THÜRINGER LANDTAG
4. Wahlperiode

Drucksache 4/4055
17.04.2008

U n t e r r i c h t u n g

durch die Präsidentin des Landtags

Siebter Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz

Der Thüringer Landesbeauftragte für den Datenschutz hat den oben genannten Bericht mit folgendem Schreiben vom 16. April 2008 zugeleitet:

"Anliegend sende ich Ihnen den 7. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz mit der Bitte um Kenntnisnahme und zur weiteren Veranlassung.
Der Bericht wurde gemäß § 40 Abs. 4 ThürDSG abschließend im Beirat vorberaten und wird am 17. April 2008 der Öffentlichkeit im Rahmen einer Pressekonferenz vorgestellt werden."

Prof. Dr.-Ing. habil Schipanski
Präsidentin des Landtags

Hinweis der Landtagsverwaltung:
Der Tätigkeitsbericht wurde an die Mitglieder des Landtags am 28. April 2008 als Broschüre verteilt. Er kann auch in der Landtagsbibliothek, im Landtagsinformationssystem und im Internet unter der Internetadresse www.landtag. thueringen.de unter obiger Drucksachennummer eingesehen werden.
Gemäß § 52 Abs. 5 GO wurde der Bericht sowie die gemäß § 40 Abs. 2 des Thüringer Datenschutzgesetzes zu erwartende Stellungnahme der Landesregierung zum Bericht an den Innenausschuss überwiesen.

Druck: Thüringer Landtag, 29. April 2008

FREISTAAT
THÜRINGEN

7. Tätigkeitsbericht

TLfD

Der Thüringer Landesbeauftragte
für den Datenschutz

Vorbemerkung zum Sprachgebrauch

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

Impressum

Herausgeber: Der Thüringer Landesbeauftragte für den Datenschutz
Jürgen-Fuchs-Straße 1, 99096 Erfurt
Postfach 90 04 55, 99107 Erfurt
Telefon: 0361/3771900, Telefax: 0361/3771904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.thueringen.de/datenschutz

Druck: WST Werbedruck Staub GmbH
Iderhoffstraße 12, 99085 Erfurt
Telefon: 0361/59058-0
E-Mail: mail@werbedruck-staub.de

Redaktionsschluss: 31. Dezember 2007

7. Tätigkeitsbericht

des Thüringer Landesbeauftragten für den Datenschutz

Berichtszeitraum:
1. Januar 2006 bis 31. Dezember 2007

Der 7. Tätigkeitsbericht steht im Internet unter der Adresse www.thueringen.de/datenschutz zum Abruf bereit.

Erfurt, im April 2008

Harald Stauch
Der Thüringer Landesbeauftragte für den Datenschutz

Inhaltsverzeichnis

Anlagen

Entschließungen zwischen den Konferenzen 2005/2006

Entschließungen der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2006 in Magdeburg

Entschließungen der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

Entschließungen der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt

Entschließungen zwischen den Konferenzen 2007

Entschließungen der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2007 in Saalfeld

Sachregister

Abkürzungsverzeichnis

Abkürz.	**Bedeutung**
AES	Advanced Encryption Standard
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
BA	Bundesagentur für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BKAG	Bundeskriminalamtgesetz
BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
BZSt	Bundeszentralamt für Steuern
CN	Corporate Network
DNA	deoxyribonucleic acet
EG	Europäische Gemeinschaft
E-Government/ eGovernment	electronic Government
EG-PassVO	EG-Passverordnung
ELSTER	Elektronische Steuererklärung
E-Mail	Elektronic-Mail (elektronische Post)
ePass	elektronischer Pass
EStG	Einkommenssteuergesetz
EU	Europäische Union
FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnisverordnung)
GG	Grundgesetz
HAMASYS	Haushaltsmanagementsystem
IFG	Informationsfreiheitsgesetz
IGLU	Internationale Grundschulleseuntersuchung
IMSI	International Mobile Subscriber Identity
INPOL	Informationssystem der Polizei
IPSec	Internet Protocol Security
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
KBA	Kraftfahrt-Bundesamt
Kfz	Kraftfahrzeug

KoopADV	Kooperationsausschuss Automatisierte Datenverarbeitung
MDR	Mitteldeutscher Rundfunk
MPLS	Multi Protocol Label Switching
OECD	Organization for Economic Co-Operation and Development
OSCI	Online Service Computer Interface
OWiG	Gesetz über Ordnungswidrigkeiten
PAG	Polizeiaufgabengesetz
PassDEÜV	Passdatenerfassungs- und Übermittlungsverordnung
PassG	Passgesetz
PC	Personal Computer
PDA	Personal Digital Assistant
PersStdG	Personenstandsgesetz
PIN	Persönliche Identifikationsnummer
PISA	Program for International Student Assessment der OECD
PKI	Public Key Infrastruktur
PNR	Passenger Name Records
RFID	Radio Frequency Identification
SAGA	Standards und Architekturen für E-Government-Anwendungen
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
StDÜV	Steuerdatenübermittlungsverordnung
StEG	Studie zur Entwicklung von Ganztagsschulen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TB	Tätigkeitsbericht
TESTA	Trans-European Services for Telematics between Administrations
thegov	Thüringer eGovernment
THOSKA	Thüringer Hochschul- und Studentenwerkskarte
ThürArchivG	Thüringer Archivgesetz
ThürBG	Thüringer Beamtengesetz
ThürDSG	Thüringer Datenschutzgesetz

ThürERVVO	Thüringer Verordnung über den elektronischen Rechtsverkehr
ThürHG	Thüringer Hochschulgesetz
ThürIFG	Thüringer Informationsfreiheitsgesetz
ThürKHG	Thüringer Krankenhausgesetz
ThürOBG	Thüringer Ordnungsbehördengesetz
ThürSchulG	Thüringer Schulgesetz
ThürStAnz	Thüringer Staatsanzeiger
ThürVerf	Verfassung des Freistaates Thüringen
ThürVSG	Thüringer Verfassungsschutzgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
TIMSS	Trends in International Mathematics Scient Study
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLfD	Thüringer Landesbeauftragter für den Datenschutz
USB	Universal Serial Bus
VIS	Vorgangsinformationssystem
ZEPTA	Zentrales Elektronisches Personalmanagementsystem für die Thüringer Allgemeine, Polizei- und Schulverwaltung
ZEVIS	Zentrales Verkehrsinformationssystem beim Kraftfahrtbundesamt
ZFER	Zentrales Fahrerlaubnisregister

1. Schwerpunkte im Berichtszeitraum

Das Ringen um die Balance zwischen Freiheit und Sicherheit stand in den letzten beiden Jahren wiederum im Vordergrund der Arbeit des TLfD. In zyklischen Schüben wurde die Diskussion um einen erweiterten Zugang der Sicherheitsbehörden zu personenbezogenen Daten nach Bekanntwerden spektakulärer Kriminalfälle oder der Vereitlung terroristischer Anschläge wie im Sommer 2006 und im Sommer 2007 geführt. Es blieb aber nicht bei einer Diskussion, sondern die Gesetzgeber in Europa, im Bund und im Land haben solche zusätzlichen Befugnisse zum Eingriff in die Privatsphäre der Menschen geschaffen oder planen sie. Beispiele hierfür sind die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten (4.1), Pläne für eine heimliche Online-Durchsuchung privater Computer (10.1) oder die geplante Kennzeichenerkennung im Thüringer Polizeiaufgabengesetz (7.1). Häufig werden bei diesen Maßnahmen Daten weit im Vorfeld von Gefahren und Straftaten erfasst und zudem von einem ganz überwiegend unverdächtigen Personenkreis. Das führt dazu, dass die Menschen unberechtigt unter einen Generalverdacht gestellt werden und Eingriffe in ihre Privatsphäre erdulden müssen. Damit werden aber häufig die Grenzen der Verhältnismäßigkeit überschritten. Andere Maßnahmen sind zwar durch einen Verdacht begründet, greifen aber so tief in die Privatsphäre ein, dass sie die im Grundgesetz garantierte Menschenwürde verletzen. Ermutigend ist es deshalb, dass das Bundesverfassungsgericht in einer Reihe von Entscheidungen solche übermäßigen Eingriffe korrigiert hat und wohl auch in noch anstehenden Entscheidungen korrigieren wird. Ebenfalls in der öffentlichen Diskussion standen die Gefahren, die aus der zunehmenden Einrichtung zentralisierter Datenbestände wie z. B. der zentralen Steuerdatei (9.2) oder einer geplanten länderübergreifenden Schülerdatenbank (13.3) entstehen können oder wie der Schutz von Kindern unter Beachtung des Datenschutzes möglich ist (11.4). Zu diesen und vielen anderen Themen erfolgte ein intensiver Austausch innerhalb der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Der Thüringer Landesbeauftragte für den Datenschutz hatte 2007 turnusgemäß zum ersten Mal den Vorsitz in diesem Gremium inne. Das erforderte einen nicht unerheblichen zusätzlichen organisatorischen Aufwand der Dienststelle zur Veranstaltung der beiden Konferenzen im Frühjahr in Erfurt und im Herbst in Saalfeld.

Bei der Kontrolltätigkeit zeigte sich eine Tendenz, wonach die Sensibilisierung für den Datenschutz sowohl hinsichtlich technisch-

organisatorischer Maßnahmen als auch bezüglich der rechtlichen Grenzen der Datenverarbeitung in den Kommunen zum Teil noch erhebliche Defizite aufweist. So mussten, auch wenn die Kommunen zahlenmäßig den größten Anteil der öffentlichen Stellen darstellen, in diesem Bereich die meisten der insgesamt 12 Beanstandungen ausgesprochen werden. Das reichte vom Verkauf von PC mit nicht gelöschten Daten (5.6), der fehlenden Einhaltung grundlegender Datenschutzvorschriften (5.5) und dem unsensiblen Umgang mit Postsendungen (5.7) über die unzulässige Datenveröffentlichung im Internet (5.4) bis hin zur Observierung von Mitarbeitern (6.3), zu unzulässigen Presseauskünften zu Personaldaten (6.3) sowie zur unbefugten Erstellung und Übermittlung eines amtsärztlichen Gutachtens (11.7). Für den kommenden Berichtszeitraum wird daher diesem Bereich besondere Aufmerksamkeit zu schenken sein. Bei der Kontrolltätigkeit zeigte sich auch erstmals ein generelles Problem im Zusammenhang mit der bundesweiten Einführung biometrischer Reisepässe (5.5). Obwohl die mit elektronisch gespeicherten Fingerabdrücken versehenen ePässe besonders sicher sein sollen, ist es für den Bürger noch nicht möglich, nach der Ausstellung die Übereinstimmung der gespeicherten mit seinen eigenen Fingerabdrücken zu überprüfen. Hier wurde der Bund aufgefordert, schnellstens für Abhilfe zu sorgen. Beim Dauerthema Videoüberwachung (5.2) bleibt zu hoffen, dass endlich eine Regelung im Thüringer Datenschutzgesetz geschaffen wird. Wichtige Hinweise für datenschutzrechtliche Mängel sind häufig auch Eingaben der Bürger. Die Überprüfung einer solchen Eingabe hat eine unzureichende Protokollierung von Datenabfragen durch die Polizei ergeben (7.8). Es sollte auch im Interesse des Ansehens der Polizei liegen, dass solche Abfragen besser dokumentiert werden, um berechtigte Vorwürfe eines Datenmissbrauchs überprüfen sowie unberechtigten Vorwürfen entgegentreten zu können. Neben der Kontrolle und der Bearbeitung von Eingaben spielt aber auch die Beratung eine zunehmende Rolle, um Datenmissstände erst gar nicht entstehen zu lassen. Das betrifft sowohl die Gesetzgebung (z. B. 7.1, 10.5 und 11.5), aber auch die datenschutzgerechte Gestaltung von Verfahren (z. B. 6.1, 11.2, 13.1, 13.7 und 15.4). Selbstverständlich waren auch Fragen zu bewerten, die sich aus dem Einsatz neuer Techniken erst langsam entwickeln. Dazu gehört zum Beispiel die Nutzung von Luftaufnahmen (12.1), die in immer höherer Auflösung vorliegen und als sog. Geodaten, auch mit anderen Daten verknüpft, neue Gefahren für die Privatsphäre darstellen. Ebenfalls noch nicht annähernd abschätzbar sind die neuen Risiken für das informationelle Selbstbestim-

mungsrecht durch den Einsatz von RFID-Technologie (14.3). Hier hat die Diskussion erst begonnen. Im technischen Bereich der Landesverwaltung befasste sich der TLfD u. a. mit der Filterung von unerwünschter elektronischer Post und Viren aus dem E-Mail-Verkehr der Landesverwaltung bei gleichzeitiger Beachtung des Telekommunikationsgeheimnisses der Beteiligten (15.7).

Insgesamt hat sich der Datenschutz in Thüringen etabliert, die Bedrohungen für die Privatsphäre der Bürger durch Staat und Wirtschaft wachsen jedoch stetig an. Deshalb ist eine funktionierende Datenschutzkontrolle wichtiger denn je.

2. Allgemeine Entwicklungen im Datenschutz

Bevor in gewohnter Weise über die Tätigkeit im Zuständigkeitsbereich des TLfD nach Fachbereichen gegliedert berichtet wird, sollen hier einige allgemein zu beobachtende Entwicklungen im Datenschutz aufgezeigt und wichtige Problemstellungen und Projekte aus dem nicht öffentlichen Bereich dargestellt werden.

Eine bereits seit einiger Zeit zu beobachtende Tendenz der Einführung zentraler Datenbanken sowie die Vernetzung dezentraler Datenbestände hat sich im Berichtszeitraum stark beschleunigt. Damit werden sowohl beim Staat als auch in der Wirtschaft bisher ungekannte Möglichkeiten geschaffen, um die Persönlichkeit des Einzelnen in weiten Teilen zu erfassen und Profile zu bilden. Eine wichtige Ursache dafür liegt sicherlich in der geradezu explosionsartigen Steigerung der Leistungsfähigkeit von Mikroprozessoren und den fast grenzenlosen und immer billiger werdenden Speicherkapazitäten. Staat und Wirtschaft setzen diese technischen Mittel ganz konsequent ein, um ihre Aufgaben effizienter erfüllen zu können. Die Wirtschaft hat schon früh erkannt, dass man in der Informationsgesellschaft mit dem Rohstoff „Information“ viel Geld verdienen kann. Deshalb werden auch personenbezogene Daten häufig in sog. Daten-Lagerhäusern (Data Warehouse) losgelöst von der ursprünglichen Verwendung zusammengefasst gespeichert und können dann mit Verfahren des sog. Datenschürfens (Data Mining) ausgewertet werden. Mit diesen Verfahren können die scheinbar zusammenhanglosen Daten des Daten-Lagerhauses nach bisher unbekannten, wissenswerten Zusammenhängen durchsucht werden. Ein Anwendungsbereich ist z. B. die Werbewirtschaft, die durch Auswertung von Datenbeständen das Konsumverhalten der

Betroffenen ermittelt, um gezielte Werbung platzieren zu können. Aber auch die Kreditwirtschaft bedient sich der Dienste von Auskunfteien, die beim sog. Scoring die o. g. Techniken zum Einsatz bringen, um die Kreditwürdigkeit der Betroffenen festzulegen.

Risiken für das Persönlichkeitsrecht ergeben sich daraus, dass durch eine Aufhebung des grundrechtlich vorgeschriebenen Gebots der Zweckbindung der Daten Profile erstellt werden und es auch zu einer unzulässigen Vorratsdatenspeicherung kommt. Derartige Praktiken sind somit eigentlich auch nicht zulässig - eigentlich. Doch gilt das Persönlichkeitsrecht nicht unbeschränkt. Einschränkungen können entweder durch ein normenklares, verhältnismäßiges Gesetz oder aber durch Einwilligung des Betroffenen vorgenommen werden. Bei der Datenerhebung mit Einwilligung besteht jedoch ein generelles Problem, mit dem der Datenschutz zunehmend konfrontiert ist: Das Datenschutzbewusstsein der Menschen hat in der Informationsgesellschaft zumindest partiell stark abgenommen. Um wirtschaftlicher Vorteile willen oder weil man die neusten Techniken ganz sorglos nutzt, lassen sich die Menschen ihre personenbezogenen Daten „abkaufen“. Das geschieht sowohl beim Einkauf mit Rabattkarten, deren Gegenleistung die Konsumprofile der Kunden sind, aber auch ganz simpel durch die unüberlegte Offenbarung der eigenen Daten beim Internetshopping bis hin zur aktiven Selbstentblößung selbst intimster Details auf Web-2.0-Plattformen wie z. B. MySpace oder StudiVZ. Hier sind selbst die Datenschutzbeauftragten ratlos und können nur warnend die Stimme erheben, dass jeder genau überlege, was er über seine Person in Zeiten des Elefantengehirns namens Internet preisgibt.

Ein Beleg für das zurückgebildete Datenschutzbewusstsein ist auch der Umstand, dass die Vorbereitungen für eine erste gesamtdeutsche Volkszählung im Jahr 2011 bislang weitgehend kritiklos erfolgt sind. Mobilisierte noch die im Jahr 1983 geplante Volkszählung bürgerbewegte Massen aus Sorge um die Allmacht des Staates und begründete das Bundesverfassungsgericht mit dem Volkszählungsurteil das Recht auf informationelle Selbstbestimmung und damit den Datenschutz, so wie wir ihn heute kennen, so wird dieses Vorhaben öffentlich so gut wie nicht wahrgenommen. Falls doch, so scheint angesichts der vielfältigen Datensammlungen von Staat und Wirtschaft ein Gewöhnungseffekt eingetreten zu sein. Tatsächlich gibt es an diesem geplanten Vorhaben auch keine fundamentale Kritik. Jedoch wird mit der vorgesehenen Kombination aus registergestützter Zählung (d. h. der

Auswertung vorhandener Datenbestände wie Melderegister, der Vermessungsbehörden und der Bundesagentur für Arbeit) und Stichprobenbefragungen (also keine Totalerhebung bei allen Bürgern) auch Neuland betreten. Gefahren entstehen dabei für die klare Trennung von Statistik und Verwaltungsvollzug. Die Datenschutzbeauftragten müssen im weiteren Verfahren darauf achten, dass es bei einer Einbahnstraße bleibt und keine personenbeziehbaren Einzeldaten aus der Statistik in die Verwaltung zurückfließen oder über eine Kombination georeferenzierter Daten (es sollen geographische Koordinatenwerte in Adress- und Gebäuderegistern erfasst werden) z. B. in Scoring- oder Ratingverfahren einfließen können.

Auch wenn in der Wirtschaft Datensammlungen mit Einwilligung der Betroffenen eingerichtet sind, muss es bestimmte Grundbedingungen zum Schutz der Betroffenen vor unangemessener Benachteiligung geben. Die Regeln im Bundesdatenschutzgesetz zu den Rechten und Pflichten von Auskunfteien sowie beim sog. Scoring (= statistisches Verfahren, mit welcher Wahrscheinlichkeit sich der Betroffene künftig in einer bestimmten Weise verhalten wird; z. B. zahlungswillig beim Kreditscoring) sind jedoch bislang nicht oder nur unzureichend vorhanden. Das Hauptdefizit beim Scoring liegt darin, dass der Betroffene meist gar nicht weiß, auf welcher Informationsgrundlage z. B. die Kreditwirtschaft zu einer für ihn ungünstigen Prognose seiner Kreditwürdigkeit gelangt ist. Damit ist ihm aber auch fast jede Möglichkeit genommen, eine unzutreffende Einstufung zu korrigieren oder aber seinen Wert durch eigene Anstrengungen zu verbessern. Die Bundesregierung hat im Berichtszeitraum einen Referentenentwurf zur Änderung des Bundesdatenschutzgesetzes vorgelegt, mit dem die Bestimmungen zu den Auskunfteien überarbeitet und erstmals Regelungen zum Scoring geschaffen werden sollen. Zwar gehen diese Überlegungen in die richtige Richtung, doch werden immer noch die Interessen der Wirtschaft denen der einzelnen Betroffenen vorangestellt. So können z. B. Auskünfte zu einem Scorewert pauschal mit der Begründung verweigert werden, es würden Geschäftsgeheimnisse offenbart. In einer Entschließung (Anlage 21) haben deshalb die Datenschutzbeauftragten des Bundes und der Länder die Bundesregierung aufgefordert, hier nachzubessern und einen fairen Interessenausgleich zu schaffen.

Auch im Urheberrecht deutet sich eine Entwicklung an, bei der die wirtschaftlichen Interessen der Urheberrechtsinhaber (v. a. der Musik-

industrie) gegenüber den Persönlichkeitsrechten der Betroffenen unangemessen bevorzugt werden sollen. Mit einem Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, das derzeit im Bundestag beraten wird, sollen u. a. Internet-Provider verpflichtet werden, auch ohne richterliche Anordnung Verkehrsdaten der Internetnutzer herauszugeben, um im Fall illegal kopierter Musik- oder Videodateien oder Software leichter ermitteln zu können. Bei allem Verständnis für die Rechtsposition der Produzenten erscheint das unangemessen, weil hier erstmals ein Eingriff in das Fernmeldegeheimnis durch Private legalisiert werden soll. Dies wurde bislang den Strafverfolgungsbehörden nur bei Straftaten von erheblicher Bedeutung zugestanden. Solche sind aber beim illegalen Herunterladen von Musikdateien nicht erkennbar. Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung (Anlage 5) an den Gesetzgeber appelliert, auf eine Einschränkung des Fernmeldegeheimnisses zur Durchsetzung wirtschaftlicher Interessen zu verzichten.

Es ist aber nicht nur die Wirtschaft, die sich des Data Warehouse und des Data Mining bedient. Vielmehr werden durch diese technischen Möglichkeiten auch Begehrlichkeiten bei den staatlichen Behörden, allen voran den Sicherheitsbehörden geweckt. Da es aber wegen der strikten Grundrechtsbindung der staatlichen Organe nicht möglich ist, allein auf der Basis von Einwilligungen (die wohl auch nicht erteilt werden würden) große Daten-Lagerhäuser einzurichten oder Datenbestände mit Datenschürftechniken durchzurastern, müssen hierzu gesetzliche Eingriffsbefugnisse geschaffen werden. Dabei wird meist nach einem schon eingespielten Muster vorgegangen. Eine neue Datenverarbeitungsbefugnis wird als zwingend notwendig, z. B. für die Bekämpfung des internationalen Terrorismus oder der organisierten Kriminalität dargestellt. Daraufhin erlässt der Gesetzgeber eine restriktive Regelung, mit der einerseits die erforderliche technische Infrastruktur geschaffen wird und andererseits eine Eingewöhnungszeit der Gesellschaft für diese Maßnahmen, die zuvor als nicht durchsetzbar galten, verbunden ist. Sind dann die kritischen Stimmen etwas abgeflaut, werden die rechtlichen Hürden abgesenkt und aus einer Ausnahmebefugnis wird nach und nach eine Standardmaßnahme. Das hat zur Folge, dass nicht nur Schwerkriminelle, sondern im äußersten Fall alle Bürger, also auch völlig unbescholtene Personen, einen solchen Eingriff in ihre Grundrechte dulden müssen. Die Beispiele hierfür sind zahlreich; angefangen bei der DNA-Analyse-Datei, der Tele-

kommunikationsüberwachung, der Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten, der Kontenabfrage beim Bundeszentralamt für Steuern bis hin zur geplanten Öffnung der Mautdaten zu Strafverfolgungszwecken. Bei der Antiterrordatei und der zentralen Steuerdatei darf man gespannt sein, wann hier erste Begehrlichkeiten zur Nutzung des jeweiligen Datenpools für andere Zwecke (also als Data Warehouse) laut werden. Insofern sind die Unterschiede in den Verhaltensmustern gar nicht so groß: hier wird gesammelt, gerastert und ausgewertet um den richtigen Kunden für sein Produkt zu finden; dort um den gesuchten Täter oder säumigen Steuerzahler dingfest zu machen. Die Grundfrage, die sich aber bei allen diesen Datenpools und deren zweckübergreifender Nutzung stellt, ist die nach der Verhältnismäßigkeit. Im Bereich der Sicherheitsgesetzgebung hat erfreulicherweise das Bundesverfassungsgericht in einer Reihe von Entscheidungen dem Gesetzgeber immer wieder die verfassungsrechtlichen Grenzen aufgezeigt.

Wegen dieser starken verfassungsrechtlichen Restriktionen gibt es auch immer wieder Versuche der Sicherheitsbehörden, Eingriffe in das informationelle Selbstbestimmungsrecht nicht selbst vorzunehmen, sondern auf Daten zurückzugreifen, die von privaten Stellen gespeichert werden (müssen). Prominentestes Beispiel dafür ist die jetzt beschlossene Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten (4.1), bei der die TK-Diensteanbieter gesetzlich zur Speicherung solcher Verkehrsdaten verpflichtet werden, die sie sonst überhaupt nicht benötigen, nur um sie im Bedarfsfall an die Strafverfolgungsbehörden herausgeben zu können. Selbst wenn es für Zugriffe auf private Daten eine gesetzliche Grundlage gibt, so werden mitunter auch die technischen Ermittlungsmöglichkeiten unter Überdehnung dieser Vorschriften und in Zusammenarbeit mit privaten Stellen genutzt, wie im Fall des Schlags gegen die Kinderpornografie in Sachsen-Anhalt Anfang 2007 geschehen. Die als großer Erfolg dargestellte Aktion „MIKADO“ wirft, ohne Berücksichtigung des konkreten Falls, die Frage auf, ob und unter welchen Voraussetzungen Strafverfolgungsbehörden auf Daten von Kreditkartenkunden oder überhaupt auf Daten, die von der Privatwirtschaft in zum Teil umfangreichen Dateien automatisiert gespeichert werden, zugreifen dürfen. Beim Abgleich einer Vielzahl von gespeicherten Daten ist zunächst an eine Parallele zu der in § 98a StPO geregelten Rasterfahndung zu denken. Eine Rasterfahndung ist jedoch an formelle Voraussetzungen geknüpft, die bei dem genannten Kreditkartenabgleich nicht vorlagen. Daher stellt sich

die Frage, ob ein derartiger rasterfahndungsähnlicher Massendatenabgleich auf der Rechtsgrundlage der allgemeinen Ermittlungsgeneralklausel nach §§ 161, 163 StPO gestützt werden kann. Um das Vorhandensein und ggf. die Anzahl und Identität ermittlungsrelevanter Personen festzustellen ist ein großer Kreis Unbeteiligter von einer solchen Maßnahme betroffen. Insbesondere fehlen bei einer derartigen Ermittlung einschränkende Eingriffsvoraussetzungen und Richtervorbehalt. Trotz des Verständnisses, das man dafür aufbringen kann, dass durch eine solche Kooperation der Kreditkartenunternehmen zahlreiche Straftaten aufgedeckt werden konnten, ist zweifelhaft, ob der Erfolg alle Mittel rechtfertigt. Der Aufschrei wäre sicherlich enorm gewesen, wenn die Kreditkartenunternehmen ihre Daten für die Steuerbehörden zur Ermittlung von Steuerschulden ausgewertet hätten.

Eine Neuerung auch aus datenschutzrechtlicher Sicht stellt die Verabschiedung eines Thüringer Informationsfreiheitsgesetzes Ende 2007 dar, wonach alle öffentlichen Stellen des Landes verpflichtet sind, Zugang zu amtlichen Informationen zu gewähren. Zu den im Landtag behandelten Gesetzentwürfen hat sich der TLfD im Rahmen der Anhörung im Innenausschuss aus datenschutzrechtlicher Sicht geäußert. Dabei wurde von Anfang an deutlich gemacht, dass die Frage, ob ein Informationsfreiheitsgesetz erlassen werden soll, nicht in die aktuelle Zuständigkeit des TLfD fällt und sich eine Äußerung hierzu, sozusagen aus der Position einer möglicherweise künftigen Aufgabenstellung heraus, verbietet. Da Zugang auch zu personenbezogenen Informationen der Landesbehörden eröffnet werden soll, gab es aber Anlass, zu der Frage Stellung zu nehmen, wie ein derartiger Informationszugang zu personenbezogenen Daten geregelt werden soll. Der Entwurf der SPD-Fraktion sah vor, dass personenbezogene Daten voraussetzungslos an Dritte offenbart werden können, wenn der Aufwand der Einholung der Einwilligung des Betroffenen nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Auch wenn zusätzlich geprüft werden sollte, ob die Offenbarung offensichtlich im Interesse des Betroffenen erfolgt, birgt dies letztlich die Gefahr, dass die Behörde ohne Beteiligung des Betroffenen eine Abwägungsentscheidung darüber trifft, was in seinem Interesse liegt und was nicht. Der Gesetzgeber hat in einer Vielzahl von Gesetzen diese Abwägung selbst vorgenommen (z. B. bei Melderegisterauskünften oder Auskünften aus dem Liegenschaftsregister), indem die Voraussetzungen für ein Auskunftsrecht festgeschrieben wurden. Darüber hinaus war kein Grund erkennbar, warum aus reiner Neugier Daten Dritter bei einer

Behörde erfragt werden können und der Betroffene das dulden soll. Wenn es um ein konkretes Verwaltungsverfahren geht, sind Auskunftsrechte in den Verfahrensgesetzen bereits geregelt. Einem möglicherweise vorgeschobenen Argument der Behörden, dass der Datenschutz eine Auskunft verhindere, obwohl der Betroffene gar nichts dagegen hat, kann durch eine Einwilligung des Betroffenen begegnet werden. Der Anregung, Zugang zu Daten Dritter nur nach Maßgabe der bereits geregelten Auskunftsansprüche oder aber einer ausdrücklichen Einwilligung des Betroffenen zu gestatten, ist der Ausschuss nicht gefolgt. Der von der CDU-Fraktion eingebrachte Entwurf, der im Wesentlichen auf die Vorschriften des IFG des Bundes verweist, hat jedoch die Hürden zum Zugang zu personenbezogenen Informationen insoweit erhöht, als reine Neugier nicht ausreicht, sondern ein rechtliches Interesse gefordert wird. Dieser Entwurf, den der Landtag auch verabschiedet hat, sieht zudem keinen Informationsfreiheitsbeauftragten vor. Auch hier ist die Frage, ob eine solche Funktion eingerichtet wird, keine datenschutzrechtliche. Wenn diese Funktion aber beim TLfD eingerichtet werden soll, wie das im Entwurf der SPD-Fraktion vorgesehen war, dann stellt sich auch die datenschutzrechtliche Frage, wie eine solche neue Aufgabe mit den Aufgaben des Datenschutzbeauftragten zu vereinbaren ist. Hierzu wurde im Rahmen der Anhörung in der Form Stellung genommen, dass der TLfD eine Doppelfunktion des Datenschutzbeauftragten und des Informationsfreiheitsbeauftragten problematisch sieht. Es handelt sich bei der Informationsfreiheit und dem Datenschutz nicht um zwei Seiten einer Medaille, jedenfalls dann nicht, wenn Zugang zu personenbezogenen Daten an Dritte gewährt werden soll. Durch Art. 69 ThürVerf ist der TLfD zur Wahrung des Rechts auf Schutz der personenbezogenen Daten verpflichtet, d. h. er muss sich im Zweifel immer für deren Schutz entscheiden.

3. Europäischer und Internationaler Datenschutz

3.1 Allgemeine Entwicklungen

Obwohl der TLfD keine Zuständigkeiten im Bereich des Europäischen und Internationalen Datenschutzes hat, beeinflusst dieses Gebiet zunehmend auch das nationale Datenschutzrecht. Deshalb soll hier ein kleiner Überblick über die allgemeinen Entwicklungen gegeben werden, von denen auch Thüringer Bürger betroffen sein können. Im Vordergrund steht, wie auf nationaler Ebene, das Verlangen ausländi-

scher Behörden, zur Bekämpfung des Terrorismus und organisierter Kriminalität immer mehr personenbezogene Daten zu erhalten.

Längere Diskussionen hat es im Berichtszeitraum zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten über den Umfang der personenbezogenen Daten der Flugreisenden in die USA gegeben, die die Fluggesellschaften über ihre Passagiere an die Sicherheitsbehörden der USA übermitteln müssen, um nicht ihre Landerechte zu verlieren. Das hierzu 2004 geschlossene sog. PNR-Abkommen (Passenger Name Records = Fluggastdatensätze) musste nach einer Entscheidung des Europäischen Gerichtshofs im Jahr 2006 gekündigt werden, da es auf einer unzutreffenden Kompetenzgrundlage geschlossen war. 2007 wurde ein neues Abkommen jetzt im Rahmen der polizeilichen und justitiellen Zusammenarbeit in Strafsachen (sog. „Dritte Säule“) abgeschlossen. Trotz weniger Verbesserungen bleibt es auch bei dem zweiten Abkommen dabei, dass eine Reihe von Daten (z. B. Kreditkartennummer, Reiseverlauf, Informationen zum Gepäck oder besondere Service- und Betreuungsinformationen) aller Reisenden den Sicherheitsbehörden der USA zur Verfügung gestellt und dort standardmäßig für 15 Jahre gespeichert werden, ohne dass der Einzelne hierzu irgend einen besonderen Anlass gegeben hat. Verschärfend kommt hinzu, dass eine Weitergabe der Daten an Drittstaaten möglich und eine unabhängige Datenschutzkontrolle nicht vorgesehen ist. Möglicherweise wird demnächst eine ähnliche Datenerhebung und -speicherung auch bei Flügen innerhalb der EU vorgenommen. Die EU-Kommission hat dazu Ende 2007 den Entwurf eines Rahmenbeschlusses vorgelegt, der einen weitgehend identischen Datenkatalog enthält und den Strafverfolgungsbehörden innerhalb der EU den Zugriff auf diese Daten ermöglichen soll.

Ebenfalls mit dem Argument der Terrorismusbekämpfung haben US-Sicherheitsbehörden nach dem 11. September 2001 immer wieder Daten aus internationalen Zahlungsanweisungen erhalten, die in einem Rechenzentrum der SWIFT in den USA gespeichert wurden. Da darunter auch Transaktionen europäischer Kunden ohne Bezug zu den USA waren, führte dies 2006 zu einer Überprüfung durch die belgische Datenschutzaufsichtsbehörde (SWIFT ist eine Genossenschaft mit Sitz in Belgien). Sowohl diese wie auch die Datenschutzgruppe nach Art. 29 EG-Datenschutzrichtlinie kamen zum Ergebnis, dass durch eine Speicherung des gesamten Datenverkehrs auch in den USA (es handelte sich um eine Sicherungskopie für eventuelle Ausfälle)

ohne ausreichende Datenschutzgarantien die Vorgaben der EG-Datenschutzrichtlinie nicht beachtet wurden. Nur großer öffentlicher Druck hat die SWIFT schließlich dazu bewegt, künftig Banküberweisungsdaten, die den innereuropäischen Zahlungsverkehr betreffen, nur in Europa zu speichern. Trotz dieser Verbesserung sei darauf hingewiesen, dass sowohl in den USA als auch in Europa weitreichende Befugnisse der Sicherheitsbehörden bestehen, um zur Bekämpfung der Terrorismusfinanzierung an Finanzdaten der Bürger zu gelangen.

Aber auch wenn Personen bekannt sind, von denen die Sicherheitsbehörden annehmen, dass sie den internationalen Terrorismus finanzieren, kann dies für unbescholtene Bürger zu Problemen führen. So geschehen bei den Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige. Auf diesen nach dem 11. September 2001 erstellten Listen sind Namen von Terrorverdächtigen wie Osama bin Laden u. a. enthalten, denen Banken, Behörden und andere Institutionen kein Geld zur Verfügung stellen dürfen. Gegen diese Listung bestand kein Rechtschutz. Außerdem waren die häufig arabischen Namen der Betroffenen nicht eindeutig einer Person zuzuordnen, mit der Folge von Verwechselungen, bei denen z. B. Sozialleistungen verweigert worden sind. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb in einer Entschließung (Anlage 4) die Bundesregierung aufgefordert, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz. Hier sind bislang nur wenige Fortschritte festzustellen. Immerhin hat der Sicherheitsrat der Vereinten Nationen eine Stelle eingerichtet, an den sich Privatpersonen direkt wenden können, um einen Antrag auf Streichung aus der Liste zu stellen.

Mit der Umsetzung des Haager Programms zur Schaffung eines gemeinsamen Raums der Freiheit, Sicherheit und des Rechts sind im Berichtszeitraum eine Vielzahl von Vorschlägen für Rechtsakte im Bereich der polizeilichen und justitiellen Zusammenarbeit in Strafsachen innerhalb der Europäischen Union vorgelegt worden, die einen immer weitergehenden Austausch derartiger Daten unter den Strafverfolgungsbehörden der EU-Mitgliedsstaaten vorsehen. Da jedoch im Bereich der sog. Dritten Säule die EG-Datenschutzrichtlinie nicht gilt, fehlt es hier an einem einheitlichem Datenschutzniveau, das die Ü-

bermittlung von sensiblen Daten der Strafverfolgungsbehörden in jeweils andere Mitgliedsstaaten als vertretbar erscheinen lässt. Dies haben auch der Europäische Rat und die EU-Kommission erkannt. Die Kommission hat 2006 den Entwurf eines Rahmenbeschlusses zum Datenschutz in der Dritten Säule vorgelegt, der einheitliche Datenschutzstandards – orientiert an den Regelungen der EG-Datenschutzrichtlinie – enthält. Dies wurde von den Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung grundsätzlich begrüßt (Anlage 6). Leider wurde dieser Rahmenbeschluss immer noch nicht vom Europäischen Rat verabschiedet. Ein Hauptstreitpunkt war die Frage, ob der Rahmenbeschluss nur den Austausch dieser Daten regeln oder nicht auch ein einheitliches Datenschutzniveau in den Mitgliedsstaaten beim Umgang mit personenbezogenen Daten durch Polizei- und Strafverfolgungsbehörden festschreiben soll. Letzteres wäre vor allem aus deutscher Sicht anzustreben, da hier ein hohes Datenschutzniveau gilt und zu befürchten wäre, dass zwar hohe Anforderungen für eine Übermittlung gelten, jedoch wenig Einfluss darauf bestünde, in welcher Weise die Empfängerstaaten die erhaltenen Daten weiterverwenden. Ende 2007 zeichnete sich ab, dass eine Mehrheit wohl nur zu Regelungen zum Datenaustausch zu erreichen wäre.

In der Eifelstadt Prüm wurde 2005 zwischen sieben EU-Mitgliedsstaaten, darunter Deutschland, ein Vertrag zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität sowie der illegalen Migration abgeschlossen. Danach sollen gegenseitige Zugriffe von Polizei und Strafverfolgungsbehörden auf Dateien (DNA-und Fingerabdruck-Indexdateien sowie Fahrzeugregister) möglich sein sowie präventive Übermittlungen personenbezogener Daten bei Großveranstaltungen mit grenzüberschreitendem Bezug oder zur Verhinderung terroristischer Straftaten erfolgen. Obwohl dieser Vertrag mit zahlreichen datenschutzrechtlichen Sicherungen versehen ist, führt der darin vorgesehene Austausch u. U. auch hier dazu, dass die Daten nicht in allen EU-Mitgliedsstaaten einem gleich hohen Datenschutzniveau unterliegen, da der Datenschutz in der Dritten Säule nicht vollständig harmonisiert ist (s. o.). Verschärft wird dieses Problem noch dadurch, dass im Rahmen der deutschen Ratspräsidentschaft dieser Vertrag durch einen Rahmenbeschluss in EU-Recht überführt wurde, und nun alle 27 EU-Staaten an diesem Datenaustausch teilnehmen.

Auch wenn sich Mitgliedsstaaten im Bereich der inneren Sicherheit höchst ungern national bindende Vorgaben abringen lassen – geht es doch hier um den Kernbereich der nationalen Souveränität – wird in letzter Zeit von den Sicherheitspolitikern auf solche Rechtsinstrumente zurückgegriffen, um Widerstände in den Mitgliedsstaaten gegen Befugniserweiterungen unter Hinweis auf zwingend geltendes oder umzusetzendes EU-Recht zu überwinden. Bestes Beispiel hierfür ist die EG-Richtlinie zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten (4.1).

Obwohl die Einwirkungsmöglichkeiten der Länder auf die EU-Gesetzgebung eingeschränkt sind, muss der verbleibende Spielraum stärker genutzt werden, um unverhältnismäßige und auch verfassungsrechtlich problematische Vorgaben auf EU-Ebene zu vermeiden.

