LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 3/1130**
3. Wahlperiode **29.02.2000**

UNTERRICHTUNG

durch den Landesbeauftragten für den Datenschutz

Vierter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz gemäß § 29 Absatz 1 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern (DSG MV)

Zugeleitet mit Schreiben des Landesbeauftragten für den Datenschutz vom 25. Februar 2000 gemäß § 29 Absatz 1 des Landesdatenschutzgesetzes

Vorwort

Das Datenschutzgesetz von Mecklenburg-Vorpommern sieht vor, dass der Landesbeauftragte für den Datenschutz dem Landtag und der Landesregierung für jeweils zwei Kalenderjahre einen Tätigkeitsbericht vorlegt. Der vorliegende Vierte Tätigkeitsbericht umfasst den Zeitraum vom 1. Januar 1998 bis 31. Dezember 1999.

Wie in den vorherigen Berichten habe ich Vorgänge ausgewählt, die einen Gesamteindruck von der Tätigkeit meiner Behörde vermitteln. Einige Beiträge schließen an Sachverhalte aus den letzten Tätigkeitsberichten an. Insofern könnte es nützlich sein, in dem einen oder anderen Fall noch einmal auf diese Berichte zurückzugreifen.

Für die konstruktive und angenehme Zusammenarbeit danke ich meinen Amtskollegen beim Bund und in den Ländern. Ein weiterer Dank gilt meinen Mitarbeitern für die engagierte, zuverlässige und sachkundige Arbeit im Berichtszeitraum sowie bei der Erarbeitung der einzelnen Beiträge dieses Berichtes.

Dr. Werner Kessel
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

Inhaltsverzeichnis

Seite

1 Einleitung ... 6

2 Modernisierung des Datenschutzrechts ... 9

2.1 Novellierung des Landesdatenschutzgesetzes längst überfällig ... 9
2.2 Novellierung des Bundesdatenschutzgesetzes ... 11
2.3 Neue Regelungen für moderne Technik ... 12
2.4 Direktwirkung der europäischen Datenschutzrichtlinie ... 13

3 Sorgen der Bürger, Einzelfälle, Beratungen, Kontrollen, Stellungnahmen ... 16

3.1 Rechtswesen ... 16
3.1.1 Täter-Opfer-Ausgleich ... 16
3.1.2 Maßvoller Umgang mit der DNA-Analyse ... 17
3.1.3 Praxis der Telefonüberwachungen ... 18
3.1.4 Entwurf eines Untersuchungshaftvollzugsgesetzes ... 20
3.1.5 Parlamentarische Kontrolle von Lauschangriffen ... 21
3.1.6 Welche Daten müssen bei Sparbuchverlust offenbart werden? ... 21
3.1.7 Wenn der Staatsanwalt zu Hause arbeitet ... 22
3.1.8 Elektronisches Grundbuch ... 23
3.1.9 Schuldnerverzeichnis bald öffentlich? ... 26
3.1.10 Notare in Mecklenburg-Vorpommern mit Sonderprivilegien ... 27
3.1.11 Staatsanwälte löschen nicht ... 30
3.1.12 Mitteilungen über Wahlrechtsausschlüsse nicht korrekt ... 34
3.1.13 Datenschutz bei laufenden Ermittlungsverfahren? ... 36
3.2 Polizei ... 37
3.2.1 INPOL-Neu ... 37
3.2.2 Verfassungsgericht stoppt Schleierfahndung ... 38
3.2.3 Polizeiliche Zusammenarbeit mit der Russischen Föderation ... 40
3.2.4 Täter-Lichtbild-System ... 40
3.2.5 Erkennungsdienstliche Behandlung eines Zeugen - volles Programm ... 41
3.2.6 Unschuldig - aber mehrfach verdächtigt ... 43
3.2.7 Leichtfertiger Umgang mit DDR-Flüchlingsakten ... 45
3.3 Das Nachrichtendienstliche Informationssystem der Verfassungsschutzbehörden ... 47
3.4 Einwohnerwesen ... 49
3.4.1 Elektronische Überwachung von Asylbewerbern geplant ... 49
3.4.2 Automatisierte Abrufverfahren in Gemeinden und Ämtern ... 50
3.4.3 Widerspruchsrecht bei Übermittlung von Meldedaten unzureichend ... 51
3.4.4 Wohnsitzwechsel - Kopie des Mietvertrages zu den Akten der Meldebehörde? ... 54
3.5 Bürgerbüro ... 55
3.6 Datenübermittlung in Planfeststellungsverfahren ... 56
3.7 Volkszählung ... 57
3.8 Telekommunikation und Medien ... 59
3.8.1 Telekommunikations-Datenschutzverordnung ... 59
3.8.2 Datenschutzbestimmungen im Rundfunkrecht ... 60

Seite

3.9 Finanzwesen 61
3.9.1 Detektiv verfolgt Hund 61
3.9.2 Pfändungsverfügung ins Blaue 62
3.9.3 Haushalts-, Kassen- und Rechnungswesen 63
3.9.4 Muss man bei Sterbefällen Vermögensangaben machen? 65
3.9.5 Kein Konto ohne Ausweiskopie? 66
3.9.6 Zweitwohnungssteuer 67
3.9.7 Elektronische Steuererklärung 69
3.10 Soziales 70
3.10.1 Gesundheitsreform (GKV 2000) - neuer Ansatz für den Datenschutz 70
3.10.2 Risiken eines neuen Datenmodells bei den Betriebskrankenkassen 71
3.10.3 Kindschaftsrecht datenschutzgerecht umgesetzt 73
3.10.4 Was das BAföG-Amt dem Antragsteller mitteilen darf 74
3.10.5 Datenverarbeitung im Auftrag von Wohngeldstellen - was ist zu beachten? 75
3.10.6 Hausbesuch vom Sozialamt 76
3.10.7 Wie stellt das Sozialamt Vermögen oder Einkommen fest? 77
3.11 Gesundheitswesen 78
3.11.1 Meldungen an das Krebsregister 78
3.11.2 Ärztliche Schweigepflicht im Bestattungsgesetz 79
3.11.3 Krankenhaus informiert Ordnungsamt über fahruntüchtigen Patienten 80
3.11.4 Notrufe werden aufgezeichnet 81
3.11.5 Prüfaufträge an den Medizinischen Dienst müssen konkret sein 83
3.11.6 Patientenakten aus dem Krankenhaus gestohlen 84
3.11.7 Diktate nicht gelöscht, Patientendaten auf dem Müll 85
3.12 Personalwesen 86
3.12.1 Was die Polizei von Bewerbern wissen will 86
3.12.2 Praxis der Stasi-Überprüfung noch zeitgemäß? 88
3.12.3 Was darf in die Personalakte aufgenommen werden? 92
3.13 Bildung, Kultur, Wissenschaft und Forschung 93
3.13.1 Chipkarte als Studentenausweis 93
3.13.2 Anfrage bei der Sekteninformationsstelle - nicht vertraulich? 94
3.13.3 Schüler im Fokus der Forschung 95
3.13.4 Forschungsprojekt über Hausarztpraxen 96
3.14 Wirtschaft und Gewerbe 97
3.14.1 Kontrolle einer Handwerkskammer 97
3.14.2 Falscher Zeitungsausschnitt in der Akte eines Schornsteinfegers 98
3.15 Land-, Forst- und Wasserwirtschaft 100
3.15.1 Daten für Abwasseranschluss an privates Unternehmen 100
3.15.2 Braucht der Wasser- und Abwasserzweckverband einen vollständigen Grundbuchauszug? 101

Seite

3.16 Technik und Organisation 101
3.16.1 Sichere Vernetzung der Landesverwaltung noch in den Kinderschuhen..... 101
3.16.2 Verschlüsselung künftig ein Standardmerkmal? 103
3.16.3 Braucht das Land ein eigenes Trustcenter?..... 104
3.16.4 Neues zur Internetnutzung 106
3.16.5 Data Warehouse 107
3.16.6 Prüfkriterien für datenschutzfreundliche Produkte (Common Criteria 2.0) 109
3.16.7 Wer weiß schon noch, was in seinem Rechner passiert?..... 110
3.16.8 Orten von Mobiltelefonen 112
3.16.9 Videoüberwachung 113
3.16.10 Orientierungshilfe für den Einsatz von Verzeichnisdiensten..... 114
3.16.11 KfZ-Zulassung via Internet..... 116
3.16.12 Neue Antragsverfahren für Ausweispapiere und Führerscheine 117
3.16.13 Bundesweite Behördenvernetzung mit TESTA..... 118

4 Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik)..... 120

5 Öffentlichkeitsarbeit 121

6 Anlagen 123

7 Abkürzungsverzeichnis 153

8 Stichwortverzeichnis 158

9 Publikationen 169

1. Einleitung

Brauchen wir mehr oder haben wir möglicherweise schon zu viel Datenschutz? Diese Frage gewinnt in unserer Informationsgesellschaft zunehmend an Bedeutung. Die Antworten darauf werden unterschiedlich ausfallen, je nachdem, wem man diese Frage stellt. So wird von Einzelnen auch heute immer noch das Grundrecht des Bürgers auf informationelle Selbstbestimmung in aller Öffentlichkeit gern als „Täterschutz“ diffamiert. Auf der anderen Seite gibt es aber bereits viele Betroffene, die angesichts der rasanten Entwicklung der Informations- und Kommunikationstechnik Orwells Visionen schon in sehr naher Zukunft als furchtbare Realität sehen.

Ein renommiertes Forschungsinstitut hat die Bevölkerung befragt und dabei festgestellt, dass allein 47 % der Befragten der Meinung sind, in der Bundesrepublik werde zu wenig für den Datenschutz getan. Lediglich 4 % haben sich gegenteilig geäußert. 52 % der Befragten in Westdeutschland und 66 % in Ostdeutschland wünschen sich, dass dem Datenschutz künftig mehr Bedeutung zukommt. Dieses Ergebnis spiegelt auch die Situation in Mecklenburg-Vorpommern ganz gut wider. In der Tagesarbeit ist insgesamt ein wachsendes Interesse der Bürger und der Verwaltungen am Datenschutz zu konstatieren. Die Anzahl der Petitionen und Anfragen öffentlicher Stellen ist im Berichtszeitraum stark gestiegen.

Zu mehr Datenschutz gehört aber nicht nur, dass der Gesetzgeber die gesetzlichen Voraussetzungen verbessert. Dazu gehört auch, dass die Stelle, die im Interesse des Bürgers die Einhaltung der datenschutzrechtlichen Bestimmungen zu kontrollieren hat, ihre Aufgabe auch tatsächlich so wahrnehmen kann, wie es der Gesetzgeber vorsieht. Das war in diesem Berichtszeitraum nicht immer ohne weiteres möglich.

So konnte beispielsweise eine Petition nicht befriedigend bearbeitet werden, weil eine öffentliche Stelle die Auskunft verweigerte. Im konkreten Fall hat ein Notar Grundbuchakten seines Nachbarn eingesehen und damit möglicherweise gesetzwidrig personenbezogene Daten zur Kenntnis genommen. Auf meine Anfrage hin teilte der Notar mit, dass er nicht als Privatperson, sondern in Amtshilfe für einen Kollegen tätig war. Er sei jedoch aufgrund der notariellen Verschwiegenheitspflicht nicht bereit, dessen Namen zu nennen. Der Notar verstößt damit gegen seine Pflicht als öffentliche Stelle des Landes, den Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Da das Justizministerium als oberste Aufsichtsbehörde hierin allerdings keine Pflichtverletzung sieht - eine durchaus bürgerunfreundliche und im Vergleich zu anderen Bundesländern eher exotisch anmutende Rechtsauffassung - war es bisher nicht möglich, diesen Vorgang abschließend zu bearbeiten. Das musste ich dem Petenten so mitteilen. Ausführlich ist der Vorgang unter Punkt 3.1.10 des vorliegenden Berichtes geschildert.

In einem anderen Fall geht es ebenfalls um eine Grundsatzentscheidung zur Kontrollbefugnis des Landesbeauftragten für den Datenschutz, und zwar in laufenden Ermittlungsverfahren (siehe dazu Punkt 3.1.13). Das Justizministerium äußert sich jedoch nicht zur Sache, sondern verweist auf die anstehende Novellierung des Landesdatenschutzgesetzes. Das Ministerium verzichtet also auf eine Bewertung des Sachverhaltes nach geltendem Recht und nimmt damit auch das Bestehen einer rechtswidrigen Situation in Kauf. Dies könnte unter Umständen dann hingenommen werden, wenn der Erlass einer entsprechenden rechtfertigenden Regelung erstens sicher zu erwarten ist und zweitens unmittelbar bevorsteht. Beides ist hier jedoch nicht der Fall. Im aktuellen Referentenentwurf für das neue Landesdatenschutzgesetz ist eine Vorschrift, die Kontrollbefugnisse derartig einschränkt, jedoch nicht vorgesehen. Zudem ist bei dem gegenwärtigen Stand der Dinge überhaupt nicht absehbar, wann unser Landesdatenschutzgesetz tatsächlich novelliert wird. Längst überfällig ist dieser Schritt allemal.

