. § 10 MBO-Ä). Für den besonderen Bereich von psychiatrischen Krankenhäusern kann es – was von Seiten des Datenschutzes durchaus akzeptiert wird – medizinisch und aus Gründen der Beweisführung bei Gerichtsverfahren sinnvoll und notwendig sein, diese Dokumente erforderlichenfalls auch über eine darüber hinausgehende Zeit aufzubewahren, wobei dann 30 Jahre die absolute Obergrenze sein sollten.

Wir empfehlen allen Krankenhäusern unseres Kontrollbereichs, grundlegende Regelungen der Patientenaktenführung und -aufbewahrung verbindlich in Archivordnungen festzulegen und sie als Dienst- oder Betriebsanweisung in Kraft zu setzen. Als erhebliches Datenschutzmanko mussten wir im kontrollierten Zentrum feststellen, dass es bislang dort – und demzufolge auch nicht im Zentren-Verbund – eine entsprechende Archivordnung nicht gibt und darüber hinaus seit Bestehen der Einrichtung noch nie Patientenakten vernichtet wurden.

Durch Inaugenscheinnahme konnten wir uns davon überzeugen, dass zwar Patientenakten nach ca. zehn Jahren von der aktuellen Registratur in eine Altregistratur überführt werden, die sich in gesonderten Räumen des Zentrums befindet. Dies wurde von uns ausdrücklich begrüßt. Keinen Anlass für Beanstandungen sahen wir in der tradierten Praxis der Führung der aktuellen Registratur und des Verfahrens bei der Anforderung von Patientenunterlagen über frühere Aufenthalte im Zentrum sowie die Entscheidungsmechanismen bei der Anforderung von Patientenunterlagen des Zentrums durch externe Stellen. Hier besteht die leider nur auf mündlicher Weisung beruhende Praxis, dass der ärztliche Direktor im Einzelfall entscheidet, ob Akten und Informationen an Kliniken, Arztpraxen, Gerichte, Versicherungen etc. übermittelt werden dürfen; auch die Art und Weise, wie dies im Einzelfall zu geschehen hat (Brief, Telefax etc.), ist nicht schriftlich geregelt. Im Rahmen der noch zu erstellenden Archivordnung haben wir das Zentrum gebeten, die oben beschriebene Praxis für diese Einrichtung bzw. den Zentren-Verbund verbindlich festzuschreiben.

Die Altregistratur, die in den Kellerräumen eines früheren Klostergebäudes auf dem Gelände des Zentrums untergebracht ist, enthält nach unserer Feststellung viele Akten, bei denen die Behandlungsabschlüsse erheblich länger als 30 Jahre zurückliegen und zum Teil sogar noch weit in das vorletzte Jahrhundert zurückreichen. So fielen uns bei Stichproben verschiedene Akten in die Hände, in denen Daten von Patienten gespeichert waren, die schon lange vor dem Jahr 1900 geboren waren (u. a. 1868, 1869 etc.). Wie uns vor Ort mitgeteilt wurde, habe man Akten von Patienten mit psychischen Erkrankungen, die vor das Jahr 1945 zurückreichten, zunächst – wie es richtig ist – dem Staatsarchiv zur Übernahme angeboten. Dieses habe jedoch nur bestimmte Dokumente übernommen und die übrigen nach Prüfung wieder an das Zentrum zurückgegeben. Gleichwohl habe man sich dort aus „medizin-historischen“ Gründen nicht dazu entschließen können, die Patientenakten endgültig zu vernichten.

Datenschutzrechtlich stellt diese Praxis einen Verstoß gegen § 9 Abs. 2 LDSG dar, wonach organisatorische Maßnahmen getroffen werden müssen, die erforderlich sind, um eine datenschutzgerechte Datenverarbeitung zu gewährleisten. Nach § 23 LDSG sind personenbezogene Daten immer dann zu löschen, wenn sie für die weitere Aufgabenerfüllung nicht mehr erforderlich sind. Altakten, die über Patienten aufbewahrt werden, die schon seit vielen Jahrzehnten verstorben sind, rechtfertigen jedenfalls keine Aufbewahrung im Rahmen der originären Aufgabenerfüllung eines Zentrums. Hierfür gibt es das Regelwerk des Archivrechts, wonach dem Staatsarchiv zunächst die Unterlagen zur Übernahme anzubieten sind und – falls diese von dort nicht übernommen werden – nach den Regelungen des Datenschutzes in geeigneter Weise zu vernichten sind. Nachdem das von uns kontrollierte Zentrum organisatorisch einem Zentren-Verbund angehört, haben wir in unserem Prüfbericht die Geschäftsführung gebeten, durch die Schaffung einer schriftlichen Registraturordnung für die gesamten dem Verbund an-

gehörenden Zentren ein den Anforderungen des Datenschutzes gerecht werdendes Regelwerk zu schaffen.

Auf die von meiner Dienststellte festgestellten Defizite hat man erfreulich rasch und professionell reagiert. So wurden wir darüber informiert, dass bereits kurz nach unserem Kontrollbesuch eine Arbeitsgruppe eingesetzt wurde, in der alle Standorte der Südwürttembergischen Zentren für Psychiatrie vertreten sind und die sich der Fragen des Umgangs mit den Altaktenbeständen annehmen soll. Darüber hinaus hat man – sozusagen im Vorgriff – bereits eine vorläufige Archivordnung für einen Übergangszeitraum verabschiedet. Die eingerichtete Arbeitsgruppe selbst hat sich zum Ziel gesetzt, eine neue gemeinsame Archivordnung mit Gültigkeit für alle Unternehmensbereiche zu erarbeiten und dabei die Art und Weise, die Dauer und den Umfang der Archivierung, aber auch die Wahrung evtl. bestehender historischer Interessen zu berücksichtigen. Mitglieder der Arbeitsgruppe sind neben dem Datenschutzbeauftragten des Zentrums, Leitende Ärzte aus dem Zentren-Verbund sowie ein Medizinhistoriker der Universität Ulm. Auch soll noch einmal mit dem zuständigen Staatsarchiv der archivrechtliche Umgang mit den Altakten abgestimmt werden. Der von der Geschäftsführung in diesem Zusammenhang geäußerten Bitte um unterstützende Beratung durch meine Dienststelle werden wir uns selbstverständlich nicht verschließen.

2.6 Patientenrechte

Eine Frage, die meine Dienststelle im Rahmen von Eingaben oder Beratungsersuchen immer wieder erreicht, betrifft das Einsichtsrecht von (Psychiatrie-)Patienten in die Krankenunterlagen. Die nachstehenden Ausführungen haben deshalb auch keinen konkreten Bezug zum Kontrollbesuch im Zentrum, sondern sollen die Ausführungen ergänzen und dadurch eine allgemeine Hilfestellung für die Praxis bei der Behandlung von Anfragen geben.

Die Pflicht für Arzt und Krankenhaus, Patientenakten über die gesamte Behandlung von der Anamnese über die Diagnose bis zur Therapie und zum Eingriff, zur postoperativen Behandlung und zur Entlassung zu führen, ist nicht nur eine sich aus dem Behandlungsvertrag ergebende Pflicht gegenüber dem Patienten, sondern nach § 10 Abs. 1 MBO-Ä eine Berufspflicht. Ging man früher noch davon aus, dass die Aufzeichnungen des Arztes diesem lediglich als eigene Gedächtnisstütze dienen und insofern für ein Einsichtnahmerecht des Patienten kein Grund bestehe, ist mittlerweile sowohl in der einschlägigen Literatur wie auch in der Rechtsprechung unumstritten, dass die Dokumentation und das Ermöglichen der Einsicht in die Krankenbehandlung für den Arzt und für den Krankenhausträger verbindliche Nebenpflichten aus dem Behandlungsvertrag darstellen (vgl. u. a. BGH, Urteil vom 23. November 1982 – VI ZR 222/79). Aus dem der Behandlung zugrunde liegenden Vertragsverhältnis in Verbindung mit dem Selbstbestimmungsrecht und der personalen Würde des Patienten (Grundrecht auf Datenschutz, das aus dem allgemeinen Persönlichkeitsrecht des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes hergeleitet wird, vgl. sog. Volkszählungsurteil des Bundesverfassungsgerichts [BVerfGE 65,1]) resultiert auch dessen Anspruch auf Einsicht in die über seine Behandlung geführten Krankenunterlagen. § 10 Abs. 2 MBO-Ä bestimmt ausdrücklich und folgerichtig, dass Patienten auf ihr Verlangen grundsätzlich ein Einsichtsrecht in die sie betreffenden Krankenunterlagen haben; ausgenommen sind nur diejenigen Teile, die subjektive Eindrücke oder Wahrnehmungen der Behandler enthalten. Dem Patienten muss eine frei verantwortliche Entscheidung über die Möglichkeit, eine ärztliche Behandlung selbstständig und kritisch überprüfen zu können, eingeräumt werden. Dies erfordert die Kenntnis des Krankheitsbilds und des in den Akten dokumentierten Behandlungsablaufs. Als Ausfluss dieses Rechts auf informationelle Selbstbestimmung kann der Patient daher vom Arzt und vom Krankenhausträger grundsätzlich auch außerhalb eines Rechtsstreits Einsicht in die ihn betreffenden Krankenunterlagen verlangen. Ein besonderes schutzwürdiges bzw. rechtliches Interesse an

der Einsichtnahme wird hierfür nicht gefordert, da sich dieses bereits aus dem allgemeinen Persönlichkeitsrecht des Patienten ergibt.

Der Bundesgerichtshof hat in seiner oben erwähnten grundlegenden Entscheidung weiter ausgeführt, dass sich das Einsichtnahmerecht des Patienten nur auf naturwissenschaftlich objektivierbare Befunde und Behandlungsfakten beziehe. Aufzeichnungen des Arztes über persönliche Eindrücke (z. B. subjektive Werturteile bzw. emotional gefärbte Bemerkungen des Arztes), die oftmals zwangloser und deutlicher abgefasst würden, könnten hingegen dem Patienten vorenthalten werden. Diese Rechtsprechung des Bundesgerichtshofs wurde durch einen Beschluss des Bundesverfassungsgerichts vom 16. September 1998 – 1 BvR 1130/98 – bestätigt und konkretisiert.

Eine Einschränkung des Einsichtnahmerechts des Patienten wegen (angeblich) entgegenstehender therapeutischer Gründe wird häufig als sog. therapeutisches Privileg bezeichnet. Dies bedeutet, dass der Arzt in Einzelfällen eine ungünstige Prognose oder eine schwerwiegende Erkrankung verschweigen oder verharmlosen darf, um die Heilungsaussichten nicht zu beeinträchtigen. Die Rechtsprechung erkennt ein solches therapeutisches Privileg jedoch nur ganz ausnahmsweise an, da ansonsten die Gefahr bestünde, dass das grundrechtlich garantierte Selbstbestimmungsrecht des Patienten ausgehöhlt würde. Die Reduktion auf eng begrenzte Ausnahmefälle wird durch eine aktuelle Entscheidung des Bundesverfassungsgerichts (Beschluss vom 9. Januar 2006 – 2 BvR 443/02) bestätigt. Diese Entscheidung betrifft zwar unmittelbar ein anderes Thema, nämlich das Auskunftsrecht eines im Maßregelvollzug Untergebrachten, gibt in seinen Leitsätzen jedoch auch über diesen Fall hinaus wichtige Auslegungshinweise:

– Der Patient hat danach generell ein geschütztes Interesse daran zu erfahren, wie mit seiner Gesundheit umgegangen wurde, welche Daten sich dabei ergeben haben und wie man die weitere Entwicklung einschätzt. Dies gilt im gesteigerten Maße für Informationen über die psychische Verfassung.
– Es bleibt nach Meinung des Gerichts ausdrücklich offen, ob die Rechtsprechung des Bundesgerichtshofs, die den Anspruch des Patienten auf Einsicht in die ihn betreffenden Krankenunterlagen grundsätzlich auf sog. objektive Befunde beschränkt und einen sog. therapeutischen Vorbehalt anerkannt hat, noch verfassungsgemäß ist.

Im Hinblick auf die sich in der Rechtsprechung abzeichnende Ausdehnung des Informationsrechts des Patienten auch bei einem psychiatrisch-medizinischen Sachverhalt wird man sich in der Auskunftspraxis nur noch in äußerst seltenen Fällen auf einen therapeutischen Vorbehalt berufen können, der dann gegebenenfalls auch einer juristischen Prüfung standhalten muss. Wenn demzufolge auch „heikle“ Notizen für den Patienten unter Umständen zukünftig einsehbar sein werden, empfiehlt es sich, dies von vornherein bei beabsichtigten Aufzeichnungen zu bedenken und vorschnelle, möglicherweise entwürdigende oder beleidigende Formulierungen gänzlich zu vermeiden.

Ergänzend sei noch darauf hingewiesen, dass das Landeskrankenhausgesetz Baden-Württemberg (LKHG) – anders als zum Teil in anderen Bundesländern – keine datenschutzrechtliche Sonderbestimmung über das Patientenauskunftsrecht enthält. Allerdings verweist § 43 Abs. 5 LKHG u. a. auf die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten (Anmerkung: Je nach Trägerschaft des Krankenhauses kann dies das Landesdatenschutzgesetz oder das Bundesdatenschutzgesetz sein). Insoweit besteht auch über diese Verweisungsvorschrift nach § 21 LDSG bzw. § 19 BDSG ein grundsätzlicher Anspruch auf Auskunft und Akteneinsicht des Patienten über die zu seiner Person gespeicherten Krankendaten.

2.7 Dienstanweisungen zum Datenschutz

Das Zentrum hatte u. a. Dienstanweisungen für die Nutzung von Personalcomputern, Laptops, Personal Digital Assistants – PDAs – und sonstigen tragbaren IT-Geräten, für die Nutzung des Internets und von USB-Geräten und -Schnittstellen sowie zu den Telefaxsystemen, zur Fernwartung und zu Telearbeitsplätzen erlassen. Dabei war besonders anzuerkennen, dass neben „klassischen“ Themen wie PC-Einsatz, Telefax oder die Nutzung des Internets auch Themenbereiche wie Einsatz von USB-Medien sowie mobile Informations- und Kommunikationstechnik (IuK) behandelt wurden. Bei einer Durchsicht stellten wir hinsichtlich dieser Unterlagen zum einen noch einen gewissen Änderungsbedarf fest. Zum anderen deckten die übersandten Regelungen nicht alle datenschutzrelevanten Bereiche ab. So fehlten in den Dienstanweisungen Vorgaben zur Konfiguration der Internet-Firewall oder lokaler Netzwerkkomponenten. Da es sich dabei um IuK-Systeme handelt, die zahlreiche datenschutzrechtliche Fragestellungen aufwerfen und für deren datenschutzgerechten Betrieb umfassende Maßnahmen konzipiert und umgesetzt werden müssen, ist es unverzichtbar, auch für deren Nutzung organisatorische Regelungen zu treffen. Diese können etwa in Vorgaben zur Konfiguration oder zu Verfahrensweisen zur Beantragung oder Änderung der im Netz vorhandenen Kommunikationsmöglichkeiten bestehen. Da das Fehlen derartiger schriftlicher Unterlagen einen datenschutzrechtlichen Mangel darstellt, wiesen wir das Zentrum darauf hin, dass noch fehlende Regelungen alsbald zu treffen sind. Zudem forderten wir das Zentrum auf, ein internes Datenschutzmanagement zu etablieren, das sicherstellt, dass bei der Konzeption neuer oder der Änderung bestehender sicherheitsrelevanter Systeme rechtzeitig die notwendigen Datenschutz- und Sicherheitsmaßnahmen berücksichtigt werden. Das Zentrum sagte zu, dies umzusetzen.

2. Abschnitt: Die gesetzliche Krankenversicherung

1. Kundenwerbung – Ein Dauerbrenner

Zu einem datenschutzrechtlichen Dauerbrenner scheint sich das Bemühen der Krankenkassen zu entwickeln, die ihnen durch das im Jahr 2003 beschlossene Gesetz zur Modernisierung der gesetzlichen Krankenkassen eingeräumte Wettbewerbsfreiheit offensiv in der Praxis zu nutzen. Dass das Werben um neue Kunden allerdings bestimmten datenschutzrechtlichen Spielregeln unterliegt, hatten wir bereits in unserem letztjährigen Tätigkeitsbericht näher beleuchtet (LT-Drucksache 14/650). Im Berichtszeitraum mussten wir erneut tätig werden und dabei insbesondere einem Spezialversicherer für Handwerker die Grenzen des datenschutzrechtlich Machbaren aufzeigen.

So ging bei uns eine Beschwerde darüber ein, dass verschiedene Arbeitgeber von zwei Regionaldirektionen dieser Krankenkasse Anfang 2007 Werbepost erhalten hatten. In Serienbriefen, denen jeweils ein Rückantwortschein angeschlossen war, baten die Regionaldirektionen die Arbeitgeber um Mitteilung, welche der bei ihnen beschäftigten Mitarbeiter und Auszubildenden bisher noch nicht bei der Krankenkasse versichert sind. Die Firmen wurden darin um die Übermittlung folgender personenbezogener Daten ihrer Beschäftigten – getrennt nach Mitarbeitern und Azubis – gebeten: Name, Vorname, Straße, Postleitzahl/Ort und Telefon. Bezüglich der Mitarbeiter wurde darüber hinaus auch noch gefragt, bei welcher Kasse diese derzeit versichert sind. Hinsichtlich der Auszubildenden war die Krankenkasse auch daran interessiert zu erfahren, wann diese ihre Ausbildung begonnen hätten und ob für sie bereits ein Vorvertrag bestehe oder nicht.

In der von uns daraufhin von der Krankenkasse eingeholten Stellungnahme vertrat diese zunächst die Auffassung, dass es § 284 Abs. 4 des Fünften Sozialgesetzbuchs – SGB V – (ohne weiteres) zulasse, Daten zur Gewinnung von Mitgliedern zu erheben, zu verarbeiten und zu nutzen. Darüber hinaus sei das Fehlen einer wirksamen datenschutzrechtlichen Einwilligungsklau-

sel in den Serienbriefen nur darauf zurückzuführen, dass die Krankenkasse einen neuen sog. Lettershop mit der Durchführung dieser Art der Kundenwerbung beauftragt habe (Outsourcing). Unsere Antwort darauf war unmissverständlich: Den Versuch, an Adress- und sonstige personenbezogene Daten von potenziellen Kunden ohne deren ausdrückliche schriftliche Einwilligung (über deren Arbeitgeber) zu gelangen, lässt § 284 Abs. 4 Satz 1 SGB V nach seinem eindeutigen Wortlaut nur dann zu, wenn die dafür benötigten Daten aus allgemein zugänglichen Quellen erhoben werden. In allen anderen Fällen stellt sich die Rechtslage wie folgt dar:

Gemäß § 67 b Abs. 1 Satz 1 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) ist eine Verarbeitung personenbezogener Daten, wozu auch die Datenerhebung zählt, nur dann zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder – was im vorliegenden Fall die einzig mögliche Alternative war – die Betroffenen in die Erhebung ausdrücklich eingewilligt haben. Die Einwilligung hätte darüber hinaus gemäß § 67 b Abs. 2 Satz 3 SGB X der Schriftform bedurft. Auch der Versuch der Krankenkasse, die Verantwortung der datenschutzrechtlichen Fehlleistung auf Dritte, den Lettershop, abzuwälzen, erwies sich als untauglich. Denn bei einem solchen Vorgehen handelt es sich um eine Datenverarbeitung im Auftrag, bei der der Auftraggeber für die Einhaltung der Vorschriften über den Datenschutz nach wie vor verantwortlich bleibt (vgl. u. a. § 80 Abs. 1 SGB X). Die sich aus dieser Verantwortlichkeit ergebende Verpflichtung beschreibt § 80 Abs. 2 SGB X näher. Danach ist der Auftraggeber zunächst gehalten, den Auftragnehmer sorgfältig auszuwählen, um anschließend den Auftrag schriftlich zu erteilen. Der Auftraggeber hat sich im Übrigen beim Auftragnehmer von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zur Wahrung eines ausreichenden Datenschutzstandards zu überzeugen.

Erfreulicherweise zeigte sich die Krankenkasse schließlich doch einsichtig und teilte uns mit, dass man nunmehr die Ablaufprozesse so gestalten wolle, dass vor einer Produktionsfreigabe an externe (Werbe-)Firmen immer erst eine Endabnahme durch ihren behördlichen Datenschutzbeauftragten zu erfolgen habe. Dadurch soll künftig vermieden werden, dass eine Einwilligungsklausel bei entsprechenden Datenerhebungen fehlt. Bezüglich der der Krankenkasse durch diese datenschutzrechtlich unzulässige Aktion bereits zugegangenen Antwortscheine zeigte man sich ebenfalls kooperativ. Letztlich konnte folgende von uns mitgetragene Lösung gefunden werden: Die Krankenkasse tritt über den Arbeitgeber an die Arbeitnehmer heran und bittet diese nachträglich um deren ausdrückliches Einverständnis in die mit der beschriebenen Werbemaßnahme ursprünglich beabsichtigte Datennutzung. Wird diese verweigert, erfolgt unverzüglich eine Datenlöschung.

Unter dem Motto „Sind Sie wirklich zufrieden mit Ihrer Krankenkasse?“ hatte dieselbe Krankenkasse im Berichtszeitraum bereits eine weitere Aktion zur Gewinnung von Neukunden gestartet. Mit dem Unterschied zur ersten Aktion, dass die mit einer Rückantwortkarte versehenen Anschreiben nunmehr von allen Regionaldirektionen in Baden-Württemberg an über 500 000 potenzielle Kunden versandt wurden. Ein betroffener Mitbürger beklagte sich bei meiner Dienststelle u. a. darüber, dass die für die Rückantwort bestimmte Postkarte an ihn (Anmerkung: die Adressdaten waren bereits aufgedruckt) keinen Hinweis darauf enthielt, dass die dort erbetenen Angaben bezüglich Telefon und E-Mail-Anschrift freiwillig erfolgen. Im Übrigen mussten wir anhand der übersandten Unterlagen feststellen, dass weder aus der Rückantwortkarte noch aus der Werbebroschüre ersichtlich wurde, wie lange die Krankenkasse die Daten bei sich zu speichern beabsichtigte. Auf der Antwortkarte hatten die Angeschriebenen drei Alternativen zum Ankreuzen: 1. Die Bitte um einen persönlichen Besuch; 2. Die Bitte um ein telefonisches Beratungsgespräch; 3. Die Bitte (lediglich) um die Übersendung von weiterem Info-Material der Krankenkasse.

Auf die datenschutzrechtliche Problematik des Vorgehens angesprochen, teilte uns die Krankenkasse mit, dass auch in diesem Fall ein Lettershop in ihrem Auftrag die Serienbriefe mit Hilfe „angemieteter“ Adressdaten durchgeführt habe. Die dem Anschreiben beigefügten Antwortkarten sollten lediglich dazu dienen, die Krankenkasse darüber zu informieren, dass Interesse an einer Kontaktaufnahme bzw. der Übermittlung von weiterem Infor-

mationsmaterial besteht. Dabei liege es nach Auffassung der Krankenkasse im Ermessen der Betroffenen, ob sie die Karte überhaupt nutzen und dabei zusätzlich ihre Telefonnummer und/oder ihre E-Mail-Anschrift als Kontaktadresse angeben. Auf diese Weise meinte die Krankenkasse den im Sozialdatenschutz verankerten Grundsatz der „Freiwilligkeit“ bei der Erhebung von Kundendaten gewahrt zu haben. Hinsichtlich der Speicherdauer teilte man uns zunächst nur lapidar mit, dass im Rahmen der beschriebenen Werbeaktion – wenn keine Mitgliedschaft zu Stande komme – die Daten dann gelöscht würden, sobald sie für die Zwecke der Mitgliedergewinnung nicht mehr benötigt werden.

Nachdem wir uns mit diesen Ausflüchten der Krankenkasse nicht zufrieden gaben und nochmals nachhakten, räumte man kleinlaut ein, dass es bisher zu diesem speziellen Thema keine betriebsinternen Regelungen in Form einer Dienstanweisung gebe. Genauere Fristen für die Speicherung und Löschung solcher im Rahmen von Werbeaktionen gewonnenen Daten seien daher noch nirgends schriftlich festgelegt. Es wurde zugesagt, dies nunmehr aufgrund unserer Anregungen und Hinweise nachzuholen. Die Krankenkasse möchte dabei – je nach Fallkonstellation – eine Streuung der Aufbewahrungsdauer bei Erwachsenen von sechs Monaten bis zu vier Jahren vorsehen sowie bei Kindern und Jugendlichen sogar so lange, wie diese noch zur Schule gehen oder studieren. Ohne dass im Zeitpunkt der Drucklegung des Tätigkeitsberichts eine abschließende Beratung gegenüber der Krankenkasse möglich gewesen wäre, halten wir bei derartigen Werbeaktionen im Grundsatz eine Höchstnutzungsdauer in Anlehnung an § 175 Abs. 4 Satz 5 SGB V für die Dauer von maximal zwei Jahren für zulässig. Etwas anderes gilt nur dann, wenn der Betroffene erneut von sich aus gegenüber der Krankenkasse wieder aktiv wird. Redlicherweise kann eine Krankenkasse nach einer so langen Zeitdauer nicht mehr davon ausgehen, dass ein einmal angeschriebener potenzieller Kunde nach über zwei Jahren an einem Wechsel der Krankenkasse noch interessiert ist. Der datenschutzrechtliche Hinweis, so wie ihn die Krankenkasse zukünftig in ihre Werbebroschüren aufnehmen möchte („Ich bin damit einverstanden, dass die [Name der Krankenkasse] meine Daten speichert und nutzt, um mich informieren und beraten zu können. Ein Widerruf ist jederzeit möglich, meine Daten werden dann gelöscht.“) stellt zwar eine Verbesserung gegenüber der bisherigen Werbepraxis dar. Gleichwohl vermag diese Formulierung die oben dargestellten datenschutzrechtlichen Bedenken meines Amts nicht vollständig auszuräumen, da sie keinen Hinweis auf die Dauer der Datenspeicherung enthält.