3.2 Europäischer Datenschutztag

Mit dem vom Europarat am 28. Januar 2007 erstmals ausgerufenen Europäischen Datenschutztag soll bei den Bürgerinnen und Bürgern in Europa das Interesse für den Datenschutz geweckt werden, denn am 28. Januar 1981 ist mit der Unterzeichnung der Europaratskonvention 108/81 zum Datenschutz begonnen worden, die am 1. Oktober 1985 in Kraft trat. Mit dieser Konvention verpflichten sich die unterzeichnenden Staaten, für die Achtung der Rechte und Grundfreiheiten, insbesondere des Persönlichkeitsrechts, bei der automatisierten Datenverarbeitung zu sorgen. Eingedenk dieses für den Datenschutz weichenstellenden Datums wollen sich die Datenschutzbeauftragten des Bundes und der Länder 2008 auf Initiative des Thüringer Landesbeauftragten für den Datenschutz bundesweit den Jugendlichen zuwenden. Ziel ist es, das Datenschutzbewusstsein insbesondere von Schülern zu stärken. Hierzu wollen der Thüringer Landesbeauftragte für den Datenschutz und seine Mitarbeiter unter dem Motto „Datenschutz macht Schule“ thüringenweit Schulen besuchen, um mit den Schulklassen rechtliche Grundlagen und aktuelle jugendrelevante Aspekte des Datenschutzes zu diskutieren. Den jungen Leuten soll vor allem bewusst gemacht werden, wie vielfältig die Bedrohungen ihrer Privatsphäre in der heutigen Informationsgesellschaft sind und was sie selbst dagegen tun können. Der Themenbogen wird sich dabei von der Thüringer Verfassung über staatliches Online-Hacking bis zum Datenschutz in der Schule spannen und auch den Risiken des Internets gebührenden Platz

einräumen. Bei entsprechender Resonanz können sich weitere schulische Datenschutzprojekte anschließen.

3.3 Kontrolle polizeilicher Ausschreibungen im Schengener Informationssystem

Obwohl es noch einige Defizite beim Datenschutzniveau und der Kontrolle im Bereich der polizeilichen und justitiellen Zusammenarbeit innerhalb der EU gibt (3.1), ist in Teilbereichen, wie z. B. beim Schengener Informationssystem, schon ein durchaus guter Stand erreicht. Das SIS wurde als eine Maßnahme nach dem Wegfall der Grenzkontrollen eingerichtet, um auch die Polizeibehörden in den Schengen-Staaten bei der Kontrolle im Inland zu unterstützen. Neben europaweit gesuchten Personen und Sachen (insbes. Kraftfahrzeuge) dürfen in diesem Informationssystem auch Personen nach Art. 99 SDÜ gespeichert werden, über die bei jedem Antreffen durch die Polizei unbemerkt eine Mitteilung an die ausschreibende Dienststelle gefertigt wird (sog. verdeckte Registrierung). Da so, wenn auch nur zufällig bei Kontrollen, ein umfangreiches Bewegungsprofil über diese Personen erstellt werden kann, ist eine solche Maßnahme nur unter engen materiellen und formellen Voraussetzungen zulässig. Dazu gehört auch, dass konkrete Anhaltspunkte vorliegen müssen, wonach der Betreffende außergewöhnlich schwere Straftaten plant oder eine Gesamtbeurteilung erwarten lässt, dass er auch künftig solche Straftaten begehen wird.

Die datenschutzrechtliche Kontrolle des Schengener Informationssystems wird von der Gemeinsamen Kontrollinstanz nach Art. 115 SDÜ ausgeübt, in der alle nationalen Datenschutzkontrollbehörden der Schengen-Staaten vertreten sind. Die Gemeinsame Kontrollinstanz hat eine Überprüfung von Ausschreibungen nach Art. 99 SDÜ in allen Schengen-Staaten angeregt, die nach denselben Kriterien durchgeführt werden sollten. Anlass waren v. a. die sehr unterschiedlichen Ausschreibungszahlen aber auch Hinweise, das System könnte von einigen Regierungen zur Überwachung politisch Andersdenkender verwendet werden. So waren von Deutschland nur ca. 1.100, hingegen von Italien über 10.000 Datensätze eingestellt. Die Datenschutzbeauftragten des Bundes und der Länder erklärten sich bereit, an einer solchen Kontrolle mitzuwirken.

Vom Bundeskriminalamt waren 10 Datensätze Thüringer Behörden mitgeteilt worden, wobei zum Zeitpunkt der Kontrolle beim Thüringer Landeskriminalamt zwei Datensätze bereits wieder gelöscht waren. Drei dieser Fälle wurden einer näheren Überprüfung unterzogen. Bei allen drei Fällen waren die materiellen Voraussetzungen für eine Ausschreibung gegeben. Lediglich in einem Fall, bei dem zunächst eine Ausschreibung auf nationaler Ebene nach § 37 PAG (Ausschreibung zur polizeilichen Beobachtung) erfolgt war, ist die Begründung für die nachträgliche Ausweitung zu einer europaweiten Ausschreibung im Schengener Informationssystem nicht schriftlich dokumentiert worden. Der Empfehlung, in solchen Fällen künftig die Erweiterungsgründe zu dokumentieren, wird das Thüringer Landeskriminalamt folgen.

Weil eine heimliche Beobachtung und Aufzeichnung von Bewegungsprofilen einen zwar zulässigen, aber nicht unerheblichen Eingriff darstellt, wird auch künftig die Einhaltung der engen Voraussetzungen zu überprüfen sein.

4. Neue Medien - Rundfunk - Telekommunikation

4.1 Vorratsdatenspeicherung

Zum 1. Januar 2008 ist eines der datenschutzrechtlich umstrittensten Gesetze der letzten Jahre in Kraft getreten. Es handelt sich dabei um eine Änderung des Telekommunikationsgesetzes, mit der alle Anbieter von öffentlichen Telekommunikationsdiensten verpflichtet werden, künftig die Telekommunikations-Verkehrsdaten all ihrer Kunden für sechs Monate auf Vorrat zu speichern, auch wenn sie diese Daten selbst zum Betrieb der Dienste oder zur Abrechnung überhaupt nicht benötigen. Damit soll die EG-Richtlinie zur Vorratsdatenspeicherung 2006/24/EG umgesetzt werden (6. TB, 4.4). Obwohl keine Inhaltsdaten erfasst werden, ist der Eingriff in die Privatsphäre gravierend, weil künftig z. B. gespeichert werden muss, wer wann wie lange mit wem telefoniert und E-Mails ausgetauscht hat sowie welche Internetseiten aufgerufen wurden. Alleiniger Zweck der Vorratsspeicherung ist es, dass die Strafverfolgungsbehörden im Nachhinein in konkreten Fällen Täter und Tatbeteiligte anhand dieser Verkehrsdaten ermitteln können. Dabei sollen diese Daten nicht nur zur Verfolgung schwerer Straftaten (wie z. B. Terrorismus oder organisierter Kriminalität) gespeichert

werden; sie sollen auch der Aufklärung geringfügiger Straftaten dienen, die mittels Telekommunikation begangen wurden.

Für die Bürger bedeutet die Neuregelung ein vollständiges Erfassen, Speichern und Verfügbarmachen ihres Kommunikationsverhaltens, ohne dass sie sich in irgendeiner Form unrechtmäßig verhalten hätten. Damit werden alle Bürger unter einen Generalverdacht gestellt. Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung (Anlage 16) auf die Unverhältnismäßigkeit der geplanten Regelung hingewiesen und die Bundesregierung aufgefordert, eine Umsetzung der EG-Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der Europäische Gerichtshof über eine bereits anhängige Klage entschieden hat. Dies blieb leider erfolglos. Allerdings wurde sofort nach dem Inkrafttreten eine Verfassungsbeschwerde eingereicht, sodass auch hier wieder einmal das letzte Wort das Bundesverfassungsgericht haben dürfte.

Die Regelung zur Vorratsdatenspeicherung stellt eine nicht akzeptable Einschränkung des Rechts auf informationelle Selbstbestimmung dar und sollte so schnell wie möglich wieder aufgehoben werden.

4.2 Telemediengesetz

Im Bereich der Tele- und Mediendienste gab es bislang unterschiedliche Regelungen, die zahlreiche Abgrenzungsfragen aufgeworfen haben. Mit der Verabschiedung des neuen Telemediengesetzes und des Neunten Rundfunkänderungsstaatsvertrags im Jahr 2007 sind diesbezüglich einige Probleme beseitigt, allerdings auch andere geschaffen worden. Das Nebeneinander von unterschiedlichen Rechtsgrundlagen für Teledienste und Mediendienste wurde durch die Zusammenfassung zu Telemedien im Telemediengesetz beseitigt. In dessen § 1 Abs. 1 werden die Telemedien durch eine Negativabgrenzung definiert. Danach sind Telemedien alle elektronischen Informations- und Kommunikationsdienste mit Ausnahme von Telekommunikationsdiensten und Rundfunk. Auch wenn mit der Zusammenfassung eine gewisse Klärung erreicht wurde, treten jetzt neue Abgrenzungsprobleme auf, z. B. ob ein Dienst als Rundfunk bzw. Telekommunikation oder aber als Telemedium anzusehen ist. In Zeiten, in denen mit dem

PC auch über das Internet telefoniert oder Rundfunkprogramme empfangen werden können und diese Dienste von einem einheitlichen Anbieter vertrieben werden, ist eine Einordnung zu den jeweiligen Diensten nicht immer einfach. Von dieser Einordnung hängt aber auch ab, welches Datenschutzrecht anwendbar und damit auch welche Datenschutzkontrollbehörde zuständig ist. Im Neunten Rundfunkänderungsstaatsvertrag wurde zudem auf die datenschutzrechtlichen Regelungen des Telemediengesetzes verwiesen.

Auf Anregung des TLfD sind im Thüringer Gesetz zu dem Neunten Rundfunkänderungsstaatsvertrag und dessen Begründung die Datenschutzkontrollzuständigkeiten für Telemedien in Thüringen nochmals klargestellt worden. Danach liegt im Grundsatz die Datenschutzaufsicht für Telemedien bei der Aufsichtsbehörde für den nichtöffentlichen Bereich nach § 38 BDSG (Thüringer Landesverwaltungsamt), sofern es sich um nicht-öffentliche Stellen handelt. Ist der Anbieter von Telemedien eine öffentliche Stelle des Landes (z. B. Webangebote der Kommunen oder ein Landesportal), dann ist hierfür der TLfD zuständig. Eigenständig bleibt in dieser Hinsicht der öffentlichrechtliche Rundfunk. Wie bereits für die Datenverarbeitung des MDR im allgemeinen, so unterfallen auch dessen Online-Angebote der Datenschutzkontrolle des Rundfunkdatenschutzbeauftragten. Als Sonderzuständigkeit unterliegt die Datenverarbeitung der privaten Rundfunkanstalten des Landes nach dem Landesmediengesetz dem TLfD. Dies gilt auch für die Telemedienangebote dieser Rundfunkanstalten. Erfahrungen mit dem neuen Telemediengesetz konnten aber noch kaum gesammelt werden.

Nach dem ersten Schritt zu einer Vereinheitlichung des Datenschutzrechts im Bereich der Neuen Medien sollten auch die Telekommunikationsdienste umfassend in dieses Regelwerk integriert werden.

4.3 E-Mail und Internet am Arbeitsplatz

Öffentliche Bedienstete haben heute in der Regel die Möglichkeit, am Arbeitsplatz das Internet zu nutzen. Dabei fallen personenbezogene Daten der Beschäftigten, ihrer Kommunikationspartner und anderer Betroffener an, zu deren Verarbeitung bestimmte datenschutzrechtliche Anforderungen zu beachten sind. Insbesondere sind E-Mail und andere Internetdienste auch geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Wenn auch private Nutzung gestat-

tet ist, muss zudem vom Dienstherrn das Telekommunikationsgeheimnis gewahrt werden. Das bedeutet, dass hinsichtlich dienstlicher und privater E-Mails zu unterscheiden ist, weil der Dienstherr aufgrund des Telekommunikationsgeheimnisses privat ein- und ausgehende E-Mails nicht zur Kenntnis nehmen darf, was auf praktische Schwierigkeiten stößt. Deshalb hatte der TLfD empfohlen, keine private Nutzung von Internet und E-Mail zuzulassen (6. TB, 6.9), es sei denn, zwei unterschiedliche – also ein dienstliches und ein privates - E-Mail-Postfach der Behörde stünden zur Verfügung, was natürlich nicht der Fall und auch nicht beabsichtigt war. Die Empfehlung wurde zwischenzeitlich insoweit modifiziert, als den Betroffenen auch die Möglichkeit eröffnet werden kann, über Internet auf ein privates E-Mail-Postfach mittels eines Webmailservices zuzugreifen und private E-Mails auf diesem Weg zu senden und zu empfangen. Damit wird eine klare Trennung von privaten und dienstlichen E-Mails erreicht. Der Dienstherr muss nicht mehr befürchten, dass private mit dienstlicher Post vermengt wird und er unzulässigerweise Inhalte zur Kenntnis nehmen könnte. Voraussetzung ist jedoch die Einwilligung der Betroffenen, dass im Verdachtfall die privaten Internetzugriffe protokolliert und bei Hinweisen auf unzulässige Zugriffe auch überprüft werden können. Das Thüringer Finanzministerium hat entsprechende Empfehlungen des TLfD aufgegriffen und in die allgemeine Richtlinie zur Nutzung des zentralen Internetzuganges und des Mailsystems des Corporate Network (CN) des Freistaats Thüringen vom 6. November 2007 (ThürStAnz Nr. 51, S. 2356f) aufgenommen. Die private Nutzung des Internets im zulässigen Rahmen ist damit nur dann zu untersagen, wenn der Betroffene die erforderliche Einwilligung in die dort beschriebene Protokollierung nicht abgibt. Zu der Richtlinie wurde auch ein Muster für eine Dienstvereinbarung zwischen Dienstherr und Personalrat sowie eine Einwilligungserklärung entwickelt.

Passend zum Thema konnte von den Datenschutzbeauftragten des Bundes und der Länder die überarbeitete Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz vom 24. September 2007 der Praxis zur Verfügung gestellt werden. Die Ausführungen in der Orientierungshilfe sind mit der bisherigen Praxis in Thüringen hinsichtlich der Spam-Filterung vereinbar, da Spams automatisch nur gekennzeichnet werden und keine Löschung oder Unterdrückung erfolgt (hierzu auch 15.7). Im Zuge der Überarbeitung stellte sich auch heraus, dass die Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Ver-

waltung an das Internet, insbesondere bei den Ausführungen zur Protokollierung und Inhaltskontrolle mittels einer Firewall (Kapitel 4), aufgrund der zwischenzeitlich geänderten gesetzlichen Grundlagen zu überarbeiten war. Da die Orientierungshilfe bereits vor geraumer Zeit erstellt worden ist, ist auch die Aktualisierung der übrigen Kapitel vorgesehen. Beide Orientierungshilfen stehen auf der Homepage des TLfD zum Abruf bereit.

5. Kommunales

5.1 Arbeitskreis Datenschutz für den öffentlichen Bereich in Thüringen

Auf Initiative der Datenschutzbeauftragten der Stadt Suhl wurde auf der konstituierenden Sitzung am 7. November 2007 von den anwesenden Datenschutzbeauftragten der Landkreise und kreisfreien Städte sowie dem Thüringer Landesbeauftragten für den Datenschutz der „Arbeitskreis Datenschutz für den öffentlichen Bereich in Thüringen“ gegründet. Vorrangiges Ziel dieses Arbeitskreises ist es, zwischen den behördlichen Datenschutzbeauftragten und dem Thüringer Landesbeauftragten für den Datenschutz ein Netzwerk zu schaffen, um sich über aktuelle Probleme des Datenschutzes aus dem Tätigkeitsfeld der behördlichen Datenschutzbeauftragten zügig austauschen zu können und diese Informationen allen Arbeitskreismitgliedern zugänglich zu machen. Daneben sind u. a. halbjährlich fachspezifische Fortbildungen sowie die Erörterung zusammenhängender Problemfelder vorgesehen.

Die Gründung dieses Arbeitskreises wird vom Thüringer Landesbeauftragten für den Datenschutz sehr begrüßt, denn auf diese Weise können datenschutzrechtliche Probleme zeitnah erörtert und Lösungen allen Arbeitskreismitgliedern zur Verfügung gestellt werden. Dies ist ein entscheidender Schritt auf dem Weg zu datenschutzrechtlichen Standards im kommunalen Bereich.

5.2 Videoüberwachung in den Kommunen

Wie bereits in den letzten Tätigkeitsberichten (4. TB, 4.8; 5. TB, 5.2.19; 6. TB 5.3.5) ist auch im aktuellen Berichtszeitraum festzustellen, dass Kommunen zunehmend sich entscheiden, für die Erfüllung ihrer ordnungsbehördlichen Aufgaben Videoüberwachung einzuset-

zen. Als Rechtsgrundlage für eine Videoüberwachung durch die Ordnungsbehörden kommt nur § 26 Satz 1 Nr. 1 ThürOBG in Frage. Der seit Inkrafttreten des ThürOBG unverändert bestehende Wortlaut dieser Regelung enthält nur eine sehr allgemein gehaltene Befugnis „zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, oder zur Erfüllung ihrer sonstigen Aufgaben soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit und Ordnung entstehen." Fraglich ist, ob der Landesgesetzgeber mit dieser Regelung überhaupt die dauerhafte Überwachungsmöglichkeit mit optisch-elektronischen Einrichtungen öffentlich zugänglicher Räume, insbesondere Plätze wie Parks und Ruhezonen, Gebäudefassaden, Denkmäler usw. im Blick hatte. Der TLfD hält es für erforderlich, § 26 Satz 1 Nr. 1 ThürOBG an die bestehende Regelung des § 33 PAG anzugleichen, da hierin die Voraussetzungen für den Einsatz von Videoüberwachung und der Umgang mit den dabei erhoben Daten detaillierter sowie restriktiver geregelt sind. Um sich ein Bild von der tatsächlichen Praxis zu verschaffen und ggf. belegen zu können, wie dringend dieser Änderungsbedarf ist, hat der TLfD Ende 2007 eine Umfrage bei allen Thüringer Kommunen eingeleitet. Diese sollen dem TLfD den Einsatz von Videoüberwachung mitteilen. Die Auswertung der Rückläufe wird in der aktuellen Diskussion einbezogen.

Darüber hinaus sieht der TLfD nach wie vor Handlungsbedarf für die Schaffung einer allgemeinen Regelung zur Videoüberwachung im ThürDSG im Zusammenhang mit der Wahrnehmung des Hausrechts durch öffentliche Stellen des Freistaats Thüringen. Bislang wird die Zulässigkeit der Videoüberwachung in und an öffentlichen Gebäuden aus den im Privatrecht bestehenden Besitz- und Eigentumsrechten hergeleitet. Eine normenklare Regelung gibt es für den öffentlichen Bereich (im Gegensatz zu anderen Bundesländern) derzeit aber nicht. Das Thüringer Innenministerium hatte sich in der Vergangenheit auf den Standpunkt gestellt, dass eine solche Spezialnorm nicht erforderlich sei und man sich hier auf die allgemeinen Datenerhebungsvorschriften des § 19 ThürDSG stützen könne. In einem Urteil des Bundesverfassungsgerichts zum Einsatz einer Videoüberwachung durch eine öffentliche Stelle in Bayern hat das Gericht hinsichtlich der Heranziehung der allgemeinen Regelung für Datenerhebungen nach dem bayerischen Datenschutzgesetz jedoch klargestellt, dass dies keine

hinreichende Ermächtigungsgrundlage für eine solche Maßnahme darstellt (BVerfG, 1 BvR 2368/06 vom 23. Februar 2007). Der TLfD befindet sich mit dem Thüringer Innenministerium hinsichtlich der Entwicklung einer Spezialnorm im Gespräch.

Die Videoüberwachung durch Thüringer Ordnungsbehörden nach § 26 Satz 1 Nr. 1 ThürOBG bedarf einer Angleichung an die Regelungen des § 33 PAG. Im ThürDSG sollte eine Bestimmung über den Einsatz von Videoüberwachung für die Durchsetzung des öffentlich-rechtlichen Hausrechts aufgenommen werden.

5.3 Fortentwicklung des Meldewesens

Mit den Änderungen im Grundgesetz zum 1. September 2006 wurde auch im Rahmen der Föderalismusreform das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Das Bundesministerium des Innern bereitet derzeit den Entwurf eines Bundesmeldegesetzes vor. Bei der damit verbundenen Neuordnung des Meldewesens gilt es nun darauf zu achten, dass dies nicht zu einer Verringerung des Niveaus des Datenschutzes und der Datensicherheit führt. Deshalb besteht seitens der Datenschutzbeauftragten die Forderung, unter Beachtung des neuesten Standes der Technik die bereits eingeleitete Vernetzung der vorhandenen Melderegister zur Modernisierung des Meldewesens fortzuführen und auf ein zentrales Bundesmelderegister zu verzichten. Mit der Neuordnung des Meldewesens sollte auch die bislang zunehmende Tendenz der Aufnahme melderechtsfremder Merkmale aus den verschiedensten Verwaltungsbereichen (z. B. Inhaber einer Waffenbesitzkarte) in die Melderegister, die letztlich zum „Gläsernen Bürger“ führen würde, umgekehrt werden. Originärer Zweck der Melderegister ist allein die Registratur der Einwohner, um deren Identität und Wohnungen feststellen und nachweisen zu können. Hierauf sollte man sich wieder besinnen und den Umfang der im Melderegister gespeicherten Daten auf das dafür erforderliche Maß beschränken. In diesem Zusammenhang sollte auch von der Aufnahme und Nutzung verwaltungsübergreifender Identifikationsmerkmale im Melderegister, wie der Steueridentifikationsnummer, wieder Abstand genommen werden, da sie zur faktischen Schaffung von Personenkennzeichen führen. Des Weiteren sind im Zuge der Modernisierung des Melderechts die bisherigen Widerspruchsregelungen auf den Prüfstand zu stellen und durch Einwilligungslösungen zu ersetzen. Der mündige Bürger sollte uneingeschränkt selbst ent-

scheiden können, ob seine Daten z. B. einer Partei für Zwecke der Wahlwerbung übermittelt werden dürfen. Darüber hinaus muss die Transparenz der Verfahren und Auskunftserteilungen für den Betroffenen weiter erhöht werden. Zugang der Behörden zu Meldedaten ist nur in dem Umfang zu erlauben, den sie zur Erfüllung ihrer gesetzlichen Aufgaben benötigen.

Im Berichtszeitraum wurde das Thüringer Meldegesetz nochmals novelliert sowie eine Meldeverordnung in Kraft gesetzt. Erforderlich war dies aufgrund von Änderungen im Melderechtsrahmengesetz des Bundes, nach denen die Länder verpflichtet waren, die Rückmeldungen über Umzüge zwischen Meldebehörden verschiedener Länder ab dem 1. Januar 2007 ausschließlich auf elektronischem Weg vorzunehmen. Des Weiteren bestand die Notwendigkeit, Bestimmungen des Thüringer Meldegesetzes zum Selbstauskunftsrecht der Einwohner und zu den Ausnahmeregelungen von der Meldepflicht dem Melderechtsrahmengesetz anzupassen. Darüber hinaus sollten bei dieser Gelegenheit auch weitere in der Vergangenheit als überarbeitungsbedürftig festgestellte Regelungen aktualisiert werden. Durch eine frühzeitige Beteiligung des TLfD sowohl an der Novellierung des Thüringer Meldegesetzes wie bei der Erarbeitung der Meldeverordnung wurden die dabei auftretenden datenschutzrechtlichen Fragen umfassend erörtert und die vom TLfD vorgetragenen Anregungen und Hinweise weitgehend berücksichtigt. Diese betrafen nicht nur den Umfang der Datenspeicherung und die Zulässigkeit von Datenübermittlungen an Behörden und Einrichtungen, sondern insbesondere auch technisch-organisatorische Probleme der Datensicherheit. Hierbei galt es vor allem, die künftigen Aufgaben und Zuständigkeiten des Thüringer Landesrechenzentrums konkret zu bestimmen, um durch entsprechende Vorgaben die Einführung eines Landesmelderegisters auszuschließen.

Die Neuordnung des Meldewesens darf nicht zur Verringerung des Niveaus des Datenschutzes und der Datensicherheit führen. Sie sollte als Chance verstanden werden, das Meldewesen wieder auf seine originären Aufgaben zurückzuführen.

5.4 Internetpräsentationen der Kommunen

Im Rahmen einer zunehmenden dienstleistungs- und serviceorientierten Verwaltung wird von den Kommunen verstärkt das Internet für

Veröffentlichungen genutzt. Problematisch wird dies jedoch dann, wenn hierbei auch personenbezogene Daten offenbart werden. Es bestehen keine Bedenken, wenn Kommunen sich und ihre Sehenswürdigkeiten via Web-Kamera im Internet präsentieren, solange eine Individualisierung zufällig aufgenommener Personen oder ein Personenbezug von bestimmten Objekten (z. B. Fahrzeugen), etwa durch Datenverknüpfungs- oder Zoomfunktionen unmöglich ist. Da dies anderenfalls zu unzulässigen Grundrechtseingriffen führen würde, sollte stets vor der Anschaffung der notwendigen Aufnahmetechnik und ihrer Einrichtung die datenschutzrechtliche Unbedenklichkeit geprüft werden.

Zwischenzeitlich wird das Internet von vielen Kommunen bereits als Medium genutzt, um Interessenten über Land und Leute zu informieren. Hierbei wollte die Stadt Meuselwitz auch einen besonderen Service bieten. So wurde der TLfD darüber informiert, dass alle Adressdaten der volljährigen Einwohner der Stadt über das Internet abrufbar seien. Im Ergebnis der weiteren Prüfungen stellte sich dann heraus, dass die Stadt die Daten einem Adressbuchverlag übermittelt hatte. Als Gegenleistung veröffentlichte der Verlag im Auftrag der Gemeinde die gedruckte Broschüre in elektronischer Form auf seiner Seite im Internet. Dies war rechtswidrig, da die Stadt weder eine Aufgabe noch eine Befugnis hatte, Melderegisterdaten öffentlich bekannt zu geben. Darüber hinaus ist auch die Übermittlung von Meldedaten an Adressbuchverlage nur erlaubt, soweit die Daten allein für die Herausgabe von Adressbüchern in Form von gedruckten Nachschlagewerken verwendet werden (§ 32 Abs. 3 Thüringer Meldegesetz). Da die Angaben bereits über mehrere Monate im Internet jedermann uneingeschränkt zur Verfügung standen, wurde die unzulässige Offenbarung von Meldedaten förmlich beanstandet und die Stadt aufgefordert, jeden weiteren Zugriff auf die Daten auszuschließen. Dem ist die Stadt unverzüglich nachgekommen.

Datenschutzrechtlich problematisch ist auch die Veröffentlichung eines kommunalen Haushalts im Internet, wenn dabei aufgrund der von den Aufsichtsbehörden vorgegebenen Detailliertheit in der Gliederung zu den Angaben über Personalausgaben insbesondere bei kleineren Organisationseinheiten bzw. bei einer geringen Anzahl von Beamten in Einzelfällen ein Personenbezug hergestellt werden kann. Hierzu hatte die Kommunalaufsicht des Thüringer Innenministeriums bei früheren Anfragen darauf verwiesen, dass die Vorschriften über

die Zuordnung der Einnahmen und Ausgaben der kommunalen Haushalte weitgehend bundeseinheitlich gestaltet seien, man aber im Rahmen der Einführung eines neuen kommunalen Haushaltsrechts eine Problemlösung anstrebe. Im Jahr 2007 wurden nunmehr im Rahmen eines Gemeinschaftsprojektes mit den kommunalen Spitzenverbänden Empfehlungen zum neuen kommunalen Finanzwesen erarbeitet, auf deren Grundlage in den nächsten Monaten dem Landtag ein Gesetzentwurf vorgelegt werden soll. Dabei ist vorgesehen, dass die Darstellung der Haushaltsansätze nicht mehr „haushaltsstellenscharf“ im kameralistischen Sinn, sondern nach dem Konten- und Produktplan der jeweiligen Kommune erfolgen soll. Insoweit wird davon ausgegangen, dass sich dabei keine personenbezogenen Zuordnungen für einzelne Mitarbeiter ergeben dürften. Eine Pflicht zur Bekanntmachung des Haushaltsplans im Internet gibt es nicht. Soweit Veröffentlichungen über den Plan in Auszügen oder Zusammenfassungen im Internet beabsichtigt sind, müssen diese auf Angaben beschränkt werden, die eine Personenbeziehbarkeit ausschließen.

Ein weiteres Problem bei den Internetpräsentationen der Kommunen stellen die unbeschränkten Veröffentlichungen von Organisationsplänen und Telefonverzeichnissen dar. So ist immer wieder festzustellen, dass Übersichten über einzelne Fachbereiche oder Dezernate mit den Daten aller Beschäftigten veröffentlicht werden, ungeachtet, ob sie Außenkontakte haben oder nicht und ob es Azubis, Praktikanten oder Studenten sind. Für die Veröffentlichung derartiger Daten gelten mangels spezialgesetzlicher Regelungen die Bestimmungen des Thüringer Datenschutzgesetzes für Datenübermittlungen an Stellen außerhalb des Geltungsbereichs des Grundgesetzes und Mitgliedsstaaten der EU. Die darin vorgegebenen hohen Anforderungen an die Zulässigkeit von derartigen Übermittlungen tragen der Tatsache Rechnung, dass Veröffentlichungen im Internet weltweit zur Verfügung stehen und daher hinsichtlich der weiteren Nutzung der Daten jeder datenschutzrechtlichen Kontrolle entzogen sind. Nach § 23 Abs. 2 ThürDSG ist somit die Veröffentlichung personenbezogener Daten durch öffentliche Stellen insbesondere nur dann erlaubt, wenn dies zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist oder der Betroffene eingewilligt hat. Als Bewertungskriterien für die Veröffentlichung der Erreichbarkeitsdaten von Mitarbeitern können somit neben der Gewährleistung der Funktionsfähigkeit der Behörde auch Gesichtspunkte der Service- und Kundenorientierung bzw. Bürgerfreundlichkeit der Verwaltung herangezogen werden. Dennoch ist

auch im Hinblick auf die Fürsorgepflicht zu prüfen, ob die wichtigen Gründe für eine Veröffentlichung die schutzwürdigen Interessen der Betroffenen überwiegen. Dies kann weder den Regelfall darstellen, noch den gesamten Mitarbeiterbestand betreffen, sondern allenfalls Bedienstete, die aufgrund ihres Aufgabenbereichs regelmäßig mit Dritten in Kontakt stehen oder bei herausgehobenen Funktionsträgern.

Da die Internetpräsentation die weitreichendste Form einer Veröffentlichung darstellt, ist dies bei der Prüfung der Verhältnismäßigkeit der Offenbarung personenbezogener Daten besonders zu berücksichtigen.

5.5 Biometrische Merkmale im elektronischen Reisepass (ePass)

Über den Beginn der Einführung von biometrischen Merkmalen im elektronischen Reisepass auf der Grundlage der EG-PassVO wurde bereits kritisch berichtet (6. TB, 5.3.4). Im Vordergrund stand hierbei die Frage, ob mit den vorgesehenen technischen Lösungen die Integrität, Authentizität und Vertraulichkeit der auf dem Chip gespeicherten personenbezogenen Daten gewährleistet werden kann. Die dafür notwendige umfassende Datensicherheitsanalyse ist jedoch nahezu unmöglich, weil die Entwicklung der technischen Standards und Verfahren teilweise auch bis zum heutigen Tag noch nicht abgeschlossen ist, was sich auch bei entsprechenden Kontrollen in Passbehörden bestätigt hat. Bei dieser Gelegenheit wurden bei der Stadtverwaltung Sömmerda zahlreiche Verstöße gegen grundlegende datenschutzrechtliche Vorschriften (wie fehlendes Sicherheitskonzept, fehlende Verfahrensfreigaben und fehlende Bestellung eines Datenschutzbeauftragten) festgestellt und nach § 39 ThürDSG beanstandet.

Seit dem 1. November 2005 werden bereits in allen neu ausgestellten Reisepässen auf einem integrierten Chip die digitalisierten Lichtbilder der Betroffenen gespeichert. Ergänzend dazu ist laut der EG-PassVO spätestens ab 1. März 2008 die Aufnahme der Fingerabdrücke vorgesehen. Mit dem Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften vom 20. Juli 2007 wurde dieser Termin in der Bundesrepublik auf den 1. November 2007 vorgezogen. Mit der Vorhaltung dieser Daten auf dem Reisepass sollen künftig die Polizeivollzugsbehörden, die Zollverwaltung sowie die Pass- und Personalausweisbehörden bzw. die Meldebehörden mittels noch zu entwickelnder technischer Geräte prüfen, ob der Inhaber des Passes mit der im Pass beschriebenen Person übereinstimmt. Vollzogen werden soll dies künftig

u. a. durch einen Vergleich des auf dem Chip des Passes gespeicherten Fingerabdrucks mit dem vom Inhaber vor Ort gescannten Fingerabdruck (Identitätsprüfung). Die Führung von sog. Referenzdateien bei einer Behörde oder die Übernahme der auf dem Chip gespeicherten Fingerabdrücke in automatisierte Verfahren ist dabei vom Gesetzgeber ausdrücklich nicht vorgesehen. Damit soll verhindert werden, dass zu einem Großteil der Bevölkerung eine erkennungsdienstliche Datei entsteht.

Da der RFID-Chip im ePass eine kontaktlose Übertragung der gespeicherten Angaben zulässt, besteht die nicht zu unterschätzende Gefahr des unbefugten Auslesens. Deshalb sollten die Passbehörden die Betroffenen bei der Ausgabe der Pässe auf diesen Sachverhalt hinweisen. Wie zwischenzeitlich Kontrollen ergaben, werden die Daten der Fingerabdrücke im Rahmen ihrer Verarbeitung zur Erstellung des Passes sowohl in den Passbehörden, wie auch bei der Bundesdruckerei aus programmtechnischen Gründen mehrfach gespeichert. Die vom Gesetzgeber vorgesehene unverzügliche Löschung dieser Datenbestände nach der Ausgabe des Passes wird aber teilweise (z. B. in Sicherungskopien) nicht konsequent umgesetzt. Darüber hinaus setzen Gemeinden ein Verfahren ein, ohne dass umfassende Kenntnisse zum Verarbeitungsprozess und den Datensicherungsmaßnahmen vorliegen. Im Hinblick auf die Sensibilität biometrischer (i. d. R. nur für erkennungsdienstliche Zwecke genutzter) Daten kann dies nicht akzeptiert werden.

Um die Rechte von Betroffenen bei der Verarbeitung personenbezogener Daten zu gewährleisten wurde in Art. 4 der EG-PassVO ausdrücklich festgelegt, dass Personen, denen ein Pass oder ein Reisedokument ausgestellt worden ist, das Recht haben, die personenbezogenen Daten in dem Reisepass oder dem Reisedokument zu überprüfen. Bei Kontrollen wurde hierzu festgestellt, dass diese Vorgabe bislang bundesweit nicht erfüllt wird. Von der Bundesdruckerei wurden bzw. werden den Passbehörden Lesegeräte zur Verfügung gestellt, mit deren Hilfe der Mitarbeiter und der Antragsteller bei der Abholung des Passes die Möglichkeit erhalten, die auf dem Chip des Passes gespeicherten Daten auf einem Bildschirm betrachten zu können. Während bei den bisherigen Lesegeräten der sog. ersten Generation lediglich die Personendaten und das Lichtbild wiedergegeben wurden, stehen einigen Passbehörden Lesegeräte der sog. zweiten Generation zur Verfügung, die sukzessiv weiter ausgeliefert werden sollen. Eine

Verbesserung für den Betroffenen oder die Passbehörde ergibt sich dadurch aber nicht. Bei diesen Geräten werden zwar auf einem Monitor auch zwei Fingerabdrücke abgebildet, eine Prüfung für den Betrachter, ob es sich bei dem Abbild um die Fingerabdrücke des Ausweisinhabers handelt, ist aber unabhängig von der Größe der Darstellung nur durch einen Fachmann möglich. Dementsprechend können auch die Passbehörden nicht sicher sein, ob tatsächlich die Fingerabdrücke des Antragstellers/Passinhabers ordnungsgemäß im Pass gespeichert sind und ob damit der Pass gültig ist (§ 11 PassG). Für den Betroffenen bedeutet das aber in letzter Konsequenz, dass die Richtigkeit der Übernahme seiner Fingerabdrücke in seinen Pass erstmals z. B. bei einer Passkontrolle vor dem Abflug in den Urlaub überprüft werden kann, mit für ihn im ungünstigen Fall äußerst negativen Folgen.

Die Argumentation des Bundesministerium des Innern, dass die Vorgaben der EG-Verordnung damit bereits erfüllt seien, da der Betroffene feststellen könne, ob überhaupt (irgendwelche) Fingerabdrücke gespeichert wären, klingt wie ein Schildbürgerstreich. In Kenntnis der Sachlage und ausgelöst durch die öffentliche Kritik des TLfD sowie kritischer Stellungnahmen anderer Landesbeauftragter für den Datenschutz wurde das Bundesministerium des Innern vom BfDI nach einem Besuch der Bundesdruckerei aufgefordert, die Anforderungen der EG-PassVO unverzüglich umzusetzen. Zwischenzeitlich hat sich auch der Innenausschuss des Deutschen Bundestags am 12. Dezember 2007 mit der Thematik befasst und den BfDI um einen Bericht gebeten.

In den Städten und Gemeinden sind mit Unterstützung des Bundes schnellstmöglich die Voraussetzungen zur Identitätsprüfung nach Art. 4 EG-PassVO zu schaffen und alle gesetzlich vorgesehenen Datenschutz- und Datensicherheitsmaßnahmen zu gewährleisten.

5.6 Datenschutzausverkauf

Der TLfD erhielt eines Tages den brisanten Hinweis, wonach die Stadtverwaltung Stadtroda ihre ausgesonderten PCs an Private veräußert habe, ohne zuvor die Festplatten ordnungsgemäß zu löschen. Deren Inhalt sei leicht rekonstruierbar und enthalte personenbezogene Daten Dritter. Hierdurch alarmiert erfolgte unverzüglich eine Kontrolle bei der Stadtverwaltung, die den Vorwurf im Wesentlichen bestätigte. Der datenschutzrechtliche Schaden konnte durch nachträgliche

Löschung der Datenträger weitestgehend begrenzt werden. Im Zuge dieser Kontrolle stellten sich allerdings eklatante Verstöße gegen das Datenschutzrecht heraus, die sich in der Vergangenheit leider immer wieder in Gemeindeverwaltungen zeigten. Trotz bisheriger Hinweise des TLfD in den zurückliegenden Tätigkeitsberichten war auch hier wiederum zu beanstanden:

- Veräußerung von Büro-PCs
  Personenbezogene Daten müssen von der öffentlichen Stelle gelöscht werden, wenn die Kenntnis dieser Daten, wie im Falle der Veräußerung, nicht mehr erforderlich ist (§ 16 Abs. 1 ThürDSG). Nach § 3 Abs. 3 Nr. 6 ThürDSG ist unter Löschen das endgültige Unkenntlichenmachen gespeicherter personenbezogener Daten zu verstehen. Endgültiges Unkenntlichmachen wird nicht durch das Erteilen eines in den Betriebssystemen enthaltenen Löschkommandos erreicht, da diese nur den Verweis, wo sich die Daten auf der Festplatte befinden, löschen. Vonnöten ist vielmehr der Einsatz spezieller Software, mit deren Hilfe der Datenträger vollständig und mehrfach überschrieben wird. Nur so wird eine Rekonstruktion der Daten mit hoher Wahrscheinlichkeit ausgeschlossen.
- Sicherheitskonzept, Freigabe und Verfahrensverzeichnis
  Nun wirklich zu den Basis-Standards zählen das Sicherheitskonzept (§ 9 Abs. 2 ThürDSG), die datenschutzrechtliche Freigabe durch die Gemeinde selbst (§ 34 Abs. 2 ThürDSG) sowie das Führen eines Verfahrensverzeichnisses beim behördeninternen Datenschutzbeauftragten (§§ 10, 10a Abs. 2 Ziffer 2 ThürDSG). Das Fehlen solcher Mindeststandards lässt auf tiefgreifende datenschutzrechtliche Verdrängungsmechanismen schließen, denen flächendeckend entgegenzuwirken ist.
- Auftragsdatenverarbeitung
  Völlig unterschätzt wird, dass im Falle der Auftragsdatenverarbeitung der Auftraggeber datenschutzrechtlich verantwortlich bleibt (§ 8 Abs. 1 ThürDSG). Die von ihm unter anderem wahrzunehmenden Auswahl- und Kontrollpflichten wurden weder vertraglich berücksichtigt noch wahrgenommen. Zur vertraglichen Ausgestaltung eines solchen Auftragsvertragsverhältnisses wird auf ein Muster in Anlage 23 zum 5. TB des TLfD hingewiesen.
- Behördeninterner Datenschutzbeauftragter
  Zur Vermeidung von Interessenkonflikten wird empfohlen, die Funktionen des behördeninternen Datenschutzbeauftragten und des Systemadministrators nicht in Personalunion auf nur einen Mitarbeiter zu übertragen.