Drei Jahre hatte der Gesetzgeber Zeit, die EG-Datenschutzrichtlinie in Landesrecht umzusetzen. Diese Frist ist in Mecklenburg-Vorpommern ebenso klang- und wirkungslos verstrichen, wie die Mahnungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie meine Hinweise und Vorschläge zur Novellierung des Landesdatenschutzgesetzes in den vorangegangenen drei Tätigkeitsberichten ungehört geblieben sind.

Für das Gesetzgebungsverfahren ist das Innenministerium unseres Landes federführend. Deshalb hatte ich dem Innenminister kurz nach den Landtagswahlen '98 empfohlen, möglichst bald die Novellierung des Landesdatenschutzgesetzes auf den Weg zu bringen. Recht zügig wurde in guter Zusammenarbeit mit mir ein Referentenentwurf erarbeitet, der sowohl den Anforderungen der EG-Richtlinie als auch der technischen Entwicklung weitgehend Rechnung trägt.

Trotzdem liegt dem Landtag bis heute kein Kabinettsentwurf vor, und wenn es so weitergeht, steht zu befürchten, dass wir den alten Bismarck in seiner Meinung über uns wieder einmal bestätigen. Darüber hinaus hat die Europäische Kommission wegen der unterlassenen Umsetzung der Datenschutzrichtlinie inzwischen ein Verfahren beim Europäischen Gerichtshof eingeleitet. Gegenstand dieses Verfahrens ist unter anderem das Datenschutzrecht in den einzelnen Bundesländern, also auch die Situation in Mecklenburg-Vorpommern. Ein mögliches Urteil könnte sein, dass Deutschland - und damit der Steuerzahler - für jeden Tag der Nichtberücksichtigung der Richtlinie nach Ablauf der Umsetzungsfrist viel Geld an die Europäische Gemeinschaft zahlen muss.

Eine bereits spürbare negative Auswirkung dieses Verstoßes gegen europäisches Recht ist die partielle Ungültigkeit des Landesdatenschutzgesetzes und anderer Datenschutzbestimmungen. Denn einige Vorschriften der Richtlinie entfalten Direktwirkung und verdrängen dadurch die entsprechenden nicht angepassten Datenschutzregelungen des Landes (siehe dazu Punkt 2.4). Jede Behörde unseres Landes muss sich daher eingehend mit der Datenschutzrichtlinie befassen und bei jedem datenschutzrelevanten Vorgang prüfen, ob nicht die Richtlinie anstelle des Landesdatenschutzgesetzes oder anstelle der Regelungen in dem betreffenden bereichsspezifischen Gesetz anzuwenden ist. Dieser sowohl den Behörden als auch dem Bürger unzumutbare Zustand sollte möglichst bald beendet werden.

Am 21. Oktober 1999 hat unser Landesverfassungsgericht eine für die Gewährleistung des Grundrechtes auf informationelle Selbstbestimmung in unserem Lande bedeutsame Entscheidung getroffen. Es hat die vom Parlament im Jahre 1998 verabschiedete gesetzliche Regelung zu den verdachts- und ereignisunabhängigen Polizeikontrollen im Wesentlichen für verfassungswidrig erklärt (siehe dazu Punkt 3.2.2). Damit hat das höchste Gericht im Lande Maßstäbe gesetzt für ein datenschutzfreundliches Polizeirecht. Es bleibt zu hoffen, dass diese Entscheidung auch bei künftigen Gesetzgebungsverfahren berücksichtigt wird.

Turnusgemäß hatte Mecklenburg-Vorpommern im Jahr 1999 den Vorsitz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Für die Frühjahrskonferenz hatte der Präsident unseres Landtages die Teilnehmer freundlicherweise in das Schweriner Schloss eingeladen. Die Herbstsitzung haben wir mit freundlicher Unterstützung des Innenministers und des Oberbürgermeisters der Hansestadt Rostock im altehrwürdigen Ständehaus in Rostock durchgeführt. Der Vorsitz war für meine kleine Behörde zwar eine große Herausforderung, aber stets interessant, und durch die engagierte Arbeit aller Mitglieder ist es uns gelungen, außergewöhnlich viele Entschließungen zu aktuellen Themen des Datenschutzes einstimmig zu verabschieden. Die Texte sind als Anlagen in diesem Bericht zu finden.

So wurde beispielsweise eine Entschließung zur Gesundheitsreform 2000 verabschiedet. Durch gemeinsame Anstrengungen aller Datenschutzbeauftragten konnte erreicht werden, dass die Bundesregierung den datenschutzrechtlichen Teil des Gesetzentwurfes zur Reform der gesetzlichen Krankenversicherung überarbeitet und unsere Empfehlungen im Wesentlichen umgesetzt hat. In der Frage der Datenverarbeitung bei den gesetzlichen Krankenkassen ist es zum Beispiel gelungen, alle Beteiligten davon zu überzeugen, im Bereich der ambulanten ärztlichen Versorgung pseudonymisierte Daten zu verarbeiten, um die Gefahr des „gläsernen“ Patienten zu bannen (siehe Punkt 3.10.1). Mit pseudonymisierten Daten ist eine unmittelbare Identifizierung eines Versicherten nicht möglich. Statt des Namens oder der Versichertennummer wird beispielsweise eine Codierung (Pseudonym) verwendet. Nur in Ausnahmefällen ist es zulässig, mit Hilfe der Verschlüsselungsfunktion daraus wieder einen Versicherten zu bestimmen. Es ist allerdings wegen anderer Schwierigkeiten in der Gesetzgebung noch nicht klar, wann diese Regelungen in Kraft treten.

Erfreulich ist auch die Entwicklung in einem wichtigen datenschutztechnischen Bereich. Nachdem die Bundesregierung sich lange mit der Frage befasst hat, ob der Einsatz von Verschlüsselungsverfahren rechtlich geregelt werden sollte, hat sie am 2. Juni 1999 die Eckpunkte der deutschen Kryptopolitik veröffentlicht. Verschlüsselungsprodukte sind nun frei verfügbar. Für Wirtschaft und Verwaltung Mecklenburg-Vorpommerns folgt daraus, dass Verschlüsselung im Sinne dieser Eckpunkte bei IT-Verfahren unseres Landes zu einem Standardmerkmal werden kann und sollte. Allerdings sind nun schnell Rahmenbedingungen zu schaffen, die eine einfache und weitgehend einheitliche Nutzung von kryptographischen Verfahren in der gesamten Landesverwaltung ermöglichen (siehe dazu Punkt 3.16.2 und 3.16.3).

2 Modernisierung des Datenschutzrechts

2.1 Novellierung des Landesdatenschutzgesetzes längst überfällig

Die Frist zur Umsetzung der EG-Datenschutzrichtlinie in nationales Recht, wozu auch das Recht der Bundesländer gehört, ist am 24. Oktober 1998 abgelaufen (siehe Punkt 2.4).

Am 27. Januar 1999 hatte das Innenministerium Mecklenburg-Vorpommern einen ersten Referentenentwurf zur Novellierung des Landesdatenschutzgesetzes vorgelegt, den ich im Wesentlichen mitgetragen habe. Nach der hausinternen Abstimmung im Innenministerium wurde der überarbeitete Entwurf am 14. Mai 1999 den verschiedenen Ressorts und mir zur Anhörung zugeleitet. Seit September 1999 liegen dem Innenministerium alle Stellungnahmen vor. Ein neuer Entwurf ist mir seitdem nicht bekannt geworden.

Der Gesetzentwurf vom Mai 1999 enthält Regelungen, die die Datenschutzrichtlinie umsetzen - darunter auch die unmittelbar geltenden Vorschriften der Richtlinie (siehe Punkt 2.4) - , und solche, die der technischen Entwicklung in der Datenverarbeitung Rechnung tragen. Beispielhaft hierfür sind folgende vorgesehene Änderungen gegenüber dem aktuellen Landesdatenschutzgesetz:

- Es werden Normen zum Grundsatz der Datenvermeidung, der frühestmöglichen Anonymisierung/Pseudonymisierung und zum Systemdatenschutz eingeführt.

- Die aus den 70er Jahren stammenden Regelungen zu den technischen und organisatorischen Maßnahmen in den Datenschutzgesetzen - die so genannten 10 Gebote - werden durch allgemeine technikunabhängige Anforderungen (siehe Punkt 2.3) ersetzt.

- Der nunmehr obligatorisch von jeder öffentlichen Stelle zu bestellende behördliche Datenschutzbeauftragte ist mit umfangreichen Rechten ausgestattet.

- Die Voraussetzungen für den Einsatz von mobilen Datenverarbeitungssystemen (z. B. Chipkarten) sowie für die Videoüberwachung und -aufzeichnung werden durch spezielle Vorschriften geregelt.

- Es wird ausdrücklich klargestellt, dass sich die Kontrollbefugnis des Datenschutzbeauftragten auch auf solche Daten erstreckt, die durch ein Berufs- oder spezielles Amtsgeheimnis besonders geschützt sind.

- Entscheidungen, die nachteilige Auswirkungen für den Betroffenen haben, dürfen im Allgemeinen nicht auf eine Verarbeitung seiner Daten gestützt werden, die ausschließlich automatisiert erfolgt.

- Die lediglich zur Datenschutzkontrolle oder Datensicherheit gespeicherten Daten dürfen nicht für andere Zwecke verarbeitet werden.

- Auch bei einer unzulässigen nicht-automatisierten Datenverarbeitung ist die verantwortliche Stelle zum Schadensersatz verpflichtet. Die Ansprüche des Betroffenen sind nicht mehr auf eine bestimmte Summe begrenzt.

Leider ist der aktuelle Entwurf vom Mai 1999 bei der Modernisierung des Datenschutzrechts auf halber Strecke stehen geblieben. Teilweise weist er sogar gravierende Verschlechterungen gegenüber dem geltenden Landesdatenschutzgesetz auf. In meiner Stellungnahme habe ich die erforderlichen Änderungen ausführlich dargestellt. Die wichtigsten Mängel sind folgende:

- Der Vorentwurf ermächtigte die Landesregierung, dem Landesbeauftragten für den Datenschutz durch Rechtsverordnung die Kontrolle der Einhaltung des Datenschutzes im nicht-öffentlichen Bereich zu übertragen. Diese Vorschrift ist gestrichen worden. Die EG-Datenschutzrichtlinie verlangt jedoch, dass die Datenschutzkontrollstellen „ ... die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr[nehmen]“. Darüber hinaus wäre es vor allem auch für die Bürger von Vorteil, für alle Belange des Datenschutzes nur einen Ansprechpartner zu haben. So ist es etwa nur schwer vermittelbar, dass der Landesbeauftragte für den Datenschutz die Sparkassen kontrolliert, für die privaten Banken aber das Innenministerium als Datenschutz-Aufsichtsbehörde zuständig ist.

- Öffentlichen Stellen, gegenüber denen eine Beanstandung ausgesprochen wurde, muss eine „angemessene Frist von mindestens sechs Wochen“ zur Stellungnahme eingeräumt werden. Diese Mindestfrist zur Stellungnahme zu Beanstandungen schwächt im Einzelfall erheblich die Rechte der betroffenen Bürger und wäre eine im deutschen Datenschutzrecht einmalige Beschränkung der Tätigkeit des Datenschutzbeauftragten. Sie ist mit der verfassungsrechtlich garantierten Unabhängigkeit des Landesbeauftragten für den Datenschutz nicht vereinbar und daher inakzeptabel.

- Im Gegensatz zum aktuellen Entwurf enthielt der Vorentwurf eine Vorschrift zur Freigabe neuer Verfahren der automatisierten Datenverarbeitung oder deren Modifikationen, die die Verantwortlichkeit bei der Einführung dieser Verfahren regelt und den Mitarbeitern vorgibt, welche davon sie bei der Erfüllung ihrer Aufgaben verwenden dürfen. Das Freigabeverfahren dient daher der Rechtssicherheit sowie der Transparenz und ist ein wichtiges Instrument zur Beherrschbarkeit der elektronischen Datenverarbeitung durch die Verwaltung, auch über den Bereich des Datenschutzes hinaus. Die Regelung des Vorentwurfs sollte wieder aufgenommen werden.

- Die Befugnis, den Umgang mit personenbezogenen Daten auch dann zu erlauben, wenn eine Rechtsvorschrift dies nicht ausdrücklich erlaubt, sondern lediglich „zwingend voraussetzt“, sollte gestrichen werden. Eine so weitgehende und unklare Befugnis ist nicht erforderlich und genügt auch nicht den vom Bundesverfassungsgericht postulierten Anforderungen an den Gesetzesvorbehalt, also dem Grundsatz, dass staatliche Eingriffe nur aufgrund klarer gesetzlicher Regelungen zulässig sind.

- Die noch im Vorentwurf vorgesehene Verordnungsermächtigung zur Regelung des Freigabeverfahrens, des Tests von Computerprogrammen, des Sicherheitskonzeptes und der Maßnahmen zur Datensicherheit sollte wieder aufgenommen werden. Eine solche, den jeweiligen technischen Rahmenbedingungen flexibel anpassbare Verordnung gewährleistet ein einheitliches Datenschutzniveau, ermöglicht den öffentlichen Stellen die datenschutzgerechte Gestaltung ihrer Verfahren und erleichtert dem Landesbeauftragten für den Datenschutz, den behördlichen Datenschutzbeauftragten und den vorgesetzten Behörden die Kontrolle der Einhaltung des Datenschutzes.