2. Das Fahrradturnier und seine Folgen

Dass der Profiradsport durch Doping-Vorwürfe ins Zwielicht gerückt ist und immer wieder neue Enthüllungen an die Öffentlichkeit gelangen, überrascht eigentlich niemanden mehr. Erstaunt waren wir allerdings, dass ein von einem Automobilclub zusammen mit einer unserer Kontrolle unterliegenden Krankenkasse veranstaltetes Fahrradturnier dunkle datenschutzrechtliche Schatten auf eine an sich gute Sache werfen konnte. Was war geschehen?

Ein verärgerter Vater hatte sich an meine Dienststelle gewandt, weil sein noch minderjähriger Sohn ohne erkennbaren Anlass von einer Krankenkasse angeschrieben worden war, obwohl weder er noch der Sohn dort familienversichert waren. Eine Nachfrage bei der Krankenkasse ergab eine überraschende Erklärung: Mit einer auf Bezirksebene durchgeführten Werbeaktion in Form eines „Berufsstarterangebots“ versuchte die Krankenkasse Jugendliche – werbestrategisch geschickt als Angebot für ein sog. Bewerbertraining verpackt – gezielt anzusprechen und sie auf diese Weise als Neukunden zu gewinnen. Im Rahmen dieser Aktivitäten wurden sowohl Familienangehörige als auch jugendliche Personen, deren Daten man im Rahmen von unterschiedlichen Aktionen (z. B. Preisausschreiben, Fahrradturniere etc.) als vermeintliche Interessenten gewonnen hatte, angeschrieben. Insgesamt erhielten auf diese Weise immerhin ca. 5 000 Personen inhaltsgleiche Werbesendungen.

Besonders ärgerlich für die Betroffenen – neben anderen von uns im weiteren Verfahren festgestellten datenschutzrechtlichen Verstößen – war, dass

die Krankenkasse die Adressdaten anlässlich eines in Oberschwaben veranstalteten Jugend-Fahrrad-Turniers erlangt hatte, das gemeinsam mit einem allgemein in gutem Ruf stehenden Automobilclub bereits vor vier Jahren (im Jahr 2002) durchgeführt worden war. Wie unsere Recherchen weiter ergaben, war seinerzeit die Abgabe einer Teilnahmeerklärung Voraussetzung, um überhaupt an diesem Fahrradturnier teilnehmen zu können. Die Erklärungen selbst mussten sowohl von den jugendlichen Teilnehmern als auch von deren Erziehungsberechtigten unterschrieben werden. Der Bitte, uns Originale dieser Teilnahmeerklärungen zur Einsicht vorzulegen, konnte man (leider) nicht mehr entsprechen, weil diese dort bereits vernichtet waren, nachdem die Krankenkasse zuvor das für sie Wichtigste – nämlich die Adressdaten der Jugendlichen – für Werbezwecke gespeichert hatte.

Auf die aus Sicht des Datenschutzes unzulässige Vorgehensweise der Krankenkasse angesprochen, räumte diese unumwunden ein, dass es für die anlässlich des Fahrradturniers gewonnenen Adressdaten und deren spätere Nutzung keine wirksamen Einwilligungserklärungen der Betroffenen gebe. Darüber hinaus entspreche die Vorgehensweise nicht den internen datenschutzrechtlichen Anforderungen, wie sie für die korrekte Ansprache von Kunden im Rahmen von Werbeaktionen im Datenschutzhandbuch der Krankenkasse festgeschrieben seien. Im Übrigen habe man auch schon vor mehreren Jahren in den internen Dienstanweisungen festgelegt, dass Adressgewinnungslisten vor Ort bei den Bezirksdirektionen archiviert werden müssten, um bei Streitfällen gegebenenfalls die ordnungsgemäße Speicherung der Daten und die Rechtmäßigkeit der Werbemaßnahmen belegen zu können. Das Datenschutzhandbuch weise ferner ausdrücklich darauf hin, dass die Archivierung unbedingt so lange zu erfolgen habe, wie die Einwilligungserklärungen der Einzelnen Grundlage für die Speicherung und Nutzung der betreffenden Daten seien. Ebenso eindeutig stellten die Handlungsanweisungen für die Beschäftigten der Krankenkasse klar, dass bei solchen Datenerhebungsmaßnahmen streng auf die Freiwilligkeit bei der Beantwortung der Fragen – wie es im Verhältnis zu Interessenten immer der Fall sein müsse – hinzuweisen ist.

Die datenschutzrechtliche Bewertung des Falls ergibt sich unmittelbar aus dem Gesetzestext. Sowohl die Gewinnung der Adressdaten im Jahre 2002 anlässlich des Fahrradturniers als auch die darauf beruhenden Anschreiben an mögliche Interessenten für eine Krankenversicherung verstießen gegen § 4 LDSG. Wesentlich ist dabei, dass versäumt wurde, die Jugendlichen und auch die Erziehungsberechtigten auf die Freiwilligkeit ihrer Angaben, den eigentlichen Zweck der Erhebung und Verarbeitung ihrer Daten, die Speicherdauer und die Möglichkeit des jederzeitigen Widerrufs der von ihnen gemachten Angaben hinzuweisen. Im Übrigen muss eine Einwilligungserklärung schon in ihrem Schriftbild deutlich vom Erscheinungsbild der sonstigen Erklärungen abgehoben sein.

Soweit aus einem solchen Vorgang überhaupt positive Schlüsse gezogen werden können, dann diese, dass die Krankenkasse selbst aktiv zur Aufklärung des Sachverhalts beigetragen und die objektiv nicht unerheblichen Datenschutzverstöße auch unumwunden eingeräumt hat. Auch konnten wir feststellen, dass es mit dem Datenschutzhandbuch der Krankenkasse tatsächlich bereits ein Regelwerk gibt, bei dessen strikter Beachtung derartige Datenschutzverstöße nicht hätten passieren dürfen. Die Krankenkasse hat zudem glaubhaft versichert, den Vorfall zum Anlass zu nehmen, im Rahmen von zusätzlichen Mitarbeiterinformationen nochmals ausführlich über die datenschutzrechtlichen Anforderungen bei der Durchführung von Werbemaßnahmen hinzuweisen und deren strikte Beachtung anzumahnen. Auf die Durchführung weiterer Fahrradturniere zur gezielten Ansprache von Jugendlichen (als eigentliche Triebfeder für diese Aktionen) hat die Krankenkasse inzwischen ebenfalls verzichtet und gegenüber meiner Dienststelle schriftlich erklärt, dass man die seinerzeit unzulässig erhobenen Adressdaten gelöscht habe.

3. Einreichung ärztlicher Verordnungen im Rahmen der häuslichen Pflege

Der regelmäßige Erfahrungsaustausch der Datenschutzbeauftragten von Bund und Ländern ist eine wichtige Erkenntnisquelle für die tägliche Arbeit

meiner Dienststelle, erfahren wir doch auf diese Weise, wenn sich andernorts neue Entwicklungen ergeben. Durch eine Umfrage eines Kollegen aus den neuen Bundesländern wurden wir darauf aufmerksam, dass Träger häuslicher Pflegedienste in der Praxis anscheinend Probleme damit haben, die Vorgaben der Richtlinie des Bundesausschusses der Ärzte und Krankenkassen über die Verordnung von „häuslicher Krankenpflege“ nach § 92 Abs. 1 Satz 2 Nr. 6 und Abs. 7 SGB V einzuhalten. Danach besteht die Verpflichtung, innerhalb von drei Arbeitstagen die Verordnung bei der die Kosten tragenden Krankenkasse einzureichen. Sehr oft kann die genannte Drei-Tages-Frist bei einem Versand der Verordnungen per Post durch die Pflegedienste nicht eingehalten werden. Datenschutzrechtliche Schwierigkeiten können sich meist dann ergeben, wenn die Verordnungen – zur Fristwahrung – von den Pflegediensten vorab per Telefax übermittelt werden.

Um die Abrechnungspraxis in Baden-Württemberg in Erfahrung zu bringen, haben wir bei der größten Krankenkasse im Land um Auskunft gebeten, wie dort mit diesen Fällen verfahren wird. Folgendes wurde uns berichtet:

Nummer 24 der genannten Richtlinie sieht lediglich vor, dass die Krankenkassen bis zur Entscheidung über die Genehmigung der Pflegemaßnahme die vom Vertragsarzt verordneten und vom Pflegedienst erbrachten Leistungen zu vergüten haben, wenn die Verordnung spätestens am dritten auf die Ausstellung folgenden Arbeitstag der Krankenkasse vorgelegt wird. Sollte eine Verordnung später bei der Krankenkasse eingehen, so hat dies zur Folge, dass die Krankenkasse nicht verpflichtet ist, die erbrachten Leistungen dem Pflegedienst zu vergüten.

Bei der von uns befragten Krankenkasse gibt es die Anordnung, dass bei Leistungspflicht der Krankenkasse eine Kostenübernahme sowohl bei Posteingang innerhalb als auch außerhalb der Frist vorgenommen wird. Sofern keine Leistungspflicht nach der oben genannten Richtlinie besteht, werden gleichwohl innerhalb der Eingangsfrist von drei Werktagen die Kosten bis zur Ablehnung übernommen. Außerhalb der Frist wird eine Kostenübernahme jedoch abgelehnt. Weiter wurde uns über die dortige Versicherungspraxis noch berichtet, dass die Krankenkasse

- die datenschutzrechtlichen Voraussetzungen bei der Datenübermittlung per Telefax – insbesondere was den Telefax-Empfang von besonders zu schützenden Daten anbelangt – in ihrem Datenschutzhandbuch in einem besonderen Kapitel geregelt hat. Dieses Verfahren soll gleichwohl nur im Ausnahmefall – auch hinsichtlich der Pflegedienste – angewendet werden;
- dadurch einen datenschutzkonformeren Weg anbietet, dass sie eine verschlüsselte Übertragungsmöglichkeit auch für „Partner im Gesundheitswesen“ über ein Internet-Portal anbietet. Sobald der Vertragspartner der Krankenkasse die ausgefüllte und unterschriebene Verpflichtungserklärung zugeschickt hat, kann der Zugang durch die Krankenkasse freigeschaltet werden. Über ein sicheres Postfach können danach die besonders schützenswerten Gesundheitsdaten zwischen Krankenkasse und dem Vertragspartner ausgetauscht werden. Die Pflegedienste können über diese Möglichkeit die Verordnungen verschlüsselt übermitteln.

Das vorstehend beschriebene Verfahren wird von meiner Dienststelle ausdrücklich begrüßt und zur Nachahmung auch für andere Krankenkassen empfohlen. Erfreulich ist, dass aufgrund unserer Nachfrage eine weitere Verfahrensverbesserung insoweit vorgenommen wurde, dass künftig die Pflegedienste, die ihre Verordnungen nach wie vor per Telefax vorab übermitteln, ausdrücklich darauf hingewiesen werden, dass ihnen die Krankenkasse über das genannte Internet-Portal eine sichere Übertragungsmöglichkeit anbietet. Parallel dazu wurden auch die Bezirksdirektionen darüber informiert.

Sollten die Pflegedienste gleichwohl das angebotene Internet-Portal nicht nutzen (können), versucht die Krankenkasse die datenschutzrechtlichen Risiken, die eine Telefaxübertragung immer mit sich führt, durch folgende zusätzliche Maßnahmen noch weiter zu mindern:

– Intern stellt die Krankenkasse künftig sicher, dass nur ein fest zugeordnetes Telefaxgerät für die Annahme und Übermittlung der Verordnungen im Pflegebereich zum Einsatz kommt. Das Gerät sollte möglichst über einen Zwischenspeicher verfügen, der verhindert, dass z. B. in den Abendstunden oder am Wochenende Telefaxausdrucke im Postkorb beim Gerät verbleiben. Ist dies kurzfristig nicht möglich, muss zumindest organisatorisch sichergestellt werden, dass keine Unbefugten von den Verordnungen Kenntnis erhalten.

– Die Krankenkasse wird die Pflegedienste veranlassen, dass diese eine feste (einprogrammierte) Kurzwahl mit der Telefax-Nummer der Krankenkasse verwenden.

Wir haben diese Vorschläge ausdrücklich begrüßt und zusätzlich empfohlen, ein in einem anderen Bundesland (Brandenburg) von einer Krankenkasse bereits praktiziertes Verfahren aufzugreifen: Danach soll die Systemlandschaft so verändert werden, dass eingehende Telefaxe entweder an den Arbeitsplatz-PC der bearbeitenden Mitarbeiter gesandt oder – was datenschutzrechtlich besonders interessant ist – nur noch per PIN-Eingabe bzw. personengebundener Chipkarte von den Telefax-Geräten abgeholt werden können. Auf die von meiner Dienststelle herausgegebenen Hinweise zum Thema „Datensicherheit beim Telefax“ wird in diesem Zusammenhang hingewiesen; sie können über unsere Homepage (http://www.baden-wuerttemberg.datenschutz.de) heruntergeladen werden.

4. Unterlagen von Fremd- und Zwangsarbeitern kommen in die Staatsarchive

Zwangsarbeit während der NS-Zeit gehört fraglos zu den dunkelsten Kapiteln der deutschen Geschichte. Unterlagen darüber wurden nicht systematisch aufbewahrt. Zu den Quellen, die über das Schicksal der Betroffenen Auskunft geben können, zählen die sog. „Hebelisten“ – dies sind die Versichertenunterlagen – der Allgemeinen Ortskrankenkassen (heute: AOK Baden-Württemberg), die bis zum heutigen Tag zuhauf noch in den Altregistraturen bei den Bezirksdirektionen lagern.

Diese Unterlagen wurden im Rahmen der Arbeit der Stiftung „Erinnerung, Verantwortung, Zukunft“ ausgewertet, um den Opfern eine finanzielle Entschädigung zukommen zu lassen. Meine Dienststelle wurde im Jahr 2000 erstmals mit den sich dabei ergebenden datenschutzrechtlichen Fragestellungen befasst (21. Tätigkeitsbericht für das Jahr 2000, LT-Drucksache 12/6020).

Es dürfte einer breiten Öffentlichkeit meist nicht bekannt sein, dass die während der NS-Zeit zur Zwangsarbeit eingesetzten Fremdarbeiter unfreiwillig Mitglied in der gesetzlichen Krankenversicherung waren und die Versicherungsunterlagen bis heute noch bei der AOK Baden-Württemberg vorhanden sind. Aus archiv- und datenschutzrechtlicher Sicht ergeben sich daraus jedoch schwierige Fragen, die auch dank der intensiven Beratung meiner Dienststelle und der ergebnisorientierten Herangehensweise von AOK und Landesarchiv einer sachgerechten und für alle Beteiligten sinnvollen Lösung zugeführt werden konnten. Eine Archivierung der Unterlagen durch das Landesarchiv wurde offenbar deshalb ins Auge gefasst, weil weder die Hauptverwaltung der AOK Baden-Württemberg noch ihre Bezirksdirektionen über eigene, archivfachlichen Ansprüchen genügende Archive verfügen. Die bei der AOK Baden-Württemberg aufbewahrten Versicherungsunterlagen von Zwangsarbeitern aus der Zeit des Nationalsozialismus werden daher ab Januar 2008 an die Staatsarchive übergeben. Die rechtliche Grundlage dafür bildet ein aus diesem Anlass abgeschlossener Archivvertrag zwischen der AOK Baden-Württemberg und dem Land Baden-Württemberg (Landesarchiv), in dem das Nähere insbesondere über die Übergabe der Unterlagen an die Archive und die Erteilung von Auskünften an Betroffene bzw. deren Angehörige geregelt ist. Wichtig war dabei für mich, dass auch nach Übergabe der Unterlagen an das Landesarchiv Auskunftsersuchen von ehemaligen Zwangsarbeitern in der gleichen Weise entsprochen werden wird, wie dies die Krankenkasse bis dahin selbst

erledigt hatte. Diesem Ziel haben die AOK Baden-Württemberg und das Landesarchiv durch entsprechende vertragliche Regelungen Rechnung getragen. Nach dem mit mir abgestimmten Vertragstext bietet die AOK Baden-Württemberg dem Landesarchiv von vornherein sowieso nur Unterlagen an, die von den einzelnen AOK-Bezirksdirektionen zur Erfüllung ihrer Aufgaben nicht mehr benötigt werden. Für – mit Zeitablauf immer unwahrscheinlicher werdende – Anfragen, mit denen sich ehemalige Zwangsarbeiter oder deren Angehörige doch noch zur Einholung von Auskünften an die Krankenkasse wenden, wurde eine eigene Vertragsklausel entwickelt: Die AOK Baden-Württemberg kann jederzeit auf die von ihr übergebenen Unterlagen für die Zwecke zurückgreifen, für die diese Unterlagen vor der Abgabe an das Landesarchiv verwendet werden durften. Somit ist gewährleistet, dass einerseits die Belange der Betroffenen weiterhin in gleicher Weise wie bisher gewahrt werden und andererseits dem Interesse der Forschung Genüge getan ist, unter Nutzung der Archive mehr Licht in dieses düstere Kapitel unserer Geschichte zu bringen.

Für mich ist dieser Fall ein Musterbeispiel dafür, dass sachgerechte Lösungen gefunden werden können, wenn die datenschutzrechtliche Beratung nach § 31 Abs. 3 LDSG rechtzeitig in Anspruch genommen wird.

3. Abschnitt: Soziales

1. Arbeitslosengeld II – quo vadis?

Auch mit Ablauf des dritten Jahres seit ihrer Einführung steht die Sozialleistung Arbeitslosengeld II weiterhin im Fokus der Öffentlichkeit. Was ist sozial gerecht? Diese Frage wird nicht nur in der Politik, sondern in vielen gesellschaftlichen Kreisen intensiv diskutiert. Betroffen von der Diskussion ist dabei nicht nur das Arbeitslosengeld II, sondern auch die in vielen Fällen vorgelagerte Versicherungsleistung Arbeitslosengeld, umgangssprachlich auch als Arbeitslosengeld I bezeichnet. Monatelang stritten SPD und Union über eine längere Zahlung des Arbeitslosengelds an ältere Arbeitnehmer. Der Koalitionsausschuss verständigte sich nun darauf, Älteren schon bald wieder länger Arbeitslosengeld zu zahlen.

Nicht allein die Dauer der Auszahlung des Arbeitslosengelds, auch die Existenz der für das Arbeitslosengeld II zuständigen Arbeitsgemeinschaften steht dieses Jahr auf dem Prüfstand. Im Mai 2007 fand vor dem Bundesverfassungsgericht in Karlsruhe die mündliche Verhandlung der Verfassungsbeschwerde von elf Landkreisen statt, die gegen die Verpflichtung, Arbeitsgemeinschaften mit der Bundesagentur für Arbeit zu bilden, geklagt hatten. In dem Verfassungsbeschwerdeverfahren – 2 BvR 2433/04 – beanstanden die Beschwerdeführer zudem die Zuweisung der Zuständigkeit für einzelne Leistungen der Grundsicherung für Arbeitsuchende ohne Ausgleich der sich daraus ergebenden Mehrkosten. Bis Redaktionsschluss für diesen Tätigkeitsbericht war nicht bekannt, wie das Bundesverfassungsgericht über die Verfassungsbeschwerde entscheiden wird; die Entscheidung soll aber noch in diesem Jahr ergehen. Die andauernde soziale Brisanz der Thematik und die ganz unterschiedlichen Probleme, die mit dem Arbeitslosengeld II verbunden sind, spiegeln sich auch in den zahlreichen Eingaben und Anfragen wider, mit denen meine Dienststelle im Berichtszeitraum wieder befasst war.

Erfreulicherweise sind aus Sicht des Datenschutzes auch positive Entwicklungen zu verzeichnen: Bereits in den vorangegangenen Tätigkeitsberichten berichteten wir vom Datenbanksystem A2LL, das die Erfassung und Verwaltung von finanziellen Leistungen für die Bezieher von Arbeitslosengeld II ermöglicht. Die Datenschutzbeauftragten des Bundes und der Länder fordern hier schon seit dem Jahr 2004 ein klar definiertes Zugriffsberechtigungskonzept und eine Protokollierung (auch) der lesenden Zugriffe. Der Bundesdatenschutzbeauftragte zog im September dieses Jahres nach einem Kontrollbesuch bei der Bundesagentur für Arbeit ein positives Resümee: Das für die Leistungsgewährung genutzte Programm A2LL verfüge nunmehr über die angemahnten, längst fälligen datenschutzrechtlichen Mindeststandards, insbesondere klar definierte, abgestufte Zugriffsberechtigungen. Zudem werden die bundesweiten Zugriffe nun lückenlos protokolliert.

2. Arbeitslosengeld II: Getrennte Aufgabenwahrnehmung – doppelte Vorlagepflicht?

Träger der Leistungen der Grundsicherung für Arbeitsuchende sind die Bundesagentur für Arbeit und die Land- bzw. Stadtkreise als kommunale Träger. Das Zweite Buch des Sozialgesetzbuchs (SGB II) sieht vor, dass die Leistungsträger – soweit der kommunale Träger nicht als sog. optierende Kommune die Aufgaben der Bundesagentur für Arbeit mit übernimmt (siehe hierzu 25. Tätigkeitsbericht für das Jahr 2004, LT-Drucksache 13/3800, und 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650) – zur einheitlichen Wahrnehmung ihrer Aufgaben Arbeitsgemeinschaften errichten. Dies kann durch privatrechtliche oder öffentlich-rechtliche Verträge bewerkstelligt werden. Aber nicht in allen Stadt- und Landkreisen konnten sich die Leistungsträger auf diese Form der Aufgabenerledigung einigen, sodass es bundesweit in knapp 20 Fällen bei der getrennten Aufgabenwahrnehmung geblieben ist. Dabei handelt es sich anscheinend um eine baden-württembergische Besonderheit: Elf Stadt- und Landkreise mit getrennter Aufgabenwahrnehmung liegen im Land.

Die getrennte Aufgabenwahrnehmung hat zur Folge, dass ein Bürger, der Arbeitslosengeld II beantragt, es mit zwei Behörden zu tun hat. Mangelnde Kundenorientiertheit ist aber nicht das einzige Problem der getrennten Aufgabenerledigung. Die Gemeindeprüfungsanstalt Baden-Württemberg hat in ihrem Geschäftsbericht 2007 festgestellt, dass das Modell sowohl qualitativ als auch fiskalisch unbefriedigende Ergebnisse liefert und Synergieeffekte faktisch ausgeschlossen sind. Die vom Gesetzgeber nur als Übergangslösung vorgesehene Konstellation der getrennten Aufgabenwahrnehmung hat auch datenschutzrechtliche Konsequenzen: Da die Aufgaben der Agentur für Arbeit und des kommunalen Trägers nicht von einer Arbeitsgemeinschaft gemeinsam erledigt werden, muss genau darauf geachtet werden, welcher Träger für welche Aufgabe zuständig ist, da hiervon auch die Zulässigkeit der Datenverarbeitung abhängig ist. Wie der folgende Fall zeigt, sieht dies allerdings manch betroffener Träger nicht so eng.

Eine Bürgerin, die Arbeitslosengeld II bezog, wandte sich an meine Dienststelle, weil das Landratsamt von ihr die Vorlage von Kontoauszügen zur Prüfung ihrer Einkommens- und Vermögensverhältnisse verlangt hatte. Die Petentin machte u. a. geltend, dass die Prüfung der Hilfebedürftigkeit der Agentur für Arbeit und nicht dem Landratsamt obliege. Da die Leistungsbezieherin in der Angelegenheit auch eine Petition beim Landtag eingereicht hatte, wandte sich das Ministerium für Arbeit und Soziales, das gegenüber dem Petitionsausschuss des Landtags Stellung zu nehmen hatte, an meine Dienststelle und bat ebenfalls um eine Bewertung des Anliegens der Petentin.

Datenschutzrechtlich stellte sich die Angelegenheit wie folgt dar: Das Arbeitslosengeld II umfasst Leistungen zur Sicherung des Lebensunterhalts einschließlich der angemessenen Kosten für Unterkunft und Heizung. Die Bundesagentur für Arbeit ist Träger der Regelleistung zur Sicherung des Lebensunterhalts, während der kommunale Träger die Leistungen für Unterkunft und Heizung zu übernehmen hat. Für beide Teilleistungen ist Voraussetzung, dass der Betroffene hilfebedürftig ist, das heißt, dass er seinen Lebensunterhalt nicht aus eigenen Kräften und Mitteln sichern kann und die erforderliche Hilfe nicht von anderen erhält. Der Gesetzgeber hat aber nicht vorgesehen, dass jeder Träger eigenständig feststellt, ob der Betroffene hilfebedürftig ist. Vielmehr handelt es sich um einen einheitlichen Leistungsanspruch, der zwingend ein einheitliches Ergebnis in der Beurteilung der Hilfebedürftigkeit erfordert. Die Befugnis zur Feststellung der Hilfebedürftigkeit hat der Gesetzgeber der Agentur für Arbeit zugewiesen. Dies hat zur Folge, dass die Agentur für Arbeit den Sachverhalt insoweit auch aufzuklären hat und vom Betroffenen gegebenenfalls die Vorlage von Beweisurkunden verlangen kann. Da der kommunale Träger, der die Kosten für Unterkunft und Heizung maßgeblich zu tragen hat, ein ureigenes Interesse daran hat, Leistungen nur an wirklich Bedürftige zu zahlen, ist im Zweiten Buch des Sozialgesetzbuchs vorgesehen, dass er der Feststellung der Agentur für Arbeit zur Hilfebedürftigkeit widersprechen kann. In diesem Fall entscheidet eine gemeinsame Einigungsstelle, der ein Vorsitzender und jeweils ein Vertreter

der Agentur für Arbeit und des widersprechenden Trägers angehören. Die Agentur für Arbeit hat die von ihr zur Höhe des Einkommens und Vermögens des Betroffenen erhobenen Informationen dem kommunalen Träger nach Maßgabe der datenschutzrechtlichen Vorschriften zuzuleiten, damit dieser prüfen kann, ob er der Feststellung der Agentur für Arbeit widersprechen möchte, und den Widerspruch gegebenenfalls begründen kann.