Der TLfD wird angesichts dieser Mängel seine Beratungs- und Kontrolltätigkeit im kommunalen Bereich intensivieren. Die unter 5.1 dargstellte Gründung des kommunalen datenschutzrechtlichen Arbeitskreises stellt auf diesem Wege einen wichtigen Meilenstein dar.

5.7 Umgang mit Postsendungen

Aufgrund einer Anfrage befasste sich der TLfD im Berichtszeitraum auch mit den allgemeinen Regelungen zum Umgang mit Postsendungen im Landratsamt des Saale-Orla-Kreises. Ausgangspunkt war dabei zunächst das Schreiben eines Gerichts, welches an den Landkreis allgemein adressiert war und aus dessen Inhalt der konkrete Adressat nicht erkennbar wurde. Statt bei dem Gericht nachzufragen, wurden alle Mitarbeiter des Hauses per E-Mail über den Eingang des Schreibens unter Angabe des Aktenzeichens des Gerichtes sowie des Namens des Betroffenen informiert, mit der Bitte, sich zu äußern, ob man ein solches Schreiben erwarten würde. Diese Verfahrensweise wurde sowohl vom behördlichen Datenschutzbeauftragten wie auch vom TLfD kritisiert, weil dadurch unzulässigerweise personenbezogene Daten offenbart wurden. Gleichzeitig wurden bei dieser Gelegenheit vom TLfD auch Hinweise zur Dienstanweisung zum Umgang mit Postsendungen gegeben, die gerade neu gefasst werden sollte.
Kritisiert wurde und wird hierbei insbesondere die Regelung, nach der grundsätzlich jede auf dem üblichen Postweg eingehende Postsendung, auch wenn sie an ein konkretes Amt adressiert ist, in einer zentralen Poststelle des Landratsamtes geöffnet wird. Eine ungeöffnete Weiterleitung erfolgte lediglich bei Postsendungen, die an den Landrat oder den ersten Beigeordneten persönlich adressiert sind, Sendungen an die Fachdienste Kreiskasse und Gesundheit sowie solche, die mit dem ausdrücklichen Vermerk „vertrauliche Personalsache“ oder „Vergabesache“ beschriftet sind und Briefe an den Personalrat und den Geheimschutzbeauftragten. Dies ist aber zum Schutz von Daten, die besonderen Geheimhaltungsvorschriften unterliegen, nicht ausreichend, so dass weitere Ausnahmeregelungen zur ungeöffneten Weiterleitung von Postsendungen gefordert wurden.

Allerdings blieben die Argumente des TLfD unbeachtet. Das Landratsamt berief sich auf seine Organisationshoheit und die Verpflichtung aller Mitarbeiter auf das Datengeheimnis. Außerdem informierte es den TLfD nicht über das weitere Verfahren, sodass dieses Verhal-

ten formell beanstandet und die Aufsichtsbehörde um Unterstützung gebeten wurde. Dabei wurde nochmals nachdrücklich darauf hingewiesen, dass die Postregelung nicht akzeptiert werden kann, weil die datenschutzrechtlichen Grundsätze und Vorschriften für die gesamte Tätigkeit einer Behörde und somit auch bei der Organisation des verwaltungsinternen Handelns gelten (§ 21 Abs. 5 ThürDSG). Daher sind die Leiter von Behörden in ihren Entscheidungen im Rahmen ihrer Organisationshoheit nicht völlig frei. Das Erforderlichkeitsprinzip verlangt auch hierbei von der verantwortlichen Stelle eine aktive Gestaltung ihrer technisch-organisatorischen Verfahrensabläufe, sodass nicht nur im geringst möglichen Umfang personenbezogene Daten verarbeitet werden, sondern auch so wenig wie möglich Mitarbeiter Kenntnis davon erhalten. Eine Verpflichtung der Mitarbeiter zur Geheimhaltung rechtfertigt allein keinesfalls Regelungen, die eine Kenntnisnahme von personenbezogenen Daten ermöglichen, ohne dass diese zur Aufgabenerfüllung benötigt werden. Letztlich zeigen auch die Erfahrungen des TLfD, dass Schweigepflichten allein nicht in jedem Fall die unzulässige Offenbarung von personenbezogenen Daten gegenüber Dritten ausschließen. Vorrangiges Ziel des Datenschutzes ist es aber nicht, Verstöße zu ahnden, sondern durch geeignete technische und organisatorische Maßnahmen zu verhindern. Dies ist auch bei der Organisation des Postlaufs zu beachten, zumal dort bei Postöffnungen im besonderen Maße auch die spezialgesetzlichen Vorschriften zur Geheimhaltung zu berücksichtigen sind, z. B. zum Arzt-, Sozial-, Adoptions- oder Steuergeheimnis. Es gilt eben die Schweigepflicht nach § 203 StGB auch unter Schweigeverpflichteten. Ebenso wird z. B. in § 35 Abs. 1 SGB I ausdrücklich bestimmt, dass das Sozialgeheimnis auch innerhalb eines Leistungsträgers durch geeignete Abschottungsmaßnahmen zu gewährleisten ist. Darüber hinaus ergeben sich nicht nur aus den Adressaten sondern teilweise auch aus den Absendern Hinweise auf einen besonders schützenswerten Inhalt. So fordert z. B. § 44 BZRG, dass Auskünfte an Behörden nur an den der Entgegennahme oder Bearbeitung betrauten Bediensteten zur Kenntnis gebracht werden dürfen. Dass darüber hinaus jede mit dem Zusatz „persönlich“ beschriftete Postsendung verschlossen dem Adressaten zu übergeben ist, sollte eigentlich selbstverständlich sein.

Zwischenzeitlich wurde unter Einbeziehung des Landesverwaltungsamtes als Aufsichtsbehörde erreicht, dass Postsendungen mit dem ausdrücklichen Vermerk „persönlich“, „vertraulich“, „verschlossen“

oder „eigenhändig“ sowie Sendungen an den Datenschutz- bzw. Frauen- oder Gleichstellungsbeauftragten verschlossen weitergeleitet werden. Warum aus Sicht des Landratsamtes die Öffnung eines Teils der an die einzelnen Ämter direkt adressierten Postsendungen durch die zentrale Poststelle erforderlich sein soll, wurde bislang nicht ausreichend begründet. Da es weiterhin weder nachvollziehbar noch für Betroffene vermittelbar ist, weshalb private Schreiben an die Personalstelle, die Beihilfestelle, das Jugendamt oder das Sozialamt im Landratsamt nur dann vertraulich behandelt werden, wenn dies auf dem Umschlag ausdrücklich vermerkt wird, steht eine abschließende Klärung hierzu noch aus.

Neben der Einhaltung des materiellen Datenschutzrechts haben die öffentlichen Stellen die Grundsätze und Vorschriften zum Datenschutz gemäß § 21 Nr. 5 ThürDSG auch bei der Organisation des verwaltungsinternen Handelns zu beachten.

5.8 Reform des Personenstandsrechts

Ende 2006 hat der Bundestag das Gesetz zur Reform des Personenstandsrechts beschlossen. Neben einigen datenschutzrelevanten Änderungen zur Registerführung wurden auch solche zur Kommunikation mit Behörden, anderen Stellen und dem Bürger aufgenommen. Schließlich wurde auch der Zugang zu älteren Personenstandseintragungen erleichtert. Dies betrifft insbesondere die Benutzungsvorschrift für Privatpersonen, die nicht zu den unmittelbaren Verwandten eines Verstorbenen gehören. So ist es derzeit noch nicht möglich, Auskünfte aus einem Sterberegister über einen entfernten Verwandten zu erhalten, wenn dies nicht zur Durchsetzung von Rechtsansprüchen zwingend erforderlich ist. Dies war bei den betroffenen Personen stets auf Unverständnis gestoßen. Mit § 7 Abs. 2 i. V. m. § 5 Abs. 5 PersStdG wurde nunmehr eine Bestimmung aufgenommen, wonach nach Ablauf von 80 Jahren eines Eintrags im Ehe- und Lebenspartnerschaftsregister, nach Ablauf von 110 Jahren eines Eintrags im Geburtenregister oder nach Ablauf von 30 Jahren eines Eintrags im Sterberegister die archivrechtlichen Bestimmungen für die Benutzung von Archivgut gelten. Damit kann jedermann, der ein berechtigtes Interesse begründen kann (z. B. Genealogen), Auskunft aus dem jeweiligen Register erhalten. Als Zeitpunkt für das Inkrafttreten der Änderungen im Personenstandsgesetz wurde vom Gesetzgeber der 1. Januar 2009 bestimmt. Da bis zu diesem Zeitpunkt noch die bisherigen Regelungen

gelten, sollten die Standesämter bei entsprechenden Auskunftsersuchen nicht nur, wie eine Anfrage beim TLfD zeigte, auf die derzeitige Rechtslage, sondern insbesondere auch auf die ab dem 1. Januar 2009 geltenden Bestimmungen hinweisen.

Soweit Standesämter aufgrund der derzeitigen Rechtslage Auskünfte noch verweigern müssen, die nach dem 1. Januar 2009 erlaubt sind, sollten die Auskunftssuchenden darüber informiert werden.

6. Personaldaten

6.1 Zentrales Personalverwaltungssystem

Zur Einführung eines einheitlichen, damals noch als Personalinformationssystem bezeichneten Verfahrens zur Verarbeitung von Personaldaten, wurde im 6. TB (6.1) berichtet. Zwischenzeitlich wurde das Thüringer Landesrechenzentrum beauftragt, unter Verwendung der eGovernment-Basis-Lizenzen mit der Erstellung und Einführung eines landesweiten, nunmehr als Personalmanagementsystem benannten Verfahrens, das den Namen ZEPTA (Zentrales Elektronisches Personalmanagementsystem für die Thüringer Allgemeine, Polizei- und Schulverwaltung) erhalten hat, zu beginnen. Die Datenschutzbeauftragten des Bundes und der Länder haben Handlungsempfehlungen zu Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung zustimmend zur Kenntnis genommen (abrufbar über die Homepage des TLfD), die hier genutzt werden konnten.

Zur Vorbereitung der Einführung des ZEPTA fanden im Berichtszeitraum für die zukünftigen Nutzer mehrere Workshops statt. Im begleitenden Lenkungsausschuss „Personalmanagementsystem“ ist neben allen Ministerien auch der TLfD vertreten. Derzeit wird das Verfahren für erste Geschäftsbereiche pilotiert. Kennzeichnend für das System ist, dass alle zu verarbeitenden Personaldaten zentral auf einem Server im Zentrum für Informationsverarbeitung abgelegt werden sollen, wobei eine logische Trennung der Daten der verschiedenen Ressorts vorgenommen wird. Dies ist deshalb notwendig, weil nur zuständige Mitarbeiter der personalverwaltenden und –bewirtschaftenden Stellen auf die jeweiligen Daten der in ihrem Zuständigkeitsbereich beschäftigten Betroffenen zugreifen dürfen. Diese zentrale Speicherung bietet den Vorteil, dass die Daten an einer Stelle verfügbar sind. Ansinnen, die zentral gespeicherten Daten durch die Einrichtung von automati-

sierten Abrufverfahren auch in anderen Anwendungen zu nutzen, scheiterten jedoch daran, dass dafür die nach § 104 Abs. 1 Satz 3 Thüringer Beamtengesetz erforderliche Rechtsgrundlage fehlt. Grundtenor muss bleiben, dass Datenübermittlungen in der Herrschaft der jeweiligen personalverwaltenden Stelle verbleiben müssen. Dies schließt jedoch nicht aus, dass Personaldaten über gegebenenfalls einzurichtende Schnittstellen an zuständige andere Stellen übermittelt werden (z. B. Zentrale Gehaltsstelle). Die Umsetzung wesentlicher datenschutzrechtlicher Eckpunkte wurde zugesagt:

- Die Daten sollen auf dem Zentralserver verschlüsselt und für jede Personalverwaltung logisch getrennt abgelegt werden.
- Datenübertragungen sollen ebenfalls nur verschlüsselt erfolgen.
- Alle Aktivitäten mit Ausnahme des rein lesenden Zugriffs durch Berechtigte sollen protokolliert werden.
- Datenschutzrechtliche Freigaben sind durch die jeweils für die Bediensteten zuständigen Stellen zu erteilen.
- Es sind jeweils Vereinbarungen zur Auftragsdatenverarbeitung mit dem Thüringer Landesrechenzentrum und dem Zentrum für Informationsverarbeitung abzuschließen.

Nachdem bereits wesentliche datenschutzrechtliche Eckpunkte geklärt wurden, soll die abschließende Bewertung erfolgen, wenn der Pilotbetrieb ausgewertet ist und die Einzelheiten der beabsichtigten Nutzung feststehen.

6.2 Was darf geprüft werden, wenn Mitarbeiter (zu) oft krank sind

Im Berichtszeitraum war aufgrund von Beschwerden und Presseberichten der Frage nachzugehen, welche zulässigen Mittel der Arbeitgeber hat, um zu überprüfen, ob es sich bei Fehltagen um krankheitsbedingte Abwesenheiten oder um „krankfeiern“ handelt. Probleme gibt es dann, wenn auch mit Gesundheitsdaten der Mitarbeiter umgegangen werden soll.

Aufgrund eines aus der Sicht des Landratsamts Nordhausen schwerwiegenden Fehlverhaltens und von Unregelmäßigkeiten bei Krankmeldungen einer Mitarbeiterin sollten die Möglichkeiten dienstrechtlicher Konsequenzen geprüft werden. Aus den von der Mitarbeiterin vorgelegten Krankschreibungen ergaben sich Fragen, weil sich die Atteste teilweise zeitlich überschnitten und sich die Zeitangaben zur

Arbeitsunfähigkeit nicht mit dem Unterschriftsdatum deckten. Noch als die Mitarbeiterin arbeitsunfähig geschrieben war, meldete sie sich telefonisch bei der Dienststelle und kündigte an, im Anschluss an die Krankschreibung zu einem Facharzt zu gehen. Die Dienststelle vermutete, dass es sich nur um einen Vorwand handeln könnte, um blau zu machen und entschied sich, den Arztbesuch durch eine Observierung zu überprüfen. Damit wurde der für die Dienststelle tätige Objektschutz beauftragt. Vorgabe war, die Observierung zeitlich zu begrenzen und die Maßnahme abzubrechen, wenn die Betroffene einen Facharzt aufsucht oder das Zuständigkeitsgebiet verlässt. Die Verfolgung wurde in einem Protokoll festgehalten, in dem genau dokumentiert und durch eine Fotoaufnahme und ein Kraftfahrzeugkennzeichen belegt war, wann und wo sich die Mitarbeiterin in Begleitung durch eine andere Person an diesem Tag aufgehalten hat. Das Protokoll endete mit Verlassen des Zuständigkeitsgebiets. Damit nicht genug. Es erfolgte ein weiterer Observierungsauftrag, als die Mitarbeiterin auch am Folgetag der Arbeit fernblieb. Erst aufgrund der telefonischen Meldung der Betroffenen, sie sei erneut krank geschrieben, wurde die Beobachtung abgebrochen. Statt einer Information über die verdeckten Ermittlungen durch die Dienststelle musste die Betroffene von Nachbarn erfahren, dass das Wohnhaus offensichtlich beschattet werde.

Der Umstand, dass sich aus Arbeitsunfähigkeitsattesten Fragen ergeben, begründet noch keine Erforderlichkeit der Prüfung der Richtigkeit der Ankündigung eines Mitarbeiters, er werde an einem bestimmten Tag zum Arzt gehen. Entscheidend für eine ordnungsgemäße Arbeitsbefreiung aufgrund einer Erkrankung ist allein die Vorlage einer ärztlichen Bescheinigung. Soweit Zweifel an der Arbeitsunfähigkeit eines Mitarbeiters bzw. an der Ordnungsmäßigkeit der Krankschreibung bestehen, kann der Arbeitgeber gemäß § 275 Abs. 1a SGB V von der gesetzlichen Krankenkasse des Arbeitnehmers verlangen, eine gutachterliche Stellungnahme des Medizinischen Dienstes zur Überprüfung der Arbeitsunfähigkeit einzuholen. Bei Beamten besteht bei Vorliegen der Voraussetzungen die Möglichkeit, ein amtsärztliches Attest zu verlangen. Eine Erforderlichkeit für die Überprüfung des Arztbesuchs bestand unter keinen Gesichtspunkten, zumal im zu Grunde liegenden Fall die Einschaltung des Medizinischen Dienstes sogar erfolgt war.

Die Observierung war darüber hinaus weder geeignet noch verhältnismäßig, um die Rechtmäßigkeit der Krankschreibung zu überprüfen. Vielmehr wurde mit der Observierung massiv in die Privatsphäre eingegriffen, deren Schutz ausdrücklich in Art. 6 ThürVerf gewährleistet ist. Es wurde bei der Gelegenheit der Observierung eine Vielzahl von Daten erfasst, die in keiner Weise mit dem zu ermittelnden Sachverhalt in Verbindung standen; auch wurden Daten völlig unbeteiligter Dritter erhoben. Als schwerwiegenden Verstoß gegen datenschutzrechtliche Vorschriften wurde dies gemäß § 39 ThürDSG beanstandet. Die Stelle war aufgefordert, die mit der Observation verbundenen Unterlagen unter Beachtung der Vorgaben des § 16 ThürDSG aus dem Vorgang zu entfernen und ggf. zu vernichten sowie die Betroffene hierüber zu informieren. Dem kam das Landratsamt Nordhausen nach.

Bevor eine öffentliche Stelle im absoluten Ausnahmefall eine Observierung eines Mitarbeiters in Erwägung ziehen kann, sind sämtliche zulässigen rechtlichen Maßnahmen auszuschöpfen. Im Falle von Krankschreibungen ist eine Begutachtung durch den Amtsarzt bzw. den Medizinischen Dienst vor einem intensiveren Eingriff in die Privatsphäre eines Betroffenen angezeigt.

Bekanntlich sieht § 22 Abs. 1 Thüringer Urlaubsverordnung vor, dass man sich als Beamter bis zu 3 Tage auch ohne ärztliches Attest auskurieren darf. Erst wenn eine Krankheit länger dauert, ist die Vorlage eines ärztlichen Attests erforderlich, es sei denn, für die Dienststelle bestand Anlass, die Vorlage eines ärztlichen Attestes bereits vorher zu fordern. Bei Arbeitsunfähigkeit ohne ärztliches Attest besteht unter Umständen Nachfrage- oder gar Nachprüfungsbedarf, wenn solche Abwesenheiten beispielsweise immer auf bestimmte Wochentage fallen oder der versagte freie Tag rein zufällig durch Krankheit gewährt werden muss. Andererseits hat der Dienstherr auch seinen Fürsorgeverpflichtungen nachzukommen, wenn sich Fehltage häufen und diese beispielsweise auf die Arbeitsbedingungen oder das Arbeitsklima in der Dienststelle zurückzuführen wären.

Das Thüringer Innenministerium sah sich veranlasst, Krankmeldungen ohne Vorlage eines ärztlichen Attests nachzugehen, um erforderlichenfalls entsprechende Maßnahmen zu ergreifen. Dabei sollten mit Mitarbeitern, bei denen aus der Jahresbetrachtung mehr als fünf Fälle der Krankmeldung ohne Krankenschein zu entnehmen waren, Gesprä-

che mit dem Ziel geführt werden, eine Erklärung für das Fernbleiben vom Dienst zu erhalten. Bei einer datenschutzrechtlichen Kontrolle in der betroffenen Personalverwaltung war festzustellen, dass in der Tat Gespräche mit zwei Mitarbeitern geführt worden waren. Dabei wurde nicht nach konkreten Erkrankungen gefragt, was zweifellos unzulässig gewesen wäre. Ob von betroffenen Mitarbeitern diesbezüglich Angaben gemacht wurden, konnte nicht festgestellt werden, weil darüber keine Aufzeichnungen vorlagen und auch keine konkreten Hinweise oder Beschwerden von betroffenen Mitarbeitern vorgebracht wurden. Was sich allerdings in diesem Zusammenhang als formal nicht ganz korrekt erwies, war die Praxis der Weitergabe von Korrekturbelegen im Krankheitsfall vom für die Zeiterfassung zuständigen Mitarbeiter an die allgemeine Personalverwaltung. Dies diente der Erfassung auch von Krankheitstagen ohne Attest im Personalverwaltungssystem. Zwar ist dies grundsätzlich zulässig, hätte aber in der Dienstvereinbarung zur Zeiterfassung aus Gründen der Transparenz und Nachvollziehbarkeit für die Betroffenen geregelt werden müssen. Die Dienstvereinbarung ist daraufhin entsprechend geändert worden.

Für die Personalverwaltung besteht selbstverständlich die Möglichkeit, häufige oder auffällige Krankmeldungen ohne ärztliches Attest mit den Betroffenen zu erörtern, um ggf. dienstrechtliche Maßnahmen einzuleiten. Konkrete Erkrankungen dürfen dabei nicht erfragt werden. Der Umgang mit Arbeitszeitdaten muss für die Betroffenen transparent gestaltet werden. Dies ist Aufgabe der Dienstvereinbarung.

Eine an den TLfD herangetragene Anfrage, ob eine Polizeidienststelle berechtigt sei, eine Liste auszulegen, in der jeder Beamte seine gesundheitlichen Beeinträchtigungen eintragen sollte, war eindeutig mit „nein“ zu beantworten. Zum einen besteht bei der Eintragung in eine Liste das Problem, dass der jeweils nachfolgende eintragende Bedienstete die vorherigen Eintragungen zur Kenntnis nehmen kann, wofür keinerlei Zulässigkeit besteht. Zum anderen handelt es sich bei der Erfassung von gesundheitlichen Beeinträchtigungen oder Erkrankungen von Bediensteten um besonders sensible personenbezogene Daten, die nur auf einer konkreten Rechtsgrundlage erfolgen darf.

Auf Nachfrage zur Rechtsgrundlage und zum Zweck einer solchen Liste hat die Polizeiinspektion Gotha geltend gemacht, zum zweckmäßigen Personaleinsatz und auch zur Wahrnehmung der Fürsorge-

pflicht gegenüber der Beamten sei es erforderlich, Bedenken zur Einschränkung der Dienstfähigkeit zu erkennen. Im Falle einer Diabeteserkrankung, bei der zur Therapie die Insulingabe erfolgen müsse, bestehe regelmäßig eine erhebliche Einschränkung der Dienstfähigkeit. Die eingeschränkte Dienstfähigkeit sei insbesondere im Polizeibereich mit Gefahren sowohl für die Bediensteten als auch für Außenstehende verbunden. Aus dem Umstand, dass derartige Erkrankungen für andere ersichtlich sein können, hatte die Dienststelle zunächst keine besondere Vertraulichkeit erkannt. Selbst wenn einzelne Bedienstete im kollegialen Umfeld keinen Hehl aus ihrer Erkrankung machen, bildet dies keine Rechtsgrundlage für die Abfrage durch die Dienststelle. Aufgrund der Hinweise des TLfD wurden die in Einzelfällen ausgefüllten Listen unverzüglich vernichtet. Damit war eine weitere Verarbeitung unzulässig erhobener personenbezogener Daten ausgeschlossen. Zur Lösung des Problems wurde als allenfalls gangbarer Weg angeregt, die Bediensteten in einem ausführlichen Merkblatt auf eventuell eingeschränkte Dienstfähigkeiten und die damit verbundenen Gefahren hinzuweisen und aufzufordern, sich ggf. unverzüglich mit dem Amtsarzt in Verbindung zu setzen, der eine eingeschränkte Dienstfähigkeit festzustellen hat. Dabei ist auch zu berücksichtigen, dass der Amtsarzt der Dienststelle grundsätzlich keine Einzelheiten zu gesundheitlichen Einschränkungen mitteilen darf und sich auf die Feststellung der Dienstfähigkeit, eingeschränkten Dienstfähigkeit oder Dienstunfähigkeit beschränken muss.

Wenn einer Dienststelle möglicherweise durch Information oder Verhalten bekannt ist, dass ein Bediensteter z. B. auf Insulingaben angewiesen ist und damit nur eingeschränkt dienstfähig sein könnte, kann dies zum Anlass genommen werden, eine amtsärztliche Untersuchung anzuordnen. Es wäre jedoch unverhältnismäßig, alle Bediensteten ohne konkreten Anlass zu untersuchen.

6.3 Unzulässige Presseauskünfte zu Personaldaten

Es ist sicherlich schmerzhaft für eine Kommune, wenn der Haushalt durch nicht geplante Zahlungen zusätzlich belastet wird. Die Gründe hierfür können sehr unterschiedlich und ggf. auch Zahlungsverpflichtungen an Einzelpersonen sein. Einer Veröffentlichung der Identität der Zahlungsempfänger stehen in diesen Fällen grundsätzlich datenschutzrechtliche Bestimmungen entgegen, auch wenn die Presse entsprechende Auskünfte begehrt. Im vorliegenden Fall hatte ein leiten-

der Mitarbeiter aufgrund eines aktuellen Urteils eine nicht unbeachtliche Gehaltsnachzahlung verlangt. Dies wurde, auf welchem Wege auch immer, der örtlichen Presse bekannt. Statt sich bei der diesbezüglichen Nachfrage auf die für den Umgang mit Personaldaten gebotene Vertraulichkeit und Geheimhaltung zu berufen, wurde von dem Landratsamt Weimarer Land die Information bestätigt und mit weiteren Angaben ergänzt. Begründet wurde die Zulässigkeit der Presseauskünfte damit, dass die Dienstbezüge der leitenden Mitarbeiter in öffentlicher Sitzung im Kreistag beschlossen worden seien. Dieser Auffassung konnte nicht gefolgt werden, da es sich im vorliegenden Fall unzweifelhaft um Personaldaten handelte, deren Umgang im Thüringer Beamtengesetz eindeutig geregelt ist. Unter Berücksichtigung, dass das Landratsamt bereits zwei Jahre zuvor unbefugt personenbezogene Daten im Zusammenhang mit der Vergabe von Fördermitteln veröffentlicht hatte (6. TB, 5.3.6), wurden die Bekanntgabe der Personaldaten gegenüber der Presse beanstandet und Maßnahmen gefordert, die eine Wiederholung ausschließen. Im Ergebnis dessen wurden alle Mitarbeiter des Landratsamtes insbesondere auch im Hinblick auf Anfragen seitens der Presse nochmals aktenkundig über die zu beachtenden datenschutzrechtlichen Bestimmungen belehrt.

Die Offenbarung von personenbezogenen Daten aus Personal- oder Verwaltungsunterlagen gegenüber der Presse ist grundsätzlich auszuschließen.

6.4 Panne beim Zugriff auf Personalaktendaten

§ 97 Abs. 3 ThürBG bestimmt, dass Zugang zur Personalakte nur Beschäftigte haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Dies gilt auch für den Zugang im automatisierten Abrufverfahren. Aus der Presse war im Berichtszeitraum zu entnehmen, dass Beurteilungslisten der Polizeidirektion Nordhausen im lokalen Intranet für alle dort Zugriffsberechtigten zur Verfügung standen. Unstreitig durfte dies nicht so sein. Auch wenn letztendlich im Intranet „nur“ die Namen, Besoldungsgruppe und Dienststellennummer sowie der Beurteilungswert belegt waren, handelte es sich dabei um Personalaktendaten, die nicht für alle im Intranet zugriffsberechtigten Bediensteten zugänglich sein durften. Dazu kam es, weil aufgrund von Abwesenheiten und Vertretungen versehentlich

der allgemeine Zugriff auf diese Datei nicht ausgeschlossen war. Nach Bekanntwerden des Vorfalls wurden die technischen und organisatorischen Maßnahmen getroffen, um unbefugten Zugriff auszuschließen. Die weitere Anregung, Personalaktendaten grundsätzlich zu verschlüsseln, um einen hohen Sicherheitsstandard zu erreichen, wurde jedoch bislang nicht aufgegriffen.

Aufgrund der Sensibilität von Personalaktendaten sind immer geeignete Sicherheitsmaßnahmen zum Ausschluss unbefugter Zugriffe insbesondere im automatisierten Verfahren zu treffen.

7. Polizei

7.1 Novellierung des Polizeiaufgabengesetzes

Schon im letzten Tätigkeitsbericht wurde auf die Notwendigkeit hingewiesen, das Polizeiaufgabengesetz an die Rechtsprechung des Bundesverfassungsgerichts zum Schutz des Kernbereichs privater Lebensgestaltung anzupassen (6. TB, 7.1). Anlass dafür gab die Entscheidung zum sog. Großen Lauschangriff (Urteil vom 3. März 2004 - 1 BvR 2378/98). Zudem sollten die Vorgaben des Urteils zur präventiven Telekommunikationsüberwachung im Niedersächsischen Sicherheits- und Ordnungsgesetz (Urteil vom 27. Juli 2005 – 1 BvR 668/04) eingearbeitet werden. Doch bevor ein Gesetzentwurf vorgelegt wurde, kam es bereits zur nächsten Entscheidung des Bundesverfassungsgerichts, diesmal zur präventiven Rasterfahndung im Nordrhein-Westfälischen Polizeigesetz (Beschluss vom 4. April 2006 - 1 BvR 518/02). Auch deren Vorgaben sollten Eingang in die Novelle finden. Der im Frühjahr 2007 von der Landesregierung vorgelegte Gesetzentwurf (Thüringer Gesetz zur Änderung sicherheits- und verfassungsschutzrechtlicher Vorschriften) beschränkt sich nicht auf diese Vorgaben, sondern enthält auch erweiterte Eingriffsbefugnisse der Polizei z. B. zum Einsatz von Kennzeichenerkennungssystemen. Außerdem sind in dem Artikelgesetz Änderungen des Verfassungsschutzgesetzes (8.1), des Thüringer Gesetzes zur Ausführung des Artikel 10-Gesetzes und des Thüringer Sicherheitsüberprüfungsgesetzes vorgesehen.

Nach dem Gesetzesvorschlag sollen Angaben, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, bei der Wohnraumüberwachung (sog. Großer Lauschangriff; § 35 PAG) und den sonstigen

verdeckten Ermittlungsmaßnahmen (§ 34 PAG) einem absoluten Erhebungsverbot sowie einem weitreichenden Verwertungsverbot unterliegen. Damit würden die Vorgaben des Bundesverfassungsgerichts weitgehend umgesetzt, wenn auch mit einer nur schwer verständlichen Gesetzesformulierung. Die zu diesem Regelungsvorschlag teilweise geäußerte Kritik, dass bestimmte Gruppen von Berufsgeheimnisträgern (z. B. Geistliche und Strafverteidiger) gegenüber anderen Berufsgeheimnisträgern (z. B. Journalisten und Parlamentarier) ohne sachlichen Grund benachteiligt werden, kann jedenfalls aus datenschutzrechtlichen Erwägungen nicht geteilt werden, weil dieses Erhebungs- und Verwertungsverbot ausnahmslos für alle Berufsgeheimnisträger gilt. Unterschiedlich behandelt werden Fälle, in denen über bevorstehende Straftaten oder Gefahren für hochrangige Rechtsgüter gesprochen wird. Hier ist der Kernbereich nach der Rechtsprechung des Bundesverfassungsgerichts gar nicht betroffen. Wird also über geplante Straftaten gesprochen, dann darf ein solches Gespräch in Wohnungen heimlich abgehört werden, jedenfalls solange nicht über Intimes gesprochen wird. Weil aber Strafverteidiger oder auch Geistliche naturgemäß häufiger als andere Berufsgeheimnisträger über Straftaten mit den Betroffenen sprechen, sollen Gespräche mit diesem Personenkreis in Wohnungen oder Geschäftsräumen generell von der Wohnraumüberwachung ausgenommen werden, selbst dann, wenn der Kernbereich privater Lebensgestaltung nicht betroffen ist. Diese Argumentation ist nachvollziehbar. Auch wenn es wünschenswert erschiene, alle Berufsgeheimnisträger gleich zu behandeln, geht es hier nicht um eine Benachteiligung der einen, sondern um eine teilweise Privilegierung bestimmter anderer Berufsgeheimnisträger, die von der Rechtsprechung des Bundesverfassungsgerichts nicht verlangt wird.

Der Kernbereichsschutz ist aber bei dem Änderungsvorschlag zur präventiven Telekommunikationsüberwachung (§ 34a PAG) nicht umfassend gewährleistet. Hier soll zunächst der Telefonverkehr aufgezeichnet werden und erst bei der Auswertung ein Verwertungsverbot festgestellter kernbereichsrelevanter Daten greifen. Es wird also bewusst in Kauf genommen, dass auch kernbereichsrelevante Gesprächsinhalte erhoben werden. Genau das widerspricht dem vom Bundesverfassungsgericht vorgegebenen absoluten Erhebungsverbot. Im Gegensatz zur Wohnung, bei der die Vermutung sehr viel größer ist, dass bei Gesprächen von miteinander vertrauten Personen der Kernbereich betroffen ist, kann man das sicher nicht von vorneherein bei einem Telefonat prognostizieren. Um den Vorgaben des Bundes-

verfassungsgerichts nachzukommen, müssen aber auch solche Vorkehrungen in das Gesetz aufgenommen werden, damit es bei vorhersehbaren Gesprächen mit Kernbereichsrelevanz erst gar nicht zu einer Datenerhebung kommt.

Bei allen drei Befugnisnormen (§§ 34, 34a und 35 PAG) ist zudem kein absolutes, sondern nur ein relatives Verwertungsverbot kernbereichsrelevanter Daten vorgesehen. Danach dürften diese Daten zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person verwendet werden. Begründet wird das damit, dass unmittelbare Gefährdungen hochwertiger Rechtsgüter wie Leib und Leben es rechtfertigen, dass auch der in der Menschenwürde verankerte Kernbereich privater Lebensbereich angetastet wird. Das ist aber in Art. 1 Abs. 1 Satz 1 GG und Art. 1 Abs. 1 Satz 1 ThürVerf sehr klar anders geregelt, wenn es heißt: „Die Würde des Menschen ist unantastbar.“. Es darf daher weder eine Abwägung mit anderen Verfassungsgütern noch eine Abwägung nach Maßgabe der Verhältnismäßigkeitsprüfung stattfinden. Dementsprechend geht das Bundesverfassungsgericht auch davon aus, dass ein Eingriff in den Kernbereich privater Lebensgestaltung unzulässig ist. Zudem ist eine Situation, bei der unbeabsichtigt Intimitäten aufgezeichnet worden sind, die später zur Gefahrenabwehr benötigt werden, nicht vorstellbar. Betrifft das Gespräch nämlich die Gefahren oder die geplanten Straftaten, dann ist trotz der Vertraulichkeit der Gesprächsteilnehmer untereinander der Kernbereich privater Lebensgestaltung erst gar nicht betroffen.

Die in § 33a PAG („Datenerhebung durch Kennzeichenerkennungssysteme“) vorgesehene neue Eingriffsbefugnis ist problematisch und weckt Erinnerungen an ein umstrittenes Pilotprojekt am Rennsteigtunnel im Jahr 2003 (5. TB, 7.5 und unten 7.6). Die damals fehlende Rechtsgrundlage soll nunmehr im Polizeiaufgabengesetz geschaffen werden. An der geplanten Regelung ist besonders zu kritisieren, dass alle vorbeifahrenden Fahrzeuge erfasst werden, ohne dass die Betroffenen einen konkreten Anlass dafür geboten haben und zudem keine konkrete Gefahrenlage vorausgesetzt wird. Der Polizei soll es künftig erlaubt sein, mobil oder an Kontrollstellen die Kennzeichen aller vorbeifahrenden Kraftfahrzeuge zu erfassen und sie dann in Sekundenschnelle mit dem Fahndungsbestand oder anderen polizeilichen Dateien abzugleichen. Sofern kein Treffer festgestellt wird, sollen die erfassten Daten unverzüglich wieder gelöscht werden. Man könnte nun meinen, das wäre nicht so schlimm, weil es ja nur gesuchte Straftäter

betrifft. Aber weit gefehlt: Weil dieser Fahndungsbestand gesetzlich nicht definiert und damit nicht beschränkt ist, könnte die Polizei ganz nach ihrem Belieben interpretieren, welche Daten in den Fahndungsbestand aufgenommen werden oder mit welcher ihrer sonstigen Dateien sie die erfassten Kennzeichen abgleicht. So ließe es der Wortlaut zu, dass mit Dateien abgeglichen wird, in denen nur sehr geringfügige Regelübertretungen, wie z. B. Verkehrsordnungswidrigkeiten, gespeichert sind. Das wäre aber nicht mehr verhältnismäßig. Zweifelhaft ist außerdem, ob das Land überhaupt eine umfassende Gesetzgebungskompetenz für die geplante Kennzeichenerkennung besitzt. Sofern es um eine Fahndung nach Straftätern geht, liegt eine solche Kompetenz ausschließlich beim Bund.

In einer vom Innenausschuss des Thüringer Landtags durchgeführten Anhörung hatte der TLfD die Gelegenheit, seine Kritik an dem Gesetzentwurf zu erläutern. Bis zum Redaktionsschluss war noch nicht erkennbar, ob diese aufgegriffen wird. Wie es scheint, beeinflusst das Bundesverfassungsgericht nicht nur die Entstehungsphase des Gesetzes, sondern auch dessen Behandlung im Parlament. Offenbar nimmt man dort die Verfassungsbeschwerden gegen vergleichbare Regelungen zu Kennzeichenerkennungssystemen in den Polizeigesetzen von Hessen und Schleswig-Holstein sehr ernst, weshalb die weitere Behandlung des Gesetzes im Innenausschuss bis zu einer Entscheidung des Gerichts in dieser Sache im Frühjahr 2008 verschoben wurde.

Der Gesetzgeber ist aufgerufen, die Vorgaben des Bundesverfassungsgerichts zum Kernbereichsschutz vollständig umzusetzen. Eine Regelung zu Kennzeichenerkennungssystemen muss normenklar konkretisiert und soweit eingeschränkt werden, sodass keine unverhältnismäßige Verarbeitung von Daten Unverdächtiger erfolgt.

7.2 Verwaltungsvorschrift zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten durch die Polizei und die Gemeinden

Im Rahmen der Verwaltungsmodernisierung wurden vom Thüringer Innenministerium Ende 2006 mehrere Verwaltungsvorschriften zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten aus den Jahren 1991 und 1998 überarbeitet und zu einer neuen Verwaltungsvorschrift „Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Polizei und die Gemeinden“ zusammengefasst.

In diesem Zusammenhang wurde auch der TLfD um eine datenschutzrechtliche Prüfung sowie um Anregungen und Hinweise für die Neufassung von Regelungen gebeten. Im Ergebnis wurde für die Polizei und die Gemeinden eine umfassende Anleitung und Entscheidungshilfe erarbeitet, in der auch die sich in diesem Zusammenhang ergebenden datenschutzrelevanten Probleme ausführlich behandelt werden. Berücksichtigt wurden dabei im besonderen Maße Fragen der Erforderlichkeit und Verhältnismäßigkeit und deren praktische Umsetzung. In der Verwaltungsvorschrift werden die betreffenden Behörden nochmals ausdrücklich auf den obersten Grundsatz der Datenerhebung hingewiesen: der Erhebung der Daten beim Betroffenen. Erst wenn alle Möglichkeiten der Anhörung des Betroffenen mittels Anhörungsbogen, durch eine Vorladung oder ggf. durch das Aufsuchen ausgeschöpft sind, sollen die Ermittlungen bei anderen Behörden (z. B. Anforderung von Lichtbildern bei den Pass- und Melderegistern) oder öffentlichen Stellen erfolgen. Nur für den Fall, dass auch dies zu keinem befriedigenden Ergebnis führt, dürfen unter Beachtung der Verhältnismäßigkeit auch nicht öffentliche Stellen (z. B. Nachbarn oder Betriebsangehörige bei Firmenfahrzeugen) befragt werden. Hinsichtlich der Nutzung des Frontfotos werden die Ermittlungsbehörden verpflichtet, die Offenbarung von Daten unbeteiligter Dritter im Rahmen der Fahrerermittlung zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten grundsätzlich auszuschließen. Seit der Veröffentlichung der Verwaltungsvorschrift hat den TLfD keine weitere Anfrage oder Beschwerde zum Umgang mit personenbezogenen Daten bei der Verfolgung von Verkehrsordnungswidrigkeiten erreicht.