– Die Verfassungsschutzbehörde soll nahezu völlig aus dem materiellen Anwendungsbereich des Landesdatenschutzgesetzes herausgenommen werden. Das Landesverfassungsschutzgesetz (LVerfSchG) enthält zwar selbst eine Reihe von bereichsspezifischen Vorschriften zum Datenschutz, regelt diesen Bereich aber nur unvollständig. Dies steht im Gegensatz zu § 7 Abs. 1 Satz 3 LVerfSchG, der die subsidiäre Geltung des Landesdatenschutzgesetzes anordnet. Vor allem entsteht dadurch aber eine Lücke, die insbesondere vor dem Hintergrund des Volkszählungsurteils (BVerfGE 65, 1) verfassungsrechtlich äußerst bedenklich ist. Beispielsweise wird durch die nunmehr fehlenden Vorschriften zum technischen Datenschutz eines der Hauptziele der Novellierung, nämlich „den gestiegenen Anforderungen an die Datensicherheit“ gerecht zu werden, konterkariert. Die beabsichtigte Änderung ist daher völlig unverständlich und inakzeptabel.

Die Landesregierung ist in der Pflicht, dem Landtag möglichst bald einen - angesichts der schon um deutlich mehr als ein Jahr überschrittenen Umsetzungsfrist der Datenschutzrichtlinie - überfälligen Gesetzentwurf zu präsentieren, der eine echte Fortentwicklung des Datenschutzes sowohl im rechtlichen als auch im technischen Bereich bedeutet.

2.2 Novellierung des Bundesdatenschutzgesetzes

Die Bundesregierung beabsichtigt, das Bundesdatenschutzgesetz in zwei Schritten zu novellieren. Die erste Stufe soll vor der Sommerpause 2000 abgeschlossen werden, die zweite bis zum Ende der Legislaturperiode des Bundestages.

Im ersten Schritt sollen neben der Umsetzung der EG-Datenschutzrichtlinie (siehe Punkt 2.4) Vorschriften zum Prinzip der Datenvermeidung, zur Videoüberwachung sowie zur Chipkartenanwendung geschaffen und die Datenschutzregelungen des Informations- und Kommunikationsdienste-Gesetzes (siehe Dritter Tätigkeitsbericht, Punkt 2.2) übernommen werden.

Ziel der zweiten Stufe ist die Neukonzeption des Bundesdatenschutzgesetzes und die Aufnahme weiterer Technikregelungen. Sobald es vom Zeitpunkt her sinnvoll erscheint, bildet sich auf Initiative des Bundesbeauftragten für den Datenschutz (BfD) eine Ad-Hoc-Arbeitsgruppe der Datenschutzbeauftragten zur Novellierung des Bundesdatenschutzgesetzes. Die Arbeitsgruppe wird sich dafür einsetzen, dass diejenigen Forderungen der Datenschutzbeauftragten (siehe Dritter Tätigkeitsbericht, Punkt 2.4), die im ersten Schritt noch nicht berücksichtigt wurden, in der zweiten Stufe Eingang in das Bundesdatenschutzgesetz finden.

2.3 Neue Regelungen für moderne Technik

Die Regelungen zu den technischen und organisatorischen Maßnahmen in den Datenschutzgesetzen, etwa § 17 DSG MV oder § 9 BDSG mit der dazugehörigen Anlage - die so genannten 10 Gebote - , stammen aus den 70er Jahren und orientieren sich an der damaligen Technik und Datenverarbeitungsstruktur. Diese Zeit war bestimmt von zentral organisierten Rechenzentren. Telekommunikation und Vernetzungen spielten nur eine untergeordnete Rolle. Die Datensicherheitsüberlegungen waren deshalb geprägt von der Vorstellung einer monolithischen Großrechnerwelt und primär verbunden mit dem Schutz der Rechner, die in hermetisch abgeschlossenen Rechenzentren betrieben wurden. In einer Zeit, in der Datenverarbeitung zunehmend dezentral in teilweise weltumspannenden Rechnernetzen betrieben wird, sind solche Regelungen nur noch bedingt oder gar nicht mehr wirksam.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder (AK Technik) - siehe auch Punkt 4 - hat allgemeine technikunabhängige Anforderungen vorgeschlagen, die die bisherigen „10 Gebote“ ersetzen sollen. Maßgeblicher Bestandteil der entsprechenden Vorschriften sollte die Pflicht zur Gewährleistung der folgenden Punkte sein:

Vertraulichkeit:	nur Befugte dürfen personenbezogene Daten zur Kenntnis nehmen können
Integrität:	personenbezogene Daten müssen während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben
Verfügbarkeit:	personenbezogene Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können
Authentizität:	personenbezogene Daten müssen jederzeit ihrem Ursprung zugeordnet werden können
Revisionsfähigkeit:	es muss festgestellt werden können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat
Transparenz:	die Verfahrensweisen bei der Verarbeitung personenbezogener Daten müssen vollständig, aktuell und in einer Weise dokumentiert sein, dass sie in zumutbarer Zeit nachvollzogen werden können

Gegenüber den bisherigen Regelungen wird dadurch vor allem Folgendes erreicht:

- Die Sicherheitsziele sind technologieunabhängig und bilden einen allgemeingültigen Sicherheitsrahmen, der auch bei neuen Formen der Datenverarbeitung Bestand haben wird.

- Die vorgeschlagenen Regelungen führen zu mehr Rechtssicherheit, da sie Anforderungen definieren, die im Bereich der IT-Sicherheit „verstanden“ werden, in der Praxis anwendbar sind, für jede Form der Datenverarbeitung und jede technische Architektur Gültigkeit haben und einer methodischen Vorgehensweise bei ihrer Umsetzung zugänglich sind.

- Die Ziele definieren eine „Messlatte“, an der die Sicherheit eines Datenverarbeitungs-Systems abgelesen und überprüft und wodurch seine Kontrollierbarkeit sichergestellt werden kann.

- Die Begriffe stimmen mit denen überein, die in der einschlägigen Sicherheitsliteratur und in der EG-Datenschutzrichtlinie verwendet werden.

- Datenschutzkontrolleure, Sicherheitsexperten, Systembetreiber, Softwarespezialisten und Entwicklungsingenieure sprechen die „gleiche“ Sprache.

Neben diesen Regelungszielen hat der AK Technik auch konkrete Maßnahmen vorgeschlagen, wie die Freigabe automatisierter Verfahren vor deren erstmaliger Anwendung, die Verschlüsselung personenbezogener Daten auf Systemen oder Datenträgern bei mobilem Einsatz oder Transport und die technische Koppelung der automatisierten Datenverarbeitung an die Prüfung der Benutzerberechtigung. Diese Vorkehrungen orientieren sich einerseits am Stand der gegenwärtigen Technik, von ihnen ist andererseits aber gleichwohl zu erwarten, dass sie längere Zeit Bestand haben werden.

Darüber hinaus wurden Empfehlungen zur Regelung für spezielle Techniken, beispielsweise Chipkarten sowie Fernmess- und Fernwirkdienste, gegeben. Schließlich hat der AK Technik Vorschläge zur Formulierung des Grundsatzes der Datensparsamkeit, der zur Beherrschung der immer größer werdenden Datenflut unabdingbar ist, und zur Definition der dafür nötigen Instrumente der Anonymisierung und Pseudonymisierung sowie der Verschlüsselung unterbreitet.

Es ist zu hoffen, dass der Gesetzgeber im Bund und in den Ländern die vorstehenden Anregungen bei der Überarbeitung der Datenschutzgesetze aufgreift, damit die durch die EG-Datenschutzrichtlinie angestoßene Novellierung auch die Technikregelungen einbezieht und so zu der dringend notwendigen umfassenden Modernisierung des Datenschutzrechts führt.

2.4 Direktwirkung der europäischen Datenschutzrichtlinie

Die europäische Datenschutzrichtlinie ist am 24. Oktober 1995 verabschiedet worden und hätte bis zum 24. Oktober 1998 in nationales Recht umgesetzt werden müssen (siehe Dritter Tätigkeitsbericht, Punkt 2.4). Mittlerweile ist dies in den meisten Mitgliedstaaten der Europäischen Union erfolgt, in Deutschland aber nur zu einem geringen Teil. Das Bundesdatenschutzgesetz wird frühestens im Jahr 2000 an die Vorgaben der Richtlinie angepasst werden (siehe dazu Punkt 2.2). Von den sechzehn Bundesländern haben bisher nur Brandenburg und Hessen ihre Datenschutzgesetze unter Berücksichtigung der Datenschutzrichtlinie novelliert. Auch Mecklenburg-Vorpommern ist seiner Pflicht zur Überarbeitung des Landesdatenschutzgesetzes nicht nachgekommen (siehe dazu Punkt 2.1). Das ebenfalls zu ändernde bereichsspezifische Datenschutzrecht haben weder Bund noch Länder angepasst.

In dieser Situation ist die Frage zu klären, ob die europäische Datenschutzrichtlinie für deutsche Behörden erst maßgeblich ist, wenn sie in deutschen Gesetzen ihren Niederschlag gefunden hat oder ob sie zuvor schon Wirkungen entfaltet.

Im Gegensatz zu den in den Mitgliedstaaten unmittelbar geltenden europäischen Verordnungen können die in den Richtlinien der Europäischen Gemeinschaft (EG) enthaltenen Regelungen erst dann angewendet werden, wenn sie in das nationale Recht der Mitgliedstaaten umgesetzt worden sind. Eine Ausnahme davon - also die Direktwirkung einer Richtlinie - kommt nach den Grundsätzen der ständigen Rechtsprechung des Europäischen Gerichtshofes dann in Betracht, wenn die Umsetzungsfrist abgelaufen ist und die Richtlinie dem Einzelnen ein hinreichend bestimmtes und unbedingtes Recht im Verhältnis gegenüber dem Staat gewährt. Sie muss also zum sachlichen Regelungsgehalt und zum erfassten Personenkreis eindeutig bestimmte Vorgaben treffen, und die Umsetzung der Forderungen darf nicht von gestalterischen Entscheidungen der Mitgliedstaaten abhängen. Ob diese Merkmale gegeben sind, kann aber nicht pauschal geprüft werden, sondern es sind die einzelnen Bestimmungen der jeweiligen Richtlinie zu betrachten.

Die EG-Datenschutzrichtlinie enthält einige Vorschriften, die die oben genannten Voraussetzungen erfüllen. Diese Regelungen gelten daher zugunsten der Bürger auch in Mecklenburg-Vorpommern unmittelbar und sind von den Behörden bereits jetzt zu beachten:

Begriff der „Datei“

Der Dateibegriff der Richtlinie geht weiter als der des § 3 Abs. 2 DSG MV und lässt insbesondere Ausnahmen und Einschränkungen wie die in § 2 Abs. 2 Satz 1 DSG MV formulierte Privilegierung vorübergehend erstellter Dateien nicht mehr zu. Auch für diese Dateien gelten daher alle Vorschriften des Landesdatenschutzgesetzes, etwa § 16 DSG MV (Dateibeschreibung und Geräteverzeichnis).

Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung von Daten über

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,
- die Gewerkschaftszugehörigkeit,
- die Gesundheit oder
- das Sexualleben

ist nur dann zulässig, wenn sie aufgrund von Spezialvorschriften oder einer ausdrücklichen Einwilligung der Betroffenen erfolgt. Die allgemeinen Vorschriften §§ 6 bis 14 DSG MV sind nicht mehr anwendbar.

Information Betroffener bei der Datenerhebung

Abweichungen von den entsprechenden Vorschriften § 8 Abs. 3 und 4 DSG MV ergeben sich vor allem insoweit, als die Betroffenen nunmehr generell unaufgefordert auch zu unterrichten sind über

- die Rechtsgrundlagen der Datenverarbeitung,
- die bestehenden Auskunfts- und Berichtigungsrechte,
- die Pflicht beziehungsweise Freiwilligkeit der Beantwortung der Fragen und mögliche Folgen einer unterlassenen Beantwortung (wenn die Erhebung bei den Betroffenen erfolgt) und
- die Kategorien (zusammenfassende thematische Beschreibung) der Daten, die verarbeitet werden (wenn die Erhebung nicht bei den Betroffenen erfolgt).

Auskunftsrecht

Artikel 12 geht wesentlich weiter als der korrespondierende § 20 DSG MV. So ist den Betroffenen nunmehr auch Auskunft zu erteilen über

- den Zweck der einzelnen Verarbeitungen (nicht nur der Speicherung) ihrer Daten,
- die Kategorien ihrer verarbeiteten Daten,
- den logischen Aufbau der automatisierten Verarbeitung ihrer Daten und
- die Berichtigung, Löschung oder Sperrung der Daten, deren Verarbeitung unzulässig ist, insbesondere wenn diese Daten unvollständig oder unrichtig sind.

Die Einschränkungen in § 20 Abs. 1 Satz 2 (Erforderlichkeit der Angaben der Betroffenen zum Auffinden der Daten in Akten) und Abs. 2 DSG MV (keine Auskunft bei Speicherung wegen Aufbewahrungsvorschriften oder zu Zwecken der Datensicherung oder Datenschutzkontrolle) stehen im Widerspruch zur Richtlinie und können daher den Auskunft Suchenden nicht mehr entgegengehalten werden.