Nicht zulässig ist es aber, dass der kommunale Träger, wenn ihm die Feststellung der Agentur für Arbeit zur Hilfebedürftigkeit nicht passt, auf eigene Faust ermittelt und vom Antragsteller Nachweise zur Höhe seines Einkommens und Vermögens verlangt. Hält der kommunale Träger die Sachverhaltsaufklärung der Agentur für Arbeit für unzureichend, hat er im Einigungsstellenverfahren auf weitergehende Ermittlung hinzuwirken. Das Ministerium für Arbeit und Soziales ist meiner Auffassung gefolgt.

Da im Land unterschiedliche rechtliche Bewertungen kursierten, ob und in welchem Umfang der kommunale Träger bei getrennter Aufgabenwahrnehmung die Hilfebedürftigkeit zu prüfen hat, sah das Ministerium weiteren Abklärungsbedarf mit dem Landkreistag, dem Städtetag und der Gemeindeprüfungsanstalt. Ergebnis der Abstimmung aller beteiligten Stellen war eine „Gemeinsame Bewertung des Landkreistags Baden-Württemberg, des Städtetags Baden-Württemberg, des Landesbeauftragten für den Datenschutz, der Gemeindeprüfungsanstalt Baden-Württemberg und des Ministeriums für Arbeit und Soziales als oberster Rechtsaufsicht über die kommunalen Träger nach dem SGB II zur Frage der Prüfung der Hilfebedürftigkeit nach § 44 a SGB II in der Organisationsform der getrennten Aufgabenwahrnehmung“, in der noch einmal ausdrücklich auf die wesentlichen Punkte hingewiesen wurde. Die Bewertung wurde inzwischen an die Stadt- und Landkreise verteilt.

3. Arbeitslosengeld II: Die Bettlägerigkeitsbescheinigung

Die Agentur für Arbeit soll im Einvernehmen mit dem kommunalen Träger mit jedem erwerbsfähigen Hilfebedürftigen eine Eingliederungsvereinbarung abschließen. Zweck der Eingliederungsvereinbarung ist die Konkretisierung der im Zweiten Buch des Sozialgesetzbuchs abstrakt geregelten Grundsätze des Förderns und Forderns. Durch die Vereinbarung werden die Rechte und Pflichten sowohl des Hilfebedürftigen als auch der Behörde verbindlich festgelegt. Ferner sollen hierdurch die Akzeptanz und die Eigenverantwortung des Hilfebedürftigen erhöht werden. Kommt eine Vereinbarung zwischen Behörde und dem Hilfebedürftigen nicht zustande, besteht nach dem Gesetz aber auch die Möglichkeit, dass die Behörde (einseitig) einen Verwaltungsakt erlässt, der die Vereinbarung ersetzt.

Ein Bürger, der Arbeitslosengeld II bezog, wandte sich Hilfe suchend an meine Dienststelle. Die für ihn zuständige Arbeitsgemeinschaft hatte, da die Eingliederungsvereinbarung von ihm nicht unterschrieben war, einen vereinbarungsersetzenden Verwaltungsakt erlassen. In diesem war geregelt, dass der Petent Zeiten der Krankheit ausschließlich mit einer Bettlägerigkeitsbescheinigung nachzuweisen habe. Allein eine vorliegende Arbeitsunfähigkeitsbescheinigung reiche nicht aus.

Von meiner Dienststelle zur Stellungnahme aufgefordert, erklärte die betroffene Arbeitsgemeinschaft, die Vorlage einer Bettlägerigkeitsbescheinigung sei lediglich für Fälle gedacht, in denen sich der Kunde der Meldepflicht und der Möglichkeit, einen Integrationsplan zu erarbeiten, durch Vorlage von Krankmeldungen entziehe. Weiterhin gelte dies nicht für alle Arbeitsunfähigkeitszeiten, sondern lediglich für die Tage, an denen der Kunde zu einem Termin bei der Arbeitsgemeinschaft erscheinen oder an Schulungsmaßnahmen teilnehmen solle. Der Petent habe bisher Einladungen der Arbeitsgemeinschaft Folge geleistet. Daher bestehe objektiv keine Veranlassung, eine Bettlägerigkeitsbescheinigung zu verlangen. Eventuell sei dies aufgrund nicht dokumentierter Äußerungen des Petenten „vorbeugend“ in den Verwaltungsakt aufgenommen worden. Im Ergebnis schien die Arbeitsgemeinschaft ihr Vorgehen für zulässig zu halten.

Dem konnte ich nicht folgen: Die in der Eingliederungsvereinbarung enthaltene Verpflichtung, Zeiten der Krankheit ausschließlich durch eine Bett-

lägerigkeitsbescheinigung nachzuweisen, dürfte zur Erreichung des von der Arbeitsgemeinschaft verfolgten Zwecks von vornherein wenig geeignet sein, da es durchaus Krankheiten gibt, bei denen der Erkrankte zwar nicht der Bettruhe bedarf, aber dennoch nicht arbeitsfähig bzw. nicht in der Lage ist, zu einem Meldetermin zu erscheinen oder an einer Schulungsveranstaltung teilzunehmen. Erwerbsfähige Hilfebedürftige sind nach dem Zweiten Buch des Sozialgesetzbuchs verpflichtet, dem zuständigen Leistungsträger spätestens vor Ablauf des dritten Kalendertags nach Eintritt der Arbeitsunfähigkeit eine ärztliche Bescheinigung über die Arbeitsunfähigkeit und deren voraussichtliche Dauer vorzulegen; die Arbeitsgemeinschaft ist berechtigt, die Vorlage der ärztlichen Bescheinigung früher zu verlangen. Gründe, weswegen es im Falle des Petenten erforderlich gewesen sein könnte, Zeiten der Krankheit – die in der Eingliederungsvereinbarung auch gar nicht eingegrenzt waren – ausschließlich mit einer Bettlägerigkeitsbescheinigung nachzuweisen, wurden von der Arbeitsgemeinschaft nicht vorgetragen. Der vorliegende Fall und insbesondere die Stellungnahme der betroffenen Arbeitsgemeinschaft zeigen, dass dort die datenschutzrechtlichen Kenntnisse nicht sonderlich ausgeprägt sind und offenkundig auch das notwendige Einfühlungsvermögen den Kunden gegenüber fehlt.

4. Datenabgleich beim Wohngeld

Das Wohngeldgesetz ermächtigt die Wohngeldstellen, die zum Haushalt rechnenden Familienmitglieder und Personen von Wohn- und Wirtschaftsgemeinschaften zur Vermeidung von Leistungsmissbrauch regelmäßig im Wege eines Datenabgleichs in verschiedener Hinsicht zu überprüfen. Beispielsweise darf kontrolliert werden, welche Zinseinkünfte aus Kapitalvermögen die Betroffenen erhalten und ob und für welche Zeiträume andere Sozialleistungen, bei denen auch Kosten der Unterkunft berücksichtigt werden, beantragt oder empfangen werden. Der Datenabgleich ist auch in automatisierter Form zulässig. Das Wohngeldgesetz ermächtigt die Landesregierungen, durch Rechtsverordnung das Nähere über das Verfahren eines solchen automatisierten Datenabgleichs zu regeln.

Baden-Württemberg hat dieses Jahr als drittes Bundesland nach Hamburg und Nordrhein-Westfalen eine Verordnung über den automatisierten Datenabgleich bei Leistungen nach dem Wohngeldgesetz erlassen. In der Verordnung ist vorgesehen, dass Einzelheiten des Datenübermittlungs- und Datenabgleichverfahrens, insbesondere des Aufbaus der Datensätze, der Übermittlung, der Prüfung und Berichtigung von Datensätzen von den an dem automatisierten Datenabgleich beteiligten Stellen unter Beteiligung des Landesbeauftragten für den Datenschutz in Verfahrensgrundsätzen einvernehmlich festgelegt werden.

Das Wirtschaftsministerium übersandte meiner Dienststelle daher Ende Mai dieses Jahres einen Entwurf der Verfahrensgrundsätze zur Stellungnahme. Zu den übersandten Unterlagen gehörte u. a. eine Aufzählung der Sozialdaten, die ein sog. Anfragesatz enthält (beispielsweise Name, Vorname, Geburtsdatum, Anschrift). Die Wohngeldstellen übermitteln diesen Anfragesatz über eine zentrale Landesstelle der Datenstelle der Träger der Rentenversicherung. Die Datenstelle gleicht die im Anfragesatz enthaltenen Sozialdaten mit den ihr ebenfalls vorliegenden Daten von Beziehern von Sozialhilfe und Arbeitslosengeld II ab. So kann geprüft werden, ob ein rechtswidriger Doppelbezug vorliegt. Das Wohngeldgesetz selbst regelt abschließend, welche Sozialdaten für den Datenabgleich von der Wohngeldstelle an die Datenstelle übermittelt werden dürfen. Auch der Abgleich ist auf diese Daten zu beschränken. Der uns vorliegende Anfragesatz enthielt jedoch Sozialdaten, die im Gesetz nicht vorgesehen sind: So war geplant, den Geburtsnamen des Leistungsempfängers und, soweit dem Leistungsempfänger in der Deutschen Rentenversicherung eine aktuelle Versicherungsnummer zugeordnet werden kann, auch diese in den Datenabgleich mit einzubeziehen.

Auf meinen Hinweis, dass die in dem Anfragesatz enthaltenen Sozialdaten über die im Wohngeldgesetz abschließend aufgezählten hinausgehen, wurde mitgeteilt, dass die Übermittlung dieser Angaben die „Trefferquote“ beim Datenabgleich um ein Vielfaches erhöhe. Außerdem bestünden Be-

strebungen der Bundesregierung, die entsprechende Vorschrift im Wohngeldgesetz zumindest um den Geburtsnamen zu ergänzen. Diese Argumentation ändert nichts an der Rechtswidrigkeit des geplanten Vorgehens. Außerdem ist auf Folgendes hinzuweisen: Der automatisierte Datenabgleich stellt einen sehr weit reichenden Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. Regelmäßig werden alle zum Haushalt rechnenden Familienmitglieder und Personen von Wohn- und Wirtschaftsgemeinschaften in verschiedener Hinsicht überprüft, ohne dass im Einzelfall ein konkreter Anlass erforderlich wäre. Deshalb ist es umso wichtiger, dass die Umsetzung des automatisierten Datenabgleichs in rechtlich einwandfreier Art und Weise erfolgt.

Aufgrund der Ausführungen meiner Dienststelle hat das Ministerium schließlich mitgeteilt, eine Übermittlung des Geburtsnamens der Leistungsempfänger an die Datenstelle werde bis zu einer Änderung des Wohngeldgesetzes nicht erfolgen. Ich begrüße dies und gehe davon aus, dass sich das Wirtschaftsministerium außerdem dafür einsetzt, dass auch eine Einbeziehung der Versicherungsnummer in den Datenabgleich mangels gesetzlicher Grundlage nicht erfolgt.

5. Unterhalt für die Schwiegermutter?

Bei bestimmten Sozialleistungen gehen Unterhaltsansprüche des Leistungsberechtigten für die Zeit, für die Leistungen erbracht werden, auf den Sozialleistungsträger über. Möchte der Sozialleistungsträger den Unterhaltsanspruch gegenüber dem Verpflichteten geltend machen, muss er sich zunächst über dessen finanzielle Situation unterrichten. In diesem Zusammenhang kommt es immer wieder auch zu datenschutzrechtlichen Fragestellungen:

So wandte sich ein Bürger an uns, dessen Mutter vom Sozialamt Hilfe zur Pflege erhielt. Das Sozialamt interessierte sich nicht nur für das Einkommen des Petenten, sondern auch für das Einkommen von dessen Ehefrau. Diese wollte keine Auskunft zu ihrem Einkommen erteilen, da sie mit der Schwiegermutter „nicht in einer Linie stehe“. Der Petent schickte daher nur die Angaben zu seinem Einkommen an den Sachbearbeiter des Sozialamts zurück. Trotzdem erhielt der Petent anschließend einen Berechnungsbogen für Unterhaltszahlungen vom Sozialamt, auf dem auch ein Einkommen für seine Frau angegeben war. Das angegebene Einkommen entsprach auch ziemlich genau dem, was die Ehefrau tatsächlich verdiente. Der Verdacht des Petenten und seiner Frau war nun, dass das Sozialamt Informationen über das Einkommen der Ehefrau beim Finanzamt eingeholt hatte. Wir baten das betroffene Sozialamt, zu dem Vorgang Stellung zu nehmen. Dabei stellte sich heraus, dass sich die Befürchtungen des Petenten und seiner Frau nicht bestätigt hatten; der Petent selbst hatte dem Sozialamt im Zuge des Verfahrens Unterlagen, aus denen das Einkommen seiner Ehefrau ersichtlich war, zugesandt.

Zu der Frage, ob das Sozialamt Kenntnis von der Höhe des Einkommens der Ehefrau zur Erfüllung seiner Aufgaben benötigte, haben wir dem Petenten und seiner Ehefrau mitgeteilt, dass eine solche Datenerhebung – zumindest wenn sich die Ehefrau wie im vorliegenden Fall nicht aus eigenem Einkommen unterhalten kann – aus Sicht des Datenschutzes nicht zu beanstanden ist: Das Erheben von Sozialdaten durch einen Sozialleistungsträger ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem Sozialgesetzbuch erforderlich ist. Die Mutter des Petenten erhielt im vorliegenden Fall vom Sozialamt Hilfe zur Pflege. Bei dieser Sozialleistung geht, wenn die leistungsberechtigte Person für die Zeit, für die Leistungen erbracht werden, nach bürgerlichem Recht einen Unterhaltsanspruch hat, dieser bis zur Höhe der geleisteten Aufwendungen grundsätzlich auf den Träger der Sozialhilfe über.

Nach dem Bürgerlichen Gesetzbuch sind Verwandte in gerader Linie, also beispielsweise Mutter und Sohn, einander unterhaltspflichtig. Die Ehefrau des Sohns ist gesetzlich nicht verpflichtet, ihrer Schwiegermutter Unterhalt zu leisten. Insoweit scheinen die Einkommensverhältnisse der Ehefrau tatsächlich zunächst ohne Belang zu sein. Jedoch ist der Sohn gegenüber seiner

Mutter nur zu Unterhalt verpflichtet, wenn er leistungsfähig ist. Dies bedeutet, dass er bei Berücksichtigung seiner sonstigen Verpflichtungen im Stande sein muss, ohne Gefährdung seines eigenen angemessenen Unterhalts den Unterhalt für seine Mutter zu gewähren. Vorrangig ist der Petent aber seiner Ehefrau und seinen eigenen Kindern und erst dann seinen sonstigen Verwandten, etwa seiner bedürftigen Mutter, zum Unterhalt verpflichtet. Wenn seine Ehefrau nun über keine oder nur geringfügige Einkünfte verfügt, muss der Petent seine Mittel vorrangig für deren Unterhalt einsetzen, was seine Möglichkeiten schmälert, Leistungen gegenüber seiner sozialhilfebedürftigen Mutter zu erbringen. Verfügt andererseits die Ehefrau über nennenswerte Einkünfte, muss der Petent für den Unterhalt der Ehefrau nicht mit aufkommen, sodass ihm mehr Mittel bleiben, seine Mutter zu unterstützen. Daraus ergibt sich, dass für die Leistungsfähigkeit eines verheirateten Unterhaltsverpflichteten die wirtschaftliche Lage seines Ehegatten durchaus von Bedeutung sein kann, auch wenn der Ehegatte selbst keinesfalls unterhaltspflichtig ist.

4. Teil: Hochschulwesen, Finanzen und Statistik

1. Die Klägerdatei des Wissenschaftsministeriums

Die seit langem heftig umstrittenen allgemeinen Studiengebühren wurden inzwischen auch in Baden-Württemberg eingeführt: Nach einer Änderung des Landeshochschulgebührengesetzes vom Dezember 2005 erheben die staatlichen Hochschulen und die Berufsakademien nun Studiengebühren in Höhe von 500 EUR je Semester. Wegen der datenschutzrechtlichen Aspekte, mit denen ich mich im Gesetzgebungsverfahren befasst hatte, verweise ich auf meinen 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910. Es ist nicht verwunderlich, dass die Kontroversen ihre Fortsetzung fanden, als erstmals für das Sommersemester 2007 entsprechende Gebührenbescheide ergingen; eine beträchtliche Zahl von Studierenden – im Februar 2007 sollen es ca. 2 500 gewesen sein – klagte nämlich gegen die Gebührenbescheide. Somit standen bei den Verwaltungsgerichten nicht nur die jeweiligen Bescheide, sondern letztlich das diesen zugrunde liegende Landeshochschulgebührengesetz auf dem Prüfstand. Angesichts der hochschulpolitischen Brisanz der Angelegenheit war es daher auch nicht verwunderlich, dass die Klageverfahren vom Wissenschaftsministerium als dem federführenden Ressort aufmerksam verfolgt wurden. Als datenschutzrechtlich problematisch erwies sich dabei, dass das Ministerium auch Namen und andere personenbezogene Daten der Klägerinnen und Kläger wissen wollte. Im Einzelnen:

Im Februar dieses Jahres wurden wir darauf hingewiesen, dass das Wissenschaftsministerium seit Dezember 2006 in mehreren Schreiben an die Hochschulen und Berufsakademien im Land Informationen zu den Klageverfahren einholen wollte. Zunächst wurden von den Hochschulen sogar Kopien der jeweiligen Klage- oder Antragsschrift gefordert. Im Januar 2007 schraubte das Wissenschaftsministerium seine Anforderungen zurück und erklärte, dass es sich im Fall sog. reiner Formularklagen (die im Februar 2007 etwa 96 Prozent aller Klagen ausmachten) mit einer tabellarischen Übersicht der Klägernamen mit den jeweiligen gerichtlichen Aktenzeichen begnüge.

Ich wandte mich sogleich an das Wissenschaftsministerium, das mir in seiner Stellungnahme im Wesentlichen mitteilte, dass

- sich ein hochschul- und gerichtsübergreifender Koordinierungsbedarf ergeben habe,
- die Übersichten mit Klägernamen und gerichtlichen Aktenzeichen ausschließlich dazu dienen würden, einen schnellen Überblick über den Verfahrensstand zu gewinnen,
- bei diesen Übersichten keine Beschränkung auf das gerichtliche Aktenzeichen möglich sei, weil das „Abtippen langer Reihen von Zahlen ohne Sinnbezug zu einem Sachverhalt durch Kräfte der Hochschulen“ zu fehleranfällig gewesen wäre, und
- das Wissenschaftsministerium als Fachaufsichtsbehörde nach § 67 Abs. 2 Satz 1 Nr. 3 des Landeshochschulgesetzes für die Klagen verantwortlich sei.

Damit war in keiner Weise schlüssig dargelegt, weshalb – und darauf kommt es kurz gesagt letztendlich an – das Ministerium zur Erfüllung seiner Aufgaben auf die Kenntnis aller Klägernamen angewiesen ist. Zunächst ist zu beachten, dass die jeweiligen Hochschulen keine rechtlich unselbstständigen Untergliederungen des Landes, sondern als rechtsfähige Körperschaften des öffentlichen Rechts selbstständige juristische Personen sind, die auch als solche verklagt werden können. Klagegegner in den Gebührenprozessen ist demnach z. B. eine bestimmte Universität und nicht das Land Baden-Württemberg in Gestalt des Wissenschaftsministeriums. Eine Befugnis, über alle Klägernamen informiert zu werden, ergibt sich auch nicht aus der Funktion des Ministeriums als Fachaufsichtsbehörde. Zwar unterliegen die Hochschulen im Gebührenwesen der Fachaufsicht des Wis-

senschaftsministeriums. Im Einzelfall darf eine Fachaufsichtsbehörde auch den Namen und andere relevante Daten einer Bürgerin oder eines Bürgers zur Kenntnis nehmen, z. B. wenn im Rahmen einer Fachaufsichtsbeschwerde die Vorgänge bei einer nachgeordneten Stelle zu überprüfen und der Beschwerdeführer dann über das Ergebnis der Prüfung zu informieren ist. Nur: Eine solche detaillierte fachaufsichtliche Prüfung aller den Klageverfahren zugrunde liegenden Fälle konnte und wollte auch das Wissenschaftsministerium gar nicht vornehmen. Im Übrigen ist es für mich nicht nachvollziehbar und darüber hinaus geradezu kurios, wenn das Wissenschaftsministerium – das bei der Novellierung des Landeshochschulgesetzes die Stärkung der Eigenverantwortung der Hochschulen propagierte – den Hochschulen nicht zutraut, in Klageverfahren selbstständig einfache Angelegenheiten zu erledigen und etwa mit einem kurzen Satz dem Verwaltungsgericht die Zustimmung zum Ruhen des Verfahrens zu erklären. Darauf, dass nach Meinung des Wissenschaftsministeriums das Personal der Hochschulen angeblich nicht in der Lage sein soll, gerichtliche Aktenzeichen fehlerfrei „abzutippen“, will ich hier gar nicht eingehen.

Ich teilte dem Ministerium das Ergebnis meiner datenschutzrechtlichen Prüfung zunächst sofort telefonisch mit und vereinbarte zur raschen Bereinigung der datenschutzrechtlichen Probleme eine Besprechung in meiner Dienststelle, bei der ich gegenüber den Vertretern des Wissenschaftsministeriums unmissverständlich klarstellte, dass die Erhebung der Klägernamen in den Fällen der Formularklagen rechtswidrig war. Von einer förmlichen Beanstandung sah ich nur deswegen ab, weil mir die Mitarbeiter des Ministeriums versicherten, dass die Daten zu den Formularklagen im Ministerium bereits gelöscht worden seien; zudem wolle man dort meine Rechtsauffassung künftig beachten. Dementsprechend konnte ich gegenüber der Öffentlichkeit, darunter sicher auch einigen besorgten Klägerinnen und Klägern, in einer Pressemitteilung berichten, dass die Daten der Kläger gegen die Studiengebühr überwiegend gelöscht worden seien. Als positiv konnte ich – ohne dass dieser Umstand dem Ministerium zugute gehalten werden konnte – auch verbuchen, dass sich die rechtswidrige Datenverarbeitung quantitativ in Grenzen hielt. Denn die Hochschulen hatten – im Unterschied zum Ministerium – ihre datenschutzrechtliche Sensibilität durchaus unter Beweis gestellt und dem Ministerium nur in ca. 300 Fällen die Daten zu den Formularklagen übermittelt. So weit, so gut.

Im März zeigte mir allerdings ein Blick in die Landtagsdrucksachen 14/884 und 14/887, bei denen es um Anträge mehrerer Abgeordneter zur Klägerdatei des Wissenschaftsministeriums ging, dass offenbar doch nicht alle Probleme ausgeräumt waren. Das Wissenschaftsministerium hatte dort nämlich am 1. März 2007 (also nach der genannten Besprechung vom 23. Februar 2007) erklärt, die Übersichten mit den Klägernamen seien „ausreichend, aber auch erforderlich“ gewesen. Diese Stellungnahmen waren – vorsichtig formuliert – geeignet, dem nicht Eingeweihten einen falschen Eindruck zu vermitteln. Dies galt nicht nur hinsichtlich der inhaltlichen Aussage, sondern auch hinsichtlich wesentlicher Umstände des Verfahrens: Die Äußerungen des Ministeriums vermittelten jedenfalls den Eindruck, als ob eine datenschutzrechtliche Prüfung und Beratung durch meine Dienststelle niemals stattgefunden hätte oder unbeachtlich gewesen wäre. Ende März hatte ich dann Gelegenheit, im Wissenschaftsausschuss des Landtags meine datenschutzrechtliche Auffassung näher zu erläutern. Dabei interpretierte der Wissenschaftsminister die Aussagen in den beiden Landtagsdrucksachen dahingehend, dass sein Ministerium meine Rechtsauffassung beachte, aber nicht gezwungen werden könne, diese zu teilen. Wenn das Wissenschaftsministerium künftig die datenschutzrechtlichen Anforderungen – auch ohne innere Überzeugung – beachtet, soll es mir recht sein.

2. Der automatisierte Kontenabruf durch Finanzämter und andere Behörden

Bereits seit mehr als zwei Jahren können Finanzämter und andere Behörden im Wege eines automatisierten Abrufverfahrens ermitteln, welche Bankkonten ein Bürger bei welchen Banken unterhält. Diese Abrufmöglichkeit ist seit ihrer Einführung umstritten und geht, wie ich in meinem 25. Tätigkeitsbericht für das Jahr 2004 feststellte (LT-Drucksache 13/3800, sowie

die dort als Anhang 10 abgedruckte Entschließung), mit erheblichen datenschutzrechtlichen Problemen einher. In diesem Jahr sorgte das Bundesverfassungsgericht, das über dagegen erhobene Verfassungsbeschwerden zu entscheiden hatte, für Klarstellungen und für Korrekturen an dem Verfahren:

– § 93 Abs. 7 der Abgabenordnung (AO), der den Finanzbehörden unter bestimmten Voraussetzungen Kontenabrufe erlaubt, ist mit dem Grundgesetz, also auch mit dem verfassungsrechtlichen Transparenzgebot und der Rechtsschutzgarantie des Artikels 19 Abs. 4 GG, vereinbar. Routinemäßige und anlasslose Abfragen „ins Blaue hinein" sind unzulässig. Das jeweilige Verfahrensrecht gewährleistet dem von einem Kontenabruf Betroffenen ein grundsätzliches Auskunftsrecht, von dem er spätestens dann auch tatsächlich Gebrauch machen kann, wenn die jeweilige Behörde das Ergebnis des Kontenabrufs mit für ihn nachteiligen Folgen verwertet hat.
– § 93 Abs. 8 AO (in der vom Gericht geprüften, inzwischen überholten Fassung) verstößt gegen das Gebot der Normenklarheit, da er den Kreis der Behörden, die ein Ersuchen zum Abruf von Kontostammdaten stellen können, und die Aufgaben, denen solche Ersuchen dienen sollen, nicht hinreichend bestimmt festlegt. Damit hat das Bundesverfassungsgericht die bereits mit oben genannter Entschließung geäußerte Kritik der Datenschutzbeauftragten des Bundes und der Länder bestätigt.