Verwaltungsvorschriften mit eindeutigen, rechtskonformen Handlungsanweisungen können einen wirksamen Beitrag zur Durchsetzung des Datenschutzes leisten.

7.3 Polizeiliche Datenverarbeitung bei der Fußball-WM 2006

Die Fußball-Weltmeisterschaft 2006 war im Rückblick betrachtet sicherlich ein großartiges Ereignis unter dem Motto „Die Welt zu Gast bei Freunden“. Gleichzeitig war dieses Großereignis aber auch eine enorme Herausforderung für die Sicherheitskräfte. Um die Sicherheit zu gewährleisten, haben die Behörden im Vorfeld der Fußballspiele eine große Zahl personenbezogener Daten verarbeitet. In diesem Kontext waren die Datenschutzbeauftragten des Bundes und der Länder sowohl beratend als auch kontrollierend tätig.

Ein Baustein des Sicherheitskonzeptes zur Fußball-WM 2006 war die Nutzung der Verbunddatei „Gewalttäter Sport“ des Informationssystems der Polizei von Bund und Ländern. Diese beim Bundeskriminalamt geführte Datei wird von den Polizeien des Bundes und der Länder gespeist und gleichzeitig für Abrufe genutzt. Zweck der Datei ist es, solche Personen zu erfassen, die bei gewalttätigen Ausschreitungen im Zusammenhang mit Sportveranstaltungen in Erscheinung getreten sind, um künftige Gewalttaten zu verhindern. Neben den Personalien und bislang begangenen Straftaten sind auch Maßnahmen der Gefahrenabwehr wie Personalienfeststellung, Platzverweise, Ingewahrsamnahme oder Beschlagnahme von Waffen erfasst, aber nur, wenn eine Prognose ergibt, dass der Betroffene künftig Straftaten von erheblicher Bedeutung begehen wird. Vor der Fußball-Weltmeisterschaft wurde Anfang 2006 eine Kontrolle bei der Polizeiinspektion Erfurt-Süd vorgenommen. Hier arbeiten die sog. szenekundigen Beamten, die sich insbesondere um die Fans von Rot-Weiß-Erfurt kümmern. Bei den dort stichprobenartig eingesehenen Fällen konnte nach Erläuterung durch den zuständigen Sachbearbeiter die Prognose, die zur Aufnahme der Fälle in die Datei führte, nachvollzogen werden. Allerdings war hier die Dokumentation unzureichend. Dies hätte z. B. im Krankheitsfall oder beim Wechsel des zuständigen Sachbearbeiters dazu geführt, dass die Voraussetzungen zur Rechtmäßigkeit der Aufnahme des Falles nur schwer überprüft werden könnten. Deshalb wurde die Polizei aufgefordert, eine zusammengefasste Dokumentation der tatsächlichen Grundlagen sowie der Prognoseentscheidung vorzunehmen, was auch geschehen ist.

Festgestellt wurde noch ein weiteres Problem: In einem Freitextfeld war die Aufforderung enthalten „Bei Antreffen schriftliche Info an die szenekundigen Beamten Erfurt, Fax 0361/….“. Das hatte zur Folge, dass bei jeder zufälligen Kontrolle, auch ohne jeden Bezug zu Sportveranstaltungen (z. B. Grenzkontrollstelle bei einer Urlaubsfahrt), eine schriftliche Information von der kontrollierenden Dienststelle an die Polizeiinspektion Erfurt-Süd geschickt und dort in den Vorgang abgeheftet wurde. Bei der Kontrolle räumten die Beamten ein, dass sie mit dieser Information für ihre Aufgabenerfüllung nichts anfangen können. Dieses Verfahren entspricht jedoch exakt demjenigen bei einer Ausschreibung zur polizeilichen Beobachtung nach § 37 PAG. Danach kann die Polizei unter sehr engen Voraussetzungen Personen in das Informationssystem der Polizei einstellen. Bei jedem Antreffen durch die Polizei bundesweit erfolgt dann eine Rückmeldung an die

ausschreibende Polizeidienststelle. Dadurch kann ein umfassendes Bewegungsprofil der Betroffenen entstehen. Deshalb ist eine solche Maßnahme nur bei der Gefahr der künftigen Begehung von besonders schweren Straftaten und auch nur durch Anordnung des Dienststellenleiters möglich. Diese Voraussetzungen lagen bei den kontrollierten Stichproben nicht vor. Deshalb wurde die PD Erfurt aufgefordert, diesen Rückmeldevermerk nur in denjenigen Fällen in der Datei zu belassen, in denen diese strengen materiellen und formellen Anforderungen erfüllt sind. Erst nach längerer Prüfung unter Einbeziehung des Thüringer Innenministeriums wurde die Einordnung dieses Vermerks als polizeiliche Beobachtung nach § 37 PAG akzeptiert und sämtliche Polizeibehörden angewiesen, derartige Vermerke ausschließlich unter den Voraussetzungen des § 37 PAG vorzunehmen.

Weiterer wichtiger Baustein des Sicherheitskonzepts war das Akkreditierungsverfahren, bei dem alle Personen, die Zugang zu besonders geschützten Bereichen der Stadien hatten (z. B. Pressevertreter, Ordner, Caterer, private Sicherheitsdienste), eine Sicherheitsüberprüfung durch die Polizei- und Verfassungsschutzbehörden durchlaufen mussten. Dazu wurde von der FIFA bei der Antragstellung die Einwilligung der Betroffenen eingeholt. Zu einer weiteren Mitwirkung der Betroffenen kam es danach regelmäßig nicht, sondern es wurde allein auf der Grundlage des Abgleichs mit den Dateien der Sicherheitsbehörden eine sicherheitsbehördliche Empfehlung (Zustimmung oder Ablehnung) gegenüber der FIFA erteilt. Die im letzten Tätigkeitsbericht (6. TB, 7.7) berichteten Unzulänglichkeiten sind nur zum Teil ausgeräumt worden. So wurde in den Datenschutzhinweisen zumindest transparent gemacht, dass auch der Verfassungsschutz beteiligt wird sowie die Betroffenen sich zur Ausübung ihrer Datenschutzrechte an die zuständigen Datenschutzbeauftragten wenden können. Letztlich nicht geklärt werden konnte die unterschiedliche Auffassung zur Erforderlichkeit einer gesetzlichen Rechtsgrundlage zur Beteiligung des Verfassungsschutzes an derartigen Zuverlässigkeitsüberprüfungen. Allein die Einwilligung der Betroffenen in das Verfahren kann eine fehlende gesetzliche Aufgabenzuweisung zur Mitwirkung des Verfassungsschutzes an derartigen Überprüfungsverfahren nicht ersetzen. Letztlich hat die Mehrheit der Datenschutzbeauftragten diese Verfahrensweise wegen des Ausnahmecharakters dieses Großereignisses akzeptiert.

Eine stichprobenartige Kontrolle des Verfahrens beim Thüringer Landeskriminalamt hat ergeben, dass Ablehnungsempfehlungen eher zurückhaltend ausgesprochen wurden und auch das Verfahren ordnungsgemäß abgewickelt worden ist. So wurden insgesamt 1.567 Datensätze von der Zentralstelle beim Bundeskriminalamt zur Überprüfung an das Thüringer Landeskriminalamt übermittelt, von denen in 42 Fällen eine Ablehnungsempfehlung (etwa 2,7 %) gegenüber der FIFA ausgesprochen wurde. Treffer in den polizeilichen Dateien gab es jedoch weit mehr als die 42 abgelehnten Fälle. Das zeigt, dass hier in jedem Einzelfall abgewogen wurde, ob die vorhandenen Daten eine solche Ablehnung rechtfertigen. So wurde in jedem Trefferfall telefonisch Kontakt mit dem zuständigen Sachbearbeiter aufgenommen oder die Akten zur Beurteilung herangezogen. Positiv ist hervorzuheben, dass die Ablehnungsentscheidungen ausführlich und nachvollziehbar dokumentiert waren, was leider nicht in allen Bereichen der Polizeiarbeit selbstverständlich ist (siehe oben und 10.3). In einem Fall hatte sich der Betroffene, der in der Datei „Gewalttäter Sport“ enthalten war, mit Erfolg gegen die Ablehnung gewandt. Diese Eintragung war fast fünf Jahre alt und lag damit kurz vor der Löschungsfrist.

Weil sich das Verfahren aus Sicht der Sicherheitsbehörden bewährt hatte, kam es jedoch auch nach der Fußball-Weltmeisterschaft 2006 bei anderen Anlässen wie dem Papst-Besuch in Bayern oder dem G-8-Gipfel in Heiligendamm zum Einsatz. Da damit eine Tendenz erkennbar wurde, dieses Verfahren als Standardmaßnahme allein auf der Basis von Einwilligungen zu etablieren, haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 18) nochmals deutlich gemacht, dass derartige Verfahren wegen des damit verbundenen Eingriffs in Grundrechte nicht allein auf der Basis von Einwilligungserklärungen durchgeführt werden können.

Ob derartige Zuverlässigkeitsüberprüfungen bei Großveranstaltungen überhaupt in dieser Form erforderlich sind, ist nach wie vor zweifelhaft. Sollen sie gleichwohl weiterhin erfolgen, muss hierzu eine normenklare, aber auch verhältnismäßige gesetzliche Regelung geschaffen werden.

7.4 Löschung von Daten im Informationssystem der Polizei

Seit einiger Zeit beschäftigen sich die Datenschutzbeauftragten des Bundes und der Länder mit der Frage, wann Datensätze zu erkennungsdienstlichen Behandlungen (v. a. Nachweis über vorhandene Fingerabdrücke und Lichtbilder) im Informationssystem der Polizeien des Bundes und der Länder beim Bundeskriminalamt zu löschen sind. Eigentlich gibt es hierzu klare Vorgaben im Bundeskriminalamtgesetz. Bei den vom Bundeskriminalamt geführten sog. Verbunddateien trägt nach § 12 Abs. 2 BKAG für die bei der Zentralstelle gespeicherten Daten diejenige Behörde die datenschutzrechtliche Verantwortung, die die Daten eingegeben hat. Diese Stelle trifft nach § 32 Abs. 9 BKAG auch die Pflicht zur Löschung der Daten. Wurde also ein Datensatz über eine erkennungsdienstliche Behandlung durch eine Thüringer Polizeibehörde in die Verbunddatei eingegeben, dann ist dieser Datensatz auch nach den Vorgaben der eingebenden Stelle vom Bundeskriminalamt wieder zu löschen, spätestens dann, wenn die zugehörige Kriminalakte vernichtet wurde. Hier nimmt das Bundeskriminalamt nun einen Kunstgriff vor, für den es keine Rechtsgrundlage im Bundeskriminalamtgesetz gibt. Mit der Eingabe der Daten in die Zentraldatei geht das Bundeskriminalamt von einer sog. „Besitzübernahme“ der Daten aus. Danach soll der Besitz der Daten nun beim Bundeskriminalamt liegen und das anliefernde Landeskriminalamt nur noch Mitbesitz an dem Datensatz haben. Dies hat dann zur Folge, dass das Bundeskriminalamt ab diesem Zeitpunkt eine eigene Prüffrist zur Löschung (in der Regel 10 Jahre) vergibt, die teilweise länger als die Löschfrist des Landes ist.

Bei einer Stichprobenkontrolle im Thüringer Landeskriminalamt hat sich dieser Umstand bestätigt. So wurden Datensätze festgestellt, die ursprünglich vom Thüringer Landeskriminalamt in das System eingegeben worden waren und nach deren Löschung in den Landesdateien weiterhin vom Bundeskriminalamt im Verbundsystem zum bundesweiten Abruf durch die Polizeibehörden bereitgehalten werden. Dieser Befund wurde dem BfDI mitgeteilt und um eine Prüfung gebeten. Bislang hat der BfDI jedoch noch keine Änderung dieser Praxis erreichen können (vgl. auch 21. TB des BfDI, 5.2.4.1).

Die Löschung der von der Thüringer Polizei im Verbundsystem INPOL eingegebenen Daten muss in allen Fällen umgesetzt werden.

Dazu muss das Bundeskriminalamt zu einem gesetzmäßigen Umgang mit Daten aus den Ländern veranlasst werden.

7.5 Polizeiliche Auskünfte an Wohnungsunternehmen ohne Rechtsgrundlage

Eine zu unbürokratische Verhaltenweise hat die Polizeiinspektion Jena an den Tag gelegt, als sie auf eine Anfrage eines städtischen Wohnungsunternehmens diesem polizeiliche Erkenntnisse zu Mitarbeitern eines von ihm beauftragten privaten Sicherheitsdienstes übermittelte. Hintergrund waren Beschwerden von Mietern, wonach Mitarbeiter des Sicherheitsdienstes in Straftaten verwickelt seien. Dies führte dazu, dass das Wohnungsunternehmen den Vertrag mit dem Sicherheitsdienst kurzfristig kündigte. Als der Sicherheitsdienst gegen die Kündigung des Vertrags gerichtlich vorging, sah sich das Wohnungsunternehmen offenbar in Beweisschwierigkeiten hinsichtlich der Unzuverlässigkeit der Mitarbeiter des Unternehmens. Die im Rahmen einer Sicherheitspartnerschaft zwischen Wohnungsunternehmen, Ordnungsamt und Polizei bestehenden guten persönlichen Kontakte wurden von dem Wohnungsunternehmen genutzt, um von der Polizeiinspektion Jena unbürokratisch zu erfahren, in welchen Fällen von angezeigten Straftaten gegen Mitarbeiter des Sicherheitsdienstes ein Strafverfahren eingeleitet wurde und welche Verfahren mit einer Verurteilung beendet worden sind. Dieser Anfrage kam die Polizeiinspektion umfassend nach und teilte dem Unternehmen eine Liste mit insgesamt 26 Tatvorwürfen zu drei Mitarbeitern des Sicherheitsdienstes mit, die zum Teil weder die Justizaktenzeichen noch den Verfahrensausgang enthielten und damit mehr Vermutungen aussprachen als Klarheit zu erbringen. Zudem teilte die Polizeiinspektion mit, dass Verwechslungen nicht ausgeschlossen werden könnten, da weder Geburtstag und –ort noch die Anschrift der Betroffenen bekannt sei.

Eine Überprüfung hat ergeben, dass es für eine solche Datenübermittlung keine Rechtsgrundlage im Polizeiaufgabengesetz gibt. Nach § 41 Abs. 3 Satz 2 PAG dürfen personenbezogene Daten an private Dritte nur übermittelt werden, wenn es zur Erfüllung polizeilicher Aufgaben oder zur Beseitigung erheblicher Nachteile für das Gemeinwohl oder schutzwürdiger Belange einzelner erforderlich ist. Beides lag hier nicht vor, da es nicht Aufgabe der Polizei ist, die Zuverlässigkeit des Personals von Sicherheitsdiensten zu überprüfen. Zu einer solchen Sicherheitsüberprüfung ist auch das städtische Wohnungsunternehmen

nicht befugt. Vielmehr hat die Zuverlässigkeit von Personal im Bewachungsgewerbe das Ordnungsamt anhand gesicherter und umfassender Erkenntnisse aus dem Bundeszentralregister nach § 9 Bewachungsverordnung zu überprüfen. Dieses war hier aber gar nicht beteiligt worden. Erschwerend kam bei dieser Datenübermittlung hinzu, dass neben der Weitergabe von ungesicherten Erkenntnissen sich die Polizeiinspektion keine Gewissheit über die Identität der Personen verschafft hat, zu denen die Auskünfte erteilt wurden. Diese Verletzung datenschutzrechtlicher Vorschriften wurde formell nach § 39 Abs. 1 ThürDSG beanstandet und die Stelle neben den bereits eingeleiteten disziplinarischen bzw. strafrechtlichen Maßnahmen aufgefordert, durch organisatorische Maßnahmen eine Wiederholung einer solchen Datenübermittlung auszuschließen. Neben einer Auswertung und Schulung der Mitarbeiter zu den Datenübermittlungsnormen wurde daraufhin festgelegt, dass künftig vor einer Übermittlung personenbezogener Daten an andere Behörden und privaten Stellen nach § 41 Abs. 3 PAG das Einvernehmen mit dem behördeninternen Datenschutzbeauftragten hergestellt werden soll. Das ebenfalls der Kontrolle des TLfD unterliegende städtische Wohnungsunternehmen hat erst nach Erteilung rechtlicher Hinweise eingesehen, dass auch die Erhebung dieser Daten unzulässig war.

Obwohl in der Dienststelle angemessene Maßnahmen zur Einhaltung datenschutzrechtlicher Vorschriften eingeleitet wurden gibt der Fall Anlass, in der Thüringer Polizei insgesamt solchen Übermittlungen polizeilicher Erkenntnisse an andere Behörden und Stellen zur „Erhöhung der Sicherheit“ größere Aufmerksamkeit in der Fortbildung zu schenken.

7.6 Verkehrsüberwachungstechniken in den Autobahntunneln

Bereits im 6. TB (7.8) wurde über die an der Tunnelkette der Bundesautobahn 71 eingesetzte Abstands- und Geschwindigkeitsüberwachungsanlage berichtet. Damals ging es um zunächst nicht vorhandene technisch-organisatorische Regelungen, die nachgebessert worden sind. Ausgangspunkt war ein Testbetrieb zur automatisierten Kennzeichenerkennung, der im Jahr 2003 mangels einer Rechtsgrundlage im Polizeiaufgabengesetz gestoppt werden musste. Der im Landtag diskutierte Entwurf einer Novelle der Sicherheitsgesetze (7.1) enthält nun einen Vorschlag für eine solche Rechtsgrundlage.

Nachdem man mit einer anlassunabhängigen Videoüberwachung, die alle Autofahrer erfasst hätte, nicht erfolgreich war, wurde im Anschluss daran ein entgegengesetzter und richtiger Ansatz gewählt. Die neue Videoüberwachungstechnik sollte nur dann zum Einsatz kommen, wenn sich Verkehrsteilnehmer regelwidrig verhalten und auch nur so viel erfassen, wie unbedingt zur Prüfung und Ahndung dieses Regelverstoßes notwendig ist. Die anderen sich rechtskonform verhaltenden Verkehrsteilnehmer sollen nur in dem unbedingt erforderlichen Umfang erfasst werden.

Dieser Ansatz wurde sehr konsequent verfolgt, indem im Vorfeld des Tunnels „Alte Burg“ jeweils in der einfahrenden Fahrtrichtung drei Arten von Kameras mit unterschiedlichen Aufgaben installiert wurden. Die erste Kamera (Selektionskamera) lässt den Blick am weitesten in die Ferne schweifen und beobachtet den allgemeinen Verkehr. Stellt sie aufgrund der voreingestellten Werte fest, dass sich ein Fahrzeug zu schnell oder in zu geringem Abstand zum vorausfahrenden Fahrzeug nähert, dann aktiviert sie die Aufzeichnung der zweiten Kamera (Tatkamera), die das Tatgeschehen erfassen soll. Für beide Kameras wird eine Auflösung verwendet, die zwar das Fahrzeug eindeutig erkennen lässt und das Tatgeschehen beweissicher erfasst, jedoch vorerst weder das Kennzeichen noch den Fahrer identifiziert. Das ist erst nach einem weiteren Verfahrensschritt möglich. Dabei zeichnet zum Abschluss die dritte Kamera (Identkamera) gesondert auf der jeweiligen Fahrspur das Fahrzeug in der Nahaufnahme auf, um Kennzeichen und Fahrer erkennen und feststellen zu können.

Bei der Auswertung wird nun durch einen Beamten zuerst überprüft, ob der automatisch aufgezeichnete Vorgang tatsächlich eine vorwerfbare Regelverletzung darstellt. So könnten die Fahrer z. B. reagiert und abgebremst haben oder der Ablauf auf dem Video zeigt, dass das hintere Fahrzeug den geringen Abstand gar nicht verursacht hat, sondern ein Fahrzeug vor ihm in die Lücke gestoßen ist. Ist das Ergebnis negativ, dann kommt es gar nicht zu einem Ordnungswidrigkeitenverfahren. Eine Zuordnung des Videos mit dem Kennzeichen ist nicht notwendig und die Daten werden wieder gelöscht. Erst wenn sich der Verdacht erhärtet hat, wird durch die Zusammenführung des Tatvideos mit dem Video der Identkamera eine Zuordnung zu einer konkreten Person vorgenommen. Damit wird hier durch den intelligenten Einsatz der Technik eine Erfassung und auch Auswertung personenbezogener Daten vorbildlich auf das unbedingt erforderliche Maß beschränkt.

Die Verarbeitung solcher Bildaufnahmen zur Verfolgung von Verkehrsverstößen ist hier durch § 46 Abs. 1 OWiG i. V. m. § 100f Abs. 1 Nr. 1 StPO (ab 1. Januar 2008: § 100h Abs. 1 Nr. 1 StPO) gedeckt.

Dieser sehr restriktive Ansatz erwies sich aber im praktischen Einsatz insoweit zu eng, als die Identkameras nur mit der Tatkamera der jeweiligen Fahrspur gekoppelt waren. So kam es in sehr vielen Fällen vor, dass zwar die Tatkamera beweissicher den Geschwindigkeits- oder Abstandsverstoß dokumentiert hatte, das Fahrzeug danach aber kurzfristig die Fahrspur wechselte und damit die Identkamera ins „Leere“ filmte. Deshalb hat das Thüringer Innenministerium unter Beteiligung des TLfD einen Test durchgeführt, bei dem jeweils die Identkameras beider Fahrspuren synchron aktiviert wurden. Daraufhin hat sich die Zahl dieser Fälle deutlich verringert. Gegen diese geringfügige Erweiterung der Aufzeichnungsmöglichkeiten bestanden letztlich auch deswegen keine Bedenken, da auch hier nur auf Videosequenzen zugegriffen wird, bei denen ein konkreter Verdacht der Regelüberschreitung vorliegt.

Nach Fertigstellung der Einhausung der Bundesautobahn 4 bei Jena im Frühjahr 2007 entstand die Vermutung, dass auch hier ohne Freigabe Videoaufnahmen von Rasern gemacht werden könnten. Eine Nachfrage beim Thüringer Innenministerium ergab, dass in diesem Fall keine Videokameras, sondern Fotoapparate im Einsatz waren. Diese arbeiten mit einem Infrarotblitz, der kaum sichtbar ist. Das Fehlen eines Blitzlichtes führte bei Autofahrern offenbar zu der Vermutung einer Videoüberwachung, zumal auch zur Tunnelsicherheit zahlreiche Videokameras installiert sind, die aber nicht der Verkehrsüberwachung dienen. Richtig war allerdings, dass zur Einstellung der Geräte ein Testbetrieb ohne die erforderliche Errichtungsanordnung über einige Tage erfolgte. Das Thüringer Innenministerium reagierte umgehend und veranlasste die Behebung dieser formellen Mängel. Zudem wurden alle im Testbetrieb erhobenen Daten gelöscht. Im Vergleich mit dem im Jahr 2003 festgestellten Datenschutzverstoß im Rahmen des Testbetriebs zur Kennzeichenerkennung handelte es sich dabei um einen geringen Mangel. Damals fehlte neben der formellen Voraussetzung einer Freigabe auch jegliche Rechtsgrundlage für eine Datenerhebung, die bei normalen Geschwindigkeitsmessgeräten unzweifelhaft vorliegt.

Neue technische Ermittlungsmethoden können auch so ausgestaltet werden, dass die Rechte Unbeteiligter nicht unverhältnismäßig beeinträchtigt werden. Dazu sollte jedoch auch ein (lohnender) zusätzlicher Aufwand in Kauf genommen werden.

7.7 Einsatz von Videotechnik zur Verfolgung von Rotlichtverstößen

Ende 2005 wandte sich ein Rechtsanwalt an den TLfD, weil er Zweifel daran hatte, ob die von der Polizei verwendete Videotechnik zur Verfolgung von Rotlichtverstößen rechtmäßig zum Einsatz kam. Seinem Mandanten wurde vorgeworfen, eine Ampel bei Rot überfahren zu haben. Als Beweismittel diente eine Videoaufzeichnung, von der der Anwalt bei einer Akteneinsicht eine Kopie erhalten hatte. Stutzig machte ihn dabei, dass nach dem dokumentierten Rotlichtverstoß seines Mandanten das Band noch einige Sekunden weiterlief, als die Ampel schon wieder auf Grün geschaltet war. Nach Sichtung des Bandausschnitts war nicht klar, ob hier möglicherweise länger aufgezeichnet wurde, als erforderlich und damit auch zulässig.

Ein Kontrollbesuch bei der Verkehrspolizeiinspektion Jena hat dies nicht bestätigt. Hier konnte folgende Verfahrensweise festgestellt werden: Zwei mobile Videokameras sind in Fahrtrichtung und in der Gegenrichtung an der Ampel aufgestellt, um das Geschehen einschließlich der Ampel zu erfassen. Der Beamte vor Ort aktiviert jeweils nach der Umschaltung der Ampel von Grün auf Gelb die Aufzeichnung. Kommt der Verkehr an der Haltelinie zum Stehen, wird die Aufzeichnung manuell sofort beendet. Fahren jedoch ein oder mehrere Fahrzeuge bei Rot über die Ampel, dann wird die Aufzeichnung erst dann beendet, wenn die Ampel wieder auf Grün geschaltet hat. Bei Rotlichtverstößen wird dann der entsprechende Videoausschnitt zur Fahrerermittlung und als Beweismittel gesichert. Kommt es zu keinem Rotlichtverstoß, wird die Videosequenz später gelöscht.

Damit ist sichergestellt, dass nur dann eine Aufzeichnung personenbezogener Daten erfolgt, wenn der Verdacht einer Verkehrsordnungswidrigkeit besteht. Rechtliche Grundlage hierfür ist § 46 Abs. 1 OWiG i. V. m. § 100f Abs. 1 Nr. 1 StPO (ab 1. Januar 2008: § 100h Abs. 1 Nr. 1 StPO), der Bildaufnahmen ohne Wissen der Betroffenen zulässt, wenn die Erforschung des Sachverhalts auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Dabei dürfen auch

die unvermeidbar betroffenen Personen miterfasst werden, z. B. Verkehrsteilnehmer auf der Gegenfahrbahn.

Die Kontrolle hat ergeben, dass die Nutzung von Videotechnik zur Verfolgung von Rotlichtverstößen aufgrund von Erfahrungen in anderen Bundesländern eingeführt wurde, da diese Technik zuverlässigere Ergebnisse liefere. Allerdings erstreckte sich die Errichtungsanordnung des Verfahrens nur auf die Verfolgung von Abstandsverstößen (7.6). Die Polizeidirektion Jena wurde daher aufgefordert, die Errichtungsanordnung an die tatsächliche Nutzung auch zum Zweck der Verfolgung von Rotlichtverstößen anzupassen. Zwar entsprach die bei der Kontrolle festgestellte Verfahrensweise inhaltlich datenschutzrechtlichen Anforderungen, war aber nicht schriftlich festgelegt. Deshalb wurde die Polizeidirektion Jena auch aufgefordert, begleitende organisatorische Regelungen zum Umgang mit personenbezogenen Daten in dem Verfahren zu erlassen. Diese Forderungen wurden daraufhin erfüllt. Da anzunehmen ist, dass auch andere Polizeidienststellen in Thüringen Videotechnik für Rotlichtverstöße einsetzen, wurde das Thüringer Innenministerium aufgefordert, diese Thematik in die Überarbeitung der Richtlinien für die polizeiliche Verkehrsüberwachung einzubeziehen. Bislang ist das noch nicht erfolgt.

Führen technische Weiterentwicklungen zu erweiterten Ermittlungsmöglichkeiten, ist zu prüfen, ob die gesetzlichen Grundlagen für daraus entstehende weitere Gefährdungen der Privatheit ausreichen. Selbst wenn das so ist, müssen jedoch die organisatorischen Regelungen zum Umgang mit personenbezogenen Daten angepasst werden. Das Thüringer Innenministerium sollte daher die angekündigte Überarbeitung der Richtlinie zügig abschließen.

7.8 Protokollierung von ZEVIS-Abfragen unzureichend

ZEVIS stellt ein wichtiges Instrument der Polizei bei der Gefahrenabwehr und Verfolgung von Ordnungswidrigkeiten und Straftaten dar. Weil aber bundesweit einem Großteil der Polizisten der Zugriff auf die dort gespeicherten Datensätze von ca. 50 Millionen Kfz-Haltern und derzeit über 23,2 Millionen Fahrerlaubnisinhabern (täglich erfolgen 70 000 Halter- und Fahrerlaubnisabfragen) ermöglicht wird, besteht auch das Risiko, dass die eine oder andere Anfrage unbefugt erfolgt. Weil eine unbefugte Abfrage technisch nicht verhindert werden kann, sieht das Straßenverkehrsgesetz neben der Grundprotokol-

lierung aller Abfragen beim Kraftfahrtbundesamt auch eine Zusatzprotokollierung vor, bei der der Anlass des Abrufs und Angaben festgehalten werden, die es ermöglichen, die für den Abruf verantwortliche Personen festzustellen. Damit soll insbesondere eine nachträgliche Datenschutzkontrolle ermöglicht werden. Dass dies in der Praxis zu Problemen führen kann, zeigt folgender Fall.

Eine Petentin bekam einen Anruf, mit dem sich eine Verkehrsteilnehmerin über ihre verschmutze Kleidung beschwerte und die Reinigungskosten ersetzt haben wollte. Eine Stunde zuvor hatte die Petentin offenbar im Vorbeifahren die Betreffende nass gespritzt. Auf ihre verwunderte Nachfrage, woher sie ihre Daten habe, antwortete sie, sie habe eben gute Freunde bei der Polizei. Die Überprüfung über den BfDI beim Kraftfahrtbundesamt ergab tatsächlich zum fraglichen Zeitpunkt eine Abfrage im ZEVIS. Über das Thüringer Landeskriminalamt als Zentralstelle für die polizeiliche Datenverarbeitung wurde dann die weitere Überprüfung veranlasst. Dort wurde zunächst ermittelt, welcher Polizeidienststelle und welchem Beamten zum Abrufzeitpunkt die Kennung zugeordnet war. Dabei stellte sich heraus, dass die Kennung einer von der Thüringer Bereitschaftspolizei zur Unterstützung der Polizeiinspektion Erfurt-Nord zugewiesenen Beamtin zugeordnet war. Bei der Befragung der Beamtin konnte sich diese nicht mehr an das abgefragte Kennzeichen erinnern. Das war auch nicht verwunderlich, weil sie an diesem Tag zusammen mit einem Kollegen als „Abfragebeamtin“ sämtliche Datenabfragen im Rahmen eines geschlossenen Einsatzes für 35 Beamte der Bereitschaftspolizei erledigte. Außer der Aufzeichnung des Funkverkehrs zu diesem Einsatz, der zum Zeitpunkt der Überprüfung bereits gelöscht war (Aufbewahrungsfrist 3 Monate), sind keine Aufzeichnungen dokumentiert worden, welcher der Einsatzbeamten welche Daten zur Abfrage an die Abfragebeamtin übermittelte und aus welchem Grund. Mit dieser unzureichenden Protokollierung war es also nicht möglich, die mit der Petition aufgeworfene Frage abschließend zu klären, ob die tatsächlich erfolgte Abfrage der Daten der Petentin rechtlich zulässig war. Nach den hierzu vorliegenden Fakten erscheint das mehr als zweifelhaft. Deshalb ist der TLfD noch mit dem Thüringer Innenministerium im Gespräch, die Protokollierung von solchen Sammelabfragestellen so zu verbessern, dass eine effektive Kontrolle der Rechtmäßigkeit der Abrufe auch tatsächlich möglich ist.

Anlass zur Kritik gab in diesem Fall auch die Art und Weise, wie von Seiten der Polizeibehörden die datenschutzrechtliche Überprüfung betrieben wurde. Obwohl sich die Petentin auch mit einer Anzeige an die Polizeidirektion Erfurt gewandt hatte, wurden dort die durch den TLfD veranlassten Ergebnisse der Protokolldatenabfrage beim Kraftfahrtbundesamt nicht in das zwischenzeitlich gegen unbekannt eingeleitete Ermittlungsverfahren einbezogen. Man bemühte sich offenbar nicht sehr intensiv um eine Zuordnung des Datenabrufs zu einem konkreten Beamten, weil eine solche Abfrage - selbst wenn sie stattgefunden hätte - als zulässig angesehen worden ist. Daher hat die Staatsanwaltschaft Erfurt das Ermittlungsverfahren eingestellt. Da die Begründung der Einstellungsverfügung bei Redaktionsschluss noch nicht vorlag, kann dieser Einzelvorgang noch nicht abschließend bewertet werden.

Abfragen aus dem ZEVIS darf die Polizei nicht durchführen, um die Daten anschließend an Dritte weiterzuleiten, die einen möglichen Schadensersatzanspruch gegen den Kfz-Halter haben. Auch wenn das vielleicht bürgerfreundlich erschiene, so ist dazu nach § 39 Abs. 1 StVG allein das Kraftfahrtbundesamt oder die Kfz-Zulassungsstelle befugt. Zu diesem Ergebnis könnte man aber auch schon durch einen Blick in § 32 Abs. 1 Nr. 2 i. V. m. § 2 Abs. 2 PAG gelangen, worauf sich die Polizei allerdings unzutreffend als Rechtfertigung für die Abfrage berief. Danach darf die Polizei nur dann personenbezogene Daten zum Schutz privater Rechte erheben, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und ohne polizeiliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert würde. Hier ist nicht im Ansatz erkennbar, weshalb die Geschädigte ihre möglichen Schadensersatzansprüche nur durch polizeiliche Hilfe hätte durchsetzen können. Eine Auskunft über die Kfz-Halterin hätte sie bei der Kfz-Zulassungsstelle sicherlich auf der Grundlage von § 39 Abs. 1 StVG erhalten, allerdings wohl nur gegen Zahlung einer Verwaltungsgebühr!

Die Protokollierungen von ZEVIS-Abfragen durch die Thüringer Polizei müssen künftig in der Weise erfolgen, dass in allen Fällen eine datenschutzrechtliche Kontrolle möglich ist. Der TLfD wird sich in seiner Kontrolltätigkeit dieser Problematik verstärkt annehmen.

8. Verfassungsschutz

8.1 Änderung des Thüringer Verfassungsschutzgesetzes

Mit einem im Landtag eingebrachten Entwurf eines Artikelgesetzes (Thüringer Gesetz zur Änderung sicherheits- und verfassungsschutzrechtlicher Vorschriften) sollen außer im Polizeiaufgabengesetz (7.1) auch im Thüringer Verfassungsschutzgesetz die Vorgaben des Bundesverfassungsgerichts zum Kernbereichsschutz umgesetzt werden. Hierzu wurde von der Landesregierung vorgeschlagen, auf die Wohnraumüberwachung zu verzichten. Die Landesregierung ist dabei der Auffassung, dass damit die Anforderungen zum Kernbereichsschutz im Bereich des Verfassungsschutzes umgesetzt sind. Das ist jedoch nicht der Fall: Nach § 7 Abs. 1 i. V. m. § 6 Abs. 1 ThürVSG hat das Landesamt für Verfassungsschutz die Befugnis, durch heimliche Maßnahmen wie Bild- und Tonaufzeichnungen auch personenbezogene Daten verdeckt zu erheben. Auch wenn dies nicht in der Wohnung des Betroffenen erfolgt, handelt es sich doch um eine verdeckte Datenerhebung, bei der nach der Rechtsprechung des Bundesverfassungsgerichts Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung getroffen werden müssen. Selbst wenn eine private Unterhaltung z. B. auf einer Parkbank mit Vertrauten nicht dieselbe Vertraulichkeitserwartung wie innerhalb einer Wohnung auslöst, so handelt es sich auch nicht um ein öffentlich gesprochenes Wort, bei dem keinerlei Vorkehrungen zum Kernbereichsschutz zu treffen wären. Deshalb muss der Entwurf insoweit nachgebessert werden.

Der Entwurf sieht außerdem die Übernahme der Vorschriften des Terrorismusbekämpfungsergänzungsgesetzes in das Landesrecht vor. Gegen die Beibehaltung und Erweiterung der Befugnisse der Verfassungsschutzbehörden auf Bundesebene haben sich die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 8) ausgesprochen. Kritisiert wurde dabei insbesondere, dass keine wirkliche Evaluierung der Vorschriften durch eine unabhängige Stelle vorgenommen wurde. Daher wurde dem Innenausschuss des Landtags in der durchgeführten Anhörung empfohlen, zumindest eine solche unabhängige Evaluierung in das Verfassungsschutzgesetz aufzunehmen. Bis zum Redaktionsschluss war noch nicht erkennbar, ob die Änderungsanregungen durch den Thüringer Landtag aufgegriffen werden.

Der Gesetzgeber sollte dafür sorgen, dass auch im Thüringer Verfassungsschutzgesetz die Vorgaben des Bundesverfassungsgerichts zum Schutz des Kernbereichs privater Lebensgestaltung umgesetzt werden. Darüber hinaus ist eine unabhängige Evaluierung der zusätzlichen Befugnisse des Verfassungsschutzes vorzusehen.

8.2 Antiterrordatei

Lange wurde kontrovers darüber diskutiert, ob zur Aufklärung und Bekämpfung des internationalen Terrorismus erstmals in Deutschland eine gemeinsame Datei von Polizei und Nachrichtendiensten eingerichtet werden sollte. Mit dem Antiterrordateigesetz vom 22. Dezember 2006 wurde die gesetzliche Grundlage für diese Datei nun geschaffen. Der Betrieb beim Bundeskriminalamt startete am 30. März 2007 unter Beteiligung von Stellen der Polizeien und Nachrichtendienste des Bundes und der Länder, darunter auch das Thüringer Landeskriminalamt und das Thüringer Landesamt für Verfassungsschutz. Es ist nachvollziehbar, dass sowohl Polizei als auch Nachrichtendienste in die Lage versetzt werden sollen, solche Erkenntnisse über Terrorverdächtige auszutauschen, die in den jeweiligen Dienststellen bereits vorliegen, um sich nach möglichen Anschlägen nicht vorwerfen zu lassen, es seien nicht alle rechtlich zulässigen Aufklärungsmöglichkeiten ausgeschöpft worden. Dazu müssen die beteiligten Stellen jedoch wissen, dass es über solche Personen Erkenntnisse auch bei anderen Dienststellen gibt. Deshalb wäre aus datenschutzrechtlicher Sicht gegen eine reine Hinweis- bzw. Indexdatei auch nichts einzuwenden gewesen. Die jetzt eingeführte Regelung ist aber sehr viel weiter gefasst und in vielerlei Hinsicht verfassungsrechtlich bedenklich.

Hauptkritikpunkt ist die Beeinträchtigung des in Art. 97 Satz 2 ThürVerf verankerten Gebots zur Trennung von Polizeibehörden und Verfassungsschutz (sog. Trennungsgebot). Danach stehen dem Landesamt für Verfassungsschutz keine polizeilichen Befugnisse und Weisungen zu. In § 5 Abs. 3 ThürVSG wird dies noch etwas präzisiert, wonach das Landesamt für Verfassungsschutz die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen darf, zu denen es selbst nicht befugt ist. Dabei handelt es sich nicht nur um eine organisatorische und rechtliche Trennung der Behörden, sondern auch um eine grundsätzlich getrennte Informationsverarbeitung. Der Datenaustausch muss so begrenzt werden, dass die organisatorische Trennung nicht durch

wechselseitige Unterstützung und Hilfsmaßnahmen umgangen wird. Deshalb darf der Verfassungsschutz Daten an die Polizei nur in engen Grenzen übermitteln, z. B. wenn sich ein konkreter Verdacht für bestimmte gravierende Straftaten ergeben hat. Die Nachrichtendienste dürfen im Gegensatz zu den Strafverfolgungsorganen auch ohne konkreten Verdacht für Straftaten mit verdeckten Ermittlungsmethoden Daten erheben und zudem auf Vorrat sammeln, deren Richtigkeit nicht unbedingt gesichert belegt sein muss. Diese Möglichkeiten haben die Nachrichtendienste u. a. nur deshalb erhalten, weil sie eben keine polizeilichen Befugnisse haben, um auf der Grundlage einer sehr vagen Datenlage gegen Einzelne vorzugehen. Könnte nun aber die Polizei ungehindert auf die Daten der Nachrichtendienste zugreifen, dann würde sie Informationen erhalten, zu deren Erhebung sie nach ihren gesetzlichen Grundlagen keinesfalls befugt wäre. In einer solchen Umgehung der Erhebungsvorschriften wäre eine Verletzung des Trennungsgebots zu sehen. Genau das ist aber bei dem sog. Eilfallzugriff vorgesehen. Hier darf die Polizei in der Antiterrordatei im Eilfall auf Daten der Nachrichtendienste zugreifen, ohne dass zuvor die einspeichernde Stelle, z. B. das Landesamt für Verfassungsschutz, prüfen kann, ob die Voraussetzungen für eine Übermittlung der Daten an die Polizei vorliegen.