Ausnahmen und Beschränkungen

Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte der Betroffenen aus den Artikeln 10, 11 und 12 für bestimmte Zwecke einschränken, wie zum Schutz der öffentlichen Sicherheit oder anderer Personen. Die Betroffenenrechte dürfen aber nur beschränkt werden, wenn dies durch Gesetz, Rechtsverordnung oder Satzung zugelassen ist. Auf Verwaltungsvorschriften, Erlasse, Dienstanweisungen oder Verfügungen oder gar auf die bloße - auch möglicherweise zutreffende - Feststellung, dass einer der Zwecke die Einschränkung notwendig macht, kann eine Verkürzung der Rechte nicht gestützt werden.

Widerspruchsrecht der Betroffenen

Betroffenen steht nunmehr auch bei rechtmäßigen Verarbeitungen ihrer personenbezogenen Daten ein Widerspruchsrecht zu. Die Verarbeitungen sind in solchen Fällen nur dann zulässig, wenn die datenverarbeitenden Stellen nach pflichtgemäßem Ermessen entscheiden, dass die schutzwürdigen Belange konkret Betroffener hinter dem öffentlichen Interesse an den Verarbeitungen der Daten zurückzustehen haben. Das Widerspruchsrecht kann zum Beispiel zum Tragen kommen, wenn sensible Daten zu verarbeiten sind und der zuständige Bearbeiter eine dem Betroffenen nahestehende Person ist oder dem Betroffenen durch die Verarbeitung seiner Daten ein Schaden entstehen könnte.

In diesem Umfang ist die Datenschutzrichtlinie seit dem 24. Oktober 1998 unmittelbar geltendes, von allen öffentlichen Stellen des Landes anzuwendendes Recht und geht insoweit auch dem Landesdatenschutzgesetz von Mecklenburg-Vorpommern vor. Entgegenstehende bereichsspezifische Rechtsvorschriften kommen nur zur Anwendung, sofern die Richtlinie solche Ausnahmen zulässt.

Dieser Zustand stellt die öffentlichen Stellen vor große praktische Schwierigkeiten, da sie vor jeder Anwendung von bereichsspezifischen Vorschriften oder Bestimmungen des Landesdatenschutzgesetzes prüfen müssen, ob nicht entgegenstehende oder ergänzende Normen der EG-Datenschutzrichtlinie anzuwenden sind. Erschwerend kommt hinzu, dass diese Regelungen sich nicht der deutschen Rechtsbegriffe bedienen oder gleichlautende Begriffe - beispielsweise „Widerspruch“ - anders gebrauchen.

Um diese sowohl für die Verwaltung als auch für die Betroffenen unbefriedigende Situation zu beenden, kann nur dringend empfohlen werden, die datenschutzrechtlichen Vorschriften möglichst bald an die Vorgaben der Richtlinie anzupassen.

3 Sorgen der Bürger, Einzelfälle, Beratungen, Kontrollen, Stellungnahmen

3.1 Rechtswesen

3.1.1 Täter-Opfer-Ausgleich

Bereits in der Vergangenheit habe ich eine gesetzliche Regelung zum Täter-Opfer-Ausgleich gefordert (siehe Dritter Tätigkeitsbericht, Punkt 3.1.4). Im Mai 1999 hat die Bundesregierung hierzu einen Gesetzentwurf (BR-Drs. 325/99) eingebracht. Erklärtes Ziel ist es, durch Einbeziehung einer so genannten Ausgleichsstelle einen außergerichtlichen Ausgleich zwischen Beschuldigtem und Opfer einer Straftat stärker als bisher zu fördern.

Kernstück datenschutzrechtlicher Überlegungen ist die Frage, ob Institutionen zur Durchführung des Ausgleichverfahrens von den Staatsanwaltschaften umfassende Informationen, insbesondere über Opfer von Straftaten, erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben. Der Gesetzentwurf sieht hierzu vor, dass das Opfer eine Datenübermittlung an eine Ausgleichsstelle nur dann verhindern kann, wenn es diese ausdrücklich ablehnt. Das Bundesjustizministerium (BMJ) begründet diese Regelung damit, dass die Ausgleichsstellen lediglich auf diese Weise geeignete Fälle zügig erhalten und so das Instrument des Täter-Opfer-Ausgleichs effektiv nutzen können.

Aus Sicht des Datenschutzes sollten die Vermittlungsstellen jedoch erst dann die Daten erhalten, wenn Beschuldigter und Opfer vorher eingewilligt haben. Auch beim Täter-Opfer-Ausgleich muss das Recht auf informationelle Selbstbestimmung beider Parteien gewahrt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 58. Konferenz im Oktober 1999 in Rostock ihre Position noch einmal einstimmig in Form einer Entschließung verdeutlicht (siehe 14. Anlage). Es bleibt zu hoffen, dass der Gesetzgeber die datenschutzrechtlichen Argumente berücksichtigt.

3.1.2 Maßvoller Umgang mit der DNA-Analyse

Im September 1998 ist das DNA-Identitätsfeststellungsgesetz in Kraft getreten. Damit hat der Bundesgesetzgeber eine gesetzliche Grundlage für die Erhebung und Speicherung so genannter genetischer Fingerabdrücke in einer bundesweiten Datei für Zwecke künftiger Strafverfahren geschaffen. Die so genannte DNA-Analyse ermöglicht, Verdächtige als Täter zu identifizieren beziehungsweise mit hoher Wahrscheinlichkeit auszuschließen. Zu diesem Zweck wird Personen Körpermaterial (zum Beispiel Blut, Speichel oder Haarwurzeln) entnommen, untersucht und mit dem am Tatort aufgefundenen Spurenmaterial verglichen. Da mit diesem modernen Verfahren der Strafverfolgung weit in das Persönlichkeitsrecht der Betroffenen eingegriffen wird, ist ein adäquater datenschutzrechtlicher Schutzstandard zu gewährleisten.

Die bereits vor der Verabschiedung des DNA-Identitätsfeststellungsgesetzes errichtete Dateianordnung, die auch jetzt noch in geringfügig geänderter Fassung gültig ist, entspricht diesem Schutzstandard nicht. Nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes bedarf es für die molekulargenetische Untersuchung einer richterlichen Anordnung. Der Richter hat unter anderem die Prognose zu treffen, ob Grund zu der Annahme besteht, dass gegen den Betroffenen künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Die Dateianordung ermöglicht jedoch die Erhebung und Speicherung von DNA-Profilen auch ohne richterliche Anordnung, sofern der Betroffene in die molekulargenetische Untersuchung eingewilligt hat.

Die Einwilligung, beispielsweise von Strafgefangenen, wird jedoch - insbesondere kurz vor der Entlassung - selten frei von psychischen Zwängen sein. Gefangene könnten annehmen, dass sich ihre Einwilligung unter Umständen positiv auf den Haftvollzug auswirken und eine Weigerung das Gegenteil bedeuten könnte. Einwilligungslösungen müssen jedoch stets frei von staatlichem Zwang sein.

Anlass zu dieser Diskussion gaben einige Bundesländer, die die DNA-Analysen ohne richterlichen Beschluss durchführten (vergleiche Länderumfrage des Landeskriminalamtes Niedersachsen vom September 1999). Mecklenburg-Vorpommern gehörte bisher nicht zu diesen Ländern. Inzwischen hat unser Innenministerium jedoch mitgeteilt, dass man sich wohl der Vorgehensweise der anderen Bundesländer anschließen werde. Das Ministerium begründet diesen Schritt mit einer nunmehr anderen Auslegung des Identitätsfeststellungsgesetzes und zitiert die Rechtsmeinung einiger Strafrechtskommentatoren sowie eine Entscheidung des Landgerichts Stralsund vom 6. Juli 1999 (Az III Qs 96/99 LG Stralsund).

Die Rechtsprechung in diesem Bereich ist tatsächlich nicht einheitlich. So sind einerseits Entscheidungen von zuständigen Amts- und auch Landgerichten ergangen, worin der staatsanwaltschaftliche Antrag auf richterliche Anordnung zurückgewiesen wurde, weil eine „Einwilligung“ vorgelegen hätte (so auch Landgericht Hamburg, Entscheidung vom 31. August 1999; Az 612 Qs 81/99). Andererseits gibt es einen Beschluss des Landgerichtes Nürnberg-Fürth vom 22. Juli 1999 (Az 1 Os 26/99), in dem die Erforderlichkeit einer richterlichen Anordnung für molekulargenetische Analysen nach dem Identitätsfeststellungsgesetz bejaht wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer 58. Sitzung am 7./8. Oktober 1999 in Rostock ihre Position zu dieser umstrittenen Thematik in einer Entschließung verdeutlicht und einer „Einwilligungslösung“ eine klare Absage erteilt (siehe 18. Anlage). Es bleibt abzuwarten, ob und in welcher Form die Innen- und Justizministerien des Bundes und der Länder auf die bisherige Praxis in den Ländern Einfluß nehmen.

3.1.3 Praxis der Telefonüberwachungen

Die Zahl der Telefonüberwachungen ist in den letzten Jahren sowohl bundesweit als auch landesweit sprunghaft angestiegen. Deutschland gehört mittlerweile zu den Ländern, in denen am häufigsten abgehört wird. Das Bundesjustizministerium (BMJ) nennt Zahlen zwischen 11.000 und 13.400 betroffenen Telefonanschlüssen für 1998. Die Gründe dafür sind zahlreich. Zum einen liegt das an der zusätzlichen Nutzung von Handys. Zum anderen wurde der Katalog der Straftaten, der eine Telefonüberwachung erlaubt, in der Vergangenheit mehrfach erweitert. Seit 1968 sind mehr als 20 Straftaten zusätzlich in den Katalog des § 100 a StPO aufgenommen worden, unter anderem Bandendiebstahl, schwerer Bandendiebstahl, gewerbsmäßige Hehlerei, Bandenhehlerei, Geldwäsche und auch Verstöße gegen das Waffen-, das Ausländer-, das Asylverfahrens- oder das Betäubungsmittelgesetz.

Weil Telefonüberwachungen erheblich in die Persönlichkeitssphäre der Betroffenen, unter denen sich meistens auch unbescholtene Bürger befinden, eingreifen, wird es aus Sicht der Datenschutzbeauftragten höchste Zeit zu prüfen, ob sich die gewünschten Erfolge bei der Verbrechensbekämpfung auch tatsächlich einstellen. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits auf ihrer 48. Konferenz im September 1994 gefordert, dass eine Auswertung polizeilicher Befugnisse (auch der Telefonüberwachung) ergebnisoffen, qualitativ und wissenschaftlich begleitet erfolgen soll. Das ständige Anmahnen hat teilweise Erfolg gezeigt. Es gibt inzwischen einen Projektauftrag des Innenministeriums Schleswig-Holstein an die Verwaltungsfachhochschule Altenholz (bei Kiel) aus dem Jahre 1998, verdeckte Ermittlungsmaßnahmen zu untersuchen. Die Länder Hamburg und Mecklenburg-Vorpommern wollen sich ebenfalls daran beteiligen.

Des Weiteren hat das Bundesministerium der Justiz im August 1999 ein Forschungsvorhaben zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO“ öffentlich ausgeschrieben. Es bleibt abzuwarten, ob diese Untersuchungen Erkenntnisse dafür bringen, dass alle polizeilichen Befugnisse in dem bisherigen Ausmaß weiterhin auch tatsächlich benötigt werden. Andernfalls müsste der Gesetzgeber konsequenterweise handeln und polizeiliche Befugnisse wieder einschränken.

Um mir ein Bild von der Praxis der Telefonüberwachung im Lande zu machen, habe ich bei der Staatsanwaltschaft Schwerin im Dezember 1998 stichprobenartig ausgewählte Akten kontrolliert und dabei folgendes festgestellt:

Abhören im Bereich der „Drogenkriminalität“

Ich habe Akten zu eingeleiteten Ermittlungsverfahren wegen des Verdachtes des gewerbsmäßigen Handelns mit Betäubungsmitteln geprüft. Telefonüberwachungen waren dort ordnungsgemäß beantragt und auch durchgeführt worden. In sämtlichen Fällen wurden die Ermittlungsverfahren eingestellt, da die angeordneten Maßnahmen keinen Beweis dafür erbracht hatten, dass sich die Beschuldigten wegen unerlaubten Handeltreibens strafbar gemacht haben könnten. Zwar ergaben sich häufig Anhaltspunkte dafür, dass unerlaubter Besitz von Betäubungsmitteln vorlag. Hierbei handelte es sich jedoch (im Gegensatz zum Handeltreiben) nicht um eine Tat, die das Abhören des Telefons erlaubt. Von einer Bestrafung wurde in diesen Fällen abgesehen.

Abhören und Protokollieren von Verteidigergesprächen

Gespräche zwischen Beschuldigten und Verteidigern dürfen nicht abgehört werden (§ 148 StPO). Die Kontrolle ergab jedoch, dass keine organisatorischen oder technischen Maßnahmen getroffen wurden, die dieses Verbot tatsächlich wirksam umsetzen. Ich habe daher empfohlen, durch geeignete Maßnahmen sicherzustellen, dass in diesen Fällen weder abgehört noch aufgezeichnet und auch nicht auszugsweise protokolliert wird. Dazu müßte die Aufzeichnung von Gesprächen bei bestimmten Rufnummern unterdrückt werden. Eine Antwort des Landeskriminalamtes zu dieser Empfehlung steht noch aus.