Die Verfassungswidrigkeit des § 93 Abs. 8 AO führte nicht zu dessen Nichtigkeit. Das Bundesverfassungsgericht räumte dem Gesetzgeber für eine verfassungsgemäße Neuregelung eine Frist bis zum 31. Mai 2008 ein. Der Bundesgesetzgeber setzte prompt bereits im August 2007 eine geänderte Fassung des § 93 Abs. 8 AO in Kraft, in der nun klar zum Ausdruck kommt, welche Sozialbehörden beim Vollzug welcher Vorschriften (z. B. die Behörden, die für die Verwaltung der Grundsicherung für Arbeitsuchende nach dem Zweiten Buch des Sozialgesetzbuchs zuständig sind) mit Kontenabrufen arbeiten dürfen.

Nach gerichtlicher Klärung verfassungsrechtlicher Fragen und der Nachbesserung durch den Gesetzgeber kommt es nun entscheidend darauf an, dass die am automatisierten Kontenabruf beteiligten Behörden auch datenschutzkonform verfahren. Daher werde ich die Praxis der baden-württembergischen Behörden, die meiner Beratung und Kontrolle unterliegen, im Auge behalten.

3. Die Ablösung der Lohnsteuerkarte durch ein zentrales Abrufverfahren

Der Entwurf der Bundesregierung für das Jahressteuergesetz 2008 reicht in seiner Bedeutung – anders als der Titel zunächst vermuten lässt – weit über das kommende Jahr hinaus. Denn nach diesem Gesetzentwurf soll die altbekannte Lohnsteuerkarte letztmals für das Jahr 2010 ausgestellt und ab 2011 durch ein elektronisches Abrufverfahren (ElsterLohn II) ersetzt werden. Das geplante Verfahren hat – anders als zuweilen in der Presse dargestellt – nicht die Einführung einer „elektronischen Lohnsteuerkarte" zum Gegenstand, bei der etwa nur die bisherige Verwendung von Papier und Pappe durch elektronische Vorgänge ersetzt wird. Die darüber weit hinausreichende Tragweite des Unterfangens zeigt sich erst bei genauerer Betrachtung des § 39 f des Einkommensteuergesetzes (EStG), der nach diesem Gesetzentwurf mit der Überschrift: „Elektronische Lohnsteuerabzugsmerkmale" in das Einkommensteuergesetz eingefügt werden soll:

– Die Lohnsteuerabzugsmerkmale (darunter die Religionszugehörigkeit als Merkmal für den Kirchensteuerabzug) sollen bundesweit zentral bei einer einzigen Stelle, dem Bundeszentralamt für Steuern, anderen Daten hinzugespeichert werden. Bei diesen anderen Daten handelt es sich nach § 139 b Abs. 3 AO u. a. um die steuerliche Identifikationsnummer, die Namen, die Anschrift, den Geburtstag und den Geburtsort aller Einwohner Deutschlands. Dieses datenschutzrechtlich ohnehin höchst bedenkliche zentrale Einwohnerregister soll also um weitere, teilweise sensible Daten angereichert werden. Dies wäre zumindest ein weiterer

großer Schritt in Richtung eines verfassungswidrigen allgemeinen Personenkennzeichens, zu dem die steuerliche Identifikationsnummer zu werden droht.

– Das Bundeszentralamt für Steuern hält die Identifikationsnummer, den Geburtstag, Merkmale für den Kirchensteuerabzug und Lohnsteuerabzugsmerkmale, wie z. B. die Steuerklasse und die Zahl der Kinderfreibeträge, zum automatisierten Abruf durch den Arbeitgeber bereit. Dabei müssen natürlich wirksame Vorkehrungen gegen unberechtigte Abrufe getroffen werden. Es ist fraglich, ob die vorgesehene Regelung, wonach sich der Arbeitgeber für den Abruf der Lohnsteuerabzugsmerkmale zu authentifizieren und seine Wirtschafts-Identifikationsnummer sowie die Identifikationsnummer und den Tag der Geburt des Arbeitnehmers mitzuteilen hat, dafür ausreichend ist.

Eine angemessene Würdigung dieser gravierenden Aspekte ist dem Gesetzentwurf leider nicht zu entnehmen. Daher appellierte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer an den Bundestag und den Bundesrat gerichteten Entschließung vom 25./26. Oktober 2007, die Umstellung von der Lohnsteuerkarte auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen (vgl. Anhang 9).

Der Bundestag hat sich von diesem Appell offenbar nicht beeindrucken lassen und hat am 8. November 2007 den Entwurf des Jahressteuergesetzes 2008 in einer Fassung angenommen, die nach wie vor (nun allerdings als zukünftiger § 39 e EStG) die Einführung des zentralen elektronischen Abrufverfahrens vorsieht. Bei Redaktionsschluss für diesen Tätigkeitsbericht hatte sich der Bundesrat, dessen Zustimmung für den Erlass des Jahressteuergesetzes 2008 erforderlich ist, noch nicht abschließend mit dem Gesetzentwurf befasst. Bereits Anfang November habe ich das hiesige Finanzministerium – das mich erfreulicherweise frühzeitig über den Gesetzentwurf informiert hatte – gebeten, die in der Entschließung aufgezeigten datenschutzrechtlichen Bedenken gegen die Ablösung des Lohnsteuerverfahrens durch ein elektronisches Abrufverfahren bei den Beratungen des Bundesrats zu berücksichtigen. Es ist bemerkenswert, dass sich der Bundesrat bereits im September in einer Stellungnahme dafür ausgesprochen hatte, den Gesetzentwurf hinsichtlich des Authentifizierungsverfahrens so zu überarbeiten, dass eine sichere Identifizierung und Nachverfolgung des Anfragenden ermöglicht wird. Es erscheint jedoch fraglich, ob über den Bundesrat noch datenschutzrechtliche Verbesserungen des Gesetzentwurfs erreicht werden können.

4. Das Projekt OpenELSTER

ELSTER (ein Kürzel für: ELektronische STeuerERklärung) ist eines der vielen sog. eGovernment-Projekte. Der Einsatz der dabei entwickelten EDV-Verfahren (z. B. ELSTER-Lohn; vgl. 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910) ist bislang auf den Bereich der Steuerverwaltung beschränkt. Teil dieses ELSTER-Vorhabens ist ein sog. Authentifizierungsdienst. Seine Aufgabe besteht darin, die Identität der elektronischen Kommunikationspartner zu überprüfen. Quasi beiläufig wurde meiner Dienststelle nun mitgeteilt, dass als „Beitrag der Finanzverwaltungen zur Steigerung der Attraktivität deutscher eGovernment-Projekte“ die obersten Finanzbehörden des Bundes und der Länder mit dem Projekt OpenELSTER die Nutzung des ELSTER-Authentifizierungsdienstes auch anderen staatlichen und kommunalen Stellen anbieten sollen. Bereits ein erster Blick in das Konzept offenbarte ein gravierendes datenschutzrechtliches Problem: Ab 2008 sollte die steuerliche Identifikationsnummer im Sinne von § 139 b AO – deren Vergabe im Juli 2007 begonnen hat und derzeit noch läuft – unter Mitwirkung der jeweils betroffenen Bürger auch an Stellen außerhalb der Steuerverwaltung übermittelt und von diesen verarbeitet werden. Mit einer ausufernden Verwendung dieser Identifikationsnummer außerhalb der Finanzbehörden wäre der verfassungswidrigen Entstehung eines allgemeinen Personenkennzeichens Tür und Tor geöffnet. Der Bundesgesetzgeber war datenschutzrechtlich gut beraten, als er bereits Ende 2003 mit Schaffung der gesetzlichen Grundlagen für die Identifikationsnummer ausdrückliche Nut-

zungsbeschränkungen verhängte, die eine strikte Zweckbindung der Identifikationsnummer bewirken. Nach § 139 b Abs. 2 AO gilt nämlich:

- Die Erhebung und Verwendung der Identifikationsnummer ist zunächst nur den Finanzbehörden erlaubt, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist oder eine Rechtsvorschrift die Erhebung oder Verwendung der Identifikationsnummer ausdrücklich erlaubt oder anordnet.
- Stellen außerhalb der Finanzverwaltung dürfen die Identifikationsnummer nur erheben oder verwenden, soweit dies für Datenübermittlungen zwischen ihnen und den Finanzbehörden erforderlich ist oder eine Rechtsvorschrift die Erhebung oder Verwendung der Identifikationsnummer ausdrücklich erlaubt oder anordnet.
- Einwilligungserklärungen, die darauf gerichtet sind, eine nach diesen Bestimmungen nicht zulässige Erhebung oder Verwendung der Identifikationsnummer zu ermöglichen, sind unwirksam.

Demnach können die gesetzlichen Nutzungseinschränkungen nicht einmal dann überwunden werden, wenn die Betroffenen ihre Einwilligung erklären, etwa indem sie ihre jeweilige Identifikationsnummer nach Öffnung des ELSTER-Authentifizierungsdienstes freiwillig zur Nutzung durch Stellen außerhalb der Finanzbehörden freigeben.

Das Projekt OpenELSTER war, als ich Mitte September dieses Jahres davon erfuhr, bereits so weit gediehen, dass die Finanzministerien des Bundes und des Freistaats Bayern als Frist für eine Rückmeldung aus den Ländern, ob dort Interesse an der Nutzung von OpenELSTER besteht, den 31. Oktober 2007 terminiert hatten. Daher wandte ich mich umgehend an alle Ministerien des Landes, wies auf die Nutzungsbeschränkungen des § 139 b Abs. 2 AO hin und bat, diese bei allen Überlegungen zur Nutzung des ELSTER-Authentifizierungsdienstes zu beachten. Zudem bat ich das Finanzministerium, darauf hinzuwirken, dass bei der Nutzung des ELSTER-Authentifizierungsdienstes durch Behörden außerhalb der Finanzverwaltung generell auf die Übermittlung der Identifikationsnummer verzichtet wird. Darauf teilte mir das Finanzministerium mit, dass es mein Schreiben an das für die Entwicklung von ELSTER zuständige bayerische Finanzministerium übersandt und darauf hingewiesen habe, dass die von mir aufgeworfenen datenschutzrechtlichen Fragen geklärt werden müssen. Darüber hinaus hat unser Finanzministerium das Bundesministerium der Finanzen gebeten, den Datenschutzbeauftragten des Bundes und der Länder eine bundeseinheitlich abgestimmte Stellungnahme zukommen zu lassen. Eine solche Stellungnahme oder sonstige weitere Äußerungen seitens der Finanzverwaltung lagen mir bei Redaktionsschluss für diesen Tätigkeitsbericht leider noch nicht vor. Ich gehe davon aus, dass jedenfalls bis zur Klärung dieser gravierenden datenschutzrechtlichen Fragen staatliche und kommunale Stellen außerhalb der baden-württembergischen Finanzverwaltung auf die Verwendung der Identifikationsnummer im Rahmen von OpenELSTER verzichten.

Wegen der bundesweiten Dimension des Projekts arbeite ich in dieser Sache eng mit dem Bundesdatenschutzbeauftragten sowie mit meinen Kolleginnen und Kollegen in den anderen Bundesländern zusammen. Die anhand des Projekts OpenELSTER offenbar gewordenen Probleme legen es nahe, eine Ausweitung des mit der Identifikationsnummer zentral gespeicherten Datenkatalogs – so wie derzeit im Zusammenhang mit der Abschaffung der Lohnsteuerkarte vorgesehen – mit ganz besonderer Aufmerksamkeit zu betrachten. Wegen der Einzelheiten verweise ich auf den Beitrag „Die Ablösung der Lohnsteuerkarte durch ein zentrales Abrufverfahren“ unter Nummer 3 dieses Abschnitts. Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2007 gefasste Entschließung „Zentrale Steuerdatei droht zum Datenmoloch zu werden“ (vgl. Anhang 9) hat somit unter ihrem Punkt 3 auch OpenELSTER zum Gegenstand.

5. Die Vorbereitung der Volkszählung 2011 ist bereits in vollem Gang

2011 soll in Deutschland, ebenso wie in der gesamten Europäischen Union, die nächste Volkszählung (Zensus) stattfinden. Diese erste Volkszählung in Deutschland nach der Wiedervereinigung ist ein Unterfangen, das – auch im Hinblick auf das für den Datenschutz wegweisende Volkszählungsurteil von 1983 – bereits aufgrund der Betroffenheit aller Bürger sowie der schieren Menge der Daten und Datenverarbeitungsvorgänge große datenschutzrechtliche Aufmerksamkeit verdient. Nach dem Entwurf der Bundesregierung für das Zensusvorbereitungsgesetz 2011 soll die Volkszählung 2011 erstmalig nicht mehr im Wege einer Befragung aller Einwohner, sondern im Wesentlichen registergestützt, d. h. im Wege der Auswertung vorhandener Verwaltungsregister bei den Meldebehörden, Vermessungsbehörden sowie der Bundesagentur für Arbeit, durchgeführt werden. Mit diesem Gesetzentwurf sind – im Vorfeld eines noch zu erwartenden Gesetzes über die eigentliche Durchführung der Volkszählung – bereits entscheidende Weichenstellungen vorgesehen:

Ein wesentliches Instrument für die Durchführung des registergestützten Zensus, das sog. Anschriften- und Gebäuderegister, soll bundesweit zentral vom Statistischen Bundesamt erstellt und geführt werden. Für die Erstellung dieses Registers ist u. a. vorgesehen, dass die Meldebehörden mit Stichtag 1. April 2008 für alle gemeldeten Einwohner deren Familiennamen, Familienstand, gegenwärtige und frühere Anschrift, Geburtstag, Geburtsort, Geburtsstaat, Staatsangehörigkeit und weitere Daten an die statistischen Ämter der Länder übermitteln. Die statistischen Ämter der Länder leiten diese Daten nicht nur an das Statistische Bundesamt weiter, sondern überprüfen das Ergebnis der Zusammenführung aller Daten insbesondere auf Vollzähligkeit und Schlüssigkeit der übermittelten Daten.

Dem hiesigen Finanzministerium, das mich erfreulicherweise sehr früh am Gesetzgebungsverfahren beteiligte, konnte ich zu verschiedenen Entwurfsfassungen des Zensusvorbereitungsgesetzes meine Anmerkungen zukommen lassen. Dabei habe ich neben handwerklichen Aspekten und der Frage nach der Abgrenzung der datenschutzrechtlichen Verantwortung zwischen dem Statistischen Bundesamt einerseits und den Statistischen Landesämtern andererseits auch einen kardinalen Punkt angesprochen: Die erforderliche Abschottung der amtlichen Statistik vom Verwaltungsvollzug. Das Bundesverfassungsgericht hat 1983 in seinem Volkszählungsurteil das strikte Gebot der Trennung von Statistik (also auch der Volkszählung) und Verwaltung formuliert. Die von mir geprüften Entwurfsfassungen des Zensusvorbereitungsgesetzes ließen letztlich nicht erkennen, ob und in welcher Weise diesem Trennungsgebot Rechnung getragen werden soll. Eine von mir vorgeschlagene Formulierung, mit der insoweit mehr Klarheit in die gesetzliche Regelung gekommen wäre, fand leider keinen Eingang in den Gesetzentwurf.

Die im Gesetzentwurf bislang vorgesehenen Möglichkeiten zur Prüfung der Daten auf Vollzähligkeit und Schlüssigkeit gehen dem Bundesrat dagegen nicht weit genug. Daher forderte er – konträr zum verfassungsrechtlichen Trennungsgebot – die Zulassung der Einzelfallprüfung von Meldedaten nach der Zusammenführung mit Daten aus anderen Registern. Ich kann nur hoffen, dass sich der Bundesrat, dessen Zustimmung für den Erlass des Gesetzes nicht erforderlich ist, mit dieser Forderung nicht durchsetzt.

5. Teil: Kommunales und anderes

1. Abschnitt: Kommunales

1. Die unerwünschten Nebenwohnungsinhaber

Ein seit dem Jahr 2004 mit Nebenwohnung in einer Stadt in Baden-Württemberg gemeldeter Einwohner hat sich Hilfe suchend an unsere Dienststelle gewandt. Er brachte vor, bei seiner Anmeldung habe er sehr ausführlich darlegen müssen, wie lange er sich am Ort seiner Nebenwohnung aufhalte. Trotzdem sei er nun innerhalb kurzer Zeit mehrmals von der Meldebehörde mit der Bitte angeschrieben worden, zu den Benutzungszeiten seiner Wohnung(en) einen entsprechenden Fragebogen auszufüllen. Zuletzt habe die Stadt sogar Zwangsgeld und Geldbuße angedroht bzw. angekündigt. Der Petent fühlte sich dadurch massiv bedroht und unter Druck gesetzt.

Wir baten die Stadt um Stellungnahme zu dem geschilderten Sachverhalt. Außerdem forderten wir die Stadt auf, uns wissen zu lassen, welchen Personenkreis (alle Einwohner, nur Nebenwohnungsinhaber?) sie angeschrieben hat. Die Antwort der Stadt förderte Folgendes zu Tage:

Demnach hat die Stadt als Maßnahme zur „Ertüchtigung“ des Melderegisters – insbesondere zur Vorbereitung des Registerzensus 2011 – eine Serienbriefaktion an ausgewählte, mit Nebenwohnung dort gemeldete Einwohner durchgeführt. Angeschrieben und befragt wurden diejenigen volljährigen und unverheirateten Nebenwohnungsinhaber, deren Hauptwohnung sich nach den Berechnungen der Stadt mehr als 75 Fahrminuten von der Stadt entfernt befindet. Die Stadt berief sich dabei auf § 5 a Abs. 2 des Meldegesetzes (MG), wonach die Meldebehörde den Sachverhalt von Amts wegen zu ermitteln hat, wenn ihr bezüglich einzelner oder einer Vielzahl namentlich bekannter Einwohner konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit des Melderegisters vorliegen. Nach Ansicht der städtischen Meldebehörde waren nämlich bei dem oben genannten Personenkreis konkrete Anhaltspunkte gegeben, um zu überprüfen, ob z. B. in der Stadt Berufstätige entsprechend ihrer zum Zeitpunkt der Anmeldung gemachten Angaben weiterhin an (einzelnen) Werktagen über drei Stunden für den Hin- und Rückweg zwischen Haupt- und Nebenwohnung aufwenden.

Diesen Sachverhalt habe ich datenschutzrechtlich wie folgt bewertet:

Die Verarbeitung – das heißt auch die Erhebung – personenbezogener Daten ist nach § 4 Abs. 1 LDSG nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Nachdem die Betroffenen offensichtlich nicht eingewilligt hatten, hätte die Stadt diese nur befragen dürfen, wenn eine andere Rechtsvorschrift (in diesem Fall das Meldegesetz) das erlauben würde. Als mögliche Rechtsgrundlagen für die Datenerhebung kamen der oben zitierte § 5 a Abs. 2 MG und § 20 MG in Betracht. Der Gesetzeswortlaut des § 5 a Abs. 2 MG macht das Tätigwerden der Meldebehörde davon abhängig, dass konkrete Anhaltspunkte für die Unrichtigkeit des Melderegisters vorliegen. Nach der Gesetzesbegründung zum früheren § 20 Abs. 1 MG (jetzt: § 20 MG) sollen die Meldebehörden auch außerhalb einzelner meldepflichtiger Vorgänge in die Lage versetzt werden, auf die Richtigkeit des Melderegisters hinzuwirken, wenn tatsächliche Anhaltspunkte zu Zweifeln an den Angaben des Meldepflichtigen oder an der Richtigkeit der Melderegisterdaten Anlass geben. Solche konkreten oder tatsächlichen Anhaltspunkte konnte ich den Kriterien, nach denen die Stadt die befragten Einwohner ausgewählt hat, nicht entnehmen. Der bloße Verdacht oder gar die vage Möglichkeit einer rechtlich relevanten Änderung der Wohnungsbenutzungs- bzw. Aufenthaltszeiten und damit auch einer Änderung des Wohnungsstatus gibt der Meldebehörde nicht das Recht, die früheren Angaben des Meldepflichtigen in Frage zu stellen und diesen unabhängig von einem melde- oder mitteilungspflichtigen Vorgang erneut zu seinen Meldeverhältnissen zu befragen. Offenbar sieht das der behördliche Datenschutzbeauftragte der Stadt ebenso. Jedenfalls hat er unserer Dienststelle gegenüber die Rechtmäßigkeit der Datenerhebung nicht ausdrücklich bestätigt.

Zu betonen ist auch, dass der Meldepflichtige bei jeder Anmeldung zu erklären hat, welche weiteren Wohnungen er hat und welche Wohnung seine Hauptwohnung ist. Ferner muss er der Meldebehörde der neuen Hauptwohnung jeden späteren Wechsel der Hauptwohnung innerhalb einer Woche schriftlich mitteilen. Die Meldebehörde der Stadt hatte im Zusammenhang mit der Anmeldung des Petenten aufgrund dessen Erklärung seine Wohnung in B. als Hauptwohnung und seine Wohnung in der Stadt als Nebenwohnung ins Melderegister eingetragen. Einen Wechsel seiner Hauptwohnung hatte der Petent der Stadt nicht mitgeteilt. Deshalb konnte und musste die Stadt davon ausgehen, dass sich an dessen melderechtlichen Verhältnissen inzwischen nichts rechtlich Relevantes geändert hat. Sie durfte nicht unterstellen, der Petent habe seine gesetzliche Pflicht zur Mitteilung eines Wechsels der Hauptwohnung verletzt. Die Stadt hätte den Petenten deshalb nicht erneut zu seinen Wohnverhältnissen befragen dürfen.

Ich konnte der Stadt eine förmliche Beanstandung des Datenschutzverstoßes nicht ersparen. Ich habe gebeten, dafür Sorge zu tragen, dass solche rechtswidrige Datenerhebungen künftig unterbleiben. Den Petenten und weitere Betroffene, die sich ebenfalls in dieser Sache an mich gewandt hatten, habe ich hiervon unterrichtet und ihnen die Rechtslage erläutert.

2. Gruppenauskunft aus dem Melderegister

Zwei Bürger einer baden-württembergischen Kleinstadt wandten sich unabhängig voneinander an unsere Dienststelle. Sie zeigten sich verwundert bzw. verärgert darüber, dass ein auswärtiges Wohnungsbauunternehmen sie angeschrieben und ihr Interesse an einer Seniorenwohnung per Fragebogen erkundet hatte.

Unsere Vermutung, dass die Adressen aus dem städtischen Melderegister stammten, bestätigte sich durch die von uns angeforderte Stellungnahme der Stadt. Demnach hat diese die Adressen aller mindestens 55 Jahre alten Einwohner an das Wohnungsbauunternehmen herausgegeben. Die Stadt ging offenbar davon aus, dass diese Gruppenauskunft aus dem Melderegister wegen des mit dem Bauvorhaben verfolgten Zwecks (Ermöglichung des betreuten Wohnens) im öffentlichen Interesse liegt und damit nach dem Meldegesetz zulässig ist. Wir haben den Sachverhalt datenschutzrechtlich wie folgt bewertet:

Das Landesdatenschutzgesetz lässt die Verarbeitung personenbezogener Daten, das heißt auch deren Übermittlung an private Dritte, nur zu, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Die betroffenen Einwohner hatten in die Übermittlung ihrer Adressen an den Bauträger offenbar nicht eingewilligt. Die Stadt hätte deshalb die personenbezogenen Daten nur herausgeben dürfen, wenn das vom Meldegesetz geforderte öffentliche Interesse an einer sog. Gruppenauskunft vorgelegen hätte. Dem war jedoch nicht so. Vielmehr hatte der Bauträger ein kommerzielles Interesse an der Kenntnis der Adressen und an der Verwirklichung des Bauvorhabens. Melderechtlich reicht es nicht aus, dass das betreute Wohnen selbst im öffentlichen Interesse liegen mag.

Ich habe die Stadt darauf hingewiesen, dass durchaus Alternativen zur Herausgabe der Adressen bestanden hätten. Der Bauträger hätte z. B. durch Postwurfsendungen oder durch öffentliche Aufrufe bzw. Einladungen zu Informationsveranstaltungen den Kontakt mit der Zielgruppe suchen können. Ferner habe ich die Stadt wissen lassen, dass auch eine sog. Adressmittlung (Auskunftsuchender stellt Schreiben an die Betroffenen zur Verfügung, die von der Meldebehörde adressiert und verschickt werden) hätte in Betracht gezogen werden können. Dieses Verfahren hat aus datenschutzrechtlicher Sicht den Vorteil, dass Dritten keine personenbezogenen Daten offenbart werden und es den Adressaten freisteht, ob sie auf das Schreiben reagieren oder nicht.

In der Erwartung, dass die Stadt die datenschutzrechtlichen Vorschriften künftig beachten wird, habe ich von einer förmlichen Beanstandung des Datenschutzverstoßes Abstand genommen.