Problematisch ist auch die vage Definition, wer als Terrorverdächtiger in die Datei aufgenommen werden darf, in welchem Umfang Kontaktpersonen in der Datei erfasst werden dürfen sowie die Aufnahme sog. Freitextfelder, bei denen der Umfang der in die Datei eingestellten Daten beliebig erweitert werden könnte. Auf diese Probleme haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 7) im Rahmen des Gesetzgebungsverfahrens hingewiesen. Berücksichtigt wurde lediglich eine Klarstellung, wonach Kontaktpersonen, die mit den Terrorverdächtigen nur flüchtig oder in zufälligem Kontakt in Verbindung stehen, nicht in die Datei aufgenommen werden dürfen.

In den an die Antiterrordatei angeschlossenen Thüringer Behörden hat der TLfD kurz nach der Aufnahme des Betriebs einen ersten Informationsbesuch durchgeführt. Wegen der Einstufung der Ausführungsvorschriften als Verschlusssache können hier nur einige allgemeine Ausführungen gemacht werden. Vom Bundesministerium des Innern wurde lediglich die beim Start der Antiterrordatei am 30. März 2007 eingestellte Gesamtzahl der Datensätze mit ca. 15.000 (wegen Mehrfach-

speicherungen betrifft das ca. 13.000 Personen) angegeben. Da auch noch im Jahresverlauf 2007 der weitere Aufbau der Datei erfolgte, wird eine erste Kontrolle erst im Laufe des Jahres 2008 erfolgen. Zudem liegt dem Bundesverfassungsgericht eine Verfassungsbeschwerde gegen das Antiterrordateigesetz vor, zu der die Datenschutzbeauftragten des Bundes und der Länder in einer gemeinsamen Stellungnahme noch einmal auf die bereits beim Gesetzgebungsverfahren vorgetragenen verfassungsrechtlichen Problempunkte hingewiesen haben.

Mit dem Betrieb der Antiterrordatei sind nach wie vor verfassungsrechtliche und datenschutzrechtliche Risiken verbunden. Es besteht die Gefahr, dass zu viele zu ungesicherte Daten auch von unbescholtenen Bürgern an zu viele Stellen gelangen. Eine Klärung der verfassungsrechtlichen Fragen ist von der anhängigen Verfassungsbeschwerde beim Bundesverfassungsgericht zu erwarten. Parallel dazu wird sich der TLfD durch Kontrollen ein Bild darüber verschaffen, ob sich diese Risiken in der Praxis realisieren.

9. Finanzwesen

9.1 Der Weg zum gläsernen Steuerbürger

Mit den Neuregelungen des Unternehmenssteuerreformgesetzes 2008 zum Kontoabrufverfahren (§ 93 Abs. 7 bis 10 AO) und zur Kirchensteuer (§ 51a EStG) wurde wieder ein Stück auf dem Weg zum gläsernen Steuerbürger zurückgelegt. Die im Gesetz zur Förderung der Steuerehrlichkeit geschaffenen Regelungen wurden im Rahmen des Unternehmenssteuergesetzes 2008 nach der im Jahre 2005 geäußerten datenschutzrechtlichen Kritik (6. TB, 9.1) im Sinne des Beschlusses des Bundesverfassungsgerichts vom 13.06.2007 novelliert. Das Gericht hatte die zusätzlichen Datenabfragen im Kern aber nicht beanstandet. Wichtigste Neuregelung ist eine konkrete Aufzählung der außersteuerlichen Zwecke (v. a. Verwaltung von Sozialleistungen), für die ein Kontenabruf zulässig ist. Im Unterschied zum bisherigen Verfahren richten die hierfür zuständigen Behörden das Ersuchen ohne Beteiligung der Finanzämter unmittelbar an das Bundeszentralamt für Steuern. Für andere Zwecke ist ein Abrufersuchen nur zulässig, soweit dies durch ein formelles Bundesgesetz ausdrücklich bestimmt wird. Außerdem ist der Betroffene auf die Möglichkeit eines Kontenabrufs hinzuweisen. Das Ersuchen und dessen Ergebnis müssen zur Kontrolle ihrer Rechtmäßigkeit nunmehr dokumentiert werden.

Eine datenschutzrechtliche Kontrolle aller im Jahre 2005 über das Finanzamt Erfurt veranlassten Kontenabrufersuchen ergab, dass die überwiegende Fallzahl die Vollstreckung ausstehender Kfz-Steuern - in wenigen Fällen die steuerliche Betriebsprüfung - betrafen. Abrufe für außersteuerliche Zwecke auf Veranlassung von anderen Behörden wurden lediglich viermal durchgeführt. Dabei erfolgen die Dokumentation der Abfragen und die nachträgliche Information von Betroffenen in Fällen, in denen bisher unbekannte Konten entdeckt wurden, im Unterschied zu anderen Bundesländern, im Wesentlichen ordnungsgemäß. Zu kritisieren war jedoch, dass die Betroffenen über solche Abfragen, die den Verdacht des Vorhandenseins weiterer Konten nicht bestätigten, nicht informiert worden sind, was mit finanziellem Aufwand in Folge Portokosten begründet wurde. Aufgrund der Kritik des TLfD an dieser Praxis wurden die Thüringer Finanzämter nachfolgend angewiesen, ihrer Informationsverpflichtung nachzukommen.

Durch eine Neuregelung der Kirchensteuer, die laut Gesetzesbegründung das Steueraufkommen sichern und den Verwaltungsaufwand gering halten soll, haben die Steuerpflichtigen in einer Übergangszeit ab 1. Januar 2009 die Wahl, ob die Kirchensteuer vom zuständigen Finanzamt veranlagt oder im Abzugsverfahren von dem Abzugsberechtigten – bspw. einer Bank oder Versicherung – im Zusammenhang mit der Besteuerung der Kapitalerträge (Abzugsverfahren an der Quelle) einbehalten werden soll. Voraussetzung für das Abzugsverfahren ist, dass die Abzugsberechtigten mittels einer neu geschaffenen Datenbank beim Bundeszentralamt für Steuern, die Religionszugehörigkeit ihrer Kunden abfragen. Eine Klausel im Gesetz sieht vor, spätestens bis zum 30. Juni 2010 zu überprüfen, ob die Kirchensteuer ausschließlich im Abzugsverfahren an der Quelle zu erheben ist. Kritisch zu sehen ist, dass mit dem ausschließlichen Abzugsverfahren das sensible Datum der Zugehörigkeit bzw. Nichtzugehörigkeit zu einer Religionsgemeinschaft gegenüber Banken und Kreditinstituten offenbart werden müsste, ohne dass der betroffene Steuerzahler eine andere Wahl hat.

Künftig wird die Umsetzung der Neuregelung der Kontenabrufersuchen insbesondere für nichtsteuerliche Zwecke in der Praxis zu überprüfen sein.

Bei der Erhebung der Kirchensteuer wird darauf zu achten sein, dass nach Auslaufen der Übergangsregelung den datenschutzrechtlichen Belangen in ausreichendem Maße Rechnung getragen wird.

9.2 Zentrale Steuerdatei – Werkzeug zur Profilbildung

Eine Neuregelung des § 39e EStG sieht vor, das Lohnsteuerkartenverfahren ab 2011 durch das elektronische Abrufverfahren „ElsterLohn II“ abzulösen. Hierzu soll die beim Bundeszentralamt für Steuern in Zusammenhang mit der lebenslangen Steueridentifikationsnummer errichtete Datenbank um elektronische Lohnsteuerabzugsmerkmale wie Religionszugehörigkeit, Ehepartner, Steuerklasse und Freibeträge erweitert werden. Damit würde ein zentraler Datenpool entstehen, der neben den Daten zu lohnsteuerpflichtigen Personen auch solche über nicht lohnsteuerpflichtige Personen wie Kinder und Ehepartner enthält. In diesem einzigartigen aktuellen Datenpool über alle Bürger könnten wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpft werden. Damit würde die faktische Möglichkeit zur staatlichen Profilbildung geschaffen. Daher haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 19) gefordert, die Neuregelung nicht im Jahressteuergesetz 2008 zu beschließen. Insbesondere erscheint es zweifelhaft, ob die Aufnahme nicht lohnsteuerpflichtiger Personen in die Datenbank dem Erforderlichkeitsgrundsatz entspricht und nicht eine unzulässige Vorratsdatenspeicherung darstellt, da die betroffenen Personen keine Arbeitnehmer sind. Bedenklich ist auch, dass die elektronischen Lohnsteuerabzugsmerkmale künftig vier Millionen Arbeitgebern zum Abruf zur Verfügung stehen. Um eine rechtswidrige Informationsbeschaffung Dritter weitestgehend auszuschließen, sollten die Daten der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können. Aus der Erfahrung mit großen Datensammlungen ist auch bei dem im Bundeszentralamt für Steuern entstehenden Datenpool zu befürchten, dass die Bindung an steuerliche Zwecke künftig auf Grund von Begehrlichkeiten anderer Behörden aufgeweicht werden wird. Ungeachtet der Kritik ist die Neuregelung am 29. Dezember 2007 im Rahmen des Jahressteuergesetzes 2008 unverändert in Kraft getreten.

Künftig wird genau darauf zu achten sein, dass die faktische Möglichkeit zur Profilbildung nicht schrittweise legalisiert wird.

9.3 Probleme mit der Elektronischen Steuererklärung (Elster) und OpenElster

Der wiederholt geäußerten Kritik (5. TB, 9.6; 6. TB, 9.4) am Fehlen von Regelungen zur Datenverarbeitung im Auftrag wurde Anfang 2007 mit der Aufnahme entsprechender Bestimmungen in die „Handlungsanweisungen für den Betrieb der Elster-Clearingstellen und der Landeskopfstellen“ Rechnung getragen. Auf die Risiken einer fehlenden Authentifizierung der Absender von elektronisch übermittelten Steuerdaten hatte der TLfD bereits hingewiesen (6. T, 9.4). Die Verpflichtung, für die elektronische Übermittlung und den Abruf steuerlicher Daten ausschließlich die qualifizierte elektronische Signatur nach dem Signaturgesetz zu verwenden, wurde durch Änderung des § 87a Abs. 6 AO und der Steuerdatenübermittlungsverordnung im Jahressteuergesetz 2007 aufgehoben. Danach kann nunmehr bis Ende 2011 „auch ein anderes sicheres Verfahren“ zugelassen werden. In diesem Zusammenhang bietet die Finanzverwaltung ein Authentifizierungsverfahren an, das lediglich eine einmalige Identifizierung und Registrierung der Nutzer erfordert. Hierbei wird ein Software-Zertifikat erzeugt, das bspw. auf einem PC, auf eine Diskette oder auf dem „Elster-Stick“ – ähnlich einem USB-Stick - gespeichert werden kann und gemeinsam mit der elektronischen Steuererklärung versandt wird. Dieses Zertifikat soll die bisherige Unterschrift auf der Steuererklärung ersetzen.

Authentifizierung im Sinne des geänderten § 6 Abs. 1 StDÜV bedeutet, dass eine elektronisch übermittelte Steuererklärung nicht wie bei einer Erklärung in Papierform mit eigenhändiger Unterschrift versehen sein muss. Vielmehr wird die zuvor im ElsterOnline-Portal elektronisch durchgeführte Anmeldung des Nutzers von der Finanzverwaltung als ausreichend angesehen. Dabei kann jedoch nicht garantiert werden, dass die Steuererklärung tatsächlich von dem Steuerpflichtigen stammt und sie bei der Übermittlung unverändert blieb. Entgegen der Auffassung der Finanzverwaltung weist deren Authentisierungsverfahren systembedingt nicht die gleiche Sicherheit auf wie eine qualifizierte elektronische Signatur nach dem Signaturgesetz. Darauf haben bereits die Datenschutzbeauftragten des Bundes und der Länder während des Gesetzgebungsverfahrens zur Änderung von § 87a Abs. 6 AO in einer Entschließung (Anlage 2) hingewiesen und gefordert, Verfahren mit qualifizierter Signatur den Vorrang einzuräumen. Die qualifizierte elektronische Signatur würde hier die übermittelte

elektronische Steuererklärung mit einem mit eigenhändiger Unterschrift versehenen körperlichen Schriftstück vergleichbar machen. Dadurch könnten die Angaben in der elektronisch übermittelten Steuererklärung dem betreffenden Steuerpflichtigen rechtswirksam zugerechnet werden. Dies ermöglichte den Steuerpflichtigen nachzuweisen, dass ein unter missbräuchlicher Nutzung der Authentifizierung elektronisch übermitteltes Dokument nicht von ihnen selbst stammt. Ein Verzicht auf die qualifizierte elektronische Signatur kann hingegen in Streitfällen zu einem Nachteil für die betroffenen Steuerpflichtigen führen. Auch ist bislang der Forderung nach einer Evaluierung des Verfahrens Elster nicht Rechnung getragen worden. Verfügt der Nutzer über eine von Elster unterstützte Signaturkarte, so kann er diese auch im Rahmen des ElsterOnline-Portals einsetzen.

Nicht genug, dass die Steuerverwaltung selbst ein unsicheres Verfahren einsetzt, war beabsichtigt, über das Kommunikationsportal Elster der Finanzbehörden im Rahmen des Vorhabens OpenElster künftig kostenlos ein Zertifikat für verschiedene elektronische Behördengänge außerhalb der Finanzverwaltung bereitzustellen, um die Attraktivität deutscher eGovernment - Projekte zu steigern. Das Grobkonzept von OpenElster sah vor, die Steueridentifikationsnummer, die gemäß § 139b AO ausschließlich für steuerliche Zwecke genutzt werden darf, zur Erstregistrierung des Nutzers zu verwenden und auch den am Verfahren beteiligten nichtsteuerlichen Stellen zur Prüfung der elektronischen Zertifikate zu übermitteln. In einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder (Anlage 19) wurde eine zweckwidrige Nutzung der Steueridentifikationsnummer im Rahmen von OpenElster kritisiert und auf die bislang ausstehende Evaluierung des Verfahrens Elster hingewiesen. Wie das für die Verfahrensentwicklung von OpenElster verantwortliche Bayerische Finanzministerium zwischenzeitlich mitteilte, seien auch andere technische Lösungen zur Benutzeridentifikation denkbar, ohne dass die Steueridentifikationsnummer einer steuerfremden Behörde mitgeteilt werden muss.

Die Evaluierung des Verfahrens Elster muss erfolgen, damit das Sicherheitsniveau der derzeitigen Elster-Infrastruktur objektiv beurteilt werden kann. Sicherzustellen ist, dass spätestens mit dem Ablauf der gesetzlichen Befristung Ende 2011 die qualifizierte elektronische Signatur auch im Finanzbereich verbindlich angewandt wird. Die Datenschutzbeauftragten werden sehr darauf achten, dass sich die

Steueridentifikationsnummer durch ihre Nutzung in anderen Verwaltungsbereichen nicht als verfassungswidriges allgemeines Personenkennzeichen etablieren kann.

9.4 Werbung durch Sparkassen

Um sich am Markt zu behaupten, machen die Sparkassen, wie ihre Konkurrenten auch, Werbung in eigener Sache. Die Begehrlichkeiten, dabei die dort zur Erfüllung des Vertragsverhältnisses gespeicherten Kunden- und Kontendaten nutzen zu wollen, sind somit naheliegend. Hieraus ergab sich im Berichtszeitraum für den TLfD erneut die Notwendigkeit, datenschutzrechtlich tätig zu werden. In einem Fall bat eine Sparkasse um Bewertung einer geplanten Verfahrensweise, zukünftig die Umsatzdaten von Sparkassenkunden auszuwerten und für Beratungsgespräche mit den jeweiligen Kunden zu nutzen. Zwar hat die Sparkasse ein berechtigtes Interesse daran, die Kundendaten zu Beratungs- und somit auch für Bewerbungszwecke zu nutzen. Das schutzwürdige Interesse des Kunden an dem Ausschluss der Verarbeitung oder Nutzung seiner Daten überwiegt hier aber. Die Kundendaten dienen ausschließlich der Zweckbestimmung des Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses zwischen Sparkasse und Kunde. Die Sparkasse hat lediglich die Möglichkeit, Kunden um eine schriftliche Einwilligung zu bitten, dass deren Kontendaten zu Beratungs- oder Werbezwecken von dem Institut genutzt werden dürfen. Eine solche Einwilligung ist aber nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dem Kunden dürfen keine Nachteile entstehen, wenn dieser die Einwilligung nicht erteilt.

In einem weiteren Vorgang wollte die Sparkasse Mittelthüringen die kostenlose Führung des Girokontos nur unter der Voraussetzung anbieten, dass der Kunde sein ausdrückliches Einverständnis erklärt, auch per E-Mail und telefonisch mit weiteren Produkten der Sparkasse beraten bzw. beworben zu werden. Das Institut wollte somit die Kundendaten über die eigentliche Vertragserfüllung hinaus für die werbliche Information nutzen. Aus datenschutzrechtlicher Sicht berechtigt eine Einwilligung zur Verarbeitung und Nutzung personenbezogener Daten aber nur dann, wenn diese tatsächlich auf einer freien Entscheidung des Einwilligenden beruht. Dies war hier nicht gegeben, weil die kostenlose Kontoführung nur dann angeboten wurde, wenn der Kunde die werbliche Nutzung seiner Kontodaten „in Kauf nimmt“. Der TLfD wies in diesem Zusammenhang auch auf mehrere Urteile des Bundes-

gerichtshofs über Telefonwerbungs-Klauseln in Kontoeröffnungsformularen hin, wonach hierin unter Verstoß gegen die Gebote von Treu und Glauben eine unangemessene Benachteiligung des Kunden liege (z. B. BGH, I ZR 241/97). Denn angesichts der Vielfalt der Werbemethoden der gewerblichen Wirtschaft sei es nicht erforderlich, mit der Werbung auch in den privaten Bereich des umworbenen Verbrauchers einzudringen; der Schutz der Individualsphäre sei insoweit vorrangig. Die Sparkasse hat nach längerer Diskussion die unzulässige Vertragsklausel aus der Zusatzvereinbarung zur kostenfreien Kontoführung entfernt.

Eine Übermittlung oder Nutzung von Kundendaten zu telefonischen Werbezwecken ist der Sparkasse grundsätzlich nicht erlaubt. Eine Werbung in anderer Form unter Verwendung dieser Daten ist ohnehin nur möglich, wenn der Kunde hierin schriftlich einwilligt. Diese Einwilligung darf nicht als Bedingung an eine Vergünstigung, z. B. kostenlose Kontoführung, gekoppelt werden.

10. Justiz

10.1 Pläne für heimliche Online-Durchsuchungen privater Computer

Schlagzeilen wie „Online-Durchsuchung“ oder auch „Bundestrojaner“ haben im Jahr 2007 die Diskussion um die Balance zwischen Freiheit und Sicherheit über weite Strecken beherrscht. Anlass für die Diskussion war eine Entscheidung des Bundesgerichtshofs im Januar 2007. Darin wurde festgestellt, dass die Vorschriften der Strafprozessordnung für eine Wohnungsdurchsuchung nicht auch auf die unbemerkte Durchsuchung eines in der Wohnung befindlichen PC über das Internet anwendbar sind. Der Grund ist einleuchtend. Die Wohnungsdurchsuchung muss zwingend offen, d. h. in Anwesenheit des Betroffenen erfolgen. Auch wenn dabei der Computer mit persönlichen Daten mitgenommen wird, kann sich der Betroffene ggf. auch mit gerichtlicher Hilfe wehren, wenn z. B. allzu persönliches und vielleicht auch nicht relevantes Material auf dem PC gespeichert ist. Läuft eine solche Durchsuchung aber heimlich, d. h. ohne das Wissen des PC-Besitzers ab, ist es ihm nicht möglich, sich gegen Art, Umfang bzw. Zulässigkeit einer solchen Maßnahme rechtlich zur Wehr zu setzen. Deshalb hat der Bundesgerichtshof entschieden, dass es für eine solche Durchsuchung keine Ermächtigung im geltenden Recht gibt.

Das hat aber sofort den Bundesinnenminister und die Sicherheitsbehörden auf den Plan gerufen, die fast das ganze Jahr 2007 über nicht müde geworden sind, nun eine Rechtsgrundlage zu fordern. Ohne dies näher zu begründen wurde immer wieder betont, dass eine solche Möglichkeit zur Bekämpfung des internationalen Terrorismus unverzichtbar sei. Dabei stellte sich im Lauf der Diskussion heraus, dass nur das Ziel einer solchen Maßnahme in etwa klar war, nämlich auf Informationstechnischen Systemen (PC, externen Festplatten, PDA u. ä. Geräten) Informationen über geplante Anschläge oder sonstige schwere Straftaten zu finden. Über die technischen Mittel, dies grundgesetzkonform zu realisieren, wurde zwar viel spekuliert, jedoch wenig Konkretes von offizieller Seite dargelegt. So ist nach wie vor unklar, wie sich die Sicherheitsbehörden erfolgreich Zugang zu IT-Systemen von hochgefährlichen Kriminellen verschaffen wollen. Erhellend hat hier der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gewirkt, indem er auf der Grundlage der vor allem in Informatikerkreisen geführten öffentlichen Diskussion zur technischen Umsetzung eines solchen „Bundestrojaners“ eine Vielzahl von Möglichkeiten in einem Papier zusammengeführt und bewertet hat. Das Papier steht auf der Homepage des TLfD zum Abruf bereit. Das Fazit ist ernüchternd. Auch wenn unbekannt ist, an welche Methoden der Bundesinnenminister und seine Sicherheitsbehörden konkret denken, so gibt es für fast alle Ansätze geeignete (legale und auch illegale) Schutzmaßnahmen, mit denen sich die Verdächtigen einer solchen Maßnahme entziehen können. So stellt sich natürlich die Frage, ob die Online-Durchsuchung nicht eher geeignet ist, unbedarfte Kleinkriminelle zu fassen.

Die andauernde öffentliche Diskussion über den sog. Bundestrojaner ist zudem geeignet, das Vertrauen der Bevölkerung in die elektronische Kommunikation mit staatlichen Stellen zu beeinträchtigen. Das kann aber auch nicht verwundern, wenn der Staat nicht ausschließt, dass man sich durch die E-Mail einer Behörde oder eine von der Verwaltung angebotene Software ein Spionageprogramm einfängt, das sich auf dem PC des Nutzers einnistet und bei Bedarf die gewünschten Informationen liefert. Wenn man sich gerade derjenigen Methoden bedient, vor denen im Bereich der Computerkriminalität ständig gewarnt wird, macht man sich unglaubwürdig. Darauf haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 15) hingewiesen und die Bundesregierung aufgefordert, auf die Einführung einer solchen Maßnahme zu verzichten.

In ihrer Entschließung haben die Datenschutzbeauftragten auf ein weiteres Problem von besonderer Bedeutung hingewiesen. Dabei geht es um die Frage, wie weit der Staat zur Verfolgung von Straftaten oder zur Vorsorge vor Gefahren in den persönlichsten Bereich der Menschen eingreifen darf. Der Computer und andere IT-Systeme, wie z. B. Mobiltelefone, PDA usw., haben im Zeitalter der digitalen Verarbeitung aller Lebensäußerungen wie Texte, Mitteilungen, Fotos, Videos, akustische Memos usw. mittlerweile eine zentrale Rolle auch bei der Speicherung persönlichster Informationen erlangt. So werden auf diesen Systemen neben völlig belanglosen Dingen auch sensible Inhalte wie private Briefe, Reiseaufzeichnung, Tagebücher, Fotos, Videos oder E-Mails und ähnliches mehr gespeichert, die unbestritten dem sog. Kernbereich privater Lebensgestaltung zuzuordnen sind. Der Schutz dieses Kernbereichs ist aber nach der Rechtsprechung des Bundesverfassungsgerichts absolut, d. h. bei staatlichen Maßnahmen darf auf solche Daten nicht zugegriffen werden. Natürlich können Sicherheitsbehörden auch unbeabsichtigt auf sensible Informationen treffen, ohne dass sie danach gesucht haben. Deshalb fordert das Bundesverfassungsgericht, dass bei heimlichen Ermittlungsmaßnahmen, bei denen die Gefahr eines solchen unbeabsichtigten Zugriffs besonders hoch ist, Vorkehrungen zu treffen sind, die bereits eine Kenntnisnahme verhindern, mindestens aber sehr unwahrscheinlich machen (7.1). Nach allem, was bislang über die Techniken zur heimlichen Online-Durchsuchung bekannt ist, können aber solche Vorkehrungen gerade nicht getroffen werden, weil man z. B. einem Dateinamen nicht unbedingt entnehmen kann, welchen Inhalt die Datei hat. Wenn aber feststeht, dass sich der unantastbare Kernbereich privater Lebensgestaltung durch technische Mittel bei der Datenerhebung nicht schützen lässt, erscheint eine verfassungskonforme Regelung einer solchen Maßnahme unmöglich. Diese Frage wird derzeit im Rahmen einer Verfassungsbeschwerde gegen eine Vorschrift im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen, die eine solche heimliche Online-Durchsuchung erlaubt, vom Bundesverfassungsgericht geprüft. Das Gericht könnte dieses Verfahren zum Anlass nehmen, generelle verfassungsrechtliche Leitlinien für solche Maßnahmen im Spannungsfeld zwischen Freiheit und Sicherheit vorzugeben. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 20) nochmals ihre grundsätzliche Ablehnung der Online-Durchsuchung bekräftigt und die Bundesregierung aufgefordert, vor weiteren Schritten diese Entscheidung abzuwarten.

Es ist zu hoffen, dass das Bundesverfassungsgericht seine Rechtsprechung zum Schutz des Kernbereichs privater Lebensgestaltung auch in Bezug auf neue technische Möglichkeiten konsequent weiterentwickelt.

10.2 Neufassung der Telekommunikationsüberwachung in der Strafprozessordnung

Bundestag und Bundesrat haben den Gesetzentwurf zur „Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ Ende des Jahres 2007 entgegen aller Kritik, u. a. auch seitens der Datenschutzbeauftragten, beschlossen (zur Vorratsdatenspeicherung vgl. 4.1). Bereits mit der Entschließung am 8./9. März 2007 (Anlage 16) hatten die Datenschutzbeauftragten des Bundes und der Länder die im Referentenentwurf in Artikel 1 beabsichtigten Änderungen der StPO, die nach Regierungsangaben die Rechtsprechung des Bundesverfassungsgerichts (6. TB, 10.1 und 7.1) berücksichtigen sollten, als unzureichend kritisiert. Insbesondere hinsichtlich der Sicherstellung des Schutzes des Kernbereichs der privaten Lebensgestaltung, des Schutzes von Berufsgeheimnisträgern und der Voraussetzungen der Telekommunikationsüberwachung wurde Verbesserungsbedarf gesehen. Erfolg hatte dies allerdings nicht. Der Gesetzentwurf der Bundesregierung war gegenüber dem Referentenentwurf aus Sicht des Datenschutzes noch verschlechtert. Dies betraf den Schutz der Zeugnisverweigerungsberechtigten, die Benachrichtigungspflichten gegenüber betroffenen Personen, die aufgeweicht wurden, sowie die Voraussetzung für die Erhebung von Standortdaten in Echtzeit und den Einsatz des sog. IMSI-Catchers, der erheblich ausgeweitet werden sollte. Mit einer weiteren Entschließung haben sich die Datenschutzbeauftragten des Bundes und der Länder daher nochmals mit Nachdruck gegen die von der Bundesregierung und den Bundesratsgremien geplante weitere Verschärfung verdeckter Ermittlungsmaßnahmen gewandt (Anlage 17). Sie haben gefordert, die Freiheitsrechte der Bevölkerung nicht weiter zu untergraben und die Vorgaben des Bundesverfassungsgerichts zu beachten. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und deren besonnene Anwendung. Zwar kam es nicht zu den vom Bundesrat geforderten Verschärfungen, wozu u. a. auch der Versuch zählte, eine Rechtsgrundlage für die

Online-Durchsuchung aufzunehmen; andererseits blieb es aber auch bei den im Regierungsentwurf gegenüber dem Referentenentwurf vorgenommenen Verschlechterungen.

Durch die Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen wurde das Ziel eines umfassenden Schutzes des Kernbereichs der privaten Lebensgestaltung leider nicht vollständig erreicht.

10.3 DNA-Analyse: Erste Erfahrungen mit der Untersuchung von Körperzellen auf Einwilligungsbasis

Seit der Novellierung der forensischen DNA-Analyse im Jahr 2005 ist mit der Einwilligung eines Betroffenen nicht mehr nur die Entnahme einer DNA-Probe, sondern nunmehr auch deren Untersuchung möglich, sodass eine richterliche Anordnung hierzu entfallen kann. Dass dies eine entsprechende differenzierte Belehrung eines Betroffenen voraussetzt, wurde bereits dargelegt (6. TB, 10.2). Den TLfD erreichte bereits Anfang 2006 eine konkrete Anfrage eines Betroffenen zu einer ihm von der Kriminalpolizeiinspektion Nordhausen zugesandten Aufforderung, der Durchführung einer DNA-Analyse zuzustimmen. Er hatte über 3 Jahre davor im Zusammenhang mit strafrechtlichen Ermittlungen seine Fingerabdrücke und eine DNA-Probe freiwillig abgegeben. Die Antwort auf eine entsprechende Anfrage des TLfD gab zunächst keinen ausreichenden Aufschluss darüber, weshalb zu dem Betroffenen eine DNA-Analyse angestrebt wurde. Es wurde daher eine datenschutzrechtliche Kontrolle in der zuständigen Polizeidirektion Nordhausen durchgeführt. Selbstverständlich muss auch dann, wenn die Untersuchung einer DNA-Probe auf der Grundlage der Einwilligung eines Betroffenen stattfinden soll, eine entsprechende Prognose getroffen und dokumentiert werden, weshalb eine Untersuchung und damit auch Speicherung des Ergebnisses in der DNA-Analyse-Datei erforderlich ist. Im Ergebnis der Kontrolle konnte festgestellt werden, dass der Petent und andere Betroffene nicht leichtfertig um ihre Einwilligung zur Untersuchung der in den meisten Fällen bereits freiwillig abgegebenen DNA-Proben gebeten wurden. Zu bemängeln war allerdings die fehlende Dokumentation der erforderlichen Prognoseentscheidungen der Polizei, dass Betroffene zukünftig erhebliche Straftaten begehen werden. Da sogar bei einer richterlichen Anordnung in deren schriftlicher Begründung u. a. „die Erkenntnisse, aufgrund derer Grund zu der Annahme besteht, dass gegen den Beschul-

digten künftig Strafverfahren zu führen sein werden“ einzelfallbezogen darzulegen sind (§ 81g Abs. 3 StPO), muss dies erst recht für die Polizei gelten. Allein der Umstand, dass durch Lektüre der bisher angefallenen strafrechtlichen Ermittlungsakten (die dem Betroffenen regelmäßig verwehrt ist), eine derartige Prognose möglicherweise denkbar ist, reicht nicht aus. Zumal die Ermittlungsverfahren und die DNA-Analyse nach den Vorschriften der Strafprozessordnung durchgeführt werden, hat dem auch das einbezogene Thüringer Justizministerium zugestimmt. In der Folge wurde die Richtlinie, die das Verfahren zur Durchführung von DNA-Analysen und insbesondere zur Speicherung der Ergebnisse in der DNA-Analyse-Datei als polizeiliche Datei regelt dahingehend ergänzt, dass eine Prognoseentscheidung dokumentiert werden muss. Zu den erforderlichen Ausführungen in der Einwilligungserklärung und dem Merkblatt sind die Anregungen aus datenschutzrechtlicher Sicht übernommen worden. Das Merkblatt enthält insbesondere auch den Hinweis, dass man sich bei Fragen hierzu an den TLfD wenden kann.

Wird ein Betroffener um die Einwilligung zur Untersuchung einer DNA-Probe gebeten, muss er selbstverständlich entsprechend aufgeklärt werden. Es gibt keine Pflicht zur Erteilung der Einwilligung. Hat der Betroffene Bedenken, ob die Untersuchung der DNA-Probe bzw. auch die Speicherung seiner Daten in der DNA-Analyse-Datei gerechtfertigt ist, sollte er von der Einwilligung absehen. Dann darf eine Untersuchung der DNA-Probe nur aufgrund einer richterlichen Anordnung erfolgen.

10.4 Sexualstraftäterdatei

Nachdem immer wieder Sexualstraftaten insbesondere an Kindern durch bereits früher wegen solcher Delikte Verurteilte publik geworden sind, wurde diskutiert, in einer Datei Namen und Anschriften von Tätern für jedermann öffentlich zu machen, um mögliche Betroffene zu warnen. Die Datenschutzbeauftragten des Bundes und der Länder haben mit ihrer Entschließung (Anlage 11) Pläne für eine öffentlich zugängliche Sexualstraftäterdatei als verfassungswidrig angesehen. Bei allem Verständnis für Überlegungen und Bemühungen z. B. zu einem verbesserten Schutz von Kindern muss jedoch auch die Verhältnismäßigkeit der Mittel gewahrt werden. Durch die Veröffentlichung von Namen und Adressen von verurteilten Sexualstraftätern würden diese an eine Art elektronischen Pranger gestellt und sozial

geächtet. Darüber hinaus ist der Vorschlag einer derartigen Datei eher dazu geeignet, Misstrauen und Selbstjustiz zu fördern, eine Vermeidung von weiteren einschlägigen Straftaten ist aber äußerst fraglich.

Der Schutz der Bevölkerung vor Sexualstraftätern darf nicht verfassungsrechtliche Grundsätze aushebeln.

10.5 Thüringer Jugendstrafvollzugsgesetz

In vorangegangenen Tätigkeitsberichten wurde immer wieder darauf hingewiesen, dass auch der Jugendstrafvollzug datenschutzrechtlich einer bereichsspezifischen Regelung bedarf. Mit seiner Entscheidung vom 31. Mai 2006 hat das Bundesverfassungsgericht letztendlich den Gesetzgeber aufgefordert, den verfassungswidrigen Zustand zu beenden und bis zum 31. Dezember 2007 eine spezielle gesetzliche Grundlage für den Jugendstrafvollzug zu schaffen. Zu einer einheitlichen Regelung durch Bundesgesetz kam es jedoch nicht. Infolge der Föderalismusreform war die Gesetzgebungsbefugnis für den Jugendstrafvollzug nach Art. 70 Abs. 1 GG seit dem 1. September 2006 auf die Länder übergegangen. Der Thüringer Landtag hat Mitte Dezember 2007 gerade noch rechtzeitig vor Ablauf der Frist die erforderlichen gesetzlichen Grundlagen beschlossen.

Bei dem zur parlamentarischen Beratung von der Landesregierung eingebrachten Gesetzentwurf handelte es sich um das Ergebnis einer Arbeitsgruppe unter Federführung von Berlin und Thüringen unter Beteiligung der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland, Sachsen-Anhalt und Schleswig-Holstein, der in den genannten einzelnen Ländern mit kleineren Modifizierungen ebenfalls beraten wurde. Nachdem bereits zum Referentenentwurf seitens des TLfD Stellung genommen wurde, haben nur wenige Anregungen und Kritikpunkte in der dem Parlament vorgelegten Fassung Berücksichtigung gefunden. Auch weitere vorgebrachte Hinweise haben im beratenden Ausschuss keine Mehrheit gefunden, selbst wenn diese in den Gesetzen anderer Bundesländer bereits Niederschlag gefunden hatten. Die Stellungnahme des TLfD hat lediglich dazu geführt, dass eine bereichsspezifische Regelung zur Videoüberwachung in der Anstalt und zur Besuchsüberwachung aufgenommen wurde. Die unberücksichtigt gebliebene datenschutzrechtliche Kritik richtete sich u. a. gegen

- die Pflicht der Gefangenen, dass sie eingehende Schreiben (z. B. auch von Familienmitgliedern, von Lebenspartnern etc.) nur unverschlossen in ihrer Zelle aufbewahren dürfen, obwohl damit die Gefahr der Kenntnisnahme Unbefugter besteht,
- die Möglichkeit, dass Unterlagen aus erkennungsdienstlichen Maßnahmen im Jugendstrafvollzug, die für die dortige Sicherheit gefertigt werden, auch in polizeiliche Verwahrung genommen werden können, obwohl der Polizei keine Aufgaben im Jugendstrafvollzug zukommen,
- die Möglichkeit der Einrichtung einer zentralen Datei - mit allen für den Vollzug erforderlichen Daten und Zugriff der Anstalten und Aufsichtsbehörde -, wobei der Zweck und die Erforderlichkeit einer derartigen zentralen Datei nicht deutlich wird,
- die Möglichkeit eines Datenverbunds mit anderen Ländern und dem Bund, obwohl die geschaffene Rechtsgrundlage Zweck, Umfang, zu übermittelnde Daten, Empfänger und technisch-organisatorische Maßnahmen nicht konkret festlegt und damit nicht normenklar ist.

Positiv zu bewerten ist, dass der TLfD vor Erlass einer Rechtsverordnung mit Einzelheiten zur Einrichtung automatisierter Übermittlungsverfahren zu hören ist und hoffentlich auch Gehör finden wird.

Die praktische Umsetzung des Gesetzes über den Vollzug der Jugendstrafe wird datenschutzrechtlich zu überprüfen sein.

11. Gesundheits- und Sozialdatenschutz

11.1 Umsetzung des SGB II - Gesetz zur Fortentwicklung der Grundsicherung für Arbeitssuchende

Wer bei der ARGE Leistungen zur Sicherung des Lebensunterhalts beantragt, von dem wird zur Feststellung der Hilfebedürftigkeit (vgl. § 9 SGB II) häufig die Vorlage von Kontoauszügen der letzten sechs Monate verlangt. Die Auszüge dürfen dabei nicht, auch nicht teilweise, geschwärzt sein. Häufig wenden sich Bürger an den TLfD, die in diesem Verlangen der ARGE einen unzulässigen Eingriff in ihr informationelles Selbstbestimmungsrecht sehen. Die ARGE darf die Vorlage von Beweisurkunden verlangen, aus denen sich die Hilfebedürftigkeit ergibt, wenn die Kenntnis dieser Daten zur Aufgabenerfüllung erforderlich ist (§ 60 Abs. 1 Satz 1 Nr. 3 SGB I i. V. m. § 67a

Abs. 1 Satz 1 SGB X). Vor dem Hintergrund auch neuester Rechtsprechung in dieser Frage (vgl. Beschluss des Landessozialgerichts Schleswig-Holstein vom 25. September 2007, Az: L 11 B 137/07 AS ER) hält der TLfD grundsätzlich eine Vorlage von Kontoauszügen des letzten Monats, maximal der letzten drei Monate für ausreichend, sofern nicht Anhaltspunkte für einen Leistungsmissbrauch bestehen. Schwärzungen auf den Kontoauszügen können vom Antragsteller unter folgenden Voraussetzungen erfolgen:

- Bei laufendem Bezug von Hilfen zum Lebensunterhalt dürfen Sollbuchungen grundsätzlich geschwärzt werden.
- Bei erstmaligem oder erneut beantragtem Bezug von Hilfen zum Lebensunterhalt muss von der ARGE eine Schwärzung nicht akzeptiert werden, soweit nicht erkennbar bleibt, dass die Ausgaben z. B. nicht für kapitalbildende „Anlagen“ vorgesehen sind.
- Zu den Akten der ARGE dürfen nur Kopien genommen werden, soweit diese leistungsrelevante Daten enthalten. Die nicht erforderlichen Daten sollen auf den Kopien geschwärzt werden.