Benachrichtigungspflicht

Probleme gibt es auch hinsichtlich der Benachrichtigung der Beteiligten. Der relativ große Personenkreis umfasst neben dem Beschuldigten selbst auch die Personen, deren Anschlüsse der Beschuldigte nutzt, die Anschlussinhaber, die möglicherweise Mitteilungen für den Beschuldigten entgegennehmen oder weitergeben, und selbstverständlich alle Gesprächspartner des Beschuldigten. Würde man alle diese Personen benachrichtigen, bestünde die Gefahr, dass Gesprächsteilnehmer eine Vielzahl von Informationen über den jeweiligen Anschlussinhaber erfahren, zum Beispiel das Delikt, dessen der Betroffene beschuldigt wird. Das wiederum würde dessen Recht auf informationelle Selbstbestimmung massiv beeinträchtigen. Insbesondere gilt das dann, wenn das Verfahren gegen den Beschuldigten wegen Fehlens eines hinreichenden Tatverdachts später eingestellt werden muss.

Zu einer differenzierten Lösung kann man jedoch gelangen, wenn man Sinn und Zweck der Benachrichtigungspflicht im Verhältnis zum Gebot der unverzüglichen Löschung gemäß § 100 b Abs. 6 StPO betrachtet. Das Gebot zur unverzüglichen Löschung, das nur im Hinblick auf die Erforderlichkeit zur weiteren Strafverfolgung eingeschränkt wird, hat Vorrang vor allen weiteren Verfahrensschritten, einschließlich der Benachrichtigung. Wenn die nicht erforderlichen Unterlagen gelöscht sind, müssen die dort verzeichneten Gesprächspartner nicht mehr benachrichtigt werden. Eine Benachrichtigung der Beteiligten vor der Vernichtung ist nach der Systematik des Gesetzes nicht vorgesehen. Daher habe ich empfohlen, die Benachrichtigungspflicht auf solche Personen zu reduzieren, mit denen der Beschuldigte Telefongespräche geführt hat, deren Inhalte zur Strafverfolgung relevant sind. In diesen Fällen werden die Gesprächspartner und ihre Anschriften im Zuge der Ermittlungen bekannt geworden sein und sich somit aus der Akte entnehmen lassen.

Während meiner Kontrolle bei der Staatsanwaltschaft habe ich einen Fall vorgefunden, in dem die Beschuldigte nur unvollständig über Abhörmaßnahmen informiert wurde. Die Staatsanwaltschaft Schwerin hat hierzu ausgeführt, dass - durch die zunehmende Benutzung von Handys - Beschuldigte häufig nicht nur selbst mehrere Telefonanschlüsse, sondern auch die (mobilen) Anschlüsse anderer benutzten. Die Dezernenten sollten als Hilfsmittel entsprechende Übersichten erhalten, um alle Beteiligten im Sinne des § 101 Abs. 1 StPO und sämtliche getroffenen Maßnahmen zu erfassen.

Die Staatsanwaltschaft Schwerin hat die Empfehlungen unverzüglich umgesetzt. Es wird weiterhin verstärkt darauf zu achten sein, dass die Praxis der Telefonüberwachungen nicht noch mehr ausufert.

3.1.4 Entwurf eines Untersuchungshaftvollzugsgesetzes

Die Bundesregierung hat im Frühjahr 1999 einen Gesetzentwurf zur Regelung der Untersuchungshaft (BR-Drs. 249/99) eingebracht. Damit werden die seit langem überfälligen spezifischen Datenschutznormen für den Bereich der Untersuchungshaft geschaffen. Während des laufenden Gesetzgebungsverfahrens habe ich gegenüber unserem Justizministerium auf folgende Anforderungen hingewiesen:

- Der ungehinderte und unüberwachte telefonische Kontakt zwischen Verteidiger und Beschuldigtem muß gewährleistet sein.

- Die Überwachung der Unterhaltung mit Besuchern sowie die Kontrolle von Schriftstücken ist nur dann angemessen, wenn die Untersuchungshaft wegen Verdunkelungsgefahr angeordnet wurde. Nur für diesen Fall sollten die Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden. Liegen andere Haftgründe vor, sollten die Überwachung und die Textkontrolle nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen.

- Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt und an Forschungseinrichtungen müssen die schutzwürdigen Belange der Betroffenen im Rahmen einer Abwägung berücksichtigt werden.

– Eine erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen ist im Hinblick auf den Zweck der Untersuchungshaft und unter Berücksichtigung des Grundsatzes der Unschuldsvermutung aus datenschutzrechtlicher Sicht nicht hinzunehmen.

Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu im August 1999 eine Entschließung verabschiedet (siehe 21. Anlage), um auf das Gesetzgebungsverfahren noch wirkungsvoll Einfluss zu nehmen. Es bleibt abzuwarten, ob der Gesetzgeber die datenschutzrechtlichen Anforderungen in den Gesetzestext aufnimmt.

3.1.5 Parlamentarische Kontrolle von Lauschangriffen

Durch Verfassungsänderung vom 26. März 1998 (Bundesgesetzblatt I 610) ist der Große Lauschangriff nunmehr in Art. 13 Grundgesetz (GG) verankert worden (siehe Dritter Tätigkeitsbericht, Punkt 3.2.3). Zur Kontrolle der daraus resultierenden einschneidenden Maßnahmen sind in Absatz 6 gewisse Rahmenbedingungen festgelegt. So hat die Bundesregierung den Bundestag jährlich über den erfolgten Einsatz technischer Mittel im repressiven und im präventiven Bereich (Zuständigkeit des Bundes) zu unterrichten. Ein vom Bundestag gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus.

Die Länder haben gemäß Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Weil die grundrechtssichernde Bedeutung dieser Kontrollbefugnis besonders wichtig ist, sollte eine Regelung auf gesetzlicher Ebene auch in Mecklenburg-Vorpommern erfolgen. Festzuschreiben wäre dort, dass die Landesregierung gegenüber dem Landesparlament in regelmäßigen Abständen in anonymisierter Form über stattgefundene Lauschangriffe berichten muss. Die Parlamentarier hätten dann die Möglichkeit, sich über Art und Umfang, Häufigkeit und Effizienz solcher Maßnahmen zur Verbrechensbekämpfung zu informieren und diese entsprechend auszuwerten. Aus Gründen der Transparenz sollten die Berichte öffentlich und nicht in einem geheim tagenden Gremium erörtert werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu dieser Thematik am 17. Juni 1999 eine Entschließung verabschiedet (siehe 20. Anlage).

Die datenschutzrechtliche Position habe ich unserem Landtag gegenüber dargelegt. Der Präsident des Landtages hat mir mitgeteilt, dass sich der Ältestenrat mit dem Thema befasst. Eine abschließende Antwort steht noch aus.

3.1.6 Welche Daten müssen bei Sparbuchverlust offenbart werden?

Ein Petent, dessen Mutter ihr Sparbuch verloren hatte, wandte sich an ein Amtsgericht, um das Sparbuch für kraftlos erklären zu lassen. Das Gericht erließ daraufhin ein Aufgebot und veröffentlichte dieses in verschiedenen Zeitungen sowie dem Bundesanzeiger. Dabei wurden außer der Nummer des Sparbuches und dem Namen der ausstellenden Sparkasse auch der Name und die vollständige Anschrift der Sparbuchinhaberin sowie die genaue Höhe des Guthabens genannt.

Auf meine Nachfrage erklärte der Direktor des Gerichts, die genannten Daten würden zur eindeutigen Bestimmung des Sparbuches benötigt. Zwar bestehe ein Entscheidungsspielraum zu der Frage, wann eine eindeutige Bestimmbarkeit gegeben sei, das Vorgehen sei aber gängige Praxis.

Zur unverwechselbaren Bezeichnung eines Sparbuches sind jedoch Nummer und Name der ausgebenden Sparkasse ausreichend. Im Falle eines von der Sparkasse selbst durchgeführten Aufgebotsverfahrens nach § 2 der Sparkassenverordnung M-V werden auch nur diese Daten veröffentlicht.

Später erhielt ich eine Kopie des nach Abschluss des Aufgebotsverfahrens ergangenen Ausschlussurteils, mit dem das Sparbuch für kraftlos erklärt wurde. In diesem Urteil war das Sparbuch lediglich mit Nummer und Namen der Sparkasse sowie dem Namen der Mutter des Petenten bezeichnet. Die Höhe des Guthabens sowie die genaue Anschrift waren nicht genannt.

Der Direktor des Amtgerichts hat zugesichert, dass auf die Bekanntgabe des Guthabens und der Anschrift bei der Bearbeitung von Aufgebotssachen künftig generell verzichtet wird.

3.1.7 Wenn der Staatsanwalt zu Hause arbeitet

Die Presse berichtete über einen Fall, in dem ein Staatsanwalt Strafakten und Personalunterlagen, auch nach Beendigung seiner Tätigkeit bei der Staatsanwaltschaft, bei sich zu Hause unbearbeitet gelagert hatte. Der Mitarbeiter wurde strafrechtlich zur Verantwortung gezogen. Unabhängig von diesem Einzelfall ergaben sich hieraus datenschutzrechtliche Fragen zur Bearbeitung von Akten in der Privatwohnung und zur Nutzung privater Rechner für dienstliche Zwecke.

Das Justizministerium hat zum Umgang mit Personaldaten auf das Landesbeamtengesetz und die dazu erlassene Verwaltungsvorschrift verwiesen. Ergänzend war verfügt worden, dass Personalunterlagen nur in Diensträumen und nicht zu Hause zu bearbeiten sind. Staatsanwälte dürften hingegen Strafverfahrensakten in Privatwohnungen mitnehmen. Dies sei angesichts der erheblichen Belastungslage der Dezernenten geboten und entspräche der bundesweiten Praxis. Jeder Staatsanwalt habe sich zur Verschwiegenheit verpflichtet. Dies umfasse auch die sichere Verwahrung der Unterlagen zu Hause. Einer gesonderten Nachweisführung über die in die Privatwohnung verbrachten Akten bedürfe es daher nicht. Die Akten würden auf die Person des jeweiligen Dezernenten ausgetragen. Somit übernehme er die Verantwortung für die sichere Verwahrung und habe die Akten in seiner Privatwohnung besonders vor dem Zugriff Dritter zu schützen. Darüber hinaus dürften Staatsanwälte dienstlich beschaffte Software auch auf häuslichen Rechnern installieren und für dienstliche Zwecke nutzen.

Die Staatsanwaltschaften verarbeiten und nutzen zweifelsohne viele sensible personenbezogene Daten von den im Verfahren beteiligten Personen, wie Täter, Opfer und Zeugen. Es ist fraglich, ob für die sichere Aufbewahrung der Unterlagen im häuslichen Bereich ein gleichwertiger Schutz wie in der Dienststelle erreicht werden kann. Dies betrifft zum einen die Sicherung des Gebäudes und zum anderen den Schutz der Unterlagen vor dem unberechtigten Zugriff Dritter, die Zutritt zum Hause haben, wie Familienangehörige, Hausangestellte und Besucher. Die Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften enthält lediglich Festlegungen zur allgemeinen Aktenkontrolle. Weitergehende technische und organisatorische Maßnahmen zum Umgang mit Verfahrensakten außerhalb von Dienstgebäuden existieren jedoch nicht. Insbesondere der Verarbeitung personenbezogener Daten auf privaten Rechnern ist erhöhte Aufmerksamkeit zu widmen. Die Nutzung privater Rechner sollte der Genehmigung der Behördenleitung unterliegen, damit diese davon Kenntnis hat, wo und unter welchen Bedingungen personenbezogene Daten außerhalb der Staatsanwaltschaft verarbeitet werden. Unter datenschutzrechtlichen Gesichtspunkten ist zu gewährleisten, dass die gespeicherten Daten ebenso wie die Akten vor dem unberechtigten Zugriff Dritter geschützt sind. Das gilt vor allem für die Fälle, in denen andere Familienmitglieder ebenfalls den Rechner benutzen. Um dies sicherzustellen, dürfen beispielsweise keine personenbezogenen Daten auf der Festplatte gespeichert werden. Ferner wäre auch das Verfahren festzulegen, nach dem die Übertragung der auf den privaten Rechnern verarbeiteten Daten auf das Datenverarbeitungssystem der Dienststelle unter Berücksichtigung bestehender Sicherheitsrisiken erfolgt.

Ich habe, nicht zuletzt auch aufgrund des geschilderten Sachverhaltes, dem Justizministerium empfohlen, technische und organisatorische Maßnahmen zum Umgang mit den Verfahrensakten außerhalb von Dienstgebäuden festzulegen. Diesem Anliegen wurde nicht entsprochen, da die vorhandenen Regelungen als ausreichend erachtet werden.

Das Justizministerium hat dennoch in Aussicht gestellt, die Musterdienstanweisung zum Datenschutz zu überarbeiten und dabei auch Regelungen für den Umgang mit personenbezogenen Daten auf privaten Rechnern aufzunehmen. Sobald ein entsprechender Entwurf vorliegt, werde ich hierzu Stellung nehmen. Inwieweit die überarbeitete Dienstanweisung für die automatisierte Verarbeitung hinreichende Regelungen enthalten wird, bleibt daher abzuwarten.