3. Information des Gemeinderats

In einer Kleinstadt hatte eine Bürgerinitiative Unterschriften für die Durchführung einer Bürgerversammlung gesammelt. Ziel war es, eine Mobilfunkanlage in einem Wohngebiet zu verhindern. Der Petent, ein Mitglied der Bürgerinitiative, teilte uns mit, die Unterschriftenlisten seien der Stadtverwaltung übergeben worden. Diese habe zugesagt, sie unter Verschluss zu halten. Dennoch sei ein Teil der Unterschriftenlisten allen Mitgliedern des Gemeinderats als Sitzungsunterlage zugeleitet worden. Der Petent bzw. die Bürgerinitiative sahen in dieser städtischen Vorgehensweise einen Datenschutzverstoß.

Die von unserer Dienststelle um Stellungnahme gebetene Stadt machte geltend, nicht alle Unterschriftenlisten seien Bestandteil der Sitzungsunterlage für den Gemeinderat gewesen. Vielmehr seien die Gemeinderatsmitglieder nur über den Text des eigentlichen Antrags sowie über die personenbezogenen Daten der ersten zwölf Unterzeichner informiert worden, die sich auf demselben DIN-A4-Blatt befunden hätten. Die Stadt begründete diese Vorgehensweise damit, sie habe der Gefahr einer Verwechslung mit weiteren Anträgen in Sachen Mobilfunkanlagen begegnen wollen. Wir haben den Sachverhalt datenschutzrechtlich wie folgt beurteilt:

Nach § 4 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Die Einwilligung der Unterzeichner lag offensichtlich nicht vor. Die Weitergabe der personenbezogenen Daten der Unterzeichner – neben dem eigentlichen Antragstext in Sachen Bürgerversammlung/Mobilfunkanlage – wäre deshalb nur zulässig gewesen, wenn eine Rechtsvorschrift diese erlaubt hätte. Nach der Gemeindeordnung entscheidet zwar der Gemeinderat über die Zulässigkeit des Antrags der Bürgerschaft auf Anberaumung einer Bürgerversammlung. Deshalb war es natürlich nicht nur gerechtfertigt, sondern sogar geboten, den Antragstext mit Begründung dem Gemeinderat zur Verfügung zu stellen. Hinsichtlich der personenbezogenen Daten der Unterzeichner des Antrags ergibt sich bereits aus dem Text der Gemeindeordnung, dass der Sitzungseinladung (nur) die für die Verhandlung erforderlichen Unterlagen beizufügen sind. Die Beratungsunterlagen müssen den Gemeinderäten ermöglichen, sich über die zur Beratung und Entscheidung anstehenden Verhandlungsgegenstände zu informieren. Sie sollen den Gemeinderatsmitgliedern eine sachgerechte Urteilsbildung ermöglichen. Da der Gemeinderat über solche Anträge ohne Ansehen der unterzeichnenden Personen zu entscheiden hat, war die Mitteilung der Namen der Unterzeichner an die Gemeinderatsmitglieder nicht geeignet, zu einer sachgerechten Urteilsbildung beizutragen. Jedenfalls war die Weitergabe der personenbezogenen Daten an den Gemeinderat zu dessen Aufgabenerfüllung nicht erforderlich. Sie war deshalb datenschutzrechtlich unzulässig. Der Bürgermeister hatte übrigens in der Sitzungsvorlage bestätigt, dass das erforderliche Quorum erfüllt ist, das heißt die gesetzlich vorgeschriebene Zahl von wahlberechtigten Bürgern den Antrag unterzeichnet hat.

Wir haben der Stadt unsere Rechtsauffassung mitgeteilt und sie darauf hingewiesen, dass bei mehreren Anträgen zu demselben Thema Verwechslungen auf andere Weise ausgeschlossen werden können. Außerdem haben wir die Stadt gebeten, die datenschutzrechtlichen Vorschriften künftig zu beachten.

4. Nachwirkungen einer Bürgermeisterwahl

Eine Petentin teilte uns mit, sie habe gegen das Ergebnis der Bürgermeisterwahl in einer kleinen Gemeinde Einspruch beim zuständigen Landratsamt als Rechtsaufsichtsbehörde erhoben. Wie kommunalwahlrechtlich vorgeschrieben, hatte die Petentin ihrem Einspruchsschreiben eine Unterschriftenliste derjenigen Wahlberechtigten beigefügt, die ihrem Einspruch beigetreten waren. Die Liste habe auch die Vor- und Familiennamen sowie die Anschriften der Betroffenen enthalten. Die Petentin führte unserer Dienststelle gegenüber weiter aus, Familienmitglieder von Beigetretenen seien

von verschiedenen Personen, u. a. von einem Mitglied des Landtags von Baden-Württemberg und vom bisherigen Vorstand des Ortsvereins einer Partei, auf ihre Beteiligung an der Wahlanfechtung angesprochen worden. Inzwischen kursierten die Namen der beigetretenen Personen bereits in der gesamten Gemeinde. Die Petentin betonte, sie selbst habe bisher aus guten Gründen jegliche Nennung von Anfechtungsgründen oder von Namen der Beigetretenen gegenüber Dritten vermieden. Sie befürchte deshalb, dass Vertreter der an dem Verfahren beteiligten Behörden die datenschutzrechtlichen Vorschriften bzw. ihre Verschwiegenheitspflicht verletzt hätten. Ferner hätte nach Auffassung der Petentin die Prüfung der Wahlberechtigung der Beigetretenen aufgrund der politischen Sensibilität des Verfahrens nicht in der Gemeinde stattfinden dürfen. Zu diesem Zweck hätte die Gemeinde das Wählerverzeichnis auch an das Landratsamt herausgeben dürfen. Die Übermittlung der Daten der Beigetretenen durch das Landratsamt an die Gemeinde sei daher unnötig gewesen.

Die von uns angeforderten Stellungnahmen der beiden Behörden brachten folgendes Ergebnis:

Beide Behörden haben versichert, die Namen der Unterzeichner des Wahleinspruchs nicht an (private) Dritte herausgegeben zu haben. Auch die Mitglieder des mit der Angelegenheit befassten Gemeindewahlausschusses seien zu einer vertraulichen Behandlung der personenbezogenen Daten angehalten worden. Die Gemeinde hat ergänzend darauf hingewiesen, dass es im Rahmen der Sammlung der Unterschriften möglich gewesen sei, Namen von Unterzeichnern zur Kenntnis zu nehmen. Zum Teil hätten sich Unterzeichner auch schon vor der Einreichung des Wahleinspruchs entsprechend „geoutet“. Hinsichtlich der Prüfung der Wahlberechtigung hielten sowohl das Landratsamt als auch die Gemeinde daran fest, der gewählte Weg (Landratsamt übermittelte die Namen usw. der Unterzeichner des Wahleinspruchs an die Gemeinde; diese gab dem Landratsamt Rückmeldung über die Wahlberechtigung der Betroffenen) sei schonender gewesen als die Übermittlung des kompletten Wählerverzeichnisses durch die Gemeinde an das Landratsamt.

Nach Abschluss meiner datenschutzrechtlichen Prüfung teilte ich allen Beteiligten mit, dass ich im vorliegenden Fall einen Verstoß gegen datenschutzrechtliche Vorschriften nicht feststellen konnte. Das praktizierte Verfahren zur Prüfung der Wahlberechtigung der Unterzeichner beschränkte meines Erachtens den Umfang der übermittelten personenbezogenen Daten auf das zur Aufgabenerfüllung Erforderliche und entsprach auch dem Grundsatz der Datensparsamkeit. Es war deshalb aus datenschutzrechtlicher Sicht der vollständigen Übermittlung des Wählerverzeichnisses an das Landratsamt vorzuziehen. Jedenfalls sah ich in der gewählten Vorgehensweise keinen Grund zur Beanstandung.

2. Abschnitt: Personalwesen

1. Elektronisches Bestellen von Jahreskarten für öffentliche Verkehrsmittel

Im Rahmen der Behördenticket-Aktion können Beschäftigte des Landes über das elektronische Kundenportal des Landesamts für Besoldung und Versorgung Baden-Württemberg (im Folgenden: Landesamt) Jahreskarten für öffentliche Verkehrsmittel erwerben. Nach der Anmeldung beim Kundenportal und wenn das Landesamt festgestellt hat, dass der Betroffene Beschäftigter des Landes und damit berechtigt ist, das Behördenticket zu bestellen, ist die Bestellung gegenüber dem Unternehmen möglich, das die Bestellung abwickelt. In meinem 27. Tätigkeitsbericht für das Jahr 2006 (LT-Drucksache 14/650) musste ich bemängeln, dass vorübergehend jeder über das Internet personenbezogene Bestelldaten der Betroffenen wie Name, Wohnanschrift und Bankverbindung abrufen konnte, nachdem diese ein Behördenticket bestellt hatten. Im aktuellen Berichtszeitraum hat mein Amt sich mit der Ausgestaltung der Behördenticket-Aktion befasst.

Das Bestellen des Behördentickets über das Kundenportal des Landesamts geschieht folgendermaßen: Der Betroffene meldet sich über das Internet

beim Kundenportal an. Dazu gibt er seine Personalnummer und sein dazugehöriges Passwort ein. Im Kundenportal wählt er das Behördenticket aus, das er erwerben möchte („Job-Ticket“ oder „Firmenticket“). Daraufhin zeigt das Landesamt dem Betroffenen im Kundenportal bestimmte Daten zu seiner Person an. Durch Anklicken einer Schaltfläche auf dem Bildschirm kann der Betroffene veranlassen, dass diese Daten an das genannte Unternehmen weitergeleitet werden. Das Unternehmen erfragt vom Betroffenen gegebenenfalls weitere Daten für die Bestellung.

Aus datenschutzrechtlicher Sicht waren dabei u. a. folgende Punkte bedeutsam:

– Das Landesamt ist nach seiner Auffassung weder für das Weiterleiten der Daten des Betroffenen an das Unternehmen noch für das Verarbeiten der Daten durch das Unternehmen datenschutzrechtlich verantwortlich: Wenn der Betroffene im Kundenportal die genannte Schaltfläche anklicke, führe das lediglich dazu, dass das Landesamt die „technische“ Übermittlung der im Kundenportal angezeigten Daten an das Unternehmen übernehme. Dazu stelle das Landesamt dem Betroffenen „lediglich das Medium für die Bestellung“ zur Verfügung. Es handle sich dabei um eine Übermittlung durch den Betroffenen selbst. Das Unternehmen verarbeite die personenbezogenen Daten des Betroffenen nicht für das Landesamt (im Rahmen einer Datenverarbeitung im Auftrag). Es verarbeite diese Daten vielmehr im Auftrag des Betroffenen.

  Wir haben dem Landesamt dazu mitgeteilt, dass sich das aus den Unterlagen zur Behördenticket-Aktion, welche die Betroffenen über das Verfahren unterrichten sollen, nicht hinreichend deutlich ergibt. Die entsprechenden Ausführungen seien zu verdeutlichen und zu vereinheitlichen.

– Das Landesamt sieht inzwischen weniger Daten als ursprünglich zur Weitergabe an das Unternehmen vor. Im Kundenportal zeigt es noch folgende, weiterzugebende Daten an: Bestätigungscode, Name, Vorname, Straße und Hausnummer, Postleitzahl und Ort.

  Ob es sich dabei um die unabdingbar notwendigen Daten für das Bestellen des Behördentickets handelt oder ob auch einzelne dieser Daten noch verzichtbar sind, wäre vom Landesamt noch zu verdeutlichen.

– Der Bestätigungscode muss nach dem Vortrag des Landesamts nur in den Fällen an das Unternehmen übermittelt werden, in denen die Betroffenen ihr „Job-Ticket“ im Abonnement erhalten. Zwar liegt hinsichtlich des „Firmentickets“ kein Abonnement vor, denn es muss jährlich neu bestellt werden. Gleichwohl wurde beim Bestellen eines „Firmentickets“ im Kundenportal ein Bestätigungscode zur Weitergabe an das Unternehmen angezeigt. Eine Bestellung des „Firmentickets“ über das Kundenportal ohne Weitergabe des Bestätigungscodes war nicht vorgesehen.

  Wir haben das Landesamt darauf hingewiesen, dass dies entweder nachvollziehbar zu erläutern ist oder dass beim Bestellen eines „Firmentickets“ das Bereitstellen des Bestätigungscodes zum Weiterleiten an das Unternehmen umgehend einzustellen ist.

– Zur Frage, was mit den personenbezogenen Daten des Betroffenen bei einem Abbruch der Bestellung geschieht, erklärte das Landesamt, es setze mittlerweile ein neues Verfahren ein, das alle Daten beim Schließen der Browser oder beim Drücken der Taste „Beenden“ sofort lösche.

  Zwar werden dadurch die Daten auf dem Client des Betroffenen gelöscht. Unklar ist aus unserer Sicht aber, was auf der Seite des Servers des Unternehmens geschieht. Wir haben das Landesamt gebeten zu klären, ob bei fortschreitendem Bestellvorgang personenbezogene Daten auf der Seite des Servers des Unternehmens gespeichert werden und ob diese Daten gelöscht werden, wenn der Bestellvorgang, beispielsweise in Folge eines Netzwerkausfalls, nicht bis zum Ende durchgeführt wird.

Das Landesamt prüft gegenwärtig, inwieweit unsere Anmerkungen zur Ausgestaltung der Behördenticket-Aktion umgesetzt werden können.

2. Zugriff auf die vollständige Personalakte in Versorgungsfragen

Landesbeamte können beim Landesamt für Besoldung und Versorgung Baden-Württemberg Auskunft über die Höhe ihrer Versorgungsanwartschaft nach dem Beamtenversorgungsgesetz beantragen.

Lagen bisher dem Landesamt bei der Bearbeitung eines solchen Antrags nicht alle Daten vor, die für die Auskunft notwendig waren, dann teilte es dem Antragsteller mit, es benötige Einsicht in die Personalakte, da „wichtige Daten fehlen". Zugleich übersandte das Landesamt dem Antragsteller einen Vordruck, auf dem dieser erklären konnte, er sei damit einverstanden, dass die personalverwaltende Stelle seine Personalakte dem Landesamt übersendet. Aus datenschutzrechtlicher Sicht war dieses Vorgehen, wie in meinem 27. Tätigkeitsbericht für das Jahr 2006 (LT-Drucksache 14/650) dargestellt, u. a. aus folgenden Gründen zu bemängeln:

- Das Landesamt unterrichtete den Antragsteller nicht darüber, welche Daten fehlten. Dieser hatte somit keine Gelegenheit, die fehlenden Daten dem Landesamt selbst mitzuteilen.
- Das Landesamt beschränkte die Aktenvorlage nicht auf die Aktenteile, welche die fehlenden Daten enthielten. Es konnte daher in der vorgelegten Personalakte auch auf Daten zugreifen, die es nicht benötigte.
- Die Erklärung des Antragstellers auf dem Vordruck des Landesamts konnte überhaupt keinen Zugriff auf die Personalakte erlauben. Dafür hätte es einer wirksamen Einwilligung bedurft. Diese setzte wiederum u. a. voraus, dass dem Antragsteller zuvor mitgeteilt wurde, auf welche noch fehlenden Daten das Landesamt in der Personalakte im Einzelnen zugreifen wollte, was jedoch nicht geschah.

Das Landesamt teilte inzwischen Folgendes mit: Es sehe keine (vollständigen) Personalakten mehr ein. Wenn Daten oder Nachweise, die für Versorgungsauskünfte maßgeblich sind, dem Landesamt überhaupt nicht oder nicht vollständig vorliegen oder ihre Richtigkeit zweifelhaft ist, erhebe das Landesamt diese unmittelbar beim Antragsteller und gebe diesem gegenüber den Grund für diese Datenerhebung an. Dabei weise es darauf hin, dass der Antragsteller sich diese Nachweise gegebenenfalls bei seiner personalverwaltenden Dienststelle beschaffen könne. Zudem teile das Landesamt dem Antragsteller mit, dass er auch seine personalverwaltende Dienststelle bitten könne, die benötigten Unterlagen aus den dort vorliegenden Personalunterlagen dem Landesamt zu übersenden. Die „Bekanntmachung des Finanzministeriums über Auskünfte an aktive Beamte und Richter über ihre Versorgungsanwartschaften" vom 17. Dezember 1987, worauf die bisherige Handhabung gestützt war, werde geändert.

Damit trägt das Landesamt dem Recht der Antragsteller auf informationelle Selbstbestimmung Rechnung. Wir haben dem Landesamt zu einzelnen Punkten in seinen geänderten Vordrucken Hinweise gegeben, die aus datenschutzrechtlicher Sicht noch zu berücksichtigen sind.

3. Abschnitt: Sonstiges

1. Werbung für die nächste Hauptuntersuchung

Ein privates Unternehmen, das die Hauptuntersuchung an Kraftfahrzeugen durchführt und insoweit – als hoheitlich tätige Stelle – unserer datenschutzrechtlichen Kontrolle unterliegt, erinnerte seine Kunden schriftlich an den Termin der nächsten Hauptuntersuchung mit dem Hinweis: „Die Zeit vergeht wie im Fluge". Darüber hinaus ließ es die Kunden wissen: „Wir würden uns sehr freuen, wenn Sie uns wieder Ihr Vertrauen schenken". Dazu verwendete das Unternehmen Daten der früheren Hauptuntersuchung. Das Unternehmen hatte aber von den Betroffenen hierzu keine Einwilligungen eingeholt. Aus datenschutzrechtlicher Sicht war dies folgendermaßen zu bewerten:

Die zur Durchführung der Hauptuntersuchung erhobenen personenbezogenen Daten dürfen nur verarbeitet werden, um im Nachhinein prüfen zu

können, ob die Untersuchung selbst ordnungsgemäß erfolgt ist. Eine Verarbeitung für andere Zwecke ist nur mit schriftlicher Einwilligung des Betroffenen zulässig. Beides ergibt sich aus der Anlage VIIIb zur Straßenverkehrs-Zulassungs-Ordnung. Die Erinnerungen an die nächste Hauptuntersuchung einschließlich der Werbung in eigener Sache haben mit der Frage, ob die frühere Hauptuntersuchung ordnungsgemäß erfolgt ist, nichts mehr zu tun. Das Nutzen personenbezogener Daten hierfür stellt eine Änderung des Zwecks dar, zu welchem die Daten ursprünglich erhoben wurden.

Eine Rechtsvorschrift, nach welcher personenbezogene Daten aus einer Hauptuntersuchung – abweichend von der genannten Regelung der Anlage VIIIb zur Straßenverkehrs-Zulassungs-Ordnung – dafür verwendet werden dürfen, um an den Termin der nächsten Hauptuntersuchung zu erinnern, gibt es nicht. Daher haben wir das Unternehmen, das seine Erinnerungsschreiben auch als Service für seine Kunden versteht, darauf hingewiesen, dass es ihm unbenommen ist, die Betroffenen bei der Hauptuntersuchung um ihre Einwilligung zur Nutzung der Daten zu bitten (Näheres zu den Voraussetzungen einer wirksamen Einwilligung, etwa das Schriftformerfordernis, ergibt sich ebenfalls aus der Anlage VIIIb zur Straßenverkehrs-Zulassungs-Ordnung). Mit einer formgerechten Einwilligung der Betroffenen können dann sowohl deren Belange wie auch die Interessen des Unternehmens ohne weiteres unter einen Hut gebracht werden.

2. Behörde verschickt Unterlagen mit Gesundheitsdaten an den Falschen

Einer Zeitungsmeldung entnahmen wir, dass eine Behörde eine Postsendung an eine Person versandt hatte, die auch Unterlagen mit personenbezogenen Daten mehrerer mit Namen und Anschrift genannter Dritter enthielt; diese Unterlagen waren jedoch nicht für den Empfänger bestimmt. Dabei ging es etwa um Angaben zur Geeignetheit dieser Personen zum Führen von Kraftfahrzeugen wegen eines Alkoholproblems oder wegen einer psychischen Erkrankung; die entsprechenden ärztlichen Atteste waren ebenfalls angeschlossen.

Die von uns daraufhin um Stellungnahme gebetene Behörde teilte mit, dass die Unterlagen offensichtlich versehentlich in den für den Empfänger vorgesehenen Umschlag gesteckt worden seien. Näheres lasse sich leider nicht mehr mit hinreichender Sicherheit aufklären. Zu unserer Frage, durch welche konkreten Maßnahmen in der Behörde zum fraglichen Zeitpunkt darauf hingewirkt wurde, dass die ausgehende Post nur den vorgesehenen Inhalt hat, schrieb uns die Behörde, dass dort folgende Regelung gelte: Zum einen seien die Organisationseinheiten der Behörde angewiesen, Vorgänge nicht gesammelt in Laufmappen an die Poststelle der Behörde zu senden, sondern je Vorgang eine Laufmappe zu verwenden. Zum anderen seien die Beschäftigten der Poststellen angewiesen, alle Anlagen genau zu überprüfen und auch gebündelte Versandstücke durchzusehen. Darüber hinaus seien die Leiter der Versandstellen angewiesen, Stichproben vorzunehmen. Unter Hinweis auf den Vorfall habe die Behörde diese Maßnahmen erneut angeordnet und die Leiter der Poststellen angewiesen, diese Maßnahmen mit ihren Mitarbeitern zu besprechen.

Wir haben der Behörde mitgeteilt, dass der Versand von Unterlagen mit personenbezogenen Daten an den falschen Adressaten datenschutzrechtlich unzulässig war, auch wenn dies versehentlich geschah. Vor allem im Hinblick auf die erneut getroffenen innerorganisatorischen Maßnahmen der Behörde haben wir aber von einer Beanstandung abgesehen.

3. Ohne Steuer nicht ans Steuer

Gleich zwei neue Rechtsvorschriften aus diesem Jahr sollen dazu beitragen, dass bestimmte Steuer- und Gebührenrückstände im Land künftig der Vergangenheit angehören. Beide Vorschriften beruhen auf bundesgesetzlichen Ermächtigungen. Sie wurden uns im Entwurfsstadium zugeleitet. Auch wenn die Entwürfe keinen grundsätzlichen datenschutzrechtlichen Bedenken begegneten, waren sie aus datenschutzrechtlicher Sicht zu ändern, was teilweise geschah. Im Einzelnen ist von unserer Seite aus dazu Folgendes zu berichten:

3.1 Das Fahrzeugzulassungsverweigerungsgesetz

Nunmehr soll Schluss damit sein, dass ein Fahrzeughalter trotz rückständiger Gebühren aus vorausgegangenen Zulassungsvorgängen (hierzu gehört auch die zwangsweise Außerbetriebsetzung) die Zulassung für sein Kraftfahrzeug erhält. Das vom Landtag kürzlich erlassene „Gesetz über die Verweigerung der Zulassung von Fahrzeugen bei rückständigen Gebühren und Auslagen (Fahrzeugzulassungsverweigerungsgesetz)“ macht die Kraftfahrzeugzulassung grundsätzlich davon abhängig, dass keine entsprechenden Forderungen mehr bestehen.

Das Gesetz sieht vor, dass die Zulassungsbehörde hierzu bestimmte Angaben zum Fahrzeughalter, zum Fahrzeug sowie zu den Schulden und zu etwaigen Vollstreckungsmaßnahmen verarbeiten darf. Darüber hinaus darf die Zulassungsbehörde auch bei anderen Zulassungsbehörden anfragen, ob dort Rückstände aus früheren Zulassungen bestehen.

Unsere damalige Empfehlung, für die im Entwurf vorgesehene Bekanntgabe personenbezogener Daten des Fahrzeughalters an einen Dritten, den der Fahrzeughalter mit der Zulassung beauftragt hat, die Schriftform vorzuschreiben, hat im vorliegenden Gesetz Niederschlag gefunden. Nicht umgesetzt wurde unsere Anregung, es dabei dem Fahrzeughalter zu überlassen, ob dem Dritten ausschließlich mitgeteilt werden darf, dass überhaupt Rückstände bestehen, oder ob dem Dritten darüber hinaus auch Einzelheiten zu den Rückständen kundgetan werden dürfen. Nach dem in Kraft getretenen Gesetz hat der Fahrzeughalter vor einer Zulassung durch einen Dritten stets – ohne eine solche Wahlmöglichkeit – sein Einverständnis zu erklären, dass die Zulassungsbehörde den Dritten über die Höhe der Schulden und die vorausgegangenen Zulassungsvorgänge unterrichten darf. Bedeutsam wäre eine solche Wahlmöglichkeit auch deswegen gewesen, weil nach der Begründung des Gesetzes in Baden-Württemberg davon auszugehen ist, dass in mehr als zwei Dritteln der Zulassungsvorgänge nicht der Fahrzeughalter den Antrag auf Zulassung eines Fahrzeugs stellt, sondern Autohändler, Zulassungsdienste oder auch Familienangehörige bevollmächtigt werden, die notwendigen Unterlagen vorzulegen.

3.2 Die Verordnung der Landesregierung über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer

Die Verordnung sieht zum einen vor, dass eine Zulassungsbehörde im Falle der Steuerpflicht nach dem Kraftfahrzeugsteuergesetz 2002 ein Kraftfahrzeug erst dann zulassen darf, wenn der Fahrzeughalter eine schriftliche Ermächtigung zum Einzug der Kraftfahrzeugsteuer erteilt hat, sofern das Finanzamt darauf nicht ausnahmsweise verzichtet. Zum anderen soll die Zulassungsbehörde prüfen, ob Kraftfahrzeugsteuerrückstände des Fahrzeughalters der Zulassung entgegenstehen, und hierzu Auskünfte bei den Finanzämtern des Landes einholen dürfen. Die Prüfung der Kraftfahrzeugsteuerrückstände findet derzeit jedoch noch nicht statt, da das EDV-Verfahren, welches dafür genutzt werden soll, noch nicht einsatzbereit ist.