Wiederholt für Unruhe sorgte im Berichtszeitraum der unsägliche § 7 Abs. 3a SGB II, der die gesetzliche Vermutung anstellt, dass Partner, die länger als ein Jahr oder mit einem Kind zusammenleben oder sich Vermögensverfügungsbefugnisse eingeräumt haben, als sog. Bedarfsgemeinschaft zu qualifizieren sind. Folge ist, dass die Partner einer solchen Bedarfsgemeinschaft füreinander einzustehen haben, auch und gerade in finanzieller Hinsicht. In dem Maße, wie dieses der Fall ist, ist die ARGE von Leistungen an einen Partner der Bedarfsgemeinschaft entpflichtet. Die ARGE hat mithin ein ausgeprägtes Interesse daran, zusammenlebende hilfebedürftige Bürger zu Bedarfsgemeinschaften zu deklarieren. Betroffene monieren u. a. unangemeldete Hausbesuche, Haus- und (Kühl-)Schrankdurchsuchungen ohne Einwilligung der Betroffenen, verbale Bußgeldandrohungen und Datenerhebungen in der Nachbarschaft. Bloße Wohngemeinschaften, die länger als ein Jahr bestehen, sehen sich außer Stande, die gesetzliche Vermutung der Bedarfsgemeinschaft zu widerlegen. Abgesehen von den mangels Einwilligung unzulässigen Datenerhebungen stellt sich die Frage, ob der Bundesgesetzgeber nicht gut beraten wäre, zumindest die Beweislastumkehr zu Lasten der Partner rückgängig zu machen.

Der neue § 50 Abs. 2 SGB II, der die Bundesagentur zur verantwortlichen Stelle nach § 67 Abs. 9 SGB X erklärt, soweit ARGEn die Auf-

gaben der Agenturen für Arbeit wahrnehmen, war Gegenstand der Kritik der Datenschutzbeauftragten. Denn dieser in § 50 Abs. 2 SGB II normierten datenschutzrechtlichen Verantwortlichkeit der Bundesagentur steht die in § 44b Abs. 3 SGB II fixierte eigenverantwortliche Aufgabenwahrnehmung durch die ARGEn gegenüber. Dieser Regelungswiderspruch hat auf den Ebenen der Datenschutzbeauftragten und der ARGEn zu Kompetenzirritationen geführt, die im Interesse eindeutig handhabbarer Zuständigkeitsregelungen ausgeräumt werden sollten. Anderenfalls wurde die sich bereits manifestierende Gefahr einer Splittung der datenschutzrechtlichen Kontrollzuständigkeiten der Landesdatenschutzbeauftragten gesehen, je nachdem, ob die ARGEn Aufgaben der Arbeitsagenturen wahrnehmen oder nicht. Mit Urteil vom 20. Dezember 2007 (Az.: 2 BvR 2433/04 und 2434/04) hat das Bundesverfassungsgericht nach Kommunalverfassungsbeschwerden von Landkreisen gegen organisatorische Regelungen des Sozialgesetzbuchs II die Verfassungswidrigkeit von § 44b SGB II festgestellt. Damit wurde auch den Bedenken der Datenschutzbeauftragten Rechnung getragen. Die Entscheidung des Bundesverfassungsgerichts führt aus, dass nach der Systematik des Grundgesetzes der Vollzug von Bundesgesetzen entweder von den Ländern oder vom Bund wahrgenommen wird, nicht hingegen - wie jedoch von § 44b SGB II vorgesehen - zugleich von Bund und Land oder einer von beiden geschaffenen dritten Institution (Verbot der sog. Mischverwaltung). Zwar sei das Anliegen, die Grundsicherung für Arbeitssuchende „aus einer Hand“ zu gewähren, ein sinnvolles Regelungsziel. Dieses könne jedoch auch dadurch erreicht werden, dass der Bund für den Vollzug den Weg der bundeseigenen Verwaltung wählt, als auch dadurch, dass der Vollzug den Ländern als eigene Angelegenheit überlassen wird. Der danach vorliegende Verfassungsverstoß führt in der Regel zur Nichtigkeit der angegriffenen Norm. Mit Rücksicht auf einen geordneten Gesetzesvollzug im Bereich der Grundsicherung für Arbeitssuchende hält das Bundesverfassungsgericht angesichts der Größe der Umstrukturierungsaufgabe eine befristete Weitergeltung der nicht verfassungskonformen Regelung für gerechtfertigt, um so eine durch das Sozialstaatsprinzip gebotene Aufgabenwahrnehmung zu ermöglichen. Für eine neue verfassungskonforme Regelung hat das Bundesverfassungsgericht dem Bundesgesetzgeber eine Frist bis zum 31. Dezember 2010 gesetzt.

Die Datenschutzbeauftragten des Bundes und der Länder werden sorgsam zu beobachten haben, wie der Bundesgesetzgeber das SGB II

verfassungskonform novelliert und dabei insbesondere auch die Kontrollzuständigkeit der Datenschutzbeauftragten einer den Vorgaben des Bundesverfassungsgerichts entsprechenden Lösung zuführt.

11.2 Formulargestaltung zum Elterngeld und zur Elternzeit

Zur Erhöhung der Geburtenraten und um künftig den Müttern und Vätern die Entscheidung zu erleichtern, nach der Geburt eines Kindes dem Neugeborenen den notwendigen Schonraum für das gemeinsame Leben durch die persönliche Betreuung zu geben und deshalb für einen beschränkten Zeitraum ganz oder teilweise auf eine Erwerbstätigkeit zu verzichten, wurde mit Wirkung vom 1. Januar 2007 das Bundeserziehungsgeld durch das neue Elterngeld abgelöst. Problematisch waren dabei nicht die gesetzlichen Regelungen, sondern deren datenschutzgerechte Umsetzung aufgrund der ungewöhnlich kurzen Zeit zwischen der Vorlage des Gesetzentwurfes und dem Inkrafttreten. Trotz der Bemühungen der Länder um ein einheitliches Antragsformular für das Elterngeld konnten die dafür nötigen Prüfungen und Abstimmungen aufgrund des Zeitdrucks zur Bereitstellung der Formulare für die Antragsteller nicht abgeschlossen werden, so dass nunmehr für das Elterngeld auf der Grundlage eines kurzfristig und nur „halbherzig“ abgestimmten Entwurfs von den einzelnen Bundesländern unterschiedliche Antragsformulare genutzt werden. Da das Thüringer Ministerium für Soziales, Familie und Gesundheit den TLfD bereits zum frühestmöglichen Zeitpunkt über das Antragsverfahren zum Elterngeld informiert hatte, konnten die aus datenschutzrechtlicher Sicht gebotenen Änderungen berücksichtigt werden. Diese betrafen insbesondere die Aufnahme eindeutiger Definitionen und verständlicher Hinweise für den Antragsteller, aus denen hervorgeht, wann und unter welchen Voraussetzungen für welchen Personenkreis welche Auskünfte erteilt werden müssen. Nur dadurch lässt sich verhindern, dass Daten über das erforderliche Maß erhoben werden. Es zeigte sich aber auch hier, dass es generell hilfreich wäre, wenn die mit der Entwicklung eines Vordrucks betraute Stelle nicht nur die Erforderlichkeit der einzelnen Datenerhebungen mit der Daten verarbeitenden Stelle, sondern insbesondere auch die Verständlichkeit der Fragestellungen überprüfen würde.

Formulare, mit denen personenbezogene Daten erhoben werden, sind so zu gestalten, dass sie für den Betroffenen eindeutig, vor allem aber auch verständlich sind.

11.3 Umsetzung des Thüringer Erziehungsgeldgesetzes

Im Rahmen der Thüringer Familienoffensive wurde auch das Thüringer Erziehungsgeldgesetz novelliert. Danach erhalten seit dem 1. Juli 2006 alle Sorgeberechtigten, die ihre Hauptwohnung oder ihren gewöhnlichen Aufenthalt in Thüringen haben, für ihr Kind zwischen dem zweiten und dritten Lebensjahr unter Berücksichtigung der Geburtsfolge des Kindes ein einkommensunabhängiges Erziehungsgeld in Höhe von 150,- bis 300,- . Soweit von dem Kind ein Kindergartenplatz beansprucht wird, sind die Eltern verpflichtet, 150,- davon an die Kindereinrichtung abzutreten. Das Nähere zur Durchführung des Thüringer Erziehungsgeldgesetzes ist in einer Verordnung geregelt. Danach wird das Erziehungsgeld an die Antragsteller von den jeweiligen Wohnsitzgemeinden oder bei der Vorlage einer Abtretungserklärung durch eine Kindertageseinrichtung bzw. eine Kindertagespflegeperson an diese ausgezahlt. Für Zwecke der Planung und Nachweisführung haben die Gemeinden quartalsweise der Fachaufsicht im Landesverwaltungsamt eine zahlenmäßige Übersicht über die Inanspruchnahme des Erziehungsgeldes und der Plätze in den Tageseinrichtungen sowie zum Bearbeitungsstand der Anträge zu übergeben.

Die zum Entwurf der Verordnung vom TLfD gegebenen Hinweise, die u. a. die Zulässigkeit der Bearbeitung von Erziehungsgeldanträgen durch die Landkreise im Wege der Amtshilfe in Frage stellten oder auf Vorschriften, die unklare Vorgaben zur Datenverarbeitung enthielten, blieben weitgehend unberücksichtigt. Nach einem Hinweis durch einen Pressevertreter wurde vom TLfD auch das Antragsformular einer umfassenden datenschutzrechtlichen Prüfung unterzogen. Im Ergebnis wurde dabei festgestellt, dass eine Reihe von Daten erhoben werden sollte, die zur Antragsbearbeitung nicht erforderlich sind. Das betraf z. B. Angaben zum Familienstand, zu einem möglicherweise beabsichtigten Wohnortwechsel oder umfassende Fragestellungen zur Krankenversicherung. Man hatte dabei offenbar ohne Reflexion der neuen Rechtslage (einer einkommensunabhängigen Leistung) Fragestellungen aus dem bisherigen Antragsformular übernommen. Darüber hinaus war zunächst vorgesehen, dass den Anträgen geeignete Nachweise zur Bestätigung der Richtigkeit der Angaben, wie Kopien von Geburtsurkunden oder Meldebescheinigen beigefügt werden mussten. Es wäre aber ein Schildbürgerstreich gewesen, den Antragstellern solche gebührenpflichtigen Nachweise abzuverlangen, obwohl die

Wohnsitzgemeinde, die die Anträge bearbeitet, die erforderlichen Daten im Melderegister gespeichert hat. Deshalb wurde vom TLfD der Verzicht auf die Vorlage solcher Nachweise gefordert.

Im Ergebnis der Gespräche mit dem Thüringer Ministerium für Soziales, Familie und Gesundheit konnte das Antragsformular von vier auf zwei Seiten mit einem Ergänzungsblatt für Ausnahmefälle reduziert werden. Des Weiteren werden nur in Sonderfällen (z. B. bei Adoptionspflege und Personen mit einer Staatsangehörigkeit außerhalb der EU) sowie bei Beziehern von Kindergeld für mehrere Kinder Nachweise bzw. Kopien von Urkunden verlangt, da die Richtigkeit der Angaben im Antrag zum Wohnort und zum Sorgerecht von der Meldebehörde bestätigt werden kann. Soweit automatisierte Abrufverfahren für Meldedaten eingerichtet sind, übernimmt diese Prüfung auch die Erziehungsgeldstelle.

Wie eine Kontrolle bei der Stadt Eisenach zeigte, haben sich die Anträge in der Praxis bewährt. Da es sich aber um eine kreisfreie Stadt handelte und dort auch die Anträge zum Bundeserziehungsgeld/ Elterngeld bearbeitet werden, musste festgestellt werden, dass in der Aktenhaltung keine Trennung der Verfahren zum Bundeserziehungsgeld/Elterngeld und zum Thüringer Erziehungsgeld vorgenommen wurde. Darüber hinaus ist auf die gesonderte Vorlage einer Meldebescheinigung verzichtet worden, weil von der Erziehungsgeldstelle Zugriffsmöglichkeiten auf Meldedaten über ein automatisiertes Verfahren bestanden. Eine Kopie der Geburtsurkunde wurde von den Antragstellern aber verlangt. Zur Berechung des Thüringer Erziehungsgeldes wird von den Gemeinden ein automatisiertes Verfahren in Form einer Web-Anwendung beim Landesrechenzentrum im Rahmen einer Auftragsdatenverarbeitung genutzt. Im Rahmen der Prüfung wurde dabei festgestellt, dass neben den jeweiligen Kommunen auch das Landesverwaltungsamt Zugriff auf die Einzeldaten hat. Eine Erforderlichkeit konnte hierfür mangels einer entsprechenden Aufgabenstellung nicht festgestellt werden, da das Landesverwaltungsamt ausschließlich als Aufsichtsbehörde tätig wird. Im Ergebnis der Prüfung wurde deshalb neben der Aufhebung der Zugriffsrechte für die Aufsichtsbehörde eine Trennung der Elterngeldakten von den Thüringer Erziehungsgeldakten gefordert, mit der Maßgabe, dass die jeweiligen Unterlagen entsprechend der gesetzlichen Vorgaben aufzubewahren und anschließend zu vernichten sind. Darüber hinaus ist auf die Vor-

lage und Übernahme von Kopien der Geburtsurkunden in die Akten aufgrund der sonstigen Prüfmöglichkeiten zu verzichten.

Personenbezogene Daten dürfen in Antragsformularen nur in einem solchen Umfang erhoben werden, wie ihre Kenntnis zur Bearbeitung zwingend erforderlich ist. Nachweise sind nur erforderlich, soweit der Stelle keine anderen Unterlagen vorliegen, die die Richtigkeit der Angaben bestätigen.

11.4 Kinderschutz und Datenschutz

Die Polemik „Datenschutz darf Kinderschutz nicht verhindern“ offenbart die Hilflosigkeit einiger Politiker, die die Brisanz der Kinderschutzproblematik erst spät erkannt haben und glauben, Defizite mit dem Hinweis auf den angeblich verhindernden Datenschutz rechtfertigen zu können. Dass es bisher nicht umfassend gelungen ist, Kinderschutz wirksam und verfassungskonform zu gestalten, darf nicht zu dem anderen Extrem führen, mit dem Kinderschutz die Elterngrundrechte gleichsam aus dem verfassungsrechtlichen Bade zu schütten. Es gilt, darauf zu achten, dass Rechtsgrundlagen geschaffen werden, die die Beschränkung des Rechts der informationellen Selbstbestimmung der Eltern zugunsten des Kinderschutzes nur dann zulassen, wenn dies geeignet, erforderlich und angemessen ist. Die Grundrechtsphäre der Eltern - zu nennen sind hier neben deren Grundrecht der informationellen Selbstbestimmung auch das elterliche Erziehungsgrundrecht sowie das Grundrecht der Unverletzlichkeit der Wohnung - darf nicht auf Null reduziert werden, wenn keine konkreten Anhaltspunkte für eine Gesundheitsgefährdung des Kindes vorhanden sind. Dabei ist die Schaffung eines solchen Regelwerks, das in die hochsensiblen Beziehungen zwischen Eltern, Kind und Behörden eingreift, zugegebenermaßen kein leichtes Unterfangen. Gleichwohl ist es beispielsweise dem Thüringer Ministerium für Soziales, Familie und Gesundheit in modellhafter Weise gelungen, den Datenschutz frühzeitig in Gesetzes- und Verordnungsvorhaben zum Kinderschutz einzubinden. Auf diese Weise konnten im Vorfeld gemeinsam Regelungen gefunden werden, die das Recht der informationellen Selbstbestimmung der Eltern in verhältnismäßigem Umfang berücksichtigen. Beispiele:

- Das Thüringer Gesetz zur Verbesserung der Zusammenarbeit zwischen der Jugendhilfe, Kindertagesstätten und Schulen soll eine Gesetzeslücke im Thüringer Schulgesetz und Thüringer Kindertagesstätteneinrichtungsgesetz schließen. Bisher waren dort Rechts-

grundlagen für Übermittlungen auch von Elterndaten an das Jugendamt in Fällen der Kindeswohlgefährdung nicht vorgesehen. Künftig wird es den Schulen und Kindertagesstätten rechtlich möglich sein, bei Anhaltspunkten für eine Kindeswohlgefährdung die entsprechenden Daten an das Jugendamt zu übermitteln - so jedenfalls der mit dem TLfD abgestimmte Gesetzentwurf.

- Eingehend beraten werden musste auch der Weg, wie Wasser- und Energieversorgungsunternehmen, die im Zuge ihrer Abrechnungsaktivitäten eine Kindeswohlgefährdung feststellen (ggf. auch in Folge finanzieller Engpässe der Eltern) veranlasst werden können, diese Kenntnisse zum Wohle des Kindes einzusetzen. Dies ist weder die rechtlich vorgesehene noch die tatsächliche Aufgabe der Versorgungsunternehmen. Gefunden wurde gleichwohl eine datenschutzkonforme Lösung, die die beteiligten Interessen der Eltern, der Versorgungsunternehmen und gerade auch des Kindes zu einem sinnvollen und rechtskonformen Ausgleich bringt. Versorgungsunternehmen werden über ihre rechtlichen Möglichkeiten und Eltern über die Hilfsangebote informiert, aber eben auch darüber, dass bei aktueller Kindeswohlgefährdung Informationsweitergaben an das Jugendamt oder die Polizei durch die Versorgungsunternehmen auch gegen den Elternwillen nicht nur rechtlich zulässig, sondern notwendig und erwünscht sind.
- Damit die Jugendämter ihre Aufgaben des erzieherischen Kinder- und Jugendschutzes dem Sozialgesetzbuch VIII gemäß wahrnehmen können, sind sie auch auf die Kenntnis von Geburten angewiesen. Zu diesem Zweck müssen die entsprechenden Daten an das Jugendamt fließen, was bisher rechtlich nicht vorgesehen ist. Um im Rahmen eines Erstkontaktes die Eltern über Angebot und Hilfen des Jugendamtes und der Freien Träger der Kinder- und Jugendhilfe informieren zu können, könnte die Thüringer Meldeverordnung eine entsprechende Änderung erfahren. Der diesbezügliche Vorschlag des Thüringer Ministeriums für Soziales, Familie und Gesundheit jedenfalls wurde mit dem TLfD besprochen und ist mit dem Datenschutz kompatibel.
- Vorgesehen ist schließlich, für die Eltern Konsequenzen daran zu knüpfen, wenn sie an den Früherkennungsuntersuchungen für Kinder (U1 bis U9) nicht teilnehmen. Die hierzu notwendigen vielfältigen Datenflüsse müssen datenschutzrechtskonform ausgestaltet werden. Der TLfD wird auch hier rechtzeitig eingebunden werden.

Die Auseinandersetzung mit den datenschutzrechtlichen Implikationen des Kinderschutzes trägt dazu bei, zu verfassungskonformen Lösungen zu gelangen. Unterbleibt diese verfassungsrechtliche Ausrichtung, sind legislatives und exekutives Handeln rechtlich und damit auch gerichtlich angreifbar - unter Umständen dann auch zu Lasten des Kinderschutzes. Daher gilt es, eine verfassungsrechtlich offene Flanke gerade in Fragen des Kinderschutzes bereits im Vorfeld zu vermeiden, indem alle beteiligten Grundrechte in verfassungskonformer Weise Berücksichtigung finden. Der TLfD bietet hierzu auch weiterhin seine Mithilfe an.

11.5 Novellierung des Thüringer Rettungsdienstgesetzes

In der Vergangenheit hatte sich der TLfD auch in seinen Tätigkeitsberichten (5. TB, 5.2.9 und 6. TB, 5.3.9) mehrfach mit den Problemen bei der Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Notfallrettung befasst. Der Grundtenor war dabei stets, dass die derzeitigen Regelungen im Rettungsdienstgesetz nicht ausreichen, um den Datenschutz einheitlich und verbindlich in allen Bereichen durchzusetzen. Daneben hatten in diesem Zusammenhang u. a. auch die Aufgabenträger des Rettungsdienstes kritisiert, dass eine umfassende Qualitätskontrolle durch den ärztlichen Leiter Rettungsdienst insoweit erschwert sei, als die derzeitigen Vorschriften dem Aufgabenträger nur den Zugang zu anonymisierten Einsatzprotokollen erlauben und Ausnahmeregelungen für den ärztlichen Leiter nicht vorgesehen sind. Darüber hinaus fehlt es in Thüringen noch für die durchaus notwendigen Eingriffe in das informationelle Selbstbestimmungsrecht und das Fernmeldegeheimnis durch die Aufzeichnung von Gesprächen mit den Rettungsleitstellen im Rahmen der Notfallrettung an einer normenklaren gesetzlichen Erhebungsbefugnis. Dies ist bislang nur im Landesrettungsdienstplan geregelt, welcher keinen Gesetzesrang hat. Aus diesem Grund wird die derzeitig von der Landesregierung verfolgte Novellierung des Thüringer Rettungsdienstgesetzes ausdrücklich unterstützt. Im Rahmen der Ressortanhörung hatte der TLfD bereits Gelegenheit, sich zum Entwurf zu äußern und die aus datenschutzrechtlicher Sicht gebotenen Änderungen und Ergänzungen dem für das Rettungswesen zuständigen Thüringer Innenministerium aufzuzeigen. Diese sollen nach dem gegenwärtigen Informationsstand auch weitgehend in das Rettungsdienstgesetz aufgenommen werden.

In dem zu novellierenden Thüringer Rettungsdienstgesetz sind normenklare Regelungen zum Umgang mit allen im Rahmen der Notfallrettung zu erhebenden Daten zu treffen.

11.6 Videoüberwachung im Maßregelvollzug

Im Jahr 2007 wurde der TLfD an der Anhörung zum Gesetz zur Änderung des Thüringer Gesetzes zur Hilfe und Unterbringung psychisch Kranker beteiligt. Zum Redaktionsschluss war das Gesetzgebungsverfahren noch nicht abgeschlossen. Da bereits Videotechnik insbesondere zur Überwachung von Gebäuden in den Einrichtungen des Maßregelvollzugs eingesetzt wird oder dies beabsichtigt ist, hat der TLfD angeregt, eine eindeutige Rechtsgrundlage im Gesetz zu verankern. Das ist geboten, weil es keine allgemeine Regelung zur Videoüberwachung im Thüringer Datenschutzgesetz gibt (5.2) und zudem einige Besonderheiten im Maßregelvollzug differenzierte Regelungen erfordern. Zu unterscheiden ist dabei, ob die Videotechnik therapeutischen Zwecken oder der Gewährleistung der Ordnung und Sicherheit dient. Wird die Videotechnik für einzeltherapeutische Zwecke genutzt, dürfen Daten nur mit Einwilligung des Betroffenen bzw. seines gesetzlichen Vertreters erhoben und genutzt werden und unterliegen der ärztlichen Schweigepflicht. Eine Überwachung von Außenanlagen, Gebäuden und allgemein zugänglichen Räumen ist nur erlaubt, wenn dies zur Gewährleistung von Sicherheit und Ordnung des Maßregelvollzugs erforderlich ist. Die hierbei gespeicherten Daten dürfen nur für diese Zwecke sowie zur Strafverfolgung und für gerichtliche Verfahren verarbeitet und genutzt werden und sind unverzüglich zu löschen, wenn sie zum Erreichen des Zwecks nicht mehr erforderlich sind. In Interventions-, Aufenthalts-, Wohn- und Schlafräumen ist der Einsatz von Videotechnik nur in begründeten Einzelfällen erlaubt, soweit dies von der ärztlichen Leitung angeordnet wird und zur Abwehr einer erheblichen Gefahr für das Leben und die Gesundheit des Patienten oder Dritten unerlässlich ist. Eine Speicherung personenbezogener Daten ist in diesem Zusammenhang jedoch unzulässig, denn auch bei Bestehen eines Gefährdungspotentials – bspw. durch Selbstmordgefährdung – würde der Einsatz von Überwachungseinrichtungen in Form von Monitoren („verlängertes Auge“) ausreichen, um ein unverzügliches Eingreifen zu ermöglichen. Daher ist die Fertigung von Aufzeichnungen in solchen Fällen nicht erforderlich. Der TLfD hat in diesem Sinne entsprechende Regelungsvorschläge unterbreitet.

Der weitere Fortgang des Gesetzgebungsverfahrens zur Normierung der Videoüberwachung wird datenschutzrechtlich begleitet.

11.7 Polizei – (k)ein Wunsch ist frei

Es geschah vor nicht allzu langer Zeit im Freistaate Thüringen, dass sich über einen längeren Zeitraum hinweg zwei Bürger wiederholt mit Schriftsätzen und Anzeigeerstattungen an eine Polizeibehörde wandten. Diese nun war von solchem Verhalten genervt, zumal von den Bürgern auch Irrelevantes vorgetragen wurde. Daher wünschte sich die Polizeibehörde beim Sozialpsychiatrischen Dienst des Gesundheitsamtes eines Landkreises die Erstellung eines fachärztlichen Attestes zum psychischen Gesundheitszustand dieser Bürger, denn die Ursache für deren Verhalten könne möglicherweise in einem klinischen Befund zu finden sein. Dem Ansinnen der Polizeibehörde kam der Sozialpsychiatrische Dienst flugs nach und untersuchte die beiden Bürger, ohne sich die Frage zu stellen, ob er das durfte. Zweifel daran, ob er das Ergebnis der Polizei mitteilen durfte, hegte er auch nicht. In einem fachärztlichen Attest wurde der Polizei mitgeteilt, mit großer Wahrscheinlichkeit sei anzunehmen, dass eine psychische Krankheit Auswirkungen auf den Inhalt der Schriftsätze bzw. Anzeigen habe. Dementsprechend behandelte die Polizei dann weitere Schriftsätze bzw. Anzeigen der beiden Bürger oder auch nicht.
Diese Begebenheit ist keinem neuzeitlichen Märchenbuch entnommen, sondern spiegelt die datenschutzrechtliche Realität wider - leider! Weder verfolgte die Polizeidirektion Saalfeld mit ihrem fragwürdigen Ansinnen eine polizeirechtskonforme Aufgabe, noch finden sich Rechtfertigungsgründe für die Verletzung der ärztlichen Schweigepflicht. Die Datenverarbeitung des Sozialpsychiatrischen Dienstes konnte sich weder auf das Thüringer Datenschutzgesetz, das Thüringer Gesetz zur Hilfe und Unterbringung psychisch Kranker noch auf die §§ 203 Abs. 2 Satz 2 oder 34 StGB (Rechtfertigender Notstand) stützen. Dies führte zu einer formellen Beanstandung gegenüber dem Landratsamt des Saale-Orla-Kreises wegen Verletzung der ärztlichen Schweigepflicht notwendig.

Es bleibt zu hoffen, dass derartige Vorgänge aus dem Reich der Phantasie künftig nicht mehr die Grenze zur Realität passieren werden. Indes genügt Hoffnung allein nicht – der TLfD wird daher diesem sensiblen Bereich weiterhin sein besonderes Augenmerk widmen.

11.8 Archivierung von Patientenakten durch Privatfirma

Krankenhäuser gehen aus Kostengründen dazu über, ihre Daten durch externe Privatfirmen verwalten, insbesondere archivieren zu lassen. Gemäß § 27b Abs. 1 Satz 1 ThürKHG dürfen Patientendaten grundsätzlich nur im Krankenhaus verarbeitet, d. h. auch nur dort aufbewahrt werden. Eine Verwaltung der Daten durch eine andere Stelle (z. B. ein privates Unternehmen) im Auftrag ist gemäß § 27b Abs. 1 Satz 2 ThürKHG jedoch neben anderen Bedingungen dann zulässig, wenn eine den Voraussetzungen des § 203 StGB (Verletzung von Privatgeheimnissen; ärztliche Schweigepflicht) entsprechende Schweigepflicht beim Auftragnehmer sichergestellt ist. Ältere Rechtsprechung meinte, eine solche Schweigepflicht sei bei einem rechtlich eigenständigen und selbstverantwortlich handelnden Dienstleistungsunternehmen nicht gewährleistet. Denn dieser Personenkreis unterliege weder der Strafandrohung des § 203 Abs. 1, Abs. 2 StGB noch der des § 203 Abs. 3 (Gehilfen etc.) StGB. Somit könne die Wahrung der ärztlichen Schweigepflicht denknotwendig nicht sichergestellt werden, da die Strafandrohung des § 203 StGB insoweit leer liefe. Diese Rechtsprechung sah den Schutz der Patientendaten schließlich auch deshalb gefährdet, da ein externer Auftragnehmer nicht der Beschlagnahmefreiheit im Sinne von § 97 StPO unterliege.

Demgegenüber hat sich die Rechtsauffassung inzwischen geändert, denn Mitarbeiter eines Privatunternehmens können gemäß § 203 Abs. 2 Satz 1 Nr. 2 StGB i. V. m. § 1 Verpflichtungsgesetz als für den öffentlichen Dienst besonders Verpflichtete angesehen werden, sofern eine ordnungsgemäße Verpflichtung nach diesem Verpflichtungsgesetz erfolgte. Ist dieses der Fall, unterfallen also auch Mitarbeiter eines Privatunternehmens der Strafandrohung des § 203 Abs. 2 StGB. Damit besteht auch dort die von § 27b Abs. 1 Satz 2 ThürKHG geforderte Schweigepflicht. Zudem erstreckt sich die Beschlagnahmefreiheit gemäß § 97 Abs. 2 Satz 2 StPO auch auf personenbezogene Daten, die ein Dienstleister für eine Krankenanstalt verarbeitet. Ungeachtet weiterer datenschutzrechtlicher Aspekte, zu denen auch die Datensicherheit zählt, erscheint die Aufbewahrung von Patientenakten durch ein Privatunternehmen gemäß § 27b Abs. 1 Satz 2 ThürKHG mithin grundsätzlich zulässig. Es ist jedoch darauf hinzuweisen, dass gemäß § 27 Abs. 2 Satz 1 ThürKHG i. V. m. § 8 ThürDSG der Auftraggeber (Krankenhaus) im Fall einer Auftragsdatenverarbeitung der datenschutzrechtlich Verantwortliche bleibt.

Die Verlagerung von Verwaltungsaufgaben der Krankenhäuser auf Privatunternehmen wird nach Einschätzung des TLfD zunehmen. Dieser Prozess muss insbesondere unter dem Gesichtspunkt der Datensicherheit aufmerksam beobachtet werden.

12. Wirtschaft, Arbeit, Bau und Verkehr

12.1 Nutzung von Luftbildaufnahmen

Luftbildaufnahmen, erstellt beispielsweise von Satelliten, Flugzeugen oder Ballonen, erfassen die Erdoberfläche und dienen u. a. der Vermessungsverwaltung, der Umweltüberwachung oder der Subventionskontrolle. In Thüringen werden die Aufnahmen im Thüringer Landesluftbildarchiv gesammelt und dort für sämtliche Verwaltungszwecke zur Verfügung gestellt. Wie sich an mehreren Bürgereingaben zeigt, beauftragen insbesondere Wasser- und Abwasserverbände private Unternehmen damit, vom eigenen Verbandsgebiet Luftbildaufnahmen zu erstellen. Hierbei wird das Gebiet zu bestimmten Sonnenständen meist mit Kleinflugzeugen überflogen und mit Spezialkameras flächendeckend fotografiert. Es stellt sich die Frage, ob es sich hierbei bereits um das Verarbeiten personenbezogener Daten handelt und falls ja, welche Rechtsgrundlage dies erlaubt. Wer das Verfahren für unbedenklich hält, verweist darauf, dass eine früher bestehende Genehmigungspflicht für das Anfertigen von Luftbildaufnahmen ersatzlos entfallen sei und es sich damit um eine Nutzung von Räumen handele, die der Öffentlichkeit grundsätzlich offen stehen und auch fotografiert werden dürften. Bei dieser Betrachtungsweise ist daran zu erinnern, dass im Datenschutzrecht alles, was nicht ausdrücklich erlaubt ist, verboten ist („Verbot mit Erlaubnisvorbehalt“). Es ist daher fraglich, ob ein Fotografieren von privaten Grundstücken und Gebäuden aus der Vogelperspektive zulässig ist. Während sich ein Grundstückseigentümer mit einem hohen Sichtschutz vor neugierigen Einblicken vom Boden aus schützen kann, ist er aus der Luft jeglichen Schutzes beraubt. Darüber hinaus kann ein Grundstückseigentümer einem Dritten den Zugang zu seinem Grundstück versagen, solange das Zutrittsrecht nicht richterlich entschieden wurde. Diese Rechtsschutzmöglichkeit kann bei einer Luftbildaufnahme nicht in Anspruch genommen werden. Wie das Bundesverfassungsgericht im Zusammenhang mit der Entscheidung zur Frage der Zulässigkeit von Luftbildaufnahmen von Prominentenvillen feststellt, ist hinsichtlich eines Persönlichkeitseingriffs nicht allein auf die vorhandenen Daten, sondern

entscheidend auf deren Verarbeitungs-, Verknüpfungs- und Verwendungsmöglichkeiten abzustellen. Mithin kommt es für die Bestimmbarkeit einer Person nicht darauf an, ob eine personale Zuordnung allein anhand der Luftbilddaten möglich ist, sondern es genügt, dass ein Personenbezug via Verknüpfung von Luftbild-, Plan-, Adress- und Personendaten hergestellt werden kann.

Die bereits angesprochenen Wasser- und Abwasserzweckverbände lassen die Luftbildaufnahmen im Zusammenhang mit der Einführung von getrennten Abwassergebühren für Schmutz- und Niederschlagswasser erstellen. Um diese Gebühren getrennt zu erheben, muss den Zweckverbänden zur Berechnung der Niederschlagsmenge auf einem Grundstück bekannt sein, in welchem Verhältnis bei der gegebenen Grundstücksgröße die versiegelten, die teilversiegelten und die unversiegelten Flächen stehen. Mit der Luftbildaufnahme lässt sich der Versiegelungsgrad relativ genau bestimmen. Spätestens durch die Verschneidung der Luftbildaufnahme mit der automatisierten Liegenschaftskarte zu einem Hybridbild werden den Zweckverbänden die tatsächlichen Grundstücksverhältnisse bekannt (Lage, Eigentümer, bauliche Anlagen, Nutzungsart, Grundstücks- und Gebäudegröße usw.) und zusätzlich aus der Luftbildaufnahme die versiegelten, teilversiegelten und unversiegelten Flächen. Mit diesem Ergebnis wendet sich der Zweckverband an den Grundstückseigentümer mit der Bitte um Prüfung und Bestätigung der angegebenen Daten.

Der TLfD hält die angewandte Verfahrensweise je nach konkreter Ausgestaltung für mehr oder weniger bedenklich. Viele Zweckverbände führen das Verfahren auf die beschriebene Weise durch, ohne dass eine hierzu ermächtigende Rechtsvorschrift in Form einer Satzung vorliegt. Weder die Entwässerungssatzung, noch die Beitrags- und Gebührensatzung enthalten Regelungen über die vorgesehene Abwassergebührensplittung. In diesem Fall ergibt sich bereits aus der fehlenden Rechtsgrundlage die Unzulässigkeit der Datenverarbeitung.
Liegt eine Satzung im Zweckverband vor, die eine getrennte Gebührenberechnung für Abwasser und Niederschlagswasser vorsieht, hält der TLfD die Verfahrensweise dann für zulässig, wenn die erstellten Luftbildaufnahmen nur die unbedingt zum Erkennen des Versiegelungsgrads erforderliche Auflösung besitzt. Gegen eine maximale Bodenauflösung von etwa 20x20 cm pro (Bild-) Pixel bestehen im Regelfall keine Bedenken. Höheren Bodenauflösungen, die insbesondere Zoommöglichkeiten der Luftbildaufnahmen eröffnen, stehen

grundsätzlich persönlichkeitsrechtliche Interessen der Betroffenen entgegen.

In diesem Zusammenhang ist auch auf den Entwurf eines Thüringer Gesetzes zur Zusammenfassung der Rechtsgrundlagen und zur Neuausrichtung des Vermessungs- und Geoinformationswesens hinzuweisen. Danach soll die Einsicht in die Datenbanken des amtlichen Vermessungswesens sowie Auskünfte oder Ausgaben daraus für jedermann voraussetzungslos möglich sein. Hiergegen hat sich der TLfD in seiner Stellungnahme gewandt. Eine solche Regelung würde bedeuten, dass über die Auswertung der Liegenschaftskarte und der dazugehörigen Luftbildaufnahme des Thüringer Landesluftbildarchiv Erkundigungen über die Verhältnisse eines beliebigen Grundstücks eingeholt werden könnten und damit schutzwürdige Belange der betroffenen Grundstückseigentümer unberücksichtigt blieben. Der TLfD wird auf eine datenschutzkonforme Lösung dieser Problematik hinwirken und hierbei auch das weitere juristische Problemfeld der behördlichen Nutzung von Luftbildaufnahmen durch private Anbieter einbeziehen.

Das Erstellen von Luftbildaufnahmen privater Grundstücke kann das Persönlichkeitsrecht der Eigentümer verletzen. Durch die Verknüpfung der Luftbildaufnahmen mit dem Liegenschaftsregister liegt eine Verarbeitung personenbezogener Daten vor, die durch eine Rechtsgrundlage oder einer Einwilligung erlaubt sein muss.

12.2 Nur noch eine zentrale Führerscheindatei

Seitdem maschinenlesbare Führerscheine im Dezember 1998 eingeführt wurden, speichern die örtlichen Fahrerlaubnisbehörden die dazu notwendigen Daten nur noch automatisiert. Zur Beantragung entstandene Papierunterlagen werden nach wenigen Jahren vernichtet. Die automatisierte Speicherung der Daten erfolgt aber nicht dezentral bei den Fahrerlaubnisbehörden, sondern zentral beim Kraftfahrt-Bundesamt im Zentralen Fahrerlaubnisregister, an das die örtlichen Fahrerlaubnisbehörden Änderungen und Löschungen mitteilen. Dabei entstand ein Übertragungsproblem: Weil die Daten nur nach und nach von den örtlichen Fahrerlaubnisbehörden in das Zentrale Fahrerlaubnisregister eingestellt werden können, durften gemäß § 65 Abs. 10 Satz 2 StVG die örtlichen Fahrerlaubnisbehörden die im Zentralen Fahrerlaubnisregister gespeicherten Daten zunächst bis zum 31. Dezember 2005 weiter führen. Da abzusehen war, dass auch zu

diesem Termin noch nicht alle Daten an das Zentrale Fahrerlaubnisregister geliefert sein würden, hatte der Bundesgesetzgeber eine Verlängerung um ein Jahr beschlossen. Obwohl immer noch nicht alle Fahrerlaubnisdaten an das Zentrale Fahrerlaubnisregister übermittelt wurden und davon auszugehen ist, dass hiervon sogar die überwiegende Anzahl der Datensätze betroffen ist, erfolgte eine erneute Fristverlängerung bisher nicht. Formal ist somit die weitere Speicherung von personenbezogenen Daten in den örtlichen Fahrerlaubnisregistern eigentlich nunmehr unzulässig und die Daten sind dort deshalb zu löschen. Dies ist praktisch nicht durchführbar, da die Daten teilweise unwiederbringlich verloren gehen würden. Gegen eine unbestimmte Fristverlängerung bestehen aus datenschutzrechtlicher Sicht Bedenken, da dies eine andauernde Doppelspeicherung der Fahrerlaubnisdaten zur Folge hätte.

Die endgültige Löschung der Fahrerlaubnisdaten bei den örtlichen Fahrerlaubnisbehörden muss genau geprüft werden und ist an verschiedene technische Voraussetzungen geknüpft. Der Datenbestand muss vom Kraftfahrt-Bundesamt in das Zentrale Fahrerlaubnisregister übernommen worden sein und die Daten müssen von den örtlichen Fahrerlaubnisbehörden im automatisierten Verfahren abgerufen werden können. Dementsprechend muss ein datenschutzgerechtes Online-Dialogverfahren zum Zentrale Fahrerlaubnisregister für Anfragen und Auskünfte eingerichtet werden. Voraussetzung für eine vollständige Übermittlung der Fahrerlaubnisdaten ist aber zunächst, dass alle diese Daten bei den örtlichen Fahrerlaubnisbehörden in automatisierter Form vorliegen. Der weitere Verlauf der Angelegenheit soll sich bei den hierfür zuständigen Bundesstellen in der Diskussion befinden.
Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass bei der Online-Anbindung aller örtlichen Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister alle erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um eine integere, authentische, revisionsfähige und transparente Verarbeitung der Fahrerlaubnisdaten auf Dauer zu gewährleisten. Es handelt sich immerhin um Datensätze von ca. 50 Millionen Fahrerlaubnisinhabern, die zukünftig ausschließlich automatisiert in diesem Register verarbeitet werden sollen. Bislang ist die Frage ungelöst, inwieweit die örtlichen Fahrerlaubnisbehörden oder aber das Kraftfahrt-Bundesamt die Verantwortung für die Richtigkeit der dort gespeicherten Fahrerlaubnisdaten tragen. Es fehlen sowohl im Straßenverkehrsgesetz als auch in der Fahrerlaubnisverordnung entsprechende Vorschriften, die die Verant-

wortlichkeiten und die Verfahrensweise konkret regeln. Bisher ungeklärt ist auch, wie sich die datenschutzrechtlichen Kontrollbefugnisse zwischen dem BfDI und den LfD aufteilen.