3.1.8 Elektronisches Grundbuch

Nachdem 1993 mit dem Registerverfahrensbeschleunigungsgesetz die Rechtsgrundlagen geschaffen worden sind, um das Grundbuch in elektronischer Form führen zu können, soll auch in Mecklenburg-Vorpommern das Elektronische Grundbuch eingeführt werden. In die Planungen hierzu bin ich frühzeitig einbezogen worden (siehe Dritter Tätigkeitsbericht, Punkt 3.1.7). Zu zwei Teilaspekten des Gesamtprojektes habe ich schwerpunktmäßig beraten.

Elektronische Unterschrift

In der Grundbuchordnung (GBO) ist unter anderem festgelegt, dass jede Eintragung im Elektronischen Grundbuch mit einer elektronischen Unterschrift zu versehen ist. Mit dem vom Justizministerium initiierten Teilprojekt „Elektronische Unterschrift“ sollten Vorgaben für die Implementierung eines Systems zur gesetzeskonformen Umsetzung dieser Vorschrift in der entsprechenden Anwendungssoftware der Grundbuchämter (ARGUS-GB) erarbeitet werden. Die folgenden Forderungen des § 75 GBO machen deutlich, dass die Lösung des Problems keineswegs trivial ist:

- Eine Eintragung soll nur möglich sein, wenn die zur Führung des Grundbuches zuständige Person der Eintragung ihren Namen hinzusetzt und beides elektronisch unterschreibt.

- Die elektronische Unterschrift soll in einem allgemein als sicher anerkannten automatisierten kryptographischen Verfahren hergestellt werden.

- Die zuständige Stelle soll die elektronische Unterschrift überprüfen können.

Mitte 1998 legte ein externer Dienstleister dem Justizministerium einen Realisierungsvorschlag vor. Die datenschutzrechtliche Prüfung hat ergeben, dass dieser Vorschlag wesentliche Forderungen des § 75 GBO nicht berücksichtigt hatte. Es war beispielsweise nicht möglich, einen Grundbucheintrag der eintragenden Person durch ein kryptographisches Verfahren zuzuordnen. Die geforderte elektronische Unterschrift wurde also nicht realisiert. Darüber hinaus war nicht vorgesehen, die Authentizität des Eintragenden kryptographisch festzustellen. Im Ergebnis der Prüfung war festzustellen, dass der Vorschlag den datenschutzrechtlichen Anforderungen nicht genügte.

In den folgenden Beratungen habe ich daraufhin vorgeschlagen, dass jeder Eintragungsberechtigte in Anlehnung an das Signaturgesetz von einer justizeigenen vertrauenswürdigen Stelle (Trustcenter) sein eigenes Schlüsselpaar erhält. So könnte unter Nutzung eines asymmetrischen kryptographischen Verfahrens die von der GBO geforderte Unterschrift geleistet werden und der Eintrag wäre überprüfbar. Das Justizministerium schlug hingegen vor, lediglich die Authentisierung der Eintragenden mit Hilfe einer Chipkarte zu realisieren und mit einer einheitlichen digitalen Signatur der Grundbuchsoftware alle Eintragungen zu unterschreiben. Diese Variante wäre jedoch ohne sehr aufwendige begleitende Sicherungsmaßnahmen meines Erachtens nicht gesetzeskonform gewesen.

Das Justizministerium entschloß sich daraufhin im November 1998, das Institut für Rechtsinformatik der Universität des Saarlandes mit einem Gutachten zu beauftragen, das die Vereinbarkeit der drei Lösungsvorschläge (externer Dienstleister, Justizministerium, Datenschutzbeauftragter) mit den rechtlichen Anforderungen an die Sicherungsarchitektur bewerten sollte.

Die Gutachter kamen zu folgendem Ergebnis: Der Vorschlag des externen Dienstleisters genügt insbesondere den Anforderungen an die elektronische Unterschrift im Sinne des § 75 GBO nicht. Die Variante des Ministeriums würde zwar den rechtlichen Vorgaben entsprechen, begegnete jedoch mit Blick auf Manipulationsmöglichkeiten der Sytemverwalter Bedenken. Mein Vorschlag fand die uneingeschränkte Zustimmung, da grundbuchrechtliche Vorschriften vollständig umgesetzt werden können.

Im weiteren Verlauf des Projektes verfolgte das Justizministerium trotz der im Gutachten geäußerten Bedenken zunächst den eigenen Realisierungsvorschlag und untersuchte, welche Maßnahmen erforderlich wären, um die genannten Risiken auf ein hinnehmbares Maß zu reduzieren. Es zeigte sich jedoch, dass der Aufwand höher als zunächst angenommen werden würde. Nach der Konsultation von Hard- und Softwareherstellern und weiteren Beratungen mit meiner Behörde wurde dann doch eine Lösung mit personenbezogenen Chipkarten zur Realisierung einer echten digitalen Signatur gewählt, die weitgehend meinem Vorschlag entsprach.

Auftragsdatenverarbeitung

Die geplante zentrale Speicherung des Datenbestandes stellt hohe Anforderungen an Verfügbarkeit und Integrität, die in Mecklenburg-Vorpommern meines Erachtens zurzeit nur im Landesrechenzentrum, dem einzigen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Hochsicherheitsrechenzentrum des Landes, umgesetzt werden können. Dazu müsste das Justizministerium also die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) als Betreiber mit der Verarbeitung der Daten beauftragen.

Nach § 126 Abs. 3 GBO ist eine Auftragsdatenverarbeitung grundsätzlich zulässig, jedoch beschränkt auf Anlagen bei staatlichen Stellen oder juristischen Personen des öffentlichen Rechts. Die Nutzung von Rechnerkapazitäten privatrechtlicher Einrichtungen, deren sämtliche Anteile einem Land oder dem Bund gehören, sowie nicht-öffentlicher Stellen wurde hingegen ausdrücklich ausgeschlossen. Der Gesetzgeber hat hierbei nicht allein auf die Eigentumsfrage hinsichtlich der Anlagen abgestellt, sondern schränkt vielmehr den Adressatenkreis der Auftragnehmer ein und will damit die Daten des Grundbuches vor einem möglichen Zugriff nicht-öffentlicher Stellen schützen.

Nun wäre es aber allein aus ökonomischen Gründen wenig sinnvoll, ein weiteres, den speziellen Anforderungen der GBO genügendes Rechenzentrum bei einer staatlichen Stelle zu betreiben. Die DVZ M-V GmbH jedoch dürfte aus den oben genannten Gründen als Auftragnehmer nur dann in Betracht kommen, wenn deren Rechtsstatus oder die Bestimmungen in § 126 Abs. 3 GBO geändert würden. Die von mir erbetene Prüfung durch das Justizministerium hat ergeben, dass eine Initiative Mecklenburg-Vorpommerns zur Änderung der GBO keine Aussichten auf Erfolg hat. Eine Änderung des Rechtsstatus der DVZ M-V GmbH ist ebenfalls nicht vorgesehen. In der Landtags-Drucksache 3/825 vom November 1999 (Unterrichtung durch die Landesregierung) vertritt das Justizministerium die Auffassung, dass allein mit technischen und organisatorischen Maßnahmen (Nutzung eigener Rechner, Einsatz besonders verpflichteten Personals, Beschränkung der Tätigkeit der DVZ M-V GmbH auf die Leistung technischer Hilfestellung bei der Verarbeitung hoheitlicher Daten) den gesetzlichen Anforderungen hinreichend Rechnung getragen werden kann.

Es bleibt also abzuwarten, ob tatsächlich wirtschaftlich vertretbare Möglichkeiten zum Betrieb des Elektronischen Grundbuches in den Räumen der DVZ M-V GmbH gefunden werden, die den Vorschriften des § 126 Abs. 3 GBO genügen.

3.1.9 Schuldnerverzeichnis bald öffentlich?

Presseberichte über die Veröffentlichung von Schuldnerlisten durch eine Industrie- und Handelskammer (IHK) des Landes führten zu zahlreichen Anfragen bei meiner Behörde. Betroffene befürchteten, dass ihre Daten nunmehr für jedermann zugänglich seien und ohne Einschränkung verarbeitet und genutzt werden könnten. Eine Prüfung des Sachverhaltes ergab Folgendes:

Bei den Amtsgerichten des Landes werden nach den Vorschriften der Zivilprozessordnung (ZPO) und der Schuldnerverzeichnisverordnung Schuldnerverzeichnisse geführt. Schuldner sind in dieses Verzeichnis aufzunehmen, wenn sie im Vollstreckungsverfahren Geldforderungen der Gläubiger nicht befriedigen konnten und eine Offenbarungsversicherung abgegeben haben oder wenn sie dieser Erklärungspflicht nicht nachgekommen sind und Haft gegen sie angeordnet wurde. Auskünfte aus diesem Verzeichnis erteilt das registerführende Gericht, wenn diese erforderlich sind für Zwecke der Zwangsvollstreckung, zur gesetzlich vorgesehenen Prüfung der wirtschaftlichen Zuverlässigkeit, zur Strafverfolgung, zur Prüfung der Gewährung öffentlicher Leistungen oder um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen.

Die IHK hat mir auf Anfrage mitgeteilt, dass kammerzugehörige Unternehmen Schuldnerlisten laufend beziehen können. Die IHK hat für diesen Zweck eine nicht-öffentliche Stelle beauftragt, die Listen zu erstellen und zu vertreiben. Die Unternehmen müssen den Bezug der Listen schriftlich beantragen. Bei einer Bewilligung erhalten sie ein Merkblatt über die Bezieherpflichten, die einschlägigen Rechtsvorschriften sowie ein Formular zur Abgabe einer Verpflichtungserklärung. In der Erklärung wird der Bezieher nochmals ausdrücklich auf seine gesetzlichen Pflichten, die aus dem Bezug der Listen resultieren, hingewiesen und auf deren Einhaltung verpflichtet. Bei einem Verstoß kann das Unternehmen vom Bezug der Listen ausgeschlossen werden.

Dieses Verfahren ist grundsätzlich nicht zu beanstanden. Die IHK sowie andere gesetzlich festgelegte Adressaten erhalten Abdrucke aus dem Schuldnerverzeichnis und erteilen Auskünfte an Kammermitglieder. Sie dürfen die Schuldnerdaten in Listen zusammenfassen und den Kammermitgliedern überlassen. Zu diesem Zweck können sie sich auch eines Dritten bedienen. Meine Prüfung hatte ergeben, dass die datenschutzrechtlichen Anforderungen an die Beauftragung weitgehend berücksichtigt wurden. Die fehlende Unterwerfung unter die Kontrolle des Landesbeauftragten für den Datenschutz für diese Auftragsdatenverarbeitung wurde ergänzt.

Kammermitglieder sind allerdings nur dann berechtigt, regelmäßig Listen zu beziehen, wenn Einzelauskünfte nicht genügen, um ihre berechtigten Interessen wahrzunehmen. Diese Prüfung hatte die IHK zunächst versäumt. Im Rahmen der Bezugsverpflichtung wurde dann im Nachhinein abgefragt, warum dem Unternehmen eine Einzelauskunft nicht genügt. Künftig hat das Unternehmen gleich bei der Antragstellung darzulegen, warum der regelmäßige Listenbezug erforderlich ist.

Die IHK hat meine Hinweise berücksichtigt. Nunmehr entspricht das gewählte Verfahren den datenschutzrechtlichen Bestimmungen. Um die Persönlichkeitsrechte der in den Schuldnerlisten geführten Personen zu gewährleisten, kommt es entscheidend darauf an, dass die Unternehmen die datenschutzrechtlichen Anforderungen, insbesondere die Zweckbindung und die Löschungsverpflichtung, einhalten. Darauf werden diese im Rahmen der Bewilligung des laufenden Bezuges der Listen hingewiesen.

3.1.10 Notare in Mecklenburg-Vorpommern mit Sonderprivilegien

Notare können in Ausübung ihrer Amtstätigkeit ohne jede Begründung Einsicht in Grundbücher und Grundakten von Grundstücken nehmen. Begehrt ein Notar jedoch Grundbucheinsicht, ohne dass ein Zusammenhang mit seiner Amtstätigkeit besteht, etwa aufgrund privaten Interesses an einem Grundstück, so muss er wie jeder andere Bürger auch dem Grundbuchamt sein berechtigtes Interesse für die Einsichtnahme darlegen und erhält dann auch nur soweit Einsicht in die Unterlagen, wie sein Interesse reicht (siehe Dritter Tätigkeitsbericht, Punkt 3.1.6).

Ein Petent befürchtete, dass ein Notar seine Amtsstellung ausgenutzt und aus privatem Interesse Einsicht in das Grundbuch und die Grundakten seines Grundstücks genommen hatte. Ich habe den Notar um Auskunft zum Sachverhalt gebeten.

Er hat mich nur unvollständig informiert und sich auf seine Verschwiegenheitspflicht nach § 18 der Bundesnotarordnung (BNotO) berufen. Die notarielle Verschwiegenheitspflicht kann dem Kontrollrecht des Landesbeauftragten für den Datenschutz gemäß § 26 DSG MV jedoch nicht entgegengehalten werden. Notare sind öffentliche Stellen des Landes und fallen daher in den Anwendungsbereich des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern. Nach § 27 DSG MV sind sie somit verpflichtet, den Landesbeauftragten für den Datenschutz bei seiner Aufgabenerfüllung zu unterstützen und ihm insbesondere alle Fragen zu beantworten, die im Zusammenhang des Umgangs mit personenbezogenen Daten stehen. Da der Notar sich weigerte, mir die gewünschte Auskunft zu geben, habe ich sein Verhalten gemäß § 28 DSG MV gegenüber dem Landesjustizministerium als zuständige oberste Aufsichtsbehörde beanstandet und darum gebeten, die nötigen Maßnahmen dafür zu ergreifen, dass ich die zur Bearbeitung der Petition erforderlichen Informationen erhalte.