Unsere Hinweise zum Schriftformerfordernis für eine Einverständniserklärung des Fahrzeughalters hinsichtlich einer Bekanntgabe von Daten an Dritte und zur eindeutigen Bezeichnung der an der Datenverarbeitung beteiligten öffentlichen Stellen (Finanzämter, nicht lediglich: Steuerverwaltung) haben Aufnahme in die Verordnung gefunden. Auch bei der Verordnung wurde unserer Anregung, es dabei dem Fahrzeughalter zu überlassen, ob dem Dritten ausschließlich mitgeteilt werden darf, dass überhaupt Rückstände bestehen, oder ob dem Dritten darüber hinaus auch Einzelheiten zu den Rückständen kundgetan werden dürfen, nicht Rechnung getragen.

6. Teil: Technik und Organisation

1. Datenschutzmanagement

Jede Stelle, die personenbezogene Daten verarbeitet, muss flankierend dazu technische und organisatorische Schutzmaßnahmen ergreifen. Seitdem Baden-Württemberg über ein Landesdatenschutzgesetz verfügt, sind dessen Vorschriften über technische und organisatorische Schutzmaßnahmen weitgehend unverändert geblieben. Dass Regelungen, die noch aus einer Zeit stammen, als es noch keine PCs, kein Internet, keine drahtlosen Computernetzwerke, keine Handies, keine Chipkarten und keine RFID-Anwendungen gab, auch heute noch anwendbar sind, geht darauf zurück, dass das Landesdatenschutzgesetz lediglich allgemein formulierte Ziele vorgibt und keine bestimmten technischen oder organisatorischen Lösungen vorschreibt.

Das bedeutet jedoch auch, dass einmal getroffene Festlegungen darüber, welche konkreten technischen und organisatorischen Maßnahmen nach dem Landesdatenschutzgesetz notwendig sind, immer wieder aufs Neue zu hinterfragen sind. Änderungen können beispielsweise erforderlich sein, weil die von einer Stelle genutzte IuK-Technik der technischen Entwicklung folgend erneuert wird oder weil Sicherheitslücken der genutzten Produkte bekannt werden, gegen die bislang noch keine Schutzmaßnahmen ergriffen wurden. Die Entwicklung eines Datenschutzkonzepts ist daher eine ständige Aufgabe und keine, die etwa nur einmal bei der Einführung eines neuen Verfahrens zu erledigen wäre. Dabei ist die Aufgabe, ein Datenschutzkonzept stets auf aktuellem Stand zu halten, keineswegs trivial. Insbesondere bei ausgedehnten Computernetzwerken, wie sie heutzutage weit verbreitet sind, finden laufend technische Änderungen und Aktualisierungen statt und diese können gerade aufgrund der Vernetzung der Einzelsysteme immer weiter reichende Auswirkungen haben. Soll es nicht dem Zufall überlassen bleiben, wie systematisch diese Aufgabe bewältigt wird, muss ein umfassendes Datenschutzmanagement betrieben werden. Wer dies tun will, kann seine Vorgehensweise an einer Reihe standardisierter Vorgehensweisen (Managementstandards) orientieren.

– Allgemeine Standards zum IuK-Management

  Stellen, die möglicherweise bereits aus anderen Gründen eine standardisierte Vorgehensweise in ihrem IuK-Management eingerichtet haben oder gerade dabei sind, ein solches Management einzurichten, können damit in vielen Fällen auch eine Stärkung ihrer Datenschutz- und Datensicherheitsmaßnahmen erreichen. Dies gilt beispielsweise für Stellen, die ihr IuK-Management entsprechend dem ITIL-(Information Technology Infrastructure Library) oder dem COBIT-Standard (Control Objectives for Information and Related Technology) vornehmen. Diese zielen darauf ab, dass möglichst viele interne Betriebsabläufe standardisiert und dokumentiert werden und dass für alle Aufgaben Verantwortliche bestimmt werden. Da Datenschutz und Datensicherheit keine inhaltlichen Kernbestandteile dieser Standards sind, ist durch deren Einsatz auch nicht bereits automatisch sichergestellt, dass der IuK-Betrieb datenschutzgerecht erfolgt. Sofern eine Daten verarbeitende Stelle diese Standards jedoch bewusst auch für datenschutzrelevante Aufgaben einsetzt, kann durch die damit einhergehende Präzisierung und Dokumentation der erforderlichen Abläufe sowie die Festlegung klarer Verantwortlichkeiten das Datenschutzniveau erhöht werden.

– ISO-Normen zum IuK-Sicherheitsmanagement

  Eine aus Sicht des Datenschutzes zielgenauere Unterstützung für das Datenschutzmanagement bietet eine Vorgehensweise, die sich an mehreren international genormten Standards für den Umgang mit IuK-Sicherheitsfragen orientiert. Dafür sind insbesondere die ISO-Normen 27001 („Information Security Management Systems“), 27002 („Code of Practice for Information Security Management“) sowie die bislang nur als Entwurf vorliegende Norm 27005 („Information Security Risk Management“) von Bedeutung. Im Gegensatz zu den allgemeineren Standards ITIL oder

COBIT befassen sich diese ISO-Standards inhaltlich ausdrücklich mit dem Management von IuK-Sicherheitsfragen und benennen in allgemeiner Form Ziele des IuK-Sicherheitsmanagements. Beispiele für diese Ziele sind die Gewährleistung der Netzwerk- und Betriebssicherheit, die Realisierung einer Zugriffskontrolle (Access Control) oder die Einhaltung gesetzlicher Anforderungen (Compliance).

Ferner bieten die Normen Hilfestellung etwa bei der

- Festlegung des Anwendungsbereichs des zu erstellenden und zu pflegenden Sicherheitskonzepts,
- Definition der Sicherheitsleitlinien (Policy)
- Festlegung der Art und Weise des Risikomanagements sowie der
- Durchführung einer Risikoanalyse.

Auch wenn diese ISO-Normen bereits spezifisch auf Fragen der IuK-Sicherheit bezogen sind, können diese – und hierin liegt eine bemerkenswerte Analogie zu den in den im Landesdatenschutzgesetz enthaltenen Vorschriften zum technischen und organisatorischen Datenschutz – aufgrund ihrer allgemeinen Fassung vielfach keine Antwort auf die Frage geben, welche Schutzmaßnahmen in konkreten Fällen in Betracht kommen.

– Grundschutz-Vorgehensweise

Eine Möglichkeit, um auch bei Anwendung der erwähnten ISO-Standards Antworten auf die Frage nach den in bestimmten Fällen notwendigen Sicherheitsmaßnahmen zu erhalten, besteht darin, hierzu auf Kataloge zurückzugreifen, in denen für verschiedenste IuK-Systeme zum einen die damit verbundenen Gefährdungen und zum anderen Maßnahmen benannt werden, die zur Abwehr der genannten Gefährdungen geeignet sind. Solche Kataloge stehen beispielsweise in Gestalt der sog. Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) (www.bsi.bund.de/gshb/index.htm) zur Verfügung. Die darin für viele praxisrelevante Fallkonstellationen gegebene Übersicht über dort bestehende Gefährdungen und die zu deren Abwehr in Frage kommenden Sicherheitsmaßnahmen hat im Laufe der Zeit einen Umfang von mehreren tausend Seiten angenommen.

Für das IuK-Sicherheitsmanagement hat das BSI ein Modell entwickelt, das die Inhalte der ISO-Normen 27001 und 27002 zum IuK-Sicherheitsmanagement aufgreift und so ergänzt, dass diese in Kombination mit den Grundschutzkatalogen eine systematische Vorgehensweise zur Bestimmung und zur laufenden Aktualisierung der von einer Daten verarbeitenden Stelle zu ergreifenden technischen und organisatorischen Schutzmaßnahmen beschreiben.

2. Datenschutzfreundliche Umsetzung der Europäischen Dienstleistungsrichtlinie

Immer mehr Rechts- und Verwaltungsbereiche werden durch Vorgaben der Europäischen Union geprägt. So sorgte die Europäische Union (EU) beispielsweise bereits im Jahr 1995 durch ihre Datenschutzrichtlinie für eine Harmonisierung des Datenschutzrechts in allen Mitgliedstaaten. Auch die mit erheblichen datenschutzrechtlichen Risiken einhergehende Vorratsdatenspeicherung in der Telekommunikation geht in weiten Teilen auf eine entsprechende europäische Richtlinie zurück.

Erhebliche datenschutzrechtliche Relevanz weist auch die im Dezember 2006 verabschiedete Dienstleistungsrichtlinie auf. Mit ihr beabsichtigt die Europäische Union, europaweit eine einfache Nutzbarkeit vieler Behördendienstleistungen zu erreichen. Dieses Vorhaben, dessen Ausmaße bislang nur in Umrissen erkennbar sind, könnte auch bedeutende Auswirkungen auf die Verwaltungsorganisation und viele Verwaltungsabläufe in Baden-Württemberg haben.

2.1 Eckpunkte der Dienstleistungsrichtlinie

Die Dienstleistungsrichtlinie befasst sich mit den für die Aufnahme und Ausübung einer Dienstleistungstätigkeit geltenden Verfahren und Formalitäten. Beispiele hierfür sind die Einrichtung eines Gaststättenbetriebs, Frisörsalons oder eines Architektenbüros. Sie legt u. a. fest:

– Einheitliche Ansprechpartner

  Die Abwicklung aller dieser Verfahren und Formalitäten muss über sog. einheitliche Ansprechpartner möglich sein. Deren Einrichtung solle aber nicht die „Verteilung von Zuständigkeiten und Befugnissen zwischen Behörden“ innerhalb der Mitgliedstaaten berühren.

  Diese Vorgaben bieten noch erheblichen Gestaltungsspielraum, welche Stellen letztendlich die Rolle eines einheitlichen Ansprechpartners übernehmen sollen und welche Aufgaben diesen Stellen dazu konkret zugewiesen werden sollen.

– Vollelektronische Abwicklung

  Die Mitgliedstaaten müssen sicherstellen, dass „alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner oder bei der betreffenden zuständigen Behörde abgewickelt werden können.“

– Standardbearbeitungsfristen für Anträge mit Genehmigungsfiktion nach Fristablauf

  Die Dienstleistungsrichtlinie sieht vor, dass Anträge „unverzüglich und in jedem Fall binnen einer vorab festgelegten und bekannt gemachten angemessenen Frist bearbeitet werden“ müssen. Wird der Antrag nicht fristgerecht beantwortet, so gilt die beantragte Genehmigung als erteilt.

– Pflicht zu Warnmitteilungen

  Sobald ein Mitgliedstaat Kenntnis von „bestimmten Handlungen oder Umständen im Zusammenhang mit einer Dienstleistungstätigkeit“ erhält, „die einen schweren Schaden für die Gesundheit oder Sicherheit von Personen oder für die Umwelt in seinem Hoheitsgebiet oder im Hoheitsgebiet anderer Mitgliedstaaten verursachen können“, so muss er die übrigen betroffenen Mitgliedstaaten und die Kommission „so schnell wie möglich“ hierüber unterrichten.

– Austausch von Informationen über die Zuverlässigkeit von Dienstleistungserbringern

  „Auf Ersuchen einer zuständigen Behörde eines anderen Mitgliedstaats übermitteln die Mitgliedstaaten unter Beachtung ihres nationalen Rechts Informationen über Disziplinar- oder Verwaltungsmaßnahmen oder strafrechtliche Sanktionen und Entscheidungen wegen Insolvenz oder Konkurs mit betrügerischer Absicht, die von ihren zuständigen Behörden gegen einen Dienstleistungserbringer verhängt wurden und die von direkter Bedeutung für die Kompetenz oder berufliche Zuverlässigkeit des Dienstleistungserbringers sind.“

2.2 Datenschutzfreundliche Umsetzung der Dienstleistungsrichtlinie

Die Vorgaben der Dienstleistungsrichtlinie müssen bis Ende des Jahres 2009 in nationales Recht umgesetzt werden. Bedenkt man, dass hiervon sehr viele Verwaltungsbereiche betroffen sind und zur Umsetzung nicht nur Rechtsänderungen vorgenommen, sondern auch IuK-Systeme geplant, realisiert und in Betrieb genommen werden müssen, so wird deutlich, dass die dafür noch zur Verfügung stehenden zwei Jahre knapp bemessen sind. Schon in naher Zukunft müssen daher auch für den Datenschutz relevante Vorentscheidungen zum einen bei der Rechtsetzung und zum anderen bei der IuK-Systemgestaltung getroffen werden. Die

Datenschutzberatung hinsichtlich eines solchen Vorhabens befindet sich in einem kaum auflösbaren Dilemma: Auf der einen Seite ist es sinnvoll, Hinweise zur datenschutzgerechten Gestaltung bereits in einer möglichst frühen Phase der Systementwicklung zu geben. Auf der anderen Seite kann sich die Beratung aufgrund des frühen Entwicklungsstands nur auf wenige verlässliche Fakten stützen. Auch wenn in dieser Situation von Seiten des Datenschutzes nur erste, unvollständige Hinweise gegeben werden können, halten wir eine frühzeitige beratende Stellungnahme für sinnvoll. Inhaltlich sind derzeit für uns folgende Punkte besonders wichtig:

– Klare Rechtsgrundlagen schaffen

  Hinsichtlich der Umsetzung der Dienstleistungsrichtlinie wird gegenwärtig umfassend geprüft, wo dazu noch gesetzgeberischer Handlungsbedarf besteht. Bei der Überprüfung, ob und in wieweit auch noch entsprechende Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen oder anzupassen sind, sollte auch auf Folgendes geachtet werden:

  Die Dienstleistungsrichtlinie spricht davon, dass Stellen in den Mitgliedstaaten verpflichtet seien, sich gegenseitig „Amtshilfe“ zu leisten. Die dafür möglicherweise noch zu schaffenden Regelungen müssen, wenn sie Befugnisse zur Verarbeitung personenbezogener Daten schaffen sollen, die zulässige Art einer solchen Amtshilfe deutlich präzisieren und klar benennen, welche Stellen welche personenbezogenen Daten dazu auf welche Weise erheben, speichern, übermitteln oder in anderer Weise verarbeiten dürfen.

– Datenschutzrechtliche Verantwortlichkeiten klären

  Ein wesentlicher Gesichtspunkt bei der elektronischen Unterstützung der Umsetzung der Dienstleistungsrichtlinie stellt die notwendige Abgrenzung der Rollen und Zuständigkeiten derjenigen Stellen dar, die mit Hilfe dieser IuK-Systeme künftig personenbezogene Daten verarbeiten sollen. Nach gegenwärtigem Informationsstand sollen sowohl die EG-Kommission wie auch zahlreiche bestehende oder neu zu schaffende Stellen in den Mitgliedstaaten einzelne Aufgaben übernehmen. Datenschutzrechtlich ist daran bedeutsam, dass in den zu realisierenden IuK-Systemen in großem Umfang personenbezogene Daten verarbeitet und möglicherweise auch für eine gewisse Zeit gespeichert werden sollen. Und dabei gilt es, Klarheit darüber zu schaffen, welche dieser Stellen datenschutzrechtlich für welche Teile der insgesamt geplanten Verarbeitung personenbezogener Daten verantwortlich sein sollen. Erst wenn dies geklärt ist, kann bestimmt werden, welches Datenschutzrecht für die entsprechenden Teile der Datenverarbeitung Anwendung findet und welche Datenschutzaufsichtsbehörde die entsprechende Datenverarbeitung künftig zu kontrollieren hat.

– Datenschutzrechtliche Auftragsverhältnisse klären

  Es ist damit zu rechnen, dass einige der auf diese Weise bestimmten verantwortlichen Stellen die Verarbeitung personenbezogener Daten nicht selbst auf eigenen IuK-Systemen vornehmen, sondern, im Rahmen einer sog. „Datenverarbeitung im Auftrag“, eine oder mehrere andere Stellen damit beauftragen. Soweit baden-württembergische öffentliche Stellen als verantwortliche Stellen an der Verarbeitung personenbezogener Daten beteiligt sind, müssen sie in einem solchen Fall schriftliche Aufträge dazu erteilen.

– Spielräume für datenschutzfreundliche Lösungen nutzen

  Die zur Umsetzung der Dienstleistungsrichtlinie noch notwendigen rechtlichen und technisch-organisatorischen Vorarbeiten bieten gegenwärtig noch erhebliche Spielräume für die konkrete Ausgestaltung, die möglichst datenschutzfreundlich genutzt werden sollten. Dabei sollte auch dann, wenn IuK-Systeme zur Umsetzung der

Dienstleistungsrichtlinie eingeführt werden, eine zuständigkeitsbezogene „informationelle Gewaltenteilung“ der daran angeschlossenen Behörden insofern erhalten bleiben, als jede Stelle damit nur diejenigen Daten verarbeiten kann, die sie zur Erfüllung ihrer Aufgaben benötigt. Insbesondere im Hinblick auf die Konkretisierung der Rechtsvorschriften über die einheitlichen Ansprechpartner wird dabei von Anfang an darauf zu achten sein, dass diese keinen unbeschränkten Zugriff auf verschiedenste Fachverfahren und die darin gespeicherten personenbezogenen Daten erhalten. Eine Realisierungsvariante ist dabei datenschutzrechtlich umso problematischer, je umfassender die vorgesehenen Zugriffsmöglichkeiten sind.

Geleitet vom Grundsatz der Datensparsamkeit könnten folgende Punkte zu einer datenschutzfreundlichen Technikgestaltung beitragen:

- Beschränkung auf die zur Nachrichtenübertragung erforderlichen Funktionen anstreben

  Die zur Umsetzung der Dienstleistungsrichtlinie einzurichtenden IuK-Systeme müssen in jedem Fall ermöglichen, dass elektronische Anträge wahlweise bei den einheitlichen Ansprechpartnern oder direkt bei den zuständigen Fachbehörden gestellt und auch elektronisch beantwortet werden können. Mit anderen Worten: Sie werden eine IuK-Infrastruktur bilden, die den Austausch von Mitteilungen zwischen Bürgern, Unternehmen und öffentlichen Stellen ermöglicht. Dabei stellt sich die Frage, ob man sich bei der Gestaltung der IuK-Systeme hierauf beschränken kann oder ob möglicherweise auch Funktionen eines Informationssystems in die europaweiten IuK-Systeme aufgenommen werden müssen, über die sich personenbezogene Daten der Antragsteller oder anderer Personen auch nach Übertragung der Nachrichten noch abrufen lassen. Aus Sicht des Datenschutzes wäre es sehr zu begrüßen, wenn in den europaweit nutzbaren IuK-Systemen auf eine über die Dauer des Nachrichtentransports hinausgehende Speicherung personenbezogener Daten verzichtet werden könnte. Dadurch ließen sich die vielfältigen, mit einer solchen Informationssystem-Lösung verbundenen datenschutzrechtlichen Fragen und Probleme vermeiden, die beispielsweise bei der Festlegung des Kreises der zugriffsberechtigten Personen, der Realisierung einer passgenauen Zugriffsbeschränkung oder der Gewährleistung der rechtzeitigen Löschung auftreten können.

  Soweit ein einheitlicher Ansprechpartner oder eine andere in die Abwicklung der Verwaltungsverfahren eingebundene Stelle einzelne der übertragenen personenbezogenen Daten für eine gewisse Zeit benötigt (z. B. Informationen über Posteingang, Weiterleitung, bestehende Fristen und Erledigung der elektronisch zugegangenen Anträge), könnten diese in deren lokalen IuK-Systemen gespeichert und verarbeitet werden. Entscheidend wäre dabei jedoch, dass diese Daten einer dienststellenübergreifenden, möglicherweise sogar europaweiten Zugriffsmöglichkeit entzogen werden können.

- Flexible Nutzung vordefinierter Mitteilungen ermöglichen

  Hinsichtlich des Mitteilungs-Austauschs zielen einige Vorschläge darauf, nicht nur den Austausch beliebiger frei formulierter Nachrichten zu ermöglichen, was ja heute schon per E-Mail möglich ist, sondern ein System zur strukturierten Datenkommunikation einzurichten. Dazu könnten etwa Möglichkeiten zum Austausch standardisierter und in allen Sprachen der Mitgliedstaaten vorformulierter Mitteilungen geboten werden.

  Aus Sicht des Datenschutzes könnte es dabei Probleme geben, wenn die durch die Programmentwicklung festgelegten und als einzige zur Auswahl stehenden Mitteilungen mehr personenbezogene Daten umfassten, als dies im konkreten Einzelfall notwendig ist. Diese Probleme können sich insbesondere dann ergeben, wenn nicht die datenschutzrechtlich verantwortlichen Stellen über die

Programmentwicklung und -gestaltung entscheiden. Um dem entgegenzuwirken, muss – auch wenn bereits durch die Verfahrensentwicklung bestimmte Standardmitteilungen vordefiniert werden – stets die Möglichkeit bestehen, diese Mitteilungen nach dem für die jeweilige verantwortliche Stelle geltenden Datenschutzrecht zu konfigurieren (datenschutzkonformes Customizing). Beispielsweise sollte bei standardisierten Mitteilungen, die personenbezogene Daten umfassen, konfigurierbar sein, welche der darin enthaltenen Datenfelder eine Stelle belegen darf und welche sie, z. B. mangels Erforderlichkeit der Übermittlung, leer lassen muss. Auf Pflichtfelder sollte dabei so weit wie möglich verzichtet werden.

Zu bedenken ist auch, dass eine hiesige Stelle auf Anfragen ausländischer Stellen etwa nach den Qualifikationen eines hierzulande ausgebildeten Bürgers den in unterschiedlichen Mitgliedsländern angesiedelten Behörden u. U. auch dann unterschiedliche Daten mitteilen muss, wenn es in allen Fällen um die gleiche Dienstleistung geht. Dies kann etwa dann notwendig sein, wenn die anfragenden ausländischen Behörden über einen unterschiedlichen Aufgabenzuschnitt verfügen. Aber auch dann muss durch technische oder organisatorische Maßnahmen sichergestellt werden, dass jede anfragende Stelle nur diejenigen Informationen erhält, die sie zur Erfüllung ihrer Aufgaben benötigt.

- Beschränkung der Zugriffsmöglichkeiten der einheitlichen Ansprechpartner

  Zur notwendigen Beschränkung der Zugriffsmöglichkeiten der einheitlichen Ansprechpartner könnte entscheidend beitragen, wenn es gelänge, deren Aufgaben und die darauf abgestimmten Zugriffsmöglichkeiten so zu gestalten, dass sie sich nicht mit der inhaltlichen Bearbeitung der ihnen zugehenden Anträge befassen müssen, sondern sich darauf beschränken können, die einzelnen bei ihnen eingehenden Anträge zur inhaltlichen Bearbeitung an die jeweils dafür zuständige Fachbehörde weiterzuleiten.

  So könnte es unter Umständen genügen, wenn die einzurichtenden IuK-Systeme im Wesentlichen folgende Abläufe unterstützen: Die bei einem einheitlichen Ansprechpartner eingehenden Anträge von Dienstleistern werden von ihm an die fachlich zuständigen Stellen weitergeleitet. Der einheitliche Ansprechpartner erhält irgendwann Mitteilungen der fachlich zuständigen Stellen zurück und kontrolliert, ob alle zu beteiligenden Stellen ihre Beurteilung abgeschlossen haben oder ob es im Ablauf irgendwelche Störungen gab. Er achtet auf die Einhaltung der Fristen und wendet sich bei Bedarf an einzelne von ihm eingebundene zuständige Stellen und mahnt dort noch ausstehende Beurteilungen an. Sobald alle beteiligten Stellen dem einheitlichen Ansprechpartner das Ergebnis ihrer inhaltlichen Prüfung mitgeteilt haben, erzeugt dieser hieraus die an den Antragsteller zu sendende Antwort und leitet diese dem Antragsteller elektronisch zu.

  Damit ließen sich die datenschutzrechtlichen Probleme vermeiden, die sich ergäben, wenn man die einheitlichen Ansprechpartner auch in die inhaltliche Bearbeitung der eingehenden Anträge einbeziehen würde. Insbesondere dürfte sich dadurch vermeiden lassen, den einheitlichen Ansprechpartnern Zugriffsmöglichkeiten auf personenbezogene Daten einzuräumen, die die Fachbehörden in ihren Fachanwendungen verarbeiten.

- Zuverlässige Verfahren für die Authentifizierung der Antragsteller und für elektronische Signaturen einsetzen

  Die von der Dienstleistungsrichtlinie geforderte Möglichkeit, alle Formalitäten aus der Ferne elektronisch abwickeln zu können, erfordert, dass die Identität der Antragsteller auch dabei zuverlässig überprüft werden kann. Zudem kann es notwendig sein, wesentliche Mitteilungen, wie z. B. Anträge, elektronisch zu signieren,

um damit zu dokumentieren, dass der Unterzeichner die übersandte Erklärung tatsächlich hat abgeben wollen. Leider enthält die Dienstleistungsrichtlinie keinerlei Vorgaben dazu, auf welche Weise dies zu geschehen hat. Aus Sicht des Datenschutzes gilt es, diesen Anforderungen hohe Aufmerksamkeit zu schenken. Hochwertige Verfahren für Signaturen stehen beispielsweise mit der qualifizierten elektronischen Signatur zur Verfügung. Allerdings sind diese bislang noch nicht flächendeckend im Einsatz. Angesichts dessen ist davor zu warnen, „Übergangslösungen" vorzusehen, die mit deutlichen Einbußen gegenüber dem erreichbaren Sicherheitsniveau verbunden sind.

Ich habe das in Baden-Württemberg für die Umsetzung der Dienstleistungsrichtlinie verantwortliche Wirtschaftsministerium sowie das für die IT-Umsetzung federführende Innenministerium gebeten, diese datenschutzrechtlichen Aspekte bei den weiteren Plänen zur Umsetzung der EU-Dienstleistungsrichtlinie zu berücksichtigen.