Die Schaffung von Zentralregistern, auf die mehrere Stellen lesenden und schreibenden Zugriff haben, erfordert eindeutige und umfassende Festlegungen hinsichtlich der Verantwortlichkeiten sowie der zu ergreifenden organisatorischen und technischen Maßnahmen.

13. Bildung, Wissenschaft, Forschung

13.1 Abwicklung der Rückerstattung der Lernmittelpauschale

Nachdem unter Mitwirkung des TLfD im letzten Berichtszeitraum eine datenschutzkonforme Umsetzung der Thüringer Lehr- und Lernmittelverordnung erreicht werden konnte (6. TB, 13.1), musste sich der TLfD in diesem Berichtszeitraum mit den Durchführungsregelungen zur Abwicklung der Rückerstattung der Lernmittelpauschale befassen. In einem Normenkontrollverfahren hatte das Thüringer Oberverwaltungsgericht die Erste Verordnung zur Änderung der Thüringer Lehr- und Lernmittelverordnung vom 4. Mai 2005 wegen Verstoßes gegen finanz- und verfassungsrechtliche Grundsätze für unwirksam erklärt, mit der Folge, dass die von den Eltern gezahlten Lernmittelpauschalen wieder zurückerstattet werden mussten. Um hierbei den datenschutzrechtlichen Forderungen von Beginn an zu genügen, hatte das Thüringer Kultusministerium den TLfD gebeten, das Verfahren datenschutzrechtlich zu begleiten. Hierbei galt es insbesondere klare und eindeutige Zuständigkeiten festzulegen, den Umfang der Datenverarbeitung und die Personen, die Kenntnis von den Daten erhalten sollten, auf ein Minimum zu beschränken.

Im Ergebnis wurde ein Verfahren entwickelt, bei dem die Anträge in verschlossenen Umschlägen von den Eltern mit der Beschriftung „Rückerstattung der Lernmittelpauschale“ im Sekretariat der jeweiligen Schule abgegeben werden mussten und von dort unverzüglich und verschlossen an den Lehrmittelverantwortlichen zur Prüfung bzw. zum Abgleich mit den Einzahlungsunterlagen weitergeleitet wurden. Anschließend wurden die Anträge auf dem Dienstweg dem Thüringer Landesamt für Statistik übergeben, welches im Rahmen einer Auftragsdatenverarbeitung die Antragsdaten elektronisch für die Staatskasse, von der die Auszahlungen angewiesen wurden, aufbereiten

musste. Da in den Schulen die jeweiligen Einzahlungslisten vorlagen, konnte erreicht werden, dass der Umfang der Datenerhebungen auf dem Antragsformular zur Rückzahlung auf wenige Angaben beschränkt wurde. Beschwerden oder Kritiken zur Datenverarbeitung bei der Abwicklung der Rückerstattung der Lernmittelpauschale wurden nicht bekannt.

13.2 Bekanntgabe von Noten

Ob die Schul- oder Hochschul-(Zeugnis-, Leistungsnachweis-) Note den Mitschülern oder Kommilitonen zur Kenntnis gegeben werden darf, ist Gegenstand datenschutzrechtlicher Erwägungen. Die Qualität der Note als personenbezogenes Datum liegt im Falle ihrer Verkündung vor der Klasse nicht nur bei schlechten Noten auf der Hand. Dem entsprechend bedarf ein solcher Eingriff in das Recht der informationellen Selbstbestimmung einer Rechtsgrundlage. Zwar erlaubt z. B. das ThürSchulG (§§ 57, 48 Abs. 3) eine Datenübermittlung aus Gründen der Transparenz in pädagogischer Verantwortung. Jedoch wird dieser Aufgabe bereits dadurch entsprochen, dass die Noten – anonym – in einem Notenspiegel einschließlich Notendurchschnitt offenbart werden. Auf diese Weise sind Schüler und Eltern in der Lage, das individuelle Leistungsniveau in Relation zu dem der Klasse zu setzen.

Ein Verlesen von Noten vor der gesamten Klasse ist, von Einzelfällen einer Vorbildwirkung einmal abgesehen, datenschutzrechtlich nicht erforderlich und damit nicht zulässig.

13.3 Durchführung der Schülerstatistik

In einem Beschluss hatte die Kultusministerkonferenz bereits im Jahr 2000 festgestellt, dass für die Koordinierung politischer und planerischer Maßnahmen und auch im Rahmen der internationalen Zusammenarbeit auf dem Gebiet des Schulwesens aktuelle und vergleichbare Schuldaten der Länder unerlässlich sind. Dabei würde aber nach Auffassung der Verantwortlichen die Bereitstellung von Daten in zusammengefasster, d. h. in aggregierter Form aus den Ländern dem Informationsbedarf nicht mehr genügen, sodass man sich auf einen sog. „Kerndatensatz für schulstatistische Individualdaten der Länder“ verständigte. Mit diesem sollten in allen Bundesländern für statistische Zwecke Individualdaten der Schüler und Lehrer vorgehalten werden.

Um darüber hinaus auch die Bildungsverläufe von Schülern in Form von Schülerkarrieren (sog. Längsschnittuntersuchungen) zusammenstellen und auswerten zu können, mündete dies letztlich in der Absicht, eine einheitliche und bundesweite Datenbank mit allen Schülerindividualdaten zu schaffen. Zum Zwecke einer schülerbezogenen Datenzusammenführung sollten nach bundeseinheitlichen Kriterien Identifikationsnummern vergeben werden.

Da Totalerhebungen generell von den Datenschutzbeauftragten äußerst kritisch beurteilt werden und Unklarheiten zur Bildung und Nutzung der Schüleridentifikationsnummer im Hinblick auf eine mögliche Reanonymisierung der Daten bestehen, gibt es seitens der Datenschutzbeauftragten erhebliche Bedenken gegen die vorgesehene Schaffung einer zentralen länderübergreifenden Schülerdatenbank. In einer Entschließung (Anlage 9) haben deshalb die Datenschutzbeauftragten des Bundes und der Länder die Öffentlichkeit auf diese Probleme hingewiesen. Im Ergebnis zahlreicher Gespräche zwischen den Mitgliedern der Kommission für Statistik der Kultusministerkonferenz und Vertretern der Konferenz der Datenschutzbeauftragten des Bundes und der Länder konnte erreicht werden, dass nun auf die Schaffung einer zentralen länderübergreifenden Datenbank verzichtet wird. Gleichzeitig sollen Wege gesucht werden, um bei einem geringstmöglichen Eingriff in das informationelle Selbstbestimmungsrecht der Schüler, Lehrer und Erzieher die notwendigen statistischen Übersichten zu ermöglichen. Dazu gehören u. a. Verschlüsselungsverfahren für die Individualdatensätze, die einerseits eine Zusammenführung der dezentral gespeicherten Datensätze eines Schülers in einer Längsschnittuntersuchung erlauben, aber andererseits ausschließen, dass die Identität des Schülers rekonstruiert bzw. festgestellt werden kann und so der gläserne Schüler entsteht.

Unabdingbare Voraussetzung für das Gesamtverfahren ist aber, dass in allen Ländern für die Erhebung der Daten und ihre statistische Aufbereitung und Auswertung die notwendigen Rechtsgrundlagen geschaffen werden. In Thüringen liegen mit dem Thüringer Schulgesetz und der Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich die Rechtsgrundlagen vor, um die für die Statistik erforderlichen Individualdaten zu erheben und ausschließlich für statistische Zwecke zu verarbeiten und zu nutzen (6. TB, 5.2.1). Hinsichtlich des Umfangs der Datenerhebung müsste ggf. die Verordnung an den Kerndatensatz angepasst werden. Zu klären sind

aus datenschutzrechtlicher Sicht darüber hinaus noch eine Reihe Fragen zur Bereitstellung von Daten für bundesweite Auswertungen.

Bei Festlegungen zum einheitlichen Kerndatensatz und bei der Auswertung von Daten aus der Schulstatistik sind die statistikrechtlichen Vorgaben zur Trennung von Verwaltung und Statistik und zur Wahrung des Statistikgeheimnisses zu beachten.

13.4 Keine Umgehung des Statistikgeheimnisses

Nach § 16 Abs. 4 des Bundesstatistikgesetzes darf das Statistische Landesamt einer obersten Landesbehörde für Zwecke der Planung, nicht jedoch für die Regelung von Einzelfällen, Tabellen mit statistischen Ergebnissen übermitteln, auch soweit Tabellenfelder nur einen einzigen Fall ausweisen. Voraussetzung ist, dass diese Übermittlungen für den konkreten Fall in einer eine Bundesstatistik anordnenden Rechtsvorschrift ausdrücklich zugelassen ist. Erfüllt werden diese Voraussetzungen nach § 6 Abs. 2 des Hochschulstatistikgesetzes für die Übermittlung von Ergebnissen aus der Hochschulstatistik an das für das Hochschulwesen zuständige Thüringer Kultusministerium. Dadurch soll dem Thüringer Kultusministerium für Zwecke der Hochschulplanung der Zugang zu vollständigen und unverfälschten statistischen Aussagen über die von den Statistischen Landesämtern erhobenen Daten über die Hochschulen, ihre Studenten und das eingesetzte Personal ermöglicht werden. Gleichzeitig dient die Regelung aber auch zur Klarstellung, dass es sich bei der Übermittlung von Einzelangaben nur um unvermeidliche Ausnahmen handeln darf. Dies ergibt sich insbesondere bei verfassungskonformer Auslegung der Vorschrift. Hierbei wird deutlich, dass die Übermittlung einzelner Felder, die nur einen einzigen Fall beinhalten, nur in ihrer Funktion als Teil der Gesamtinformation erlaubt wird. Es darf aber gerade nicht um deren dominierenden Inhalt gehen, weil dies ansonsten zu einer verschleierten Übermittlung statistischer Einzeldatensätze führen und den Grundsätzen der amtlichen Statistik (Trennung von Verwaltung und Statistik, Wahrung des Statistikgeheimnisses) widersprechen würde. Daher gilt auch für die Übermittlung von Daten aus der Hochschulstatistik und hierbei insbesondere für personenbezogene Daten der Studenten und Dozenten die Verpflichtung, dass die Aufbereitung der Einzeldaten zu einer strukturierten anonymisierten Form führen muss. Diesen Vorgaben würde somit eine Gliederung widersprechen, bei der der Ausnahmecharakter zur Regel würde, d. h. wenn die geforderte

Tabellengestaltung dazu führt, dass ein großer Teil der Tabellenfelder jeweils nur einen konkreten Fall widerspiegelt, was auch für Zwecke der Planung nicht erforderlich ist, da mit den Informationen keine Einzelfälle gelöst, sondern lediglich grundlegende Strukturen dargestellt werden sollen.

Im Rahmen einer Prüfung der Umsetzung des Hochschulstatistikgesetzes wurde festgestellt, dass die Anforderungen des Thüringer Kultusministeriums an das Thüringer Landesamt für Statistik zur Übermittlung von Tabellen aus der Hochschulstatistik in einer solchen Detailliertheit gestellt waren, dass in einzelnen Tabellen in der überwiegenden Zahl der Felder nur ein einziger Fall ausgewiesen wurde. Unter Hinweis auf die Bestimmungen im Bundesstatistikgesetz und im Hochschulstatistikgesetz wurden deshalb das Thüringer Kultusministerium und das Thüringer Landesamt für Statistik aufgefordert, den Umfang der Datenübermittlungen auf das erforderliche und zulässige Maß zu beschränken, was, wie sich im Ergebnis zeigte, bei einer präzisen Angabe der jeweiligen Planungsaufgaben und der Fragestellung zur Bereitstellung der erforderlichen Tabelleninformationen durchaus möglich ist.

Auch wenn der Gesetzgeber die Übermittlung von Statistiken, in denen in einzelnen Feldern nur jeweils ein einziger Fall ausgewiesen ist, für Zwecke der Planung an oberste Landesbehörden zulässt, ist bei der Tabellengestaltung darauf zu achten, dass die Zahl der Felder, die davon betroffen sein dürfen, Ausnahmen sind. Anderenfalls würde dies einen nicht gewollten Personenbezug für eine Vielzahl der Daten ermöglichen.

13.5 Chipkarteneinsatz an Hochschulen

Vor mehr als zehn Jahren beschäftigte sich der TLfD erstmalig mit dem Einsatz von Chipkarten für Studenten und Mitarbeiter an den Thüringer Hochschulen. Inzwischen sind solche Karten an zahlreichen Hochschulen in der gesamten Bundesrepublik eingeführt. In Thüringen hat sich die Hochschulchipkarte „THOSKA“ – Thüringer Hochschul- und Studentenwerkskarte durchgesetzt, wobei eine Hochschule ihre Karte „THOSKA+“ nennt, weil dort zusätzlich zu dem unsichtbar in die Karte integrierten kontaktlosen Chip ein sichtbarer, kontaktbehafteter Kryptochip Verwendung findet, der die Nutzungsmöglichkeiten der Karte deutlich ausweitet. Die Verwendung von Studentenchip-

karten aufgrund der bis Ende 2006 gegebenen Rechtslage war nur auf freiwilliger Basis zulässig (3. TB, 13.5). Die Hochschule musste den Studierenden die Wahl lassen, ob diese die Chipkarte mit der damit verbundenen Infrastruktur verwenden oder aber auf den Studentenausweis lediglich als Identifikationsnachweis zurückgreifen wollten. Mit der am 1. Januar 2007 in Kraft getretenen Novelle des Thüringer Hochschulgesetzes wird in § 10 Abs. 3 festgelegt, dass Mitarbeiter und Studierende durch die Hochschulen zur Verwendung von Chipkarten insbesondere für Zwecke der Zutrittskontrolle, Identitätsfeststellung, Zeiterfassung, Abrechnung oder Bezahlung verpflichtet werden können. Damit ersetzte die Chipkarte den bisherigen Studentenausweis.

Wenn man nach den Gründen fragt, warum sich immer mehr Hochschulen für die Einführung einer Chipkarte entscheiden, so wird mit Einsparpotentialen in der Verwaltung gerechnet, da diese dann von den üblicherweise anfallenden Routinearbeiten, z. B. den halbjährlichen Rückmeldungen, entlastet werde. Ebenfalls soll die Karte zu einer schnelleren Abwicklung von Massenverfahren führen. Beispiele hierfür sind die bargeldlose Bezahlung in der Mensa, von Kopien oder Gebühren in der Bibliothek. Vorteile für die Studenten ergeben sich, indem diese z. B. nicht mehr ihre Zeit in langen Warteschlangen verbringen müssen und auch nicht auf die Wahrnehmung der Öffnungszeiten des Studentensekretariats angewiesen sind.

Neben den Vorteilen der Chipkarte sehen einige Studenten auch Risiken für ihr Recht auf informationelle Selbstbestimmung, die mit der Nutzung dieses Verfahrens verbunden sind. Auf der Chipkarte sind zunächst diejenigen personenbezogenen Daten sichtbar, die auch ein früherer Studentenausweis in Papierform enthielt. Dies sind das Passbild, der Name, der Vorname, das Geburtsdatum, der Studiengang mit Fachsemester, die Matrikel-Nummer sowie das Semesterticket der Bahn und die Gültigkeitsdauer des Ausweises. Für die Benutzung der Uni-Bibliothek ist auf der Rückseite noch ein Balkencode aufgedruckt. Zusätzlich sind für die Mitarbeiter der akademische Grad und die Funktionsbezeichnung aufgedruckt. Die Chipkarte findet in erster Linie als Identifikationsmedium und nicht als Datenträger Verwendung. Deshalb enthalten die Chips an personenbezogenen Daten nur die ohnehin auf der Karte sichtbaren sowie zusätzlich verschiedenen technisch relevanten Prüfnummern und ein Zertifikat mit einem öffentlichen und privaten Schlüssel.

Die erweiterten Selbstbedienungsfunktionen der Karte, die zusätzlich den bereits erwähnten Kryptochip enthält, sind nur nutzbar, wenn zusätzlich zur Karte auch eine PIN an einem der Selbstbedienungsterminals auf dem Campus eingegeben wird. Der Studierende kann dort selbständig Bescheinigungen, etwa über erworbene Prüfungsleistungen, Noten, Studienbescheinigungen usw. ausdrucken oder Adressänderungen, Prüfungsan- und -abmeldungen vornehmen. Der Benutzer kann seine PIN ändern und zur Verschlüsselung von vertraulichen Datenkommunikationen mit der Hochschule einsetzen.

In Eingaben von Studenten an den TLfD stellten diese die ausreichende Datensicherheit der Chipkarte in Frage. Die Karte sei duplizierbar, von Dritten zu sabotieren, der RFID-Chip aus großem Abstand auslesbar und der Kryptochip kurzfristig zu entschlüsseln. Hierzu ist zunächst festzustellen, dass in Anwendung von § 9 ThürDSG die Hochschule die technischen und organisatorischen Maßnahmen zu ergreifen hat, die erforderlich sind, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Bei einem Verlust der Karte sind aus datenschutzrechtlicher Sicht die Missbrauchsmöglichkeiten durch Dritte nicht grundsätzlich höher einzuschätzen als bisher bei Verlorengehen bzw. dem Diebstahl eines Schlüssels, eines Portemonnaies oder des Studentenausweises in Papierform. Soweit die Chipkarte als Sichtausweis Anwendung findet, ist davon auszugehen, dass die äußere Fälschungssicherheit eher höher einzuschätzen ist, als bei den herkömmlichen Papierausweisen. Nach Angaben einer Thüringer Hochschule seien gefälschte Studentenausweise in Papierform verschiedentlich aufgetaucht, während dies bei den Chipkarten noch nicht beobachtet worden sei.

Bei der Zutrittsfunktion dürfte es keinen Unterschied machen, ob nun ein herkömmlicher Schlüssel verloren geht oder aber eine Karte mit einem entsprechend programmierten RFID-Chip. Beim elektronischen Zutrittssystem dürfte der mögliche Schaden sogar leichter zu beheben sein, indem die Zutrittsberechtigung für die verloren gegangene Chipkarte, wie auch für alle anderen Funktionen, zentral von der Hochschule gesperrt wird. Die finanziellen Folgen des Verlustes einer Chipkarte sind unter Umständen sogar niedriger für den betroffenen Studenten. Die Karte kann maximal 50 Euro Guthaben aufladen, beim elektronischen Schließsystem entfällt ein kostenintensiver Austausch

des gesamten Schließsystems. Die als verloren gemeldete Karte wird für ungültig erklärt und der Student kann gegen eine Gebühr eine neue Karte erwerben.

Aus den Unterlagen des Herstellers ist zu entnehmen, dass ein Auslesen des Chips bis höchstens 100 Millimeter möglich ist. Ob der kontaktlose RFID-Chip auf weit größere Entfernung auszulesen ist, kann dahingestellt bleiben. Der technische Aufwand, der voraussichtlich hierfür betrieben werden müsste, insbesondere um dies unbemerkt zu tun, steht in keinem Verhältnis zu dem möglichen Nutzen. Hinsichtlich der Anwendung des Kryptochips unterliegt der Nutzer ebenso wie bei Bank- oder Kreditkarten einer gewissen Sorgfaltspflicht. So ist die individuelle PIN Dritten gegenüber geheim zuhalten. Ohne die Kenntnis dieser PIN können die beschriebenen Funktionalitäten des Chips nicht genutzt werden. Ob es möglich ist, die PIN durch eine Manipulation des Chips zu umgehen oder diese zu generieren, ist nicht bekannt. Aber auch hier dürfte der zu betreibende Aufwand den Nutzen weit übersteigen. Im Ergebnis liegen dem TLfD keine stichhaltigen Gründe dafür vor, die es erforderlich machen würden, eine Einstellung oder wesentliche Änderung des Chipkarteneinsatzes zu fordern.

Die Thüringer Hochschulen können ihren Mitgliedern und Angehörigen die Verwendung von Chipkarten verbindlich vorschreiben. Grundsätzliche datenschutzrechtliche Bedenken gegen die bisher bekannt gewordenen Systeme bestehen nicht.

13.6 Evaluationen an Hochschulen

Ganz allgemein wird unter Evaluation die Bewertung eines bestimmten Gegenstands oder auch das Ergebnis einer solchen Bewertung verstanden. Für den TLfD ist die Zuständigkeit für eine Evaluation im Hochschulbereich dann gegeben, wenn hiermit die Verarbeitung oder Nutzung personenbezogener Daten von Studierenden oder Dozenten verbunden ist. Im Regelfall betrifft dies die studentische Bewertung von Lehrveranstaltungen. Dabei teilen die Dozenten meist am Semesterende einer Vorlesung, eines Seminars, eines Kolloquiums usw. einen Erhebungsbogen an die Studierenden aus, der ausgefüllt wieder zurückgegeben werden soll. Auf den Erhebungsbögen werden die Teilnehmer um Auskunft gebeten, wie ihnen die Veranstaltung gefallen hat, was verbessert werden könnte, wie der Inhalt der Lehrveranstaltung dargebracht wurde, ob noch Fragen offen geblieben sind etc.

Diese Bewertungen erfolgen oft durch Ankreuzmöglichkeiten –„trifft voll zu“- bis –„trifft überhaupt nicht zu“-. Darüber hinaus können Felder vorgesehen sein, in denen durch die Studierenden Verbesserungs- und Änderungsvorschläge unterbreitet werden sollen.

Die Evaluationsvorhaben der Hochschulen führen bei den Lehrenden häufig zu Fragen hinsichtlich des Umgangs mit den dabei gewonnenen Ergebnissen. Den zu evaluierenden Personen sind vielfach die genauen Beurteilungskriterien der Hochschulleitung ebenso wenig bekannt, wie die sich möglicherweise daraus ergebenden Folgen oder gar Sanktionen. Festlegungen, mit welchem Gewicht die Studierendenevaluation in eine Gesamtbeurteilung eingeht, gibt es häufig nicht. Arbeitsrechtliche Konsequenzen können von den Betroffenen nicht eingeschätzt werden. Zu berücksichtigen ist auch, dass die Studierenden bei der Beurteilung einer konkreten Lehrveranstaltung völlig frei agieren können und es nicht auszuschließen ist, dass die Beurteilung nicht nur von fachlichen Kriterien geleitet ist, sondern auch von Vorlieben der Studierenden, der vorherigen Benotung durch den Lehrenden und weiteren äußeren Faktoren abhängt. Rechtfertigen muss der Studierende seine Beurteilung nicht.

Der TLfD wurde verschiedentlich um eine Beurteilung gebeten, ob eine Teilnahme an den beschriebenen Evaluationsverfahren für die Lehrenden durch die Hochschule verpflichtend vorgeschrieben werden kann. Hierbei ist zu berücksichtigen, ob die Evaluation vor oder nach dem in Kraft treten des neuen Thüringer Hochschulgesetzes durchgeführt wurde. Bis Ende 2006 konnten Lehrende nach Auffassung des TLfD nicht verpflichtet werden, an einer Evaluation zu ihrer Person teilzunehmen. Die Teilnahme war nur auf freiwilliger Basis möglich. Der Erlass einer entsprechenden hochschuleigenen Evaluationsordnung scheiterte wegen des Fehlens einer gesetzlichen Ermächtigung. Mit in Kraft treten des neuen Thüringer Hochschulgesetzes hat der Landesgesetzgeber in § 8 ThürHG eine gesetzliche Grundlage geschaffen, die die Hochschulen verpflichtet, Evaluationen durchzuführen. Dabei sind alle Mitglieder und Angehörige der Hochschulen zur Mitwirkung verpflichtet. Die Studierenden wirken ausdrücklich an der Bewertung individueller Lehrveranstaltungen mit. Das Nähere zu den Evaluationsmaßnahmen regelt der Senat durch Satzung. Hierin ist zu bestimmen, welche Daten verarbeitet und genutzt werden dürfen und wie eine Veröffentlichung der daraus gewonnenen Ergebnisse erfolgt.

Wie der dem TLfD übergebene Entwurf einer Evaluationsordnung zeigt, ist die konkrete datenschutzgerechte Umsetzung des Verfahrens schwierig. Eine gute Möglichkeit zur normenklaren Gestaltung der Satzung ist es, wenn der Evaluationsbogen selbst Bestandteil der Evaluationsordnung wird. Allerdings muss bei einer Änderung des Erhebungsbogens dann auch die entsprechende Anlage angepasst werden. Eine weitere Schwierigkeit bei der Umsetzung des Verfahrens ergibt sich daraus, dass einerseits die Studierenden zur Mitwirkung an der Evaluation verpflichtet sind, andererseits die Teilnahme aber anonym erfolgen soll. Bei einer Kontrolle der Mitwirkungspflicht kann diese Anonymität der Studierenden u. U. aber nicht mehr gewährleistet werden. Hier wurde vom TLfD vorgeschlagen, die Teilnahme der Studenten an dem Evaluationsverfahren im Interesse sachgerechter Bewertungen freiwillig zu gestalten. Bisweilen ist der Teilnehmerkreis der Studierenden in manchen Fächern überschaubar und die Teilnehmer sind dem Lehrenden oftmals einzeln bekannt. Daher kann bei einem Evaluationsbogen, der nicht nur das Ankreuzen von Kästchen, sondern eigene schriftliche Äußerungen verlangt, die Anonymität aufgrund einer möglichen Identifizierung des Schriftbildes durch den Lehrenden nicht mehr gewährleistet sein. Als Lösung hat eine Hochschule die Verfahrensweise festgelegt, dass ein Studierender die Erhebungsbögen einsammelt und diese in einen Umschlag steckt, der verschlossen im Dekanat abgegeben wird. Der Lehrende hat somit keinen unmittelbaren Zugriff auf die Bögen und enthält später nur aufbereitete Ergebnistabellen. Für nicht erforderlich hält es der TLfD, die Ergebnisse eines Evaluationsverfahrens in personenbezogener Form in der Hochschule öffentlich bekannt zu geben. Eine Veröffentlichung ist nur dann zulässig, wenn ein einzelner Lehrender hierin einwilligt oder nicht erkennbar wird. Dies wird gewährleistet durch eine Veröffentlichung von zusammengefassten Daten. Die Auswertungen beziehen sich dabei nicht auf namentlich genannte Lehrende, sondern z. B. auf die Ergebnisse eines gesamten Fachbereichs.

Aufgrund des neuen Thüringer Hochschulgesetzes dürfen die Thüringer Hochschulen die dort Lehrenden zur Teilnahme an Evaluationsverfahren verpflichten. Dies gilt auch für die Mitwirkung der Studierenden. Die Hochschulen sind aber gehalten, die diesbezüglich zu erlassenen Evaluierungssatzungen so zu gestalten, dass sich für den Betroffenen klar ergibt, welche Daten zu welchen Zwecken über ihn verarbeitet und genutzt werden. Hierbei ist der verfassungsrechtliche Erforderlichkeitsgrundsatz zu beachten.

13.7 Nationale und Internationale Schulleistungsstudien

In den letzten Jahren wurde der Begriff PISA zum Inbegriff von Schülerleistungsuntersuchungen, die je nach politischer Couleur zur Bestätigung der Richtigkeit oder der notwendigen Änderung in der Bildungspolitik herangezogen werden. Weitgehend unbeachtet bleibt dabei, dass zur Datengewinnung Eingriffe in das informationelle Selbstbestimmungsrecht der Schüler, Eltern und Lehrer erforderlich sind. Dabei handelt es sich bei PISA nur um eine der vielen, überwiegend auch internationalen Vergleichsstudien zum Bildungsstandard in Deutschland. Neben der PISA- Studie, bei der Kompetenzen der 15-jährigen Schüler im Lesen und in der mathematischen und naturwissenschaftlichen Grundbildung bisher in drei Erhebungswellen 2000, 2003 und 2006 untersucht wurden, gab es im Berichtszeitraum insbesondere für die Schüler der 4. Klassen weitere wissenschaftliche Studien wie IGLU zum Leseverständnis, TIMSS zu den Kenntnissen in den Fächern Deutsch und Mathematik, das STEG-Projekt 2006/2007 zur Entwicklung von Ganztagsschulen oder die Übergangsstudie des Max-Planck-Instituts, bei der der Übergang der Schüler der 4. Klassen von der Grundschule auf die weiteren Schulen untersucht wurde. Wie bereits bei gleichartigen Projekten in der Vergangenheit (3. TB, 13.7; 4. TB, 13.6; 6. TB, 13.5) wurden die Landesdatenschutzbeauftragten von den Verantwortlichen um eine datenschutzrechtliche Begleitung gebeten, wobei sich wiederum der Hauptschwerpunkt der datenschutzrechtlichen Beratung auf die umfassende Aufklärung aller Betroffenen und die Maßnahmen zur Gewährleistung der Vertraulichkeit der Angaben der Schüler, Eltern und Lehrer richtete. Hierbei war auch in diesem Berichtszeitraum festzustellen, dass sich im Interesse aller Betroffenen und beteiligten Stellen die rechtzeitige und konstruktive Zusammenarbeit zwischen den Forschungseinrichtungen und Datenschutzbeauftragten bewährt hat und die Hinweise und Anregungen zum Datenschutz weitgehend Berücksichtigung finden.

Im Interesse aller Betroffenen und Beteiligten empfiehlt sich, in Forschungsprojekte, bei denen personenbezogene Daten verarbeitet oder genutzt werden sollen, möglichst von Beginn an den Beauftragten für Datenschutz der Einrichtung und bei länderübergreifenden Vorhaben ggf. auch den Landesbeauftragten für den Datenschutz einzubeziehen.

13.8 Fehlende Benutzungsordnungen in Archiven

Nach § 16 ThürDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Vor einer Löschung sind die Daten dem zuständigen Archiv zur Übernahme anzubieten. Entsprechend diesen Vorgaben ist jede öffentliche Stelle verpflichtet, nach Ablauf der Aufbewahrungsfristen alle im Verwaltungsvollzug anfallenden personenbezogenen Unterlagen dem zuständigen Archiv zur Übernahme anzubieten. Dieses entscheidet nach archivarischen Grundsätzen, ob die Unterlagen in das Archiv übernommen und dauerhaft aufbewahrt werden. Zu den weiteren Aufgaben der öffentlichen Archive gehören dann gemäß § 7 Abs. 1 ThürArchivG die Erfassung, Verwahrung, Erhaltung und Erschließung des übernommenen Archivguts und dessen Bereitstellung zur Benutzung. Die damit verbundene Verfahrensweise haben die Gemeinden, Landkreise und kommunalen Verbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, die ihr Archivgut in eigener Verantwortung und Zuständigkeit archivieren, durch Satzung nach den §§ 4, 5 ThürArchivG vorgegebenen Grundsätzen zu regeln. Zur Gewährleistung des informationellen Selbstbestimmungsrechts sind in den Benutzerordnungen nach Maßgabe des Thüringer Archivgesetzes auch Bestimmungen zum Umfang der zu erhebenden Benutzerdaten und ihrer weiteren Verwendung sowie zum Antragsverfahren für die Benutzung personenbezogenen Archivguts aufzunehmen.

Bei Kontrollen, Anfragen oder Beschwerden muss immer wieder festgestellt werden, dass daran - wenn überhaupt - erst zuletzt gedacht wird. Vielen öffentlichen Stellen in Thüringen sind die Rechtsvorschriften zum Archivwesen nicht bekannt oder sie werden nicht eingehalten. Das betrifft durchaus nicht nur die kleinen Gemeinden. Grund dafür ist neben der Unkenntnis der geltenden Aufbewahrungsfristen auch die Sorge, man könne die Akten ja noch einmal benötigen. Die Verwaltungsakten werden dann solange aufbewahrt, wie der dafür benötigte Platz vorhanden ist. Teilweise werden die personenbezogenen Unterlagen nach Ablauf der Aufbewahrungsfristen nur in gesonderte Räume verbracht, die als Archiv bezeichnet werden, ohne dass überhaupt die Archivwürdigkeit der Unterlagen festgestellt wurde. Darüber hinaus wird außer Acht gelassen, dass für die weitere Nutzung dieser Unterlagen ausschließlich die archivrechtlichen Bestimmungen gelten, die in einer Satzung auf der Grundlage des Thü-

ringer Archivgesetzes festzulegen sind. Dass dies auch namhafte Archive betreffen kann, zeigte eine Anfrage zur Nutzung der Archive der Stiftung Gedenkstätten Buchenwald und Mittelbau-Dora. Hier bedurfte es erst einer förmlichen Beanstandung durch den TLfD, um eine den Vorgaben des Thüringer Archivgesetzes entsprechende für alle potentiellen Nutzer verbindliche und nachvollziehbare Benutzerordnung (Satzung) für das Archiv durchzusetzen.

Gibt es keine gesetzlichen Vorgaben, dann müssen alle Behörden und öffentlichen Einrichtungen für sämtliche Verwaltungsunterlagen Aufbewahrungsfristen festlegen. Bei einer Übernahme der Unterlagen in ein Archiv ist deren weitere Benutzung durch Satzung zu regeln.

13.9 Voreilige Meldungen an BAföG-Ämter

Durch eine Eingabe wurde bekannt, dass eine private Schule alle Auszubildenden, die unentschuldigt länger als drei Tage dem Unterricht fernblieben, an das zuständige Amt für Ausbildungsförderung meldete. Dies wurde mit § 47 Abs. 3 BAföG begründet, wonach die Schule verpflichtet ist, das Amt für Ausbildungsförderung unverzüglich zu unterrichten, wenn der Auszubildende die Ausbildung abbricht, um eine grundlose Zahlung öffentlicher Fördermittel zu vermeiden. Hierzu hat der TLfD die Auffassung vertreten, dass dieses Vorgehen dem Verhältnismäßigkeitsgrundsatz widerspricht, da sich in solchen Fällen nur selten ein Ausbildungsabbruch bestätigt. Vielmehr ist eine Übermittlung von Schülerdaten nur dann geboten, wenn tatsächliche Anhaltspunkte für einen Ausbildungsabbruch, etwa ein längeres unentschuldigtes Fernbleiben vom Unterricht, vorliegen. Nachfolgend hat das Thüringer Kultusministerium mitgeteilt, dass es den Rechtsstandpunkt des TLfD teilt und in diesem Sinne die Ämter für Ausbildungsförderung angewiesen hat.

14. Entwicklungen der automatisierten Datenverarbeitung

14.1 Entwicklungen der IuK

Der TLfD hat nach § 40 Abs. 5 ThürDSG die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung und ihre Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stel-

len zu beobachten. Im Zeitalter der Globalisierung werden zunehmend technische Normen zur Informationstechnik seitens der EU vorgegeben. Mit der neuen Richtlinie des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt (Dienstleistungsrichtlinie), wird nun auch politisch eine engere Zusammengehörigkeit der Staaten und Völker Europas bei der Nutzung des Internets vorangetrieben. So müssen nach Art. 8 Dienstleistungsrichtlinie (Elektronische Verfahrensabwicklung) alle Mitgliedstaaten 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. Diese Verpflichtung muss bis zum 28. Dezember 2009 umgesetzt werden, sodass, wenn noch nicht geschehen, nun zügig an einer entsprechenden IT-Infrastruktur gearbeitet werden muss. Für Thüringen bedeutet dies bspw. die Public-Key-Infrastruktur (PKI-Konzept) der Thüringer Landesverwaltung so voranzutreiben, dass auch tatsächlich „problemlos aus der Ferne“ elektronisch alle Verfahren abgewickelt werden können. Um die Integrität der Daten und die Authentizität des Absenders auch rechtsverbindlich sicherzustellen, bedarf es eines weitsichtigen PKI-Konzeptes (15.4).

In einer weiteren Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten wird bspw. auch für die in Deutschland seit 1. November 2007 ausgegebenen elektronischen Reisepässe mit integriertem Fingerabdruck (5.5) vorgeschrieben, dass die biometrischen Daten in Pässen und Reisedokumenten zweckgebunden nur zur Prüfung der Authentizität des Dokumentes und Identität des Inhabers genutzt werden dürfen. Analog dazu schließt das bundesdeutsche Passgesetz eine bundesweite Datenbank der biometrischen Daten aus (§ 4 Abs. 3 PassG) und untersagt zudem die Speicherung personenbezogener Daten in Dateien beim automatischen Lesen des Passes. Dies gilt auch für Abrufe aus dem polizeilichen Fahndungsbestand, die zu einer Feststellung geführt haben (§ 17 PassG). In dem bei der Polizei vorhandenen automatisierten Fingerabdruck-Identifizierungssystem befinden sich derzeit Fingerabdrücke von mehr als 3.270.000 Personen. Nach Angaben des Bundeskriminalamtes ist der Fingerabdruck als ein unveränderliches Merkmal für die kriminalistische Arbeit besonders

interessant. Monatlich werden ca. 30.000 Fingerabdruckblätter zum Abgleich mit dem automatisierten Fingerabdruck-Identifizierungssystem eingereicht. Deshalb ist aus datenschutzrechtlicher Sicht die derzeitige vorgeschriebene Zweckbindung der ePass-Daten auf EU- und Bundesebene zu begrüßen.

Ein weiteres bundesweites Verfahren, welches in dem Berichtszeitraum eingeführt wurde und bis 2010 in allen Bundesländern installiert wird, ist der Digitalfunk für Behörden und Organisationen mit Sicherheitsaufgaben. Dieses neue Sprech- und Datenfunksystem soll zukünftig der Polizei, den Feuerwehren, den Rettungskräften, der Bundesanstalt Technisches Hilfswerk, den Zollbehörden und den Nachrichtendiensten in Deutschland zur Verfügung stehen und wird mit ca. 500.000 Nutzern das weltweit größte seiner Art sein. Die derzeitige Planung sieht vor, dass bereits Mitte 2008 der Digitalfunk in den ersten von 45 Netzabschnitten für den operativ-taktischen Einsatz zur Verfügung steht. Auch wenn in der ersten Phase Thüringen noch nicht dabei sein wird, ist abzuschätzen, dass sich im kommenden Berichtszeitraum der TLfD mit dem System befassen wird. In Hamburg kam der Digitalfunk übrigens bereits zur Fußballweltmeisterschaft 2006 zum Einsatz, so dass am praktischen Beispiel technische, organisatorische und taktische Hinweise für die Projektgruppe gewonnen werden konnten.

Aber nicht nur der Digitalfunk war ein technisches Schlagwort bei der Fußballweltmeisterschaft. Die RFID-Chips auf allen Eintrittskarten, die der Kontrolle zur Identitätsprüfung an den Stadien dienten und die damit verbundene Datenverarbeitung war Neuland für die Veranstalter. RFID-Chips werden schon sehr lange von Sportveranstaltern genutzt und zunehmend auch von der Industrie und Wirtschaft eingesetzt, was aus datenschutzrechtlicher Sicht, z. B. aufgrund der Möglichkeit einer heimlichen Profilbildung, jedoch nicht unbedenklich ist (14.3). Auch das Bundesfinanzministerium dachte über neue Möglichkeiten der Authentifizierung am PC nach und bot den Behörden die Nutzung des ELSTER-Verfahrens an (9.3). Fraglich bleibt, ob es mit der in diesem Jahr geplanten Einführung des elektronischen Personalausweises, einschließlich der Möglichkeit der Nutzung der qualifizierten elektronischen Signatur, tatsächlich auf Dauer zwei Authentifizierungsstellen auf Bundesebene geben soll und ob diese im Rahmen der Datensparsamkeit erforderlich sind. Im Übrigen dürften wegen der Diskussion der Pläne für die heimliche Online-Durchsuchung (10.1)

die Bürger Angeboten des Staates eher skeptisch gegenüber stehen, so dass nicht nur die Nutzung von ELSTER, sondern alle eGovernment-Projekte auf Bundes- und Länderebene an Akzeptanz verlieren könnten. Zudem müssen sich die Bürger zunächst auf die Änderung des Telekommunikationsgesetzes einstellen, die ab 1. Januar 2008 eine verpflichtende Speicherdauer ihrer Verkehrsdaten von 6 Monaten vorsieht (4.1). Unternehmen und Behörden sind daher gut beraten, die Internet- und E-Mail Nutzung am Arbeitsplatz für dienstliche und private Nutzung konkret zu definieren (4.3). Für Thüringen hat das Thüringer Finanzministerium entsprechende Richtlinien herausgegeben, welche aber die einzelnen Behörden von ihren Pflichten hinsichtlich notwendiger technisch-organisatorischer Maßnahmen nicht entbinden (15.7). In diesem Zusammenhang sei erwähnt, dass das Corporate Network der Landesverwaltung derzeit auf MPLS umgestellt wird, so dass mit der zusätzlichen Nutzung der LiSS-Boxen eine Verschlüsselung der Daten zwischen den einzelnen Behörden auf Antrag möglich ist (15.5).