Das Ministerium hat erklärt, dass es meine Auffassung zum Kontrollrecht bei Notaren nicht teile. Es sehe im zugrunde liegenden Einzelfall keine Gefahr einer unzureichenden Datenschutzkontrolle und daher auch keinen Anlass zu entscheiden, ob §§ 26, 27 DSG MV oder § 18 BNotO Vorrang hätte. Denn im Rahmen der den Präsidenten der Landgerichte obliegenden Dienstaufsicht über die Notare werde auch die Einhaltung des Datenschutzes geprüft. Es habe daher keine Veranlassung, der Rechtsauffassung des Notars entgegenzutreten und ihm gegenüber tätig zu werden.

Ich musste daher dem Petenten mitteilen, dass ich sein Anliegen inhaltlich zunächst nicht weiter bearbeiten kann.

Gleichwohl habe ich mich in der Sache noch einmal an das Justizministerium gewandt und unter anderem wie folgt argumentiert:

- Begrenzungen der Kontrollbefugnis der Datenschutzbeauftragten kommen nur in den von der Verfassung vorgesehenen Bereichen, etwa bei der Rechtsprechung aufgrund der richterlichen Unabhängigkeit nach Artikel 97 Grundgesetz (GG), sowie in den gesetzlich geregelten Einzelfällen in Betracht, bei denen die Kontrolle durch die Datenschutzbeauftragten ausdrücklich ausgeschlossen ist. Keine der beiden Konstellationen ist bei den Notaren gegeben.

- Würde man Einschränkungen des Kontrollrechts bei Notaren akzeptieren, so wären sie auch für andere Berufs- oder besondere Amtsgeheimnisse hinzunehmen. Denn die notarielle Verschwiegenheitspflicht hat keine herausragende Stellung, die es rechtfertigen würde, ihr allein das Privileg der Nichtkontrollierbarkeit zuzuerkennen. Dies würde zu einer deutlichen Kontrolllücke und damit zu einer Einschränkung der Tätigkeit des Datenschutzbeauftragten führen, die mit der ihm durch Artikel 37 Verfassung des Landes Mecklenburg-Vorpommern und vom Bundesverfassungsgericht im so genannten Volkszählungsurteil zugedachten Stellung als Kontrollinstanz zur Wahrung des Rechts auf informationelle Selbstbestimmung der Bürger nicht vereinbar wäre. Die Dienstaufsicht bietet dafür keinen Ersatz. Ihr obliegt zwar neben anderen Aufgaben auch die Prüfung, ob die ihr unterliegende Stelle die datenschutzrechtlichen Bestimmungen einhält. Im Gegensatz zu den Datenschutzbeauftragten hat die Dienstaufsicht aber keinen verfassungsrechtlichen Auftrag für die Datenschutzkontrolle.

- Die Bürger vertrauen den Notaren sensible personenbezogene Daten an, weil sie sich darauf verlassen, dass die Notare die ihnen gemäß § 18 BNotO obliegende Verschwiegenheitspflicht einhalten. Diese zentrale Schutznorm wird entwertet und konterkariert, wenn die Datenschutzbeauftragten die Einhaltung des § 18 BNotO durch die Notare deswegen nicht prüfen dürfen, weil sich umgekehrt die Notare den Datenschutzbeauftragten gegenüber gerade auf diese Vorschrift berufen und somit eine Kontrolle zugunsten des von § 18 BNotO geschützten Personenkreises verhindern können.

  Als Besonderheit kommt im vorliegenden Fall hinzu, dass der Notar angab, für einen Kollegen Amtshilfe geleistet zu haben und diesen wegen § 18 BNotO nicht nennen dürfe. Die zugunsten der Bürger bestehende Verschwiegenheitspflicht soll in diesem Fall also offensichtlich sogar dazu herhalten, lediglich die Auskunft über eine andere öffentliche Stelle zu verweigern.

– Gemäß § 24 Abs. 2 Satz 1 BDSG erstreckt sich die Kontrolle des Bundesbeauftragten für den Datenschutz auch auf Daten, die einem Berufs- oder besonderen Amtsgeheimnis - beispielsweise der notariellen Verschwiegenheitspflicht - unterliegen. § 24 Abs. 6 BDSG überträgt ausdrücklich die im Bundesdatenschutzgesetz getroffenen Regelungen zur Kontrollbefugnis des Bundesbeauftragten für den Datenschutz auf die Landesbeauftragten. Aus diesen Vorschriften folgt dem eindeutigen Wortlaut nach das umfassende Kontrollrecht der Landesbeauftragten für den Datenschutz bei Notaren. Unser Justizministerium ist jedoch der Auffassung, § 24 Abs. 6 BDSG könne nicht angewendet werden, da es an einer konkreten Umsetzung im Landesrecht fehle.

  Dahingegen geht unser Innenministerium in einem anderen Fall - der Datenschutzkontrolle im Bereich der Sicherheitsüberprüfungen von Landesbediensteten (siehe dazu ausführlich Zweiter Tätigkeitsbericht, Punkt 2.5.1) - wie selbstverständlich von der unmittelbaren Geltung des § 24 Abs. 6 BDSG aus, obwohl dieses Gebiet aufgrund der vom Grundgesetz vorgegebenen Kompetenzverteilung durch Landesrecht geregelt ist. Zu Recht könnte man hier fragen, ob in einem solchen Fall eine Norm des Bundesdatenschutzgesetzes die Geltung von Bundesrecht anordnen kann.

  Wenn aber schon bei Landesrecht § 24 Abs. 6 BDSG direkt angewendet wird, dann muss diese Vorschrift erst recht gelten, falls es - wie bei der Bundesnotarordnung - um die Ausführung von Bundesrecht geht.

– Mecklenburg-Vorpommern ist das einzige Bundesland, in welchem der Datenschutzbeauftragte des Landes den Umgang mit personenbezogenen Daten bei Notaren nicht kontrollieren kann. Dahingegen haben Justizministerien verschiedener anderer Bundesländer es sogar abgelehnt, in die Dienstordnung für Notare einen Hinweis auf das uneingeschränkte Kontrollrecht der Datenschutzbeauftragten aufzunehmen, weil dieses Recht keiner besonderen Erwähnung in einer Dienstordnung bedürfe.

Aufgrund dieser Sachlage muss man davon ausgehen, dass auch der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern bei Notaren ein uneingeschränktes Kontrollrecht hat. Das Justizministerium weigert sich aber nach wie vor, dies anzuerkennen.

Wegen seiner grundsätzlichen Bedeutung für das Recht auf informationelle Selbstbestimmung hoffe ich, dass sich der zuständige Ausschuss unseres Landtages mit diesem Thema befasst und das Justizministerium auffordert, dafür zu sorgen, dass die Kontrollbefugnis des Datenschutzbeauftragten auch in diesem Bereich gewährleistet wird.

Die mir vorliegende Petition des Bürgers kann ich erst dann weiter bearbeiten, wenn mir ermöglicht wird, die dafür erforderlichen Informationen zu erhalten.

3.1.11 Staatsanwälte löschen nicht

Im August 1998 habe ich bei der Generalstaatsanwaltschaft (GStA) das Allgemeine Register- und Informationssystem für Gerichte und Staatsanwaltschaften - Bereich Staatsanwaltschaft (ARGUS-StA) kontrolliert. Dieses System befindet sich dort im Testbetrieb. Die GStA ist Leitstelle für den Einsatz dieses Verfahrens bei den Staatsanwaltschaften des Landes. Gemeinsam mit dem Justizministerium führt sie Tests durch und gibt Empfehlungen für Änderungen und Ergänzungen der Soft- und Hardware. Sie koordiniert die einheitliche Hard- und Softwareausstattung aller ARGUS-StA-Arbeitsplätze und unterstützt das Justizministerium bei der Ausarbeitung der erforderlichen Dienstanweisungen.

Die Prüfung des Systems hat Folgendes ergeben:

Nutzung von Echtdaten für Testzwecke

Während der Kontrolle wurde mir zunächst mitgeteilt, dass Echtdaten nur aus dem Geschäftsverteilungsplan der Generalstaatsanwaltschaft genutzt werden und im Übrigen Testdaten für die Erprobung des Systems vorgesehen sind. Im Nachhinein stellte sich jedoch heraus, dass auch Echtdaten gespeichert waren. Es handelte sich dabei um personenbezogene Daten von Verteidigern. Der Umgang mit personenbezogenen Daten selbst aus öffentlichen Quellen ist aber nur dann zulässig, wenn die Daten für die Aufgabenerfüllung tatsächlich erforderlich sind. Die Daten der Verteidiger wurden für den Test des Systems aber nicht gebraucht und waren daher zu löschen beziehungsweise zu anonymisieren.

Anmeldeverfahren

Die Anmeldeprozedur zur Nutzung von ARGUS-StA entsprach nur teilweise den datenschutzrechtlichen Anforderungen. Um ein Schutzniveau sicherzustellen, das der Sensibilität der Daten angemessen ist, müssen Passworte bestimmten Kriterien hinsichtlich Länge und Struktur genügen, damit sie nicht leicht erraten oder durch systematisches Ausprobieren ermittelt werden können. Deshalb ist es erforderlich, den Nutzern entsprechend einheitliche Vorgaben zu machen oder durch technische Maßnahmen die Passwortstruktur und -länge festzulegen. Das hier praktizierte dreistufige Passwortverfahren birgt die Gefahr in sich, dass Passworte vergessen oder notiert werden. Ich habe deshalb ein Single-Sign-On-Verfahren empfohlen, bei dem sich der Nutzer nur das erste Passwort merken muss, während das System die Verwaltung der anderen Passworte übernimmt.

Passworte sind auch nicht beim Systemadministrator zu hinterlegen, da sonst unnötigerweise zusätzliche Missbrauchsmöglichkeiten entstehen. Selbst bei ordnungsgemäßer Protokollierung von Nutzeraktivitäten wären Verarbeitungsvorgänge nicht mehr ihren Verursachern zuzuordnen, wie es in § 17 Abs. 2 Nr. 7 DSG MV (Eingabekontrolle) gefordert wird. Die Hinterlegung ist insbesondere dann entbehrlich, wenn der Systemadministrator Nutzerpassworte überschreiben kann.

Protokollierung

Die datenschutzgerechte automatisierte Verarbeitung personenbezogener Daten erfordert eine nachvollziehbare Protokollierung der Nutzeraktivitäten. Diese Forderung gewinnt insbesondere dann an Bedeutung, wenn keine weitgehende Differenzierung der Nutzerrechte möglich ist, weil dann ausschließlich durch Kontrolle der Protokolle die Ordnungsmäßigkeit der Datenverarbeitung geprüft werden kann. Den Anforderungen an die Eingabekontrolle wurde hier nur unzureichend Rechnung getragen. Die Protokollierung im System erfolgt lediglich für den Softwarehersteller, damit dieser auftretende Fehler leichter finden und beseitigen kann. Die Staatsanwaltschaften selbst werten die Protokolle nicht aus. Entsprechende Auswertewerkzeuge sind nicht vorhanden. Somit ist nicht nachvollziehbar, wer wann welche Daten eingegeben oder verändert hat. Gleiches gilt für die Dokumentation der Administrationstätigkeiten. Auch hier ist es erforderlich, dass nachträglich festgestellt werden kann, wem wann welche Rechte zugeteilt oder entzogen wurden. Es ist festzulegen, wann, in welchem Umfang und durch wen Protokolle kontrolliert und wie lange sie aufbewahrt werden. Eine effektive Protokollauswertung erfordert geeignete automatisierte Hilfsmittel.

Löschung und Sperrung von Daten

Für personenbezogene Daten, die in einem automatisierten Verfahren verarbeitet werden, ist es unabdingbar, Lösch- und Sperrmöglichkeiten vorzusehen. Personenbezogene Daten in staatsanwaltschaftlichen Dateien sind gemäß § 20 Abs. 2 BDSG zu löschen, wenn die Daten unzulässig gespeichert wurden oder zur Aufgabenerfüllung nicht mehr erforderlich sind. Die Fristen richten sich nach den Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden (AufbewBest.). In dieser Verwaltungsvorschrift ist für eingestellte Ermittlungsverfahren beispielsweise eine Frist von fünf Jahren festgelegt. Sie beginnt mit dem auf das Jahr der Weglegung folgenden Jahr. Als Jahr der Weglegung gilt das Jahr, in dem die letzte Verfügung zur Sache ergangen ist. Bei einer automationsunterstützten Schriftgutverwaltung kann die Frist auch von einem früheren Zeitpunkt, zum Beispiel dem Datum der Weglegungsverfügung, berechnet werden.