3. Der Dokumentensafe für das Verwaltungsdiensteportal service-bw

Um Bürgern und Unternehmen eine zentrale Anlaufstelle im Internet zu bieten, hat das Land Baden-Württemberg bereits vor Jahren das Verwaltungsdiensteportal service-bw (www.service-bw.de) eingerichtet und seither mehrfach erweitert. Dort kann man sich über die von der Verwaltung angebotenen Dienstleistungen informieren und diese in immer mehr Fällen auch gleich elektronisch abwickeln. Aktuell steht die Bereitstellung eines sog. Dokumentensafes im Mittelpunkt.

Mit dem Dokumentensafe will die Verwaltung allen Bürgern die Möglichkeit zur individuellen Nutzung einer elektronischen Ablage bieten. Gedacht ist dabei in erster Linie daran, dass die Nutzer darin Dokumente ablegen können, die sie für spätere elektronische Antragstellungen benötigen. Daneben soll der Dokumentensafe auch ein elektronisches Postfach für die Bürger darstellen, in das die für sie bestimmten, elektronisch erstellten amtlichen Mitteilungen und Bescheide abgelegt werden können. Dabei ist damit zu rechnen, dass im Dokumentensafe auch Unterlagen mit besonders schutzbedürftigen personenbezogenen Angaben, z. B. Einkommensnachweise oder Steuerbescheide, aufbewahrt werden. Es liegt auf der Hand, dass ein solches System eine Vielzahl datenschutzrechtlicher Fragen aufwirft, etwa:

- Wer soll unter welchen Bedingungen auf die in einem Dokumentensafe abgelegten Daten zugreifen dürfen?
- Wie ist sichergestellt, dass Unberechtigte nicht auf die Dokumente zugreifen können?
- Wie geht man damit um, wenn Bürger dieses Angebot nicht in Anspruch nehmen wollen?

Dazu teilte uns das für dieses Vorhaben federführende Innenministerium mit, dass die Nutzung des Dokumentensafes freiwillig sei und alle im Dokumentensafe gespeicherten personenbezogenen Daten durch Verschlüsselung vor unberechtigter Kenntnisnahme geschützt werden sollen. Um unberechtigte Zugriffe auf die im Dokumentensafe abgelegten Daten so weit wie möglich auszuschließen, solle die Anmeldung zum Dokumentensafe nur für solche Nutzer ermöglicht werden, die sich eine u. a. auch für die digitale Signatur nutzbare Chipkarte haben ausstellen lassen und die sich mit Hilfe dieser Chipkarte am Portal anmelden. Da die Entschlüsselung der in ihrem Dokumentensafe abgelegten Daten nur mit Hilfe eines auf dieser Chipkarte gespeicherten Schlüssels möglich sei, hält das federführende Innenministerium den Schutz vor unberechtigten Zugriffen für gewährleistet.

Diese Eckpunkte stellen auch aus Sicht des Datenschutzes wichtige Ziele dar, an denen keine Abstriche gemacht werden sollten. Gleichwohl ist darauf hinzuweisen, dass sich auch bei Umsetzung der vom Innenministerium vorgesehenen Konzeption eine unberechtigte Kenntnisnahme der im Doku-

mentensafe hinterlegten Daten technisch nicht vollständig ausschließen lässt. So sieht beispielsweise das Konzept des Innenministeriums vor, dass ein Bürger die Dokumente, die er einem elektronischen Antrag beifügen möchte, vor deren Verwendung entschlüsselt. Somit befinden sich einzelne Dokumente zumindest für einen kurzen, zur Antragstellung genutzten Zeitraum unverschlüsselt im Dokumentensafe. In dieser Zeit ist der Schutz dieser Dokumente vor unberechtigten Zugriffen entsprechend eingeschränkt.

Wir halten es deshalb für erforderlich, dass die Nutzung des Dokumentensafes nur auf freiwilliger Basis erfolgt und die Bürger umfassend über die ergriffenen Sicherheitsmaßnahmen und deren Grenzen unterrichtet werden. Zudem ist wichtig, dass die hierzu stets notwendigen Einwilligungen klar erkenntlich und unmissverständlich eingeholt werden. Leider waren in der Konzeption zur Nutzung des Dokumentensafes zunächst nur unzureichende Anforderungen daran gestellt, wie die Einwilligungen zu erklären seien: So sollte die Einwilligung zum Teil einfach durch die Nutzung einzelner Funktionen oder das Ausfüllen bestimmter elektronischer Formulare gegeben werden. Im Konzept des Innenministeriums war in dem Zusammenhang auch von „impliziter Einwilligung“ die Rede. Wir wiesen das Innenministerium darauf hin, dass eine wirksame Einwilligung nach den Anforderungen des Landesdatenschutzgesetzes zwar durchaus auch in elektronischer Form erteilt werden kann; dabei muss aber u. a. sichergestellt werden, dass die Einwilligung nur durch eine eindeutige und bewusste Handlung des Einwilligenden erfolgen kann. Eine implizite oder konkludente elektronische Einwilligung, die das Innenministerium ursprünglich für ausreichend hielt, wird daher den datenschutzrechtlichen Anforderungen nicht gerecht. Das Innenministerium hat die Konzeption mittlerweile unseren Hinweisen entsprechend angepasst.

Neben den Unzulänglichkeiten hinsichtlich der Form wies die Konzeption auch Unzulänglichkeiten hinsichtlich des Inhalts der darin vorgesehenen Einwilligungen auf. Sie sah vor, dass sich die Nutzer per Einwilligung auch mit einer unverschlüsselten Übertragung ihrer Daten einverstanden erklären können. Schon allein weil den Nutzern regelmäßig viel weniger Informationen zur Beurteilung der tatsächlich vorhandenen Gefährdungen zur Verfügung stehen dürften als den Daten verarbeitenden Stellen, wäre es nicht sachgerecht, ihnen die Verantwortung für die in einem sehr komplexen und für Außenstehende kaum durchschaubaren IuK-System zu ergreifenden Datenschutzmaßnahmen auferlegen zu wollen. Aus diesem Grund sieht es das Landesdatenschutzgesetz auch nicht vor, dass sich eine Daten verarbeitende öffentliche Stelle per Einwilligung von ihrer gesetzlichen Verpflichtung zur Realisierung der erforderlichen Schutzmaßnahmen, zu denen vielfach auch die Verschlüsselung elektronisch übertragener Daten gehören dürfte, entbinden lassen kann.

Zudem gab es in diesem Jahr Anlass zu Zweifeln, ob das Innenministerium uneingeschränkt weiterhin an dem Grundsatz der Freiwilligkeit der Nutzung des Dokumentensafes festhalten will. Entgegen unserer Bitte beschlossen die im Arbeitskreis Informationstechnik zusammenwirkenden Vertreter der Landesministerien auf Vorschlag des Innenministeriums im Frühjahr, dass der Dokumentensafe künftig zur „einheitlichen und verbindlichen Nutzung“ zur Verfügung gestellt werden soll. Noch deutlicher wurde das Innenministerium vor wenigen Wochen, als es in einem Arbeitspapier darauf hinwies, dass das Angebot von Portalfunktionen wie dem Dokumentensafe eine hoheitliche Aufgabe sei. Es führte dazu u. a. aus:

> „Bürgerinnen und Bürger sind in zunehmendem Maße den Sicherheitsrisiken des Internet ausgesetzt; dies umso mehr, je öfter sie im virtuellen Raum aktiv sind. Die wachsende Bedeutung der elektronischen Kommunikation für Wirtschaft, Verwaltung und Gesellschaft stellt deshalb den modernen Staat vor die Aufgabe, im elektronischen Kommunikationsraum ähnliche hoheitliche Funktionen wie im natürlichen Raum zu übernehmen und dort für Sicherheit, Ordnung und Rechtsverbindlichkeit zu sorgen. In diesem Sinne verhelfen ‚mein service-bw‘ und der Dokumentensafe – künftig besonders in Kombination mit der elektronischen Authentifizierungsfunktion des neuen deutschen Personalausweises – dazu, den Bürgerinnen und Bürgern im elektronischen Raum eine Identität zu

geben, die von diesen gleichermaßen und einheitlich den Online-Verfahren der Verwaltung und der Privatwirtschaft zur Verfügung gestellt werden kann."

Im Zusammenhang mit dem zuvor erwähnten Beschluss des Arbeitskreises Informationstechnik sahen wir hierin Anzeichen für eine Abkehr von dem Modell der freiwilligen Nutzung des Dokumentensafes. Wir wiesen das Innenministerium darauf hin, dass sich in diesem Fall die Verarbeitung personenbezogener Daten kaum mehr allein auf eine Einwilligung stützen ließe. Es wäre daher zu klären, welche staatlichen Stellen künftig auf der Grundlage welcher rechtlicher Vorschriften welche mit einer Verarbeitung personenbezogener Daten verbundenen hoheitlichen Aufgaben im virtuellen Raum übernehmen sollen. Klärungsbedürftig wäre ferner, welche Portalkomponenten für welche Personenkreise zur verbindlichen Nutzung vorgesehen werden sollen und aus welchen Rechtsvorschriften sich künftig die Nutzungspflicht ergeben soll. Eine Antwort des Innenministeriums auf meine dementsprechende Anfrage steht bislang noch aus.

4. Protokollierung von Zugriffen auf Internet-Angebote

Eine datenschutzrechtlich problematische Begleiterscheinung der zunehmenden Nutzung elektronischer Dienstleistungen besteht darin, dass sich Vorgänge, die in der realen Welt ganz selbstverständlich anonym abgewickelt werden können, in der elektronischen Welt vielfach aber nicht ohne weiteres anonym abwickeln lassen. Diese Problematik zeigt sich bereits, wenn man den Umgang mit gedruckten Broschüren dem Zugriff auf Internet-Angebote gegenüberstellt. Insbesondere die Anbieter und Betreiber elektronischer Angebote gehen nicht selten mit einer großen Selbstverständlichkeit davon aus, dass dabei sämtliche Nutzeraktionen detailliert protokolliert und einer späteren Auswertung zugänglich gemacht werden können. Und das, obwohl seit langem Anlass besteht, sorgsam darauf zu achten, dass Dinge, die in der realen Welt anonym erledigt werden können, auch in der elektronischen Welt anonym zu erledigen sind. Denn bereits vor mehr als zehn Jahren sorgten Bund und Länder dafür, dass strenge gesetzliche Regeln für den Umgang mit elektronischen Informationsdiensten und deren Nutzungsspuren aufgestellt wurden.

Ruft jemand eine Web-Seite auf, so bieten die dazu verwendeten Server standardmäßig die Möglichkeit, eine Reihe von Informationen über die einzelnen Zugriffe zu registrieren. Dabei können neben Datum und Uhrzeit des Zugriffs auch die IP-Adresse des abrufenden Computers sowie eine Reihe weiterer Informationen dokumentiert werden. Dazu gehören etwa eine nähere Beschreibung des Zugriffsmodus, die Bezeichnung des Dokuments, auf das zugegriffen wurde, sowie Angaben über das Betriebssystem und den Browser, die auf dem Computer des zugreifenden Internet-Nutzers verwendet werden. Schließlich kann auch der sog. Referrer erfasst werden, also die Bezeichnung derjenigen Web-Seite, von der aus die aktuell besuchte Web-Seite durch Anklicken eines Links aufgerufen wurde. Der Referrer-Eintrag kann insbesondere dann besonders aussagekräftig sein, wenn der Internet-Nutzer über eine Suchmaschine auf das aktuell besuchte Internet-Angebot gelangt ist. In diesem Fall können auch dieser Umstand sowie sämtliche vom Internet-Nutzer zur Suche verwendeten Suchbegriffe im Referrer-Eintrag der Protokolldatei festgehalten werden.

Datenschutzrechtlich ist dabei insbesondere von Bedeutung, dass IP-Adressen mit Hilfe von Zusatzwissen einzelnen Personen zugeordnet werden können und die Protokolldaten somit als personenbezogen anzusehen sind. Dies stellte auch ein wesentliches Argument für das Amtsgericht Berlin Mitte dar, das dem Bundesjustizministerium im März dieses Jahres untersagte, mit vollständigen IP-Adressen versehene Protokolldaten über den Zugriff auf dessen Internet-Angebot über das Ende der einzelnen Nutzung hinaus zu speichern. Dabei stellte es ausdrücklich klar, dass dies auch dann gelte, wenn es sich um IP-Adressen handelt, die den Nutzern von ihren Internet-Zugangs-Providern jeweils nur für eine gewisse Zeit bereitgestellt wurden (dynamische IP-Adressen).

Dass gemessen daran auch hierzulande noch einiger Änderungsbedarf besteht, ergibt sich aus der Antwort des Innenministeriums auf eine im Landtag eingebrachte Kleine Anfrage zur Speicherung von Kommunikationsspuren (LT-Drucksache 14/1830). Danach gibt es neben einigen behördlichen Web-Angeboten, bei deren Nutzung keine der in Rede stehenden Daten protokolliert werden, auch Angebote, bei deren Nutzung Protokolldaten inklusive vollständiger IP-Adresse bis zu 13 Monate oder bei einzelnen Angeboten sogar unbefristet gespeichert werden. Dies macht deutlich, dass noch erhebliche Diskrepanzen zwischen dem erwähnten Urteil des Amtsgerichts Berlin Mitte und der aktuellen Praxis der Landesverwaltung bestehen. Demgegenüber äußerte sich das Innenministerium in seiner Antwort ausweichend und teilte mit, dass „kein unmittelbarer Handlungsbedarf" bestehe. Dies gelang ihm allerdings nur, indem es konsequent vermied, das in der Sache einschlägige Amtsgerichtsurteil anzusprechen, und sich stattdessen nur auf das Urteil des Landgerichts Berlin bezog, das sich allerdings nur mit Teilaspekten des Amtsgerichtsurteils befasste. Dabei ist klar, dass das Urteil des Berliner Amtsgerichts selbstverständlich keine rechtliche Bindungswirkung für das Land Baden-Württemberg entfalten kann, da dieses nicht Prozesspartei war. Gleichwohl empfiehlt es sich, die Verwaltungspraxis im Land an den Maßstäben der amtsgerichtlichen Erkenntnisse zu überprüfen.

Ich habe daher die im Arbeitskreis Informationstechnik zusammenwirkenden IuK-Verantwortlichen der Landesverwaltung gebeten, die Vorgehensweise bei der Protokollierung der Zugriffe auf die von ihnen betriebenen Internet-Angebote zu überprüfen und dafür Sorge zu tragen, dass dabei den Anforderungen des Datenschutzrechts, insbesondere den für Internet-Angebote einschlägigen Spezialvorschriften des Telemediengesetzes, Rechnung getragen wird. Zudem habe ich darauf hingewiesen, dass öffentliche Stellen des Landes auch dann für die Einhaltung der Datenschutzvorschriften verantwortlich bleiben, wenn sie ihre Internet-Angebote nicht auf eigenen Servern bereithalten, sondern Dritte (Provider) damit beauftragt haben. Das Innenministerium reagierte hierauf rasch und teilte mit, dass es gemeinsam mit dem von ihm beauftragten Provider eine Lösung anstrebe, bei der die bislang protokollierten IP-Adressen durch nicht-personenbezogene Daten ersetzt werden. Über das weitere, möglicherweise landesweit abgestimmte Vorgehen soll demnächst auch der Arbeitskreis Informationstechnik beraten. Es ist zu hoffen, dass sich dabei zeitnah und landesweit eine datenschutzgerechte Lösung erreichen lässt.

5. Das CERT der Landesverwaltung

Die Sicherheit eines Daten verarbeitenden Systems ist unabdingbare Grundvoraussetzung für einen datenschutzrechtlich zulässigen Betrieb. Insofern begrüße ich alle Anstrengungen der Landesverwaltung, durch geeignete Maßnahmen die Sicherheit der eingesetzten Hard- und Software zu erhöhen. Deshalb waren meine Mitarbeiter und ich auch gespannt darauf, ob und inwieweit sich die Systemsicherheit der EDV der Landesverwaltung verbessert hat, nachdem ein sog. CERT für die Landesverwaltung am 20. November 2006 seinen Betrieb aufgenommen hatte.

Hinter „CERT" verbergen sich die englischen Begriffe computer emergency response team. Das erste CERT wurde Ende der achtziger Jahre des vergangenen Jahrhunderts an einer amerikanischen Elite-Universität gegründet, um Sicherheitsprobleme des Internets zu identifizieren, zu lösen und Anwender bei deren Bewältigung zu unterstützen. Das erste deutsche CERT ist ebenfalls im Hochschulbereich eingerichtet worden.

Seit einigen Jahren sprießen CERTs an allen Ecken und Enden der EDV-Landschaft wie Pilze aus dem Boden. Da wollte anscheinend auch die Landesverwaltung nicht zurückstehen und beschloss, ein CERT BWL beim Informatikzentrum Landesverwaltung Baden-Württemberg (IZLBW) einzurichten. Das ist aber beileibe nicht das einzige CERT im Land. Uns sind eine Universität (seit 1998) und ein kommunaler Informationsverband in Baden-Württemberg bekannt, die ebenfalls ein CERT betreiben.

Interessanterweise kommt diese inflationäre CERT-Gründungsphase zu einem Zeitpunkt, in dem im EDV-Bereich eine Konsolidierung auf wenige

Hard- und Softwaresysteme stattgefunden hat, sodass sich die Frage stellt, warum ein einziges deutsches CERT nicht genügt. Über neunzig Prozent aller Rechner werden mit einem Betriebssystem der Firma Microsoft ausgeliefert. Der Marktanteil bei Bürosoftware des Unternehmens dürfte sich in der gleichen Größenordnung bewegen. In der Landesverwaltung ist diese Ausstattung Landesstandard und wird auf nahezu allen Arbeitsplatz-PCs installiert. Bei der Beseitigung von Sicherheitslücken ist die Landesverwaltung wie alle anderen Nutzer auf die Versorgung mit sog. Hotfixes, Updates und Service Packs von Microsoft angewiesen. Welche Rolle einem CERT in dieser Gemengelage zukommen könnte, ist nicht klar. Unter diesem Blickwinkel stellt sich die Frage, was das CERT der Landesverwaltung besser machen will und warum man erst mehr als sieben Jahre nach der ersten Gründung eines CERT an einer baden-württembergischen Universität die Notwendigkeit eines CERT für die Landesverwaltung sieht.

Die Aktivitäten des CERT BWL bestanden nach unserem Eindruck bisher hauptsächlich im Versand von Sicherheitsinformationen. Wenn man sich die Meldungen, von denen meistens mehrere täglich per E-Mail eingehen, genauer anschaut, fallen Ungereimtheiten auf, die den Wert dieser Informationen eher fragwürdig erscheinen lassen. Hier nur wenige Beispiele:

- Mit wenigen Ausnahmen kommen alle „Sicherheitsinfos“ des CERT BWL vom CERT-Bund. Vom CERT BWL werden die Meldungen „umkuvertiert“ und an Empfänger in der Landesverwaltung weitergesandt. Aber auch das scheint nicht fehlerfrei zu funktionieren. Bei vielen Meldungen bestehen die Einleitungen aus dem Meldungstext „Sicherheitsinfo des CERT BWL zum Themenbereich HP-Unix/Linux“. Bei den betroffenen Plattformen werden dann aus unerklärlichen Gründen die Betriebssysteme „Windows Vista“ und „Microsoft Windows XP“ genannt. Wenigstens so ausgereift sollte der regelbasierte Weiterleitungsmechanismus schon sein, dass die Sicherheitsverantwortlichen nicht auf die falsche Fährte gelockt werden.
- Vollkommen im Dunkeln tappt man angesichts einer Sicherheitsinformation, die das Programm „Adobe Acrobat Reader“ betraf. Lapidar wurde erklärt, dass eine Schwachstelle in dem Programm die Ausführung beliebiger Codes erlaube. Angaben zu der betroffenen Programmversion fehlten. Wenig beruhigend ist auch der Hinweis, dass zurzeit noch kein sog. Hotfix zur Behebung der Schwachstelle vorhanden und sehr wenig Informationen über die Schwachstelle veröffentlicht worden seien. Die Empfehlung, keine PDF-Dokumente aus unsicheren bzw. unbekannten Quellen zu öffnen, erscheint angesichts des Verbreitungsgrads von PDF-Dokumenten etwas praxisfern.
- Die Einleitung einer anderen Meldung lautete „Sicherheitsinfo des CERT BWL zum Themenbereich HP-Unix/Linux“ und setzte dann im vom Bund übernommenen Teil fort mit dem Text „Mehrere Schwachstellen in IBM AIX ermöglichen die Ausführung von Programmcode mit administrativen Rechten“. Ähnliche Meldungen gibt es auch zum Betriebssystem Solaris und Mac OS X. Auch das deutet darauf hin, dass hinsichtlich des Weiterleitungsmechanismus Verbesserungsmöglichkeiten bestehen.
- Ein Mangel an Genauigkeit ist bei der Meldung „Schwachstelle im ‚QuickTime-Plugin’“ zu vermuten. Heißt es darin doch schlicht, dass ein fehlerhaftes QuickTime-Plugin einem Angreifer in verschiedenen Browsern beliebige Codeausführungen erlaube. Wie ein Administrator an Hand dieser Angaben feststellen soll, ob die von ihm betreuten PCs betroffen sind, ist nicht erkennbar.
- Um einen Fehlalarm dürfte es sich bei der Sicherheitsinfo des CERT BWL zum Themenbereich Windows/Microsoft und zum Programm xpdf handeln. In der Rubrik der betroffenen Plattformen werden die Betriebssysteme Linux und Windows genannt. Bei der Nennung von Windows dürfte es sich um einen Irrtum handeln. Xpdf als reinrassige XWindow-Anwendung läuft nicht mit den Betriebssystemen von Microsoft.
- Einen interessanten Aspekt kann man den Sicherheitsinfos schließlich doch abgewinnen. Es ist erstaunlich, wie häufig Software, die der Ge-

währleistung der Systemsicherheit dienen soll, Gegenstand von Sicherheitsinfos ist. Die Palette reicht von Virenschutzsoftware über Firewalls bis zu Verschlüsselungssoftware. Wer vermutet hat, dass Software, die Rechner und darauf gespeicherte Daten vor Angriffen schützen soll, gegen Sicherheitslücken gefeit ist, wird angesichts der Sicherheitsinfos unsanft eines Besseren belehrt.

Auch zwei selbstverfasste Sicherheitsmeldungen konnten mich von einer nachhaltigen Wirkung des CERT BWL nicht überzeugen. Zum einen wurde davor gewarnt, unbedarft auf HTML-Links in E-Mails zu klicken. Wenn man sich nicht sicher sei, solle man an Hand des Quelltexts prüfen, zu welchem WWW-Server der Link zweige. Die Absicht ist löblich, verkennt aber, dass die wenigsten Mitarbeiter der Landesverwaltung Spezialisten im Lesen von HTML-Code sind. Auch die Warnung, sich nicht als Finanzagent anwerben zu lassen, ist gut gemeint und kann vielleicht den einen oder anderen vor Unbill bewahren. Nicht erkennbar ist jedoch, dass dadurch die Sicherheit der EDV-Systeme der Landesverwaltung erhöht würde.

Zusammenfassend muss festgestellt werden, dass etliche Sicherheitsinfos Sicherheitslücken betreffen, die über den Status einer Machbarkeitsdemonstration noch nicht hinausgekommen sind. Trotzdem ist der Druck auf die für die Sicherheit der EDV-Umgebung Verantwortlichen groß, die Meldungen hinsichtlich der von ihnen betreuten EDV-Umgebung prüfen zu müssen. Fraglich ist, ob dann genügend Zeit verbleibt, zur Abwehr der tatsächlichen Gefahren geeignete Gegenmaßnahmen einzuleiten und sorgfältig durchzuführen. Hier könnte das CERT BWL eine Filterfunktion einnehmen.

Weitere Gebiete, auf denen das CERT BWL Wirkung entfalten könnte, sind naheliegend. So sollten die spezifischen Belange der EDV der Landesverwaltung deutlich herausgearbeitet und ein maßgeschneidertes Konzept erarbeitet werden. Beispielsweise könnte endlich der auch von uns angeregte Aufbau und Betrieb eines für alle Dienststellen des Landes zugreifbaren Windows Software Update Service an zentraler Stelle in Angriff genommen werden. Der Aufbau einer Sicherheitsinfrastruktur ist eine grundlegende Voraussetzung zur Erhöhung der Sicherheit der in der Landesverwaltung eingesetzten Systeme. Bei selbst erstellten verwaltungsspezifischen Anwendungen könnte Kompetenz eingebracht und dadurch proaktiv schon bei der Programmierung auf die Erhöhung der Sicherheit Einfluss genommen werden.

Zunächst ist aber das vorläufige Fazit zu ziehen, dass eine nennenswerte Erhöhung der Sicherheit der EDV-Systeme der Landesverwaltung durch die Schaffung eines CERT BWL wohl noch nicht eingetreten ist.

6. Das Antragsverfahren für den ePass

Wenn es nach den Aussagen der Sicherheitspolitiker geht, sind wir am Ziel – vorläufig jedenfalls. Endlich bekommen wir Reisepässe, die uns höchste Sicherheit garantieren. Wurde auf dem RFID-Chip der Reisepässe bisher das Gesichtsbild des Passinhabers gespeichert, so kommen seit dem 1. November 2007 zusätzlich Fingerabdrücke hinzu.