14.2 Sicherheit bei Instant Messaging

Deutschlandweit verfügen nach Angaben des aktuellen statistischen Jahrbuchs 2007 61,4 % der Haushalte über einen Internetzugang, wobei die neuen Bundesländer mit 55,6 % vertreten sind. Dabei werden die Internetanschlüsse nicht nur zum Surfen nach Wissen und zum klassischen Dateitransfer, sondern auch zunehmend für E-Mail als Kommunikationsmittel genutzt. Allerdings hat E-Mail den Nachteil, dass man nicht weiß, wann der Empfänger die zugestellten Informationen lesen wird. So sind für dringende Kontaktaufnahmen weiterhin der Telefonfestnetzanschluss mit 93,8 % und die Mobiltelefone mit 80,6 % erhalten geblieben. Zunehmend ist aber der Trend, den Kommunikationsbedarf weder mit dem Telefon noch per E-Mail über das Internet, sondern mit einem sog. „Instant Messenger“ durchzuführen. Instant Messaging-Systeme (z. B. AOL Instant Messenger, Microsoft Network Messenger, Yahoo Messenger und ICQ) stehen im Internet kostenlos bereit und sind leicht auf dem PC zu installieren. Mit einer dann noch einzurichtenden Kennung inclusive Benutzerpasswort ist dieses Programm schnell einsatzfähig. Mit Hilfe einer sog. „Buddy-Liste“ , in der der Nutzer seine Kommunikationspartner eintragen kann und jederzeit sieht, ob diese online oder offline geschaltet sind, lässt sich mit einem einfachen Klick auf den Kontaktnamen der direkte Kontakt aufbauen. Ist der Kontakt hergestellt, kann man nicht nur in

Echtzeit seinem Gegenüber Nachrichten zukommen lassen und dieser wiederum sofort antworten (Chat), sondern auch eine Sprachverbindung aufbauen. Weiterhin können u. U. Dateien, Bilder und Videos gesendet und bei entsprechender Konfiguration vorhandene Webcams zugeschaltet werden. Marktforscher gehen davon aus, dass schon heute für viele der Instant Messenger eine ähnliche Bedeutung wie Telefon oder E-Mail hat und das bis zum Jahr 2013 ca. 95 % aller Arbeitskräfte in globalen Unternehmen in Echtzeit per Instant Messaging kommunizieren werden. Besonders attraktiv ist dieses Kommunikationsmedium für Jugendliche. Medienpädagogische Studien zeigen, dass in der Altersgruppe der 12- bis 19-Jährigen die IM-Nutzung von 41% (2005) auf 72% (2007) angestiegen ist.

Mit solchen Systemen sind, aus datenschutzrechtlicher Sicht eine Reihe von Gefahren verbunden, die vor einer Installation zu beachten bzw. zu regeln sind. Beispielsweise besteht beim Einrichten eines Messenger-Profils für den Nutzer die Möglichkeit Geburtsdatum, Ort, Freizeitinteressen, Geschlecht und Adresse einzugeben. Diese Angaben werden allen anderen Nutzern des jeweiligen Instant Messenger zu Recherchezwecken zur Verfügung gestellt, um so eine schnelle und gezielte Kontaktaufnahme zu erreichen. Dies hat zum Nachteil, dass man teilweise unerwünscht kontaktiert wird, nur weil man einer gewissen Personengruppe (differenziert nach Alter, Geschlecht o. a.) angehört oder unerlaubt Werbung auf Grund eines Hobbyeintrages zugesandt bekommt. Deshalb wird empfohlen, so wenig wie möglich Informationen preiszugeben. Des Weiteren sollte man sich die Zustimmung zur Eintragung in „Buddy-Listen“ genau überlegen, da der Kontaktpartner dann leicht in Erfahrung bringen kann, wann man online ist. Dies kann innerhalb eines Unternehmens oder öffentlichen Stelle zur Mitarbeiterüberprüfung führen. Deshalb ist Systemen, die dem Nutzer die Möglichkeit geben, wahlweise sich „online“ oder „offline“ anzeigen zu lassen, der Vorrang zu geben. Hinsichtlich geplanter Datenübertragungen über einen Instant Messenger sollte man sich vorab erkundigen, ob das Produkt schon die Funktionalität besitzt, Dateien verschlüsselt zu übertragen und ob dies die Nutzung des gleichen Protokolls am anderen Client voraussetzt. Auch für Instant Messaging-Systeme gibt es bereits Softwareupdates, um Schwachstellen zu korrigieren. So war es z. B. zeitweise möglich, dass Angreifer mit präparierten JPEG-Dateien einen Pufferüberlauf am Computer erzeugen konnten, welcher u. U. zu einem Absturz des betreffenden Programms, zur Verfälschung von Anwendungsdaten, zur Beschädi-

gung von Datenstrukturen und zum Einschleusen von weiteren Programmen führen kann. Auch Hersteller von Firewalls müssen sich auf die neue Kommunikationstechnologie einstellen, um Systeme weiterhin von außen zu schützen und von innen keine Daten unbefugt durchzulassen. Das Bundesamt für Sicherheit in der Informationstechnik schätzt derzeit ein, dass öffentliche Instant Messaging-Systeme unsicher sind und nicht für vertrauliche und geheime Informationen genutzt werden dürfen (vgl. Beispielrichtlinie des Bundesamts für Sicherheit in der Informationstechnik „IT-Sicherheit im KRITIS-Unternehmen“, Seite 189).

Bei der Produktauswahl von Instant Messenger sollte nicht nur auf die Funktionalitäten für die tägliche Arbeit, sondern auch auf angebotene Sicherheitsfunktionen geachtet werden. Hinweise und Anregungen können in einer vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten Diplomarbeit „Sicherheitsaspekte von Instant Messaging“ (http://www.bsi.de/gshb/deutsch/hilfmi/diplomarbeiten/DA_Schildt_IM-Aspekte.pdf), die sehr ausführlich für die meistgenutzten Messenger die Funktionalitäten und die jeweiligen Sicherheitslücken darstellt, nachgelesen werden. Öffentliche Stellen, die private Nutzung von E-Mail und Internet am Arbeitsplatz erlauben, sind gut beraten, die Nutzung von Instant Messanger-Systemen zu untersagen.

Instant Messaging-Systeme sind schon sehr stark verbreitet und werden zunehmend an Bedeutung gewinnen. Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik sind sie weiterhin unsicher und sollten nicht zur Übertragung von vertraulichen und geheimen Informationen genutzt werden.

14.3 RFID-Technologie - das Internet (nicht nur) der Dinge

Über die Funktion der RFID-Technologie wurde bereits ausführlich berichtet (6. TB, 1.12). Zum damaligen Zeitpunkt wurde eingeschätzt, dass bei der Entwicklung der RFID-Technologie Fragen der Informationssicherheit und des Datenschutzes eine noch untergeordnete Rolle spielen. Durch Abhören der Kommunikation zwischen dem Transponder und dem Erfassungsgerät oder dem Auslesen auf dem Transponder gespeicherter Daten durch Vortäuschen eines autorisierten Erfassungsgerätes besteht weiterhin die Gefahr des Verlustes der Vertraulichkeit der zu verarbeitenden Daten. Aber auch der Verlust der Integrität der Daten durch unautorisierte Schreibzugriffe auf den

Transponder kann drohen oder die Verfügbarkeit von RFID-Systemen beispielsweise durch Störungen des Datenaustausches über Luftschnittstellen kann gefährdet sein.

Da die RFID-Technologie unaufhaltsam Einzug in den Alltag genommen hat, als Beispiel sei hier der Ticketverkauf bei der Fußball-Weltmeisterschaft 2006 genannt, und zu erwarten ist, dass neben Lebensmitteln auch Personalausweise, Geldscheine, Kleidungsstücke und beispielsweise Medikamentenpackungen mit RFID-Tags versehen werden könnten, befasste sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erneut mit der RFID-Technologie. Ihre Entschließung (Anlage 10) richtet sich insbesondere an Hersteller und Anwender im Handel und Dienstleistungssektor, diese Technologie unter Berücksichtigung des Prinzips der Datensparsamkeit, der Zweckbindung, Vertraulichkeit und Transparenz einzusetzen. So forderte sie zum Schutz der Persönlichkeitsrechte der Betroffenen eine Kennzeichnungspflicht, keine heimliche Profilbildung, die Vermeidung der unbefugten Kenntnisnahme und eine Deaktivierungsmöglichkeit. Ein Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder beobachtet die technische Entwicklung sehr aufmerksam und beschreibt in seiner Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ mit Stand 2006 detailliert die möglichen Risiken beim Einsatz solcher RFID-Systeme. Die Orientierungshilfe ist auf der Homepage des TLfD abrufbar.

Aber nicht nur die Datenschutzbeauftragten des Bundes und der Länder haben den dringenden Handlungsbedarf gesehen. So förderte das Bundesministerium für Bildung und Forschung im Rahmenprogramm Microsysteme 2004 - 2009 eine Studie „Technologieintegrierte Datensicherheit bei RFID-Systemen“. Das Bundesamt für Sicherheit in der Informationstechnik arbeitet derzeit an einem entsprechenden Entwurf einer Technischen Richtlinie, welche typische RFID-Einsatzfelder formuliert und entsprechende Maßnahmeempfehlungen enthalten wird. Auch der Europäische Datenschutzbeauftragte befürchtet in einer Stellungnahme zur „RFID-Mitteilung der EU-Kommission“, dass Gefahren von RFID-Systemen außer Acht gelassen werden könnten, da sie auf den ersten Blick keine persönlichen Daten verarbeiten. Solche Systeme können aber eine Schlüsselrolle bei der Entwicklung der europäischen Informationsgesellschaft spielen und müssten, für den Fall, dass der bestehende Rechtsrahmen nicht ausreiche, durch weitere Gesetze begleitet werden.

Falls Maßnahmen der Wirtschaft in Form von Selbstverpflichtungen keinen ausreichenden Schutz der Betroffenen gewährleisten, muss der Gesetzgeber eingreifen.

15. Technische Entwicklung in der Thüringer Landesverwaltung

15.1 Thüringer eGovernment

Im Bereich des Thüringer eGovernment sind im Berichtszeitraum einige Basiskomponenten nur langsam vorangekommen. So hat es vor allem größere zeitliche Verzögerungen beim Aufbau einer komplexen Serviceplattform für interne und externe Online-Dienstleistungen der Thüringer Landes- und Kommunalverwaltung (6. TB, 1.8) gegeben. Ende 2006 hat das Thüringer Finanzministerium schließlich den Vertrag mit dem Generalunternehmer zur Erstellung dieses Service Portals gekündigt und die Leistungen neu ausgeschrieben. Das Service Portal war Ende 2007 noch nicht fertig gestellt.

Neben dem Service Portal war der TLfD an weiteren eGovernment-Projekten beratend tätig, wie beispielsweise dem Zentralen Personalverwaltungssystem ZEPTA (6.1) oder dem Haushaltsmanagementsystem HAMASYS (15.3). Darüber hinaus wird derzeit in den einzelnen Ressorts ein Dokumentenmanagementsystem (VISkompakt) eingeführt. Wie bereits berichtet (6. TB, 5.1.3), wurde hierzu eine ressortübergreifende Arbeitsgruppe eingerichtet, an der auch der TLfD beratend mitarbeitet. Zu den datenschutzrechtlichen Fragestellungen bei derartigen Systemen hat der Arbeitskreis eGovernment der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“ zusammengestellt, die den Ressorts als Hilfestellung bei der Einführung eines solchen Systems dienen kann. Die Orientierungshilfe ist auf der Homepage des TLfD abrufbar.

Der TLfD wird auch in Zukunft im Rahmen seiner personellen Möglichkeiten beratend bei der Einführung von eGovernment-Projekten mitwirken.

15.2 eGovernment durch Nutzung des Standards OSCI

In zahlreichen Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen werden personenbezogene Daten übertragen. Dabei kann die Vertraulichkeit, Integrität und Authentizität nur durch den Einsatz dem Stand der Technik entsprechender Verschlüsselungs- und Signaturverfahren gewährleistet werden. In regelmäßigen Abständen veröffentlicht das Bundesministerium des Innern „Standards und Architekturen für eGovernment-Anwendungen“ (SAGA), in denen Standards, Verfahren und Methoden des Einsatzes der Informationstechnik in den Behörden beschrieben und Empfehlungen, insbesondere zur Gestaltung von eGovernment-Angeboten der öffentlichen Verwaltung, gegeben werden. Solche zentral festgelegten Standards tragen auch dazu bei, die Sicherstellung der Interoperabilität zwischen Anwendungen und verschiedenen Behörden zu gewährleisten. So legt Version 3.0 der SAGA bspw. das Datenübermittlungsprotokoll OSCI-Transport v1.2 obligatorisch fest (http://www.kbst.bund.de/saga). OSCI (Online Service Computer Interface) umfasst eine Vielzahl von Protokollen, die für die Anforderungen im eGovernment hinsichtlich der Unterstützung von Transaktionen in Form von Web Services und deren vollständige Abwicklung über das Internet geeignet sind und durch die OSCI-Leitstelle im Auftrag des KoopA ADV (dem der Bund, die Länder und die kommunalen Spitzenverbände angehören; www.koopa.de)) und anderer Auftraggeber erstellt werden. OSCI-Transport v1.2 gilt derzeit als sicheres Übertragungsprotokoll und ermöglicht je nach Bedarf der Anwendung auch verbindliche Online-Transaktionen durch Einsatzmöglichkeiten von qualifizierten elektronischen Signaturen. Derzeit wird das Konzept OSCI-Transport v2.0 diskutiert (www.osci.de), wobei noch nicht klar ist, ob die begrüßungswerten Datenschutz-Eigenschaften der Vorgangsversion erhalten bleiben sollen.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung die vom KoopA ADV getroffene Festlegung, in eGovernment-Projekten für die Übertragung personenbezogener Daten den Standard OSCI-Transport einzusetzen, begrüßt. Gleichzeitig weist die Konferenz darauf hin, dass die durch OSCI angestrebte durchgehende Sicherheit nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden darf (Anlage 1). Viele Bundesländer, so auch Thüringen, orientieren sich teilweise schon an den SAGA, nicht zu-

letzt, weil bereits Bundesverfahren in den Ländern vor Ort zur Anwendung kommen, die OSCI-Transport zwingend festschreiben. So schreibt bspw. die Passdatenerfassungs- und Übermittlungsverordnung allen Passbehörden vor, dass die Datenübertragung der Passantragsdaten von den Passbehörden an den Passhersteller auf der Grundlage des Übermittlungsprotokolls OSCI-Transport in der jeweils gültigen Fassung erfolgen muss bzw. bis zum 31. Oktober 2009 umzusetzen ist (7. TB, 5.5). Auch mit der Ersten Bundesmeldedatenübermittlungsverordnung wurde festgelegt, dass Meldebehörden bei Datenübertragungen zwischen den Meldebehörden unmittelbar oder über Vermittlungsstellen, über verwaltungseigene Kommunikationsnetze oder das Internet, das Datenübermittlungsprotokoll OSCI-Transport in der jeweils gültigen Fassung anzuwenden haben. Analog dazu schreibt § 5 Abs. 2 Thüringer Meldeverordnung bei der Datenübertragung an das Landesrechenzentrum die Nutzung von OSCI-Transport vor.

Auch bei der Version 2.0 von OSCI müssen bisherige Datenschutzstandards der Vorgängerversion beibehalten werden. Die Datenschutzbeauftragten sind bereit, dazu in den entsprechenden Gremien mitzuarbeiten.

15.3 Haushaltsmanagementsystem

HAMASYS, das bislang größte eGovernment-Verfahren der Thüringer Landesverwaltung (6. TB, 1.8.1), nutzen mittlerweile 118 Behörden aus allen Verwaltungszweigen mit etwa 1.000 Nutzern, in der Mehrzahl Mitarbeiter der Haushaltsabteilungen. Letztendlich werden es ca. 2.000 Nutzer sein. Anfang 2007 wurde bekannt, dass die zur Mitarbeiterschulung verwendete Datenbank keine fiktiven, sondern personenbezogene Daten zu natürlichen und juristischen Personen des privaten Rechts enthält. Der TLfD hat daraufhin gefordert, diese Daten, für deren Speicherung keine Erforderlichkeit im Zusammenhang mit Schulungszwecken besteht, zu löschen oder zu anonymisieren. Darauf hin wurde vom Thüringer Finanzministerium angewiesen, künftig nur solche Daten in der Schulungsdatenbank zu speichern, die keine Rückschlüsse auf persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zulassen und eine Löschung der personenbezogenen Daten vorgenommen. In diesem Zusammenhang wurde das Thüringer Finanzministerium darauf hingewiesen, dass zwischen den Auftraggebern und dem Zentrum für Informationsverarbeitung (Auftragnehmer) jeweils Vereinbarungen zur Auftrags-

datenverarbeitung abzuschließen sind. Nur so ist es möglich, die Rechte und Pflichten in einem solch komplexen Datenverarbeitungsprojekt praktisch handhabbar abzugrenzen.

Der TLfD wird die weitere Einführung des Verfahrens begleiten und die Nutzung des Verfahrens in einer Behörde überprüfen.

15.4 PKI-Konzept in der Thüringer Landesverwaltung

Beim Aufbau einer landesweiten PKI-Infrastruktur in der Thüringer Landesverwaltung ist u. a. festzulegen, welche Sicherheitsstandards bei der elektronischen Unterschrift durch öffentliche Stellen gelten sollen (4. TB, 15.8). Können bei einer fortgeschrittenen Signatur mehrere Bedienstete einer Stelle einen gemeinsamen Signaturschlüssel verwenden, so setzt die qualifizierte Signatur voraus, dass der zugehörige Signaturschlüssel nur einem einzelnen Bediensteten zugeordnet ist. Die dafür erforderliche Schlüsselverwaltung ist zwar aufwändiger, erfüllt aber auch höhere z. T. gesetzlich vorgeschriebene Sicherheitsanforderungen. Bislang kommt in der Thüringer Landesverwaltung nur die fortgeschrittene Signatur unter der Nutzung der TESTA-Plattform zum Einsatz und wird bspw. beim HAMASYS in der Thüringer Landesverwaltung (6. TB, 1.8.1; 7. TB, 15.3) eingesetzt. In einer neu gegründeten Arbeitsgruppe zum PKI-Konzept der Thüringer Landesverwaltung, in der Vertreter aller Ministerien und der TLfD beratend teilnehmen, wird nunmehr ein zentrales PKI-Konzept diskutiert, welches auch die Nutzung von qualifizierten elektronischen Signaturen einschließt. Als eine der Grundsatzfragen ist dabei zu klären, für welche Verfahren fortgeschrittene oder qualifizierte elektronische Signaturen in den jeweiligen öffentlichen Stellen benötigt werden. Ob der Einsatz einer qualifizierten oder nur einer fortgeschrittenen Signatur für notwendig angesehen wird, kann durchaus unterschiedlich beurteilt werden. Unabhängig von der Kostenlage ist jedoch bei Dokumenten, bei denen eine Sicherstellung der Rechtsverbindlichkeit zu gewährleisten ist, der Einsatz von qualifizierten elektronischen Signaturen gesetzlich vorgeschrieben (z. B. nach § 3a ThürVwVfG oder § 2 Abs. 3 ThürERVVO).

Neben der Frage, wann welche Signaturen zum Einsatz kommen müssen, ist durch die Arbeitsgruppe u. a. zu klären, wie die einzelnen Ressorts die eindeutige und zuverlässige Identifizierung ihrer Mitar-

beiter durch den Zertifizierungsdiensteanbieter bei der Beantragung qualifizierter Signaturschlüssel sicherstellen können (§ 5 Abs. 1 SigG). Die PKI-Infrastruktur bildet die Basistechnologie für die Umsetzung der eGovernment-Projekte der Thüringer Landesverwaltung. Während in einzelnen Bundesländern bereits richtungweisende Entscheidungen hinsichtlich einer landesweiten PKI-Struktur getroffen und umgesetzt wurden, fehlt es in Thüringen noch an zentralen Vorgaben. Insbesondere steht die Frage, will und kann sich Thüringen eine eigene PKI-Infrastruktur leisten. Diese Frage kann allerdings nicht die Arbeitsgruppe beantworten, sondern bedarf einer zentralen Entscheidung. Die Notwendigkeit, schnellstmöglich eine diesbezügliche Entscheidung herbeizuführen, wird nicht nur durch die Thüringer Verordnung über den elektronischen Rechtsverkehr deutlich, sondern auch durch die neuen EG-Vorgaben. So fordert die EG-Richtlinie über Dienstleistungen im Binnenmarkt (vom 12. Dezember 2006), bis zum 28. Dezember 2009 sicherzustellen, 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. Es wird zwar nicht ausdrücklich die Nutzung der qualifizierten elektronischen Signatur vorgeschrieben, aber es lässt sich auch schwer vorstellen, dass ohne Sicherstellung der Rechtverbindlichkeit von elektronischen Dokumenten Vorgänge auf Dauer „problemlos aus der Ferne“ effizient bearbeitet werden können.

Er muss zeitnah eine Entscheidung über eine PKI-Infrastruktur getroffen werden, in der auch der gesetzlich vorgeschriebene Einsatz der qualifizierten Signatur in allen davon betroffenen Behörden vorgesehen ist.

15.5 Leitungsverschlüsselung im CN

Es wurde bereits berichtet, dass die Vertraulichkeit bei der Datenübertragung innerhalb des CN durch Verschlüsselung der Datenströme (Leitungsverschlüsselung) abgesichert werden kann (4. TB, 15.4). Bei Bedarf konnten Behörden die dazu notwendigen Kryptoboxen beantragen, sodass von Haus zu Haus eine gesicherte Übertragung möglich war. Das entsprechende Managementsystem wurde dabei zentral durch befugte Administratoren des Thüringer Landesrechenzentrums

ausgeübt. Seit März 2005 wurden die Standorte des CN auf das moderne Netzprotokoll Multi Protocol Label Switching (MPLS) umgestellt und die Behörden schrittweise angeschlossen. MPLS ist die grundlegende Technologie, mit der die logische Trennung der Anschlüsse und Teilnetze des CN umgesetzt werden kann. Derzeit sind für den Freistaat auf Providerebene folgende Virtuelle Private Netze eingerichtet: das Landesverwaltungsnetz, das kommunale Netz und das Polizeinetz. Provider des MPLS Thüringen ist die Deutsche Telekom. Da MPLS selbst keine Funktionen für eine gesicherte Datenübertragung aufweist, sind in den Behörden zusätzliche Verschlüsselungsboxen (LiSS-Boxen) zur Datenverschlüsselung notwendig. Nach erfolgreichem Anschluss einer öffentlichen Stelle Thüringens an das definierte MPLS durch die Telekom wird vom Thüringer Landesrechenzentrum auf Antrag der jeweiligen Behörde die neue LiSS-Box in Betrieb genommen. Derzeit befinden sich 361 LiSS-Boxen im Einsatz. Diese LiSS-Boxen sind LINUX- basierte multifunktionale Sicherheitssysteme, wobei seitens des Landes nur die Funktion VPN/IPsec für eine sichere Datenübertragung genutzt wird. Die komplette Administration der LiSS-Boxen erfolgt vom Thüringer Landesrechenzentrum aus, welches auch die vom Hersteller bereitgestellten Updates und Backups auf die Boxen einspielt.

Im Ergebnis eines Informationsgespräches 2006 wurde eingeschätzt, dass mit dem für das LiSS-System eingesetzten Protokoll IPsec in der Variante ESP-Header und Tunnelmodus die Vertraulichkeit der übertragenen Daten gewährleistet wird sowie die Integrität der Daten und die Authentifizierung der Quelle geprüft werden kann. Des Weiteren entsprachen die bei der Datenübertragung eingesetzten kryptographischen Verfahren zur Absicherung der Vertraulichkeit, Integrität und Authentizität der Daten den aktuellen sicherheitstechnischen Standards. Es wurde eingeschätzt, dass es keine grundlegenden datenschutzrechtlichen Bedenken gegen den Einsatz des LiSS-Systems gibt. Die aus sicherheitstechnischer Sicht kritischen Anmerkungen zur Zugangskontrolle, Passwortwechsel und Protokollierung bei der Administration wurden teilweise vom Thüringer Landesrechenzentrum aufgegriffen und hierfür notwendige finanzielle Mittel beantragt. Derzeit werden neue Verschlüsselungsboxen im Thüringer Landesrechenzentrum getestet und auch die Forderungen des TLfD zwecks Umsetzung geprüft. Des Weiteren lag für das System keine hinreichende Dokumentation vor, sodass insbesondere für die Nutzer der ange-

schlossenen Stellen keine transparenten Informationen zu den eingesetzten sicherheitstechnischen Technologien und Maßnahmen sowie zu eventuellen Schwachstellen und hiermit möglicherweise verbundenen sicherheitstechnischen Risiken einsehbar sind. Der TLfD forderte, in einem Sicherheitskonzept die technischen und organisatorischen Maßnahmen incl. Schwachstellen darzulegen. Das Thüringer Landesrechenzentrum sicherte im Januar 2007 zu, die für das LiSS-System zu ergreifenden technischen und organisatorischen Maßnahmen in das gegenwärtig in der Überarbeitung befindliche Sicherheitskonzept für das CN zu berücksichtigen. Leider wurde dieses auch ein Jahr danach nicht umgesetzt und eine kurzfristige Fertigstellung nicht in Aussicht gestellt, was als Verletzung der Verpflichtung aus § 9 Abs. 2 ThürDSG zu bewerten ist. Dies ist umso schwerwiegender, als bereits Projekte wie HAMASYS (15.3) diese Technologie aus datenschutzrechtlicher Sicht nutzen sollten.

Aus datenschutzrechtlicher Sicht entsprechen die derzeit im Einsatz befindlichen Verschlüsselungsboxen dem Stand der Technik. Unverständlich bleibt, dass das Sicherheitskonzept des Corporate Network der Thüringer Landesverwaltung 4 Jahre keine Aktualisierung erfahren hat. Hier besteht dringender Handlungsbedarf, nicht nur weil § 9 Abs. 2 ThürDSG dies vorschreibt, sondern weil auf diesem die Sicherheitskonzepte der angeschlossenen Behörden aufbauen.

15.6 Einsatz von BlackBerry in der Thüringer Landesverwaltung

Der Thüringer Landesbeauftragte für den Datenschutz hat neben seiner Kontrollfunktion gemäß § 40 ThürDSG auch die Entwicklung und Nutzung der Informations- und Kommunikationstechnik zu beobachten, die öffentlichen Stellen zu beraten und Empfehlungen zur Verbesserung des Datenschutzes zu geben. Eine solche Entwicklung ist in der Thüringer Landesverwaltung der wachsende Bedarf an mobilen Endgeräten, die nicht nur zum telefonieren gedacht sind, sondern die E-Mails mit einem Push-Dienst (der E-Mails sofort nach Eintreffen am Server auf das Gerät weiterleitet), eine Verwaltung von Terminen und Kontakten und die Internetnutzung ermöglichen. In Anbetracht der datenschutzrechtlichen Relevanz, die mit dem Einsatz solcher mobilen IT verbunden ist, wurde bereits 2004 von Seiten verschiedener Ministerien das Thüringer Landesrechenzentrum aufgefordert, eine diesbezügliche Teststellung aufzubauen, vorhandene Schwach-

stellen aufzuzeigen und bei positivem Ergebnis ein Betreiberkonzept und ein konkretes Sicherheitskonzept entsprechend den Gegebenheiten der vorliegenden Einsatzbedingungen zum CN des Freistaats zu erstellen. Um nicht eine Vielzahl von unterschiedlichen mobilen Endgeräten in der Thüringer Landesverwaltung im Einsatz vorzufinden, wurde die Teststellung damals auf die BlackBerry-Lösung eingeschränkt, welche sich schon teilweise im Einsatz befand (6. TB, 1.3).

Im Jahr 2005 gab es Presseberichten zufolge seitens des Bundesamts für Sicherheit in der Informationstechnik Vorwürfe zur Datensicherheit beim BlackBerry. Der Produzent beauftragte daraufhin Ende Oktober 2005 das Fraunhofer Institut für Sichere Informationstechnologie, die Sicherheit der Kommunikation mit seinen BlackBerry-PDAs zu testen, um so den nach ihrer Meinung unberechtigten Vorwürfen entgegen zu wirken. Dabei wurde dem Fraunhofer Institut auch Zugriff auf streng vertrauliche Informationen gestattet. Diese Analyse gliedert sich in drei Projekte. Nach einer ersten Testphase wurden von Seiten des Fraunhofer Instituts keine Hinweise auf einen beim Produzenten liegenden Master-Key oder andere Möglichkeiten gefunden, die eine unberechtigte Kenntnisnahme oder Manipulation durch Dritte ermöglicht. Eine weitere Maßnahme zur Verbesserung der Sicherheit war die Zusammenarbeit mit einem Unternehmen, das Verschlüsselungssoftware vertreibt, wodurch nun nicht nur zusätzlich die Möglichkeit besteht, zu übertragende E-Mails zu signieren und zu verschlüsseln, sondern auch Daten auf dem BlackBerry selbst mit den gleichen Mechanismen zu sichern. Natürlich stellt sich die Frage, inwieweit andere Hersteller genau so sicher oder sicherer sind als die BlackBerry-Lösung. Diese Frage lässt sich allerdings erst dann beantworten, wenn sie den vom Bundesamt für Sicherheit in der Informationstechnik geforderten Maßstäben standhalten und sich analog einer solchen Sicherheitsanalyse des Fraunhofer Instituts unterziehen.

Seit Juli 2007 liegt nun für die Thüringer Landesverwaltung ein Abschlussbericht zur BlackBerry-Teststellung vom Thüringer Landesrechenzentrum vor. In dem Bericht werden die sicherheitstechnischen Eigenschaften des BlackBerry dargestellt und als sehr effektiv eingeschätzt. Nach Angaben des Thüringer Landesrechenzentrums liegen die Daten auf dem Gerät verschlüsselt im Speicher, sodass eine unerlaubte Kenntnisnahme der Daten unwahrscheinlich erscheint. Das größte Risiko entsteht beim eventuellen Diebstahl des Gerätes, da in

dem Zeitfenster bis zur Wirksamkeit des mit Passwort zu versehenden Bildschirmschoners der direkte Zugriff auf die gespeicherten Daten und die Funktionalität des Gerätes möglich ist. Desweiteren weist das Thüringer Landesrechenzentrum darauf hin, dass aus seiner Sicht die BlackBerry-Geräte gegenüber den Konkurrenz-Modellen eindeutige Vorteile aufweisen, besonders bezogen auf die IT-Sicherheit (z. B. Datenverschlüsselung, Support). Aus diesen Gründen sind ausschließlich BlackBerry-Geräte in der Thüringer Landesverwaltung zu verwenden. Seit dem 1. September 2007 bietet das Thüringer Landesrechenzentrum im Auftrag für den Freistaat Thüringen die BlackBerry-Technologie als Kommunikationsdienst an. Dies bedeutet mobile Kommunikationslösung im Exchange-Mail-Verbund des Freistaats Thüringen, E-Mail-Versand mit komprimären und verschlüsselten Daten bis zum Endgerät, Zugriff auf Dienstpostfach unter Nutzung der Outlook-Grundfunktionalitäten und Zugriff auf Internetinhalte und –dienste. Mit Vertragsabschluss erhalten die Auftraggeber das Betriebskonzept ausgehändigt. Die Art der benutzten Endgeräte und die zentralen Einstellungen der Policys liegen in der Verantwortung der jeweiligen Ressorts. Das gemäß § 9 Abs. 2 ThürDSG vom TLRZ zu erstellende IT-Sicherheitskonzept empfiehlt für die Übermittlung sensibler Informationen unbedingt eine AES-Verschlüsselung zu verwenden und die Maßnahmen des Thüringer Landesrechenzentrums umzusetzen.

Auf Grund der 2005 öffentlich geführten nicht abgeschlossenen kontroversen Diskussion bezüglich der IT-Sicherheit von BlackBerry garantiert das Thüringer Landesrechenzentrum derzeit für den BlackBerry-Dienst hinsichtlich der Vertraulichkeit und der Integrität nur in der Schutzkategorie „normal“ einen sicheren Betrieb. Die Entscheidung des Einsatzes solcher Geräte trägt immer die beantragende öffentliche Stelle. Da die Sicherheitsuntersuchungen durch das Fraunhofer Institut noch nicht vollständig abgeschlossen sind, wird auch seitens des TLfD vom Einsatz in sensitiven Bereichen z. B. des Landeskriminalamtes und des Verfassungsschutzes abgeraten.

Seit dem 1. September 2007 bietet das Thüringer Landesrechenzentrum die BlackBerry-Technologie als Kommunikationsdienst für den Freistaat Thüringen an. Erst nach Abschluss der technischen Überprüfung des BlackBerry im Fraunhofer Institut sollte über einen Einsatz

in sensitiven Bereichen z. B. des Landeskriminalamtes oder des Verfassungsschutzes entschieden werden.

15.7 Zentrale Spam- und Virenprüfung an der Kopfstelle des CN

Auf die Folgen von unerwünschten Werbe-E-Mails, sog. Spam-E-Mails und auf virenbehaftete E-Mails wurde bereits eingegangen (6. TB, 1.4). Schon damals zeigte sich, dass allein mit gesetzlichen Regelungen das weltweite Aufkommen von Werbe-E-Mails nicht zu unterbinden ist und seitens der empfangenden Stellen technische und organisatorische Maßnahmen zur Spam-Abwehr und gegen Virenattacken unter Berücksichtigung datenschutzrechtlicher Aspekte zu treffen sind. So sind auch an der Kopfstelle des CN zum Schutz der Einrichtungen gegen Angriffe aus dem öffentlichen Internetbereich Firewallsysteme, Cache-Systeme und ein zentrales Mail-Gateway mit Viren- und Spamfilter installiert.

Im zurückliegenden Berichtszeitraum wurde mit dem Thüringer Landesrechenzentrum die Erforderlichkeit der Protokollierungen auf dem zentralen Internetzugang und Mailsystem datenschutzrechtlich überdacht und eine Transparenz der aktuell eingerichteten Komponenten erwirkt. Im Ergebnis dessen veröffentlichte das Thüringer Finanzministerium, als Aufsichtsbehörde des Thüringer Landesrechenzentrums, die „Allgemeine Richtlinie zur Nutzung des Internetzuganges und des Mailsystems des Corporate Network (CN) des Freistaates Thüringen“ im Staatsanzeiger Nr. 51/2007. Diese Richtlinie beinhaltet zum einen Vorgaben hinsichtlich des zentralen Internetzuganges sowie für dienstliche und, falls von der jeweiligen öffentlichen Stelle erlaubt, private Nutzung. Auch wird darauf hingewiesen, dass die Nutzung der dienstlichen E-Mail-Adresse für andere als dienstliche Zwecke unzulässig ist und ohne dienstliche Notwendigkeit eine Bekanntgabe zu vermeiden ist (4.4). In der vom Thüringer Finanzministerium erlassenen Richtlinie wird zudem darauf hingewiesen, dass am zentralen Internetzugang nur in begründeten Fällen die Verbindungsdaten des Kommunikationsverkehrs protokolliert werden, wobei Datum, Uhrzeit, Zieladresse und Absenderadresse festgehalten werden können. Diese Protokollierung muss von der jeweiligen Behörde über die Fachaufsicht des Thüringer Landesrechenzentrums beantragt werden.

Wie schon beschrieben (6. TB, 1.4), werden alle E-Mails im Mailsystem durch ein Bewertungsprogramm gescannt und eine Bewertungs-

zahl im Header (Kopfzeile) der E-Mail eingetragen, sodass der verfügte Inhalt des Absenders (Betreffzeile, Nachrichtentext) unversehrt bleibt. Die Bewertung, inwieweit es sich dann tatsächlich um eine Spam-E-Mail handelt oder um eine gewünschte E-Mail, obliegt weiterhin dem Empfänger der E-Mail. Der Empfänger kann bspw. zur Arbeitserleichterung seinen Posteingang so gestalten, dass alle E-Mails mit einer hohen Bewertungszahl in einen extra angelegten Spam-Ordner zur späteren Durchsicht weitergeleitet werden. Zudem wird transparent dargelegt, wie lange E-Mails mit Virenbefall und die Verbindungsdaten der E-Mail (Datum, Uhrzeit, Absender, Adressat) gespeichert werden.

Im Intranet des Freistaates Thüringen stehen neben der Richtlinie eine Beschreibung zum Einsatz von Mail-Gateways im CN sowie ein Muster zur Einwilligungserklärung und zur Dienstvereinbarung abrufbereit zur Verfügung. Des Weiteren werden dort Statistiken zu eingehenden E-Mails, ausgehenden E-Mails, zum Aufkommen von Spam-E-Mails und Virenaufkommen veröffentlicht.

Das Thüringer Finanzministerium kommt einer wesentlichen Forderung des TLfD zur Transparenz des Verfahrens durch die Veröffentlichung der Richtlinien zur Internet- und Mailsystemnutzung samt Anlagen nach.

Anlage 1

Entschließungen zwischen den Konferenzen 2005/2006

Sicherheit bei eGovernment durch Nutzung des Standards OSCI

(Umlaufentschließung/15. Dezember 2005)

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss

Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Anlage 2

Entschließungen zwischen den Konferenzen 2005/2006

Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

(Umlaufentschließung/11. Oktober 2006)

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche

Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo

es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

Anlage 3

Entschließung
der 71. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2006 in Magdeburg

Keine kontrollfreien Räume bei der Leistung von ALG II

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung" vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

Anlage 4

Entschließung
der 71. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2006 in Magdeburg

Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z. B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwer wiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

Anlage 5

Entschließung
der 71. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2006 in Magdeburg

Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über – durch das Fernmeldegeheimnis geschützte - Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater

Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses - erstmals zur Durchsetzung wirtschaftlicher Interessen - zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Anlage 6

Entschließung
der 71. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2006 in Magdeburg

Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat*. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u.a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müs-

* KOM (2005) 475 vom 4. Oktober 2005

sen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen – unter Beachtung der richterlichen Unabhängigkeit – gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung – auch sofern sie in Akten erfolgt - einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

Anlage 7

Entschließung
der 72. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 26./27. Oktober 2006 in Naumburg

Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz - BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist ins-

besondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.
- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.
- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.
- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.
- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der

Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Anlage 8

Entschließung
der 72. Konferenz der Datenschutzbeauftragten
Bundes und der Länder
am 26./27. Oktober 2006 in Naumburg

Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der ”Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes” kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der ”Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes” ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl

die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Anlage 9

Entschließung
der 72. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 26./27. Oktober 2006 in Naumburg

Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte "Schulleben" ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen "Bildungsregisters" nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine

ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.
- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.
- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

Anlage 10

Entschließung
der 72. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 26./27. Oktober 2006 in Naumburg

Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen - zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwick-

lungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- Transparenz
  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.
- Kennzeichnungspflicht
  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.
- Keine heimliche Profilbildung
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.
- Vermeidung der unbefugten Kenntnisnahme
  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.
- Deaktivierung
  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Anlage 11

Entschließung
der 73. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. März 2007 in Erfurt

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.

Anlage 12

Entschließung
der 73. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. März 2007 in Erfurt

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.

Anlage 13

Entschließung
der 73. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. März 2007 in Erfurt

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.

Anlage 14

Entschließung
der 73. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. März 2007 in Erfurt

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 Be-

zahlung. 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.

Anlage 15

Entschließung
der 73. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. März 2007 in Erfurt

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.

Anlage 16

Entschließung
der 73. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. März 2007 in Erfurt

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 solange 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 gewährleisten. 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 i. S. v. § 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 Massendatenerhe-

bungen 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.

Anlage 17

Entschließungen zwischen den Konferenzen 2007

Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

(Umlaufentschließung/8. Juni 2007)

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.

Anlage 18

Entschließung
der 74. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. Oktober 2007 in Saalfeld

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.

Anlage 19

Entschließung
der 74. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. Oktober 2007 in Saalfeld

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 wür-

den 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 (§ 87a 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 § 139b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b 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.

Anlage 20

Entschließung
der 74. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. Oktober 2007 in Saalfeld

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.

Anlage 21

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

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 Bürgern 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.

Sachregister