Weil die Erhebung, Verarbeitung und Übermittlung so sensibler biometrischer Daten im öffentlichen Bereich neu ist, wurde vom 1. März 2007 bis zum 30. Juni 2007 ein bundesweiter Testlauf des Passantragsverfahrens durchgeführt, in dem die Eignung von Soft- und Hardware sowie die Anforderungen an die organisatorischen Randbedingungen geprüft werden sollten. In Baden-Württemberg wurden durch Verordnung zwei Städte berechtigt, für die Dauer des Tests zwei Fingerabdrücke von Passantragstellern zu erheben, zu verarbeiten und an den Passaussteller zu übermitteln, sofern die Betroffenen in die Verarbeitung einwilligten. Auf den Chips der Reisepässe dieser Passantragsteller wurden die Fingerabdrücke nicht gespeichert. Um mir möglichst frühzeitig ein Bild von dem Verfahren machen zu können, hat einer meiner Mitarbeiter dem Amt für Bürgerservice einer der beteiligten Städte einen Informationsbesuch abgestattet.

Angesichts der hochsensiblen Daten und der Missbrauchsgefahr sind an die Verarbeitung biometrischer Daten naturgemäß hohe Anforderungen hin-

sichtlich der Authentizität, der Vertraulichkeit und der Integrität der Daten zu stellen. Beim Passantrag ist insbesondere wichtig, dass die Fingerabdruckdaten nach Ablauf des Antragsverfahrens nur auf dem Chip des Reisepasses und nicht andernorts gespeichert werden; daher müssen auch temporäre Speicherungen unverzüglich gelöscht werden. Auch der Datentransport an den Passaussteller (Bundesdruckerei) muss auf allen Abschnitten der Strecke hohen Sicherheitsstandards genügen.

Im Einzelnen konnten bei dem genannten Informationsbesuch folgende Erkenntnisse gewonnen werden:

– Der Testbetrieb wurde bei der Stadt am 10. April 2007 aufgenommen. Das Ende des Testbetriebs war bundesweit auf den 30. Juni 2007 datiert. Ungefähr 80 % der Antragsteller nahmen an dem Antragsverfahren mit Fingerabdruck teil, wobei der Gebührennachlass in Höhe von 5,00 EUR eine nicht unerhebliche Rolle gespielt haben soll.

– Die für die Abwicklung des Antragsverfahrens ausgerüsteten Arbeitsplätze der Stadt bestehen aus einem Fingerabdruckscanner und einem Steuerprogramm des Scanners (Treiber). Die Installation der Software muss mit Systemrechten vorgenommen werden. Mit der Installation ist der Fingerabdruckscanner fest an das auf dem PC ablaufende Steuerprogramm gebunden. Wenn man die physikalische Verbindung zwischen Fingerabdruckscanner und Rechner unterbricht, wird der Scanner von dem Steuerprogramm nicht mehr angesteuert. Die Verwendung eines anderen Anschlusses als des bei der Installation verwendeten ist ausgeschlossen. Zur Wiederinbetriebnahme muss eine Neuinstallation der Software erfolgen.

– Von einem Antragsteller konnten keine Fingerabdrücke genommen werden. Der Antragsteller wurde von dem Programm als „ohne Hand“ klassifiziert. Das Verfahren berücksichtigte nicht den seltenen, aber Hautärzten geläufigen Fall, dass von einigen Betroffenen keine verwertbaren Fingerabdrücke genommen werden können. Das Verarbeitungsprogramm sollte aus unserer Sicht umgehend nachgebessert werden.

Hinsichtlich der Sicherheit der Anbindung des Fingerabdrucksensors an den PCs schien die Sache im Lot. Die Anzeichen deuten darauf hin, dass nur mit dem Steuerprogramm Daten aus dem Fingerabdruckscanner ausgelesen werden können. Allerdings besteht das Informationssystem zur Passantragstellung aus mehreren Komponenten. Der Fingerabdruckscanner ist nur ein Glied in der Kette der an der Anwendung beteiligten Komponenten:

– Arbeitsplatz-PC

  Zwar scheint die Datenübertragung vom Fingerabdruckscanner zum PC sicher zu sein, fraglich ist aber, ob Anwendungen sich gegenüber dem Steuerprogramm identifizieren müssen oder ob beliebige Anwendungen über das Steuerprogramm auf den Fingerabdruckscanner zugreifen können. Der Anschluss des Rechners, mit dem die Fingerabdruckscanner jeweils verbunden werden, wird durch ein Teilsystem des Betriebssystems gesteuert (Treiber für USB-Schnittstelle). Für dieses Teilsystem gibt es im Internet von jedermann abrufbare Monitorprogramme, mit denen die über die Schnittstelle transportierten Daten mitgeschnitten werden könnten. Dies sollte das Steuerprogramm aber zuverlässig unterbinden.

  Die Clientanwendung namens LEWIS Digant auf dem Arbeitsplatz-PC kommuniziert mit dem Großrechner über ein Netzwerk. Hierfür ist auf der Seite des PCs ein Subsystem (TCP/IP-Stack) verantwortlich, das die Übertragung der biometrischen Daten im Intranet mit dem auch im Internet üblichen Protokoll realisiert.

  Bedauerlicherweise ist die Sicherheit jedes PCs durch Viren, Trojaner und andere Schaden stiftende Software bedroht. Zwar gibt es für diese Bedrohungen Abwehrmaßnahmen, aber es dürfte allgemein bekannt sein, dass nicht alle Angriffe damit abgewehrt bzw. die Maßnahmen nur mit einer gewissen zeitlichen Verzögerung ergriffen werden können.

– Großrechnerverfahren

  Auf der Seite des Großrechners wird für die Antragstellung ein datenbankbasiertes Verfahren eingesetzt. Die Benutzer müssen sich über das Clientprogramm am Großrechner anmelden. Die biometrischen Daten werden bis zur Aushändigung des Reisepasses in einer Datenbank gespeichert. Nach erfolgter Aushändigung werden die Daten gelöscht.

  Wir haben die Stadt darauf hingewiesen, dass von der Datenbank vermutlich in regelmäßigen Abständen Sicherungskopien auf Magnetbändern hergestellt werden. Das heißt, dass die biometrischen Daten auch nach der Aushändigung und Löschung in der Datenbank noch auf Magnetbändern gespeichert sind. Diese Speicherung muss im Hinblick auf die Verfügbarkeit und die sequentiellen Speicherstrukturen von Magnetbändern in Kauf genommen werden. Das ist nach § 23 Abs. 4 Nr. 2 LDSG datenschutzrechtlich vertretbar, weil die Löschung unterbleiben darf, wenn sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Durch organisatorische Maßnahmen sollte jedoch sichergestellt werden, dass die Bänder so beschrieben werden, dass zeitnah alle darauf gespeicherten biometrischen Daten gelöscht werden können.

– Transport der Anträge

  Die biometrischen Daten der Antragsteller werden bei der betreffenden Stadt über zwei Netzwerke transportiert. Zum einen zwischen dem Bürgerbüro der Stadt und dem Rechenzentrum des Kommunalen Informationsverbands Baden Franken (KIVBF). Hier handelt es sich um Leitungen der Stadt, die von einem städtischen Dienstleister betrieben werden. Die Übertragung der biometrischen Daten erfolgt auf diesem Abschnitt unverschlüsselt.

  Die Übertragung der Passdaten an die Bundesdruckerei geschieht über das Verwaltungsnetz TESTA. Die Daten werden hier verschlüsselt und mit einer qualifizierten elektronischen Signatur versehen. Hierfür werden der Verwaltungsstandard XPass und das Übertragungsprotokoll OSCI eingesetzt. Insbesondere mit OSCI wird die Anforderung der Verschlüsselung und Authentifizierung der Kommunikationspartner erfüllt.

  Die üblicherweise ergriffenen Maßnahmen der Verschlüsselung sollten durch Maßnahmen der Authentifizierung der Kommunikationspartner auf der gesamten Transportstrecke ergänzt werden.

– Passaussteller

  Zusätzlich sind am Antragsverfahren EDV-Systeme des Passausstellers, nämlich der Bundesdruckerei, für die unser Amt datenschutzrechtlich nicht zuständig ist, beteiligt. Auch bei der Verarbeitung der biometrischen Daten mit diesen Systemen müssen die Daten, wenn sie auf dem Chip gespeichert wurden, gelöscht werden.

Mit der beim Testbetrieb verfügbaren Dokumentation ließen sich die aufgeworfenen Fragen nicht abschließend klären. Wir haben deshalb ein Datenschutz- und Sicherheitskonzept, wie es für den Produktionsbetrieb nach § 11 Abs. 2 Nrn. 9 und 10 LDSG erforderlich ist, gefordert.

Vermutlich Ende November 2007 können die ersten Antragsteller ihre Reisepässe mit darauf gespeicherten Fingerabdruckdaten in Empfang nehmen. Allerdings, so ist zu befürchten, werden nur wenige Dienststellen mit Hilfe von Testgeräten die in RFID-Chips von Reisepässen gespeicherten Fingerabdruckdaten auslesen können. Für den Zugriff auf die Fingerabdruckdaten, so wurde zugesagt, würde ein Zugriffsschutz namens Extended Access Control (EAC) auf der Basis eines asymmetrischen Verschlüsselungsverfahrens verwendet. Hierzu solle eine sog. Public-Key-Infrastruktur für Lesegeräte aufgebaut werden. Hinsichtlich dieser Pläne ist es inzwischen aber still geworden. Es wäre ärgerlich, wenn sich herausstellen sollte, dass die versprochene Sicherheit für längere Zeit ein Wunschtraum bleibt.

Das Verfahren zur Beantragung des ePasses wurde am 1. November 2007 bundesweit in den Produktionsbetrieb übernommen. Ich beabsichtige, das Verfahren im nächsten Jahr zu kontrollieren.

7. Das Gästebuch und personenbezogene Daten

Als ein weiteres wichtiges Datum in der Berichtsperiode muss der 1. März 2007 genannt werden. An diesem Tag trat das neue Telemediengesetz (TMG) in Kraft. Es ersetzt das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG), die gleichzeitig außer Kraft traten. Dieses Bundesgesetz ist von den Behörden und sonstigen öffentlichen Stellen im Land zu beachten, die ein sog. Internet-Portal betreiben und mit dem Portal Telemedien anbieten. Gemäß § 1 Abs. 1 TMG gilt das Gesetz für alle Anbieter von Telemedien einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

Die bisher heikle Prüfung, was ein Teledienst ist, wurde in dem Gesetz dadurch gelöst, dass es als Telemedien alle elektronischen Informations- und Kommunikationsdienste bezeichnet, die nicht Telekommunikationsdienste nach dem Telekommunikationsgesetz (TKG) sind. Dass auch diese Begriffsbestimmung zukünftig Abgrenzungsprobleme aufwirft, ist zu erwarten. Es ist ohnehin fraglich, ob eine saubere begriffliche Trennung der häufig in Mischformen – bekanntestes Beispiel ist wohl die Internet-Telefonie (Voice over IP – VoIP) – auftretenden Dienste bzw. Medien gelingen kann. Außer Frage steht jedoch, dass beispielsweise sog. Internet-Shops, kommerzielle und nicht kommerzielle Internet-Spiele wie beispielsweise Second Life, Diskussionsforen, Dokumentensafes oder E-Mail-Services wie etwa der organisierte Versand eines Newsletters Telemedien sind. Aber auch ein Gästebuch innerhalb eines Internet-Portals ist ein Telemedium, wie ein Fall aus dem Berichtszeitraum kurz nach Inkrafttreten des Gesetzes zeigte:

Eine Gemeinde im Land hatte ihr Internet-Angebot aufgefrischt und dabei auch die Funktion eines elektronischen Gästebuchs realisiert. Nunmehr kann sich jeder, der über einen Zugang zum Internet verfügt, in dem Gästebuch verewigen. Dies hat eine Bürgerin der Gemeinde auch gleich gemacht und gleichzeitig darauf hingewiesen, dass in der Link-Sammlung des Internet-Portals ein Link auf eine Einrichtung der Gemeinde, in der sie mitwirkte, fehle. Eine Mitarbeiterin der Gemeinde antwortete über das Gästebuch und stellte dar, welche Voraussetzungen und Bedingungen erfüllt sein müssen, um in die Linksammlung des Internet-Portals der Gemeinde aufgenommen zu werden. Dieser Nachrichtenaustausch blieb geraume Zeit so im Gästebuch stehen. Nach Aussage der Petentin wandte sie sich nach mehreren Wochen an den Hauptamtsleiter und bat um Löschung ihres Gästebucheintrags. Dieses Anliegen wurde jedoch vom Hauptamtsleiter abgelehnt. Die Petentin sah sich in ihrem Recht auf informationelle Selbstbestimmung verletzt und schaltete uns ein.

Im vorliegenden Fall wurde die Sache durch die Anwendung alten und neuen Rechts zusätzlich verkompliziert. Die Frage, ob und wann im Rahmen von Telemedien erhobene Daten zu löschen sind, beantwortet jedenfalls das neue Telemediengesetz in § 13 Abs. 4 Nr. 1; danach hat ein Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen, dass ein Nutzer die Nutzung eines Dienstes jederzeit beenden kann. Der Anbieter muss hierfür technische oder organisatorische Vorkehrungen treffen, z. B. dadurch, dass der Nutzer im Rahmen der Telemedien durch Maus-Klick erklären kann, dass er den Dienst beenden will. Daraufhin muss der Anbieter die im Rahmen der Telemedien erhobenen personenbezogenen Daten löschen. Den nicht unwahrscheinlichen Fall, dass die personenbezogenen Daten bei einer Systemwiederherstellung nach einem Totalausfall wieder von einem Sicherungsmedium eingespielt werden, sollte die Konzeption des Dienstes berücksichtigen. Außerdem ist eindeutig geregelt, dass der Anbieter nach Beendigung der Telemedien alle angefallenen personenbezogenen Daten über den Ablauf des Zugriffs (also auch Protokollierungsdaten) löschen muss, sofern die Daten nicht für Zwecke der Abrechnung gebraucht werden. Wenn der Anbieter keine technischen Vorkehrungen zur Beendigung des Teledienstes trifft, muss er organisatorische Vorkehrungen

ergreifen. Beispielsweise muss er dem Nutzer eröffnen, mit ihm in Kontakt treten zu können. Hierzu sind innerhalb der Telemedien für den Nutzer erkennbar die E-Mail-Adresse oder eine Telefon- bzw. Telefax-Nummer anzugeben.

Im vorliegenden Fall war keine technische Vorkehrung zur Löschung der personenbezogenen Daten getroffen worden, weshalb die Petentin den Leiter des Hauptamts um Löschung ihrer Daten gebeten hatte. Auf die Frage, welche Hinderungsgründe der Löschung entgegenstehen, antwortete die Gemeinde, dass der Eintrag in das Gästebuch freiwillig vorgenommen worden sei; insbesondere habe die Petentin freiwillig ihren Vor- und Familiennamen eingetragen. Insofern sei aus Sicht der Gemeinde davon auszugehen, dass die Petentin mit der Nennung einverstanden war. Anscheinend war man bei der Gemeinde in Verkennung der Rechtslage der Auffassung, dass mit dem Eintrag in das Gästebuch die Daten in das „Eigentum“ der Gemeinde übergingen und die Petentin hinsichtlich der Verarbeitung ihrer personenbezogenen Daten keine Rechte mehr habe. Auch der Hinweis der Gemeinde auf die Löschungsregel in § 23 LDSG war nicht zielführend, denn das Landesdatenschutzgesetz ist bei Telemedien nicht einschlägig. Hierüber und über die anzuwendenden Vorschriften habe ich die Gemeinde aufgeklärt und sie gebeten, die personenbezogenen Daten der Petentin umgehend zu löschen. Das hat die Gemeinde allerdings zunächst nicht getan, sondern erklärt, die personenbezogenen Daten stünden im Zusammenhang mit dem Verwaltungshandeln der Gemeinde und könnten deshalb aus Gründen der Dokumentation nicht gelöscht werden. Dieser Auffassung war schon deshalb nicht zu folgen, weil es sich beim Telemediengesetz um Bundesrecht handelt, das Landesrecht bricht. Mit dem Hinweis, gegebenenfalls eine Beanstandung aussprechen zu müssen, habe ich die Gemeinde schließlich doch dazu bewegen können, die personenbezogenen Daten der Petentin zu löschen.

Soweit zur Beendigung eines Teledienstes durch den Nutzer. Der Anbieter selbst hat natürlich auch das Recht, die Nutzung der von ihm angebotenen Telemedien einseitig zu beenden. Da eine zeitliche Beschränkung nicht vorgegeben ist, muss er das aber nicht tun. Wer sich also in einem Gästebuch „verewigt“, muss damit rechnen, dass er dies im wahrsten Sinn des Wortes tut. Es sei denn, er wird von sich aus aktiv.

Regelmäßig weisen nicht nur Datenschützer darauf hin, dass jeder, der sich im Internet bewegt, Spuren hinterlässt. Zumindest bei Telemedien, die in Deutschland angeboten werden, haben die Nutzer ein Recht auf Löschung ihrer im Zusammenhang mit der Nutzung gespeicherten personenbezogenen Daten. Die Zahl der angebotenen Telemedien steigt nach wie vor rasant. Für jeden Nutzer wird daher eine wachsende Herausforderung darin bestehen, den Überblick zu behalten, wo personenbezogene Daten über ihn gespeichert sind. Gleichzeitig sollten die Nutzer bedenken, welche Kommunikation sie mit welchen Telemedien abwickeln. Im vorliegenden Fall wäre der Nachrichtenaustausch mit E-Mail vermutlich die datensparsamere Alternative gewesen.

8. Meldebehörden unter falschem Verdacht

Adressdaten, möglichst garniert mit weiteren personenbezogenen Daten der Betroffenen, sind ein gefundenes Fressen für Marketingspezialisten jeder Couleur. Insofern ist kaum nachvollziehbar, warum immer noch viele Bürger an in Bahnhofshallen abgehaltenen Traumauto-Lotterien teilnehmen, deren Hauptzweck weniger in einer Preisverleihung als vielmehr im Sammeln von Adressdaten besteht. Welche Auswüchse sich hierbei ergeben können, wurde uns durch den Brief einer Petentin vor Augen geführt. Sie hatte einen Brief von einer ihr unbekannten Person erhalten, in dem diese ihr Folgendes mit blumigen Worten eröffnete:

Sie sei wie sie am 30. Mai 1965 geboren. Da es ihr Wunsch sei, ihren Geburtstag mit Leuten zu feiern, die am gleichen Tag desselben Jahres wie sie geboren wurden, wolle sie eine Geburtstagsparty organisieren und habe zu diesem Zweck eine Liste mit potenziellen Teilnehmern erstellt. Sie sei sich zwar der datenschutzrechtlichen Problematik bewusst, aber die Liste habe

nur den Zweck, die Geburtstagsparty zu organisieren. Über eine Rückmeldung würde sie sich freuen.

Dem Schreiben beigelegt war eine Liste mit 40 verschiedenen Einträgen, bestehend jeweils u. a. aus Name, Vorname, Geburtsname, Geburtsdatum, Postleitzahl, Ort, Straße und Hausnummer. Die Petentin äußerte nun den Verdacht, dass es sich bei der Liste um Daten aus Melderegistern handeln könnte und bat um eine datenschutzrechtliche Prüfung.

In diesem Zusammenhang ist erklärungsbedürftig, warum eine Befragung des Absenders für uns nicht in Frage kam. Nach dem Landesdatenschutzgesetz beschränkt sich meine Kontrollzuständigkeit auf Behörden und die sonstigen öffentlichen Stellen im Land. Im Rahmen von datenschutzrechtlichen Prüfungen kann ich daher nur öffentliche Stellen anhören. Die Befragung von Privatpersonen kommt nicht in Betracht.

Mangels anderer Anhaltspunkte war die Kontrolle einer Stadt, in der einige der angeschriebenen Personen lebten, die einzige Option für eine Prüfung. Ich beauftragte deshalb zwei Mitarbeiter, bei der Stadt eine Kontrolle des Melderegisters gemäß § 28 LDSG durchzuführen; dabei wurde Folgendes festgestellt:

- Für die Verwaltung des Melderegisters nutzt die Stadt das Verfahren LEWIS. Es handelt sich hierbei um ein Großrechnerverfahren, das vom Zweckverband Kommunale Informationsverarbeitung Reutlingen/Ulm (KIRU) betrieben wird. Beim Bürgeramt der Stadt haben 23 Mitarbeiter Zugriff auf die Anwendung. Die Mitarbeiter können in der Anwendung nur auf die Daten des Melderegisters der Stadt zugreifen. Auf Daten aus Melderegistern anderer Gemeinden besteht keine Zugriffsmöglichkeit. Dies wird durch eine verfahrensinterne Berechtigungsverwaltung gewährleistet.
- Eine Aufstellung aller in der Stadt jemals gemeldeten Personen, die am 30. Mai 1965 geboren wurden, umfasste 22 Personen. Am Tag der Kontrolle waren acht Personen, die an besagtem Datum geboren wurden, in der Stadt gemeldet. Vier Einträge der Liste waren fehlerhaft oder nicht aktuell. Bei zwei Einträgen war ein falscher Geburtsname eingetragen. Eine Person hat 2005 wieder ihren Geburtsnamen angenommen; in der Liste war hingegen noch der frühere Name aufgeführt. Eine Person war 2006 innerhalb der Stadt umgezogen; die Liste enthielt hingegen noch die alte Anschrift.

Aufgrund dieser Ergebnisse kamen wir zu dem Schluss, dass die Liste nicht von Mitarbeitern des Bürgeramts der Stadt erstellt worden sein kann. Denn neben den fünf Einträgen, deren Adresse in der Stadt lag, gab es eben weitere 35 Einträge, deren Anschriften sich in anderen Gemeinden befanden. Und darauf haben die Mitarbeiter des Bürgerbüros keinen Zugriff. Ebenso deuteten die fehlerhaften Einträge darauf hin, dass die Liste nicht aus Daten des Melderegisters der Stadt generiert wurde. Eine Vielzahl sowohl historisch als auch aktuell in dieser Stadt gemeldeter Personen war in der Liste nicht aufgeführt, was ein weiteres Indiz dafür ist, dass die Datenquelle für die Liste nicht das Melderegister der Stadt war.

Da der Zweckverband KIRU das Verfahren LEWIS für viele Gemeinden als Auftragsdatenverarbeiter betreibt, konnte nicht ausgeschlossen werden, dass die Liste dort erstellt wurde. Wir haben deshalb die Stadt bei einer Kontrolle des Zweckverbands begleitet. Dabei haben sich folgende Erkenntnisse ergeben:

- Der Zweckverband KIRU betreibt das Verfahren LEWIS gemeinsam mit dem Zweckverband Kommunale Datenverarbeitung Region Stuttgart (KDRS). Die Daten sind auf einem Großrechner gespeichert, der sich in Stuttgart befindet. Der Zweckverband KDRS bietet seinerseits den Betrieb des Verfahrens den Gemeinden der Region Stuttgart an.
- Beim Zweckverband KIRU gibt es für die Anwendungsbetreuung von LEWIS 7,5 Mitarbeiterstellen. Für die Betreuung ist es fachlich erforderlich, dass die Mitarbeiter auf die Melderegister der Gemeinden zugreifen

können, die ihre Meldedaten im Auftrag bei dem Verband verarbeiten lassen. Beim Zweckverband KDRS sind drei Mitarbeiter mit dem Datenbankmanagement betraut. Im Rahmen dieser Aufgabe können sie, sofern sie über ausreichende Kenntnisse des Aufbaus der Datenbank verfügen, auf der Ebene des Datenbankmanagementsystems auf die in Melderegistern gespeicherten personenbezogenen Daten zugreifen.

– Der Abruf im Melderegister ist den Mitarbeitern des KIRU/KDRS nur hinsichtlich der Gemeinden möglich, für die sie Auftragsdatenverarbeiter sind. Daten aus Melderegistern anderer Gemeinden können die Mitarbeiter des KIRU/KDRS nicht abrufen. Das wird durch das Berechtigungssystem gewährleistet.

– Wenn ein Bürger den Wohnort wechselt, wird im Melderegister der Wegzugsgemeinde die neue Wohnung gespeichert. Insbesondere ein Eintrag in der Liste war insofern bemerkenswert. Die Person hatte früher ihren Wohnsitz in Baden-Württemberg. Bei ihrem Wegzug gab sie eine Anschrift an, die sich in einem außereuropäischen Land befand. Diese Anschrift stimmte nicht mit der in der Liste aufgeführten Anschrift überein. Die in der Liste gefundene Anschrift war im Melderegister nicht gespeichert. Daher war davon auszugehen, dass dieser Eintrag der Liste nicht aus einem Melderegister herrührt.

Zusammenfassend kamen wir zu dem Schluss, dass mit an Sicherheit grenzender Wahrscheinlichkeit Melderegister nicht als Datenquelle für die Liste in Betracht kamen. So bleibt als mutmaßlicher Urheber das eingangs genannte Phänomen: Auch im privaten Bereich verfügen Adresshändler und andere Unternehmen sowie sonstige Organisationen über umfangreiche Datensammlungen, aus denen im vorliegenden Fall vermutlich Listen von potenziellen Partygästen erstellt worden waren.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2007:

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2007

Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest so lange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.
- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.
- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleis-

ten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.
- Für Angehörige im Sinne von § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.
- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i. S. v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.
- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.
- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht – wie im Entwurf vorgesehen – auf Beweiszwecke begrenzt werden.
- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.
- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.
- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.
- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8. Juni 2007

Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2007

Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z. B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. Oktober 2007

Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht" als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von – auch unverdächtigen – Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit – jedenfalls bei der Verfolgung von Straftaten – die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z. B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2007

Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u. a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z. B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. Oktober 2007

Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können – auch wenn die Betroffenen über die Umstände informiert wurden – diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen – zusätzlich – zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u. a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2007

Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2007

GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. Oktober 2007

Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche – teilweise sensible – Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.
- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.
- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87 a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139 b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139 b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z. B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. März 2007

Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. Oktober 2007

Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürger berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen – also auch bei Versicherungs- und Arbeitsverträgen – vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

Stichwortverzeichnis

Seite

Seite

Seite