Sind die Aufbewahrungsfristen abgelaufen und stehen die betreffenden Akten zur Vernichtung an, so müssen auch die zugehörigen Daten in ARGUS-StA gelöscht werden. In der Dateibeschreibung zum Anwendungssystem ARGUS-StA, die mir im Rahmen einer Prüfung im April 1994 vorgelegt wurde, heißt es hierzu: „Die entsprechende Transaktion des ARGUS-Anwendungssystems ist noch in Vorbereitung, weil das System erst im November 1992 eingeführt worden ist und die kürzeste Aufbewahrungsfrist 5 Jahre beträgt.“ Bis heute ist es nicht möglich, Daten, deren Speicherfristen abgelaufen sind, in ARGUS-StA zu löschen.

Die Speicherung personenbezogener Daten über die festgelegten Fristen hinaus verstößt gegen § 20 Abs. 2 Nr. 2 BDSG i. V. m. AufbewBest. und ist in jedem festgestellten Einzelfall zu beanstanden.

Zurzeit wird an entsprechenden Softwareänderungen nicht gearbeitet, weil zunächst auf die Verabschiedung des Strafverfahrensänderungsgesetzes (StVÄG) gewartet werden soll, von dem man sich detaillierte Vorgaben erhofft. Auch das Sperren von unrichtigen oder nicht mehr erforderlichen Daten wird nicht unterstützt. Teillöschungen sind ebenfalls nicht möglich, und es fehlen Archivierungskomponenten. Hier besteht dringender Handlungsbedarf. Die Lösch- und Sperrmöglichkeiten sind unverzüglich zu realisieren. Zumal andere Länder bereits unabhängig vom StVÄG über entsprechende Löschungsmöglichkeiten verfügen. Die zur Vernichtung anstehenden Akten sind auszusondern.

Weitere Softwareprodukte

Die GStA hat im Vorfeld des Kontroll- und Informationsbesuches mitgeteilt, dass sie in der Dienststelle keine automatisierten Dateien im Sinne von § 16 Abs. 1 DSG MV führt. Nachfragen während der Kontrolle ergaben jedoch, dass unter anderem mit Standardsoftwareprodukten wie Textverarbeitungsprogrammen personenbezogene Daten automatisiert verarbeitet werden. Darüber hinaus wird beispielsweise die Personaldatenverarbeitung teilweise automatisiert vorgenommen. Ebenso fällt das Betreiben der Telekommunikationsanlage in den Geltungsbereich des Landesdatenschutzgesetzes. Dateibeschreibungen nach § 16 Abs. 1 DSG MV lagen für diese Anwendungen nicht vor. Des Weiteren wurde jedem einzelnen Mitarbeiter überlassen, welche Daten er wo (lokaler PC oder Server) und für welchen Zeitraum speichert. Maßgebliches Löschkriterium ist zurzeit lediglich die Speicherkapazität der verwendeten Festplatten. Dies entspricht jedoch nicht den datenschutzrechtlichen Anforderungen.

Insbesondere Standardsoftware lässt sich in vielfältiger Weise zur Verarbeitung personenbezogener Daten nutzen. Um den zulässigen Umfang und die Art und Weise der Verarbeitung verbindlich und für alle Nutzer einheitlich festzulegen, bedarf es deshalb organisatorischer Hilfsmittel. Eine für diesen Zweck geeignete Dienstanweisung als Mittel zur Organisationskontrolle hätte vorliegen müssen. Von datenschutzgerechtem Umgang mit Standardsoftware kann nicht gesprochen werden, wenn es jedem Nutzer selbst überlassen ist, wo er welche Dateien wie lange speichert und wie er schützenswerte Daten sichert. Der Umgang mit Standardsoftware ist per Dienstanweisung für alle Nutzer einheitlich zu regeln. Insbesondere sollte festgelegt werden, welche Daten auf welchem Speichermedium (dezentral/zentral) und wie lange zu speichern sind.

Ich habe darauf hingewiesen, dass für Dateien mit personenbezogenen Daten, die von Standardsoftwareprodukten erzeugt und länger als drei Monate gespeichert werden, Dateibeschreibungen anzufertigen sind. Für mehrere inhaltlich gleichartige Dateien, wie Textdateien mit Schriftwechsel oder mit Listen, können diese Beschreibungen gemeinsam als Verfahrensbeschreibungen ausgestaltet sein, um den Aufwand in einem angemessenen Rahmen zu halten.

Dienstanweisungen/Handbücher zum Verfahren ARGUS-StA

Um Anwender auch mit dem ordnungsgemäßen Gebrauch von individuellen Softwareprodukten vertraut zu machen, sind organisatorische Vorkehrungen wie Dienstanweisungen, Anwenderrichtlinien und Benutzerhandbücher erforderlich (§ 17 Abs. 2 Nr. 10 DSG MV - Organisationskontrolle). Die gültige Dienstanweisung 1/94 für den Einsatz von ARGUS-StA entsprach nicht mehr dem Entwicklungsstand der Software. Ein Benutzerhandbuch zum Verfahren stand den Anwendern nicht zur Verfügung. Zwar wird die Dienstanweisung überarbeitet, angesichts der häufigen Softwareänderungen reicht es jedoch nicht aus, diese nur im Abstand von vier Jahren anzupassen.

Zugriffs- und Organisationskontrolle

Organisationskontrolle schließt umfassende Dokumentationspflichten ein. Zugriffsrechte müssen beispielsweise die Aufgabenverteilung entsprechend dem Geschäftsverteilungsplan widerspiegeln. Personenbezogene Kennungen und Passworte dürfen nur den zuständigen Mitarbeitern bekannt sein. Für Vertretungsfälle sollten speziell dafür eingerichtete Kennungen genutzt werden. Es muss nachvollziehbar sein, wer wann auf welche Daten zugegriffen hat. Um jederzeit feststellen zu können, ob die geltenden Zugriffsrechte den fachlichen Vorgaben entsprechen, muss der Sollzustand schriftlich dokumentiert sein.

Während der Kontrolle habe ich jedoch festgestellt, dass nicht ohne weiteres bestimmt werden kann, welche Rechte Nutzer X zum Zeitpunkt Y hat oder hatte.

Aufgrund der festgestellten Mängel habe ich dem Justizminister unseres Landes eine Beanstandung ausgesprochen.

Der Justizminister hat in seiner ersten Stellungnahme ausgeführt, dass die als unerlässlich zu betrachtenden Optimierungen der Anwendung bereits in der Vergangenheit Gegenstand gemeinsamer Erörterungen waren und meine datenschutzrechtlichen Hinweise dabei eingeflossen sind. So ist unter anderem eine Arbeitsgruppe der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz damit befasst, sich mit datenschutzrechtlichen Anforderungen bei automatisierten staatsanwaltschaftlichen Informationssystemen auseinanderzusetzen. Der für den Herbst 1999 angekündigte Abschlussbericht, in dem Anpassungen oder Neuentwicklungen empfohlen werden sollen, liegt mir noch nicht vor. Auf der Grundlage dieses Berichtes ist eine erneute Beteiligung meiner Dienststelle vorgesehen, um im Ergebnis detaillierte Aufträge zur Änderung der ARGUS-StA-Anwendung zu vergeben. Das Justizministerium hat bereits signalisiert, dass es viele meiner Empfehlungen aufgreifen wird und es als seine vordringliche Aufgabe ansieht, eine ausreichende Protokollierung sicherzustellen sowie die Löschungs- und Sperrmöglichkeiten zu schaffen.

Grundsätzlich ist zu begrüßen, dass die aus datenschutzrechtlicher Sicht erforderlichen Änderungen so schnell wie möglich vorgenommen werden sollen. Jedoch lag mir der Abschlussbericht der Arbeitsgruppe bis Redaktionsschluss nicht vor. Bereits im April des Jahres 1999 hatte ich darauf hingewiesen, dass bis zur Funktionsfähigkeit des Löschmoduls sicherzustellen ist, dass diejenigen personenbezogenen Daten nicht mehr verarbeitet und genutzt werden dürfen, die wegen Fristablaufs zu löschen gewesen wären. Unabhängig von der noch fehlenden Löschungsmöglichkeit im automatisierten Verfahren ARGUS-StA sind die aufgrund des Fristablaufs zur Vernichtung anstehenden Akten bereits jetzt auszusondern.

3.1.12 Mitteilungen über Wahlrechtsausschlüsse nicht korrekt

Bei einer Meldebehörde unseres Landes habe ich mich über die Praxis der Speicherung von Wahlrechtsausschlüssen informiert.

Anfang 1998 waren im Melderegister noch Wahlrechtsausschlüsse gespeichert, die teilweise aus dem Jahre 1990 stammten. Der Aktenrückhalt war unvollständig und nicht aktuell. Im Vorfeld der Wahlen vom Herbst 1998 hatte die Meldebehörde daher in allen Fällen bei den zuständigen Staatsanwaltschaften und Gerichten angefragt, ob die Voraussetzungen für eine weitere Speicherung des Wahlrechtsausschlusses vorliegen. Die Antworten und auch die neueren Mitteilungen über Ausschlüsse enthielten eine Vielzahl personenbezogener Daten, die über das für die Aufgabenerfüllung der Meldebehörde erforderliche Maß hinausgingen. In den Akten befanden sich vollständige Urteile, Auszüge von Urteilen und Durchschriften von Auszügen aus dem Bundeszentralregister, die nur teilweise anonymisiert waren. Die Urteile enthielten zum Teil sensible Daten über den Verurteilten, aber auch über Zeugen und Opfer. Nur wenige Mitteilungen enthielten ausschließlich die Daten, die für die Meldebehörde relevant waren.

Zur Vorbereitung und Durchführung von allgemeinen Wahlen und Abstimmungen darf das Merkmal „Wahlrechtsausschluss“ im Melderegister gespeichert werden. Die Mitteilung kommt von der Staatsanwaltschaft beziehungsweise vom Gericht (§ 13 Abs. 1 Nr. 5 Einführungsgesetz zum Gerichtsverfassungsgesetz [EGGVG], Nr. 12 Mitteilungen in Strafsachen [MiStra]). Aus datenschutzrechtlicher Sicht erscheinen zwei Punkte dringend verbesserungsbedürftig. Zum einen sind die Mitteilungen über den Wahlrechtsausschluss entsprechend Nr. 12 MiStra auf den erforderlichen Datenumfang zu beschränken. Die Übermittlung weiterer Daten ist durch keine Rechtsgrundlage gedeckt und daher unzulässig. Zum anderen ist sicherzustellen, dass künftig Wahlrechtsausschlüsse nur noch so lange im Melderegister gespeichert werden, wie die Voraussetzungen dafür vorliegen. Letzteres setzt jedoch eine Information der Meldebehörden über den maßgeblichen Endzeitpunkt des Verlustes der Wählbarkeit beziehungsweise der Aberkennung der Wählbarkeit und des Stimmrechtes voraus. Der Verlust der Rechte des Betroffenen wird zwar mit Rechtskraft des Urteils wirksam. Davon zu unterscheiden ist jedoch der für die Berechnung der Dauer des Verlustes maßgebliche Zeitpunkt. Dabei ist auf den Tag abzustellen, an dem die Freiheitsstrafe verbüßt, verjährt, erlassen oder eine angeordnete freiheitsentziehende Maßregel beendet worden ist. Diese Informationen liegen zum Zeitpunkt der Erstmitteilung noch nicht vor.

Bei dem Besuch in der Meldebehörde konnte ich feststellen, dass in Einzelfällen bereits ein Verfahren mit Folgemitteilungen praktiziert wird. So enthielt beispielsweise die Erstmitteilung einer Staatsanwaltschaft den Hinweis, dass über den maßgeblichen Zeitpunkt, von dem an die Dauer des Verlustes zu berechnen ist, zu gegebener Zeit informiert wird. Diese Verfahrensweise sichert, dass die Meldebehörden rechtzeitig über die Speichervoraussetzungen benachrichtigt werden und aufwendige Nachfragen in den Einzelfällen erspart bleiben.

Das Justizministerium unseres Landes hat auf meine Anregung hin die Gerichte und Staatsanwaltschaften auf den nach § 13 Abs. 1 Nr. 5 EGGVG in Verbindung mit Nr. 12 MiStra erforderlichen Datenumfang hingewiesen. Allerdings lehnt es Folgemitteilungen ab, weil diese nicht von Nr. 12 MiStra erfasst seien und die Meldebehörden beim Bundeszentralregister Führungszeugnisse beantragen und so die notwendigen Informationen erhalten könnten. Darüber hinaus seien Folgemitteilungen für die Justiz mit einem unverhältnismäßig hohen Verwaltungsaufwand verbunden.

Ich habe darauf hingewiesen, dass die Meldebehörden unseres Landes bereits jetzt ergänzende Informationen bei Staatsanwaltschaften und Gerichten einholen und somit die Folgemitteilungen insgesamt zu keinem wesentlich höheren Aufwand führen würden. In Einzelfällen versenden Staatsanwaltschaften mittlerweile auch schon Folgemitteilungen von sich aus.

Unabhängig von diesen rein praktischen Erwägungen habe ich auch rechtliche Bedenken, wenn Meldebehörden für diese Zwecke regelmäßig Führungszeugnisse gemäß §§ 31, 32 Bundeszentralregistergesetz (BZRG) anfordern. Die Führungszeugnisse enthalten bedeutend mehr Daten, als die Meldebehörden für die Prüfung der Dauer des Wahlrechtsausschlusses benötigen. Regelmäßige Anfragen beim Bundeszentralregister führen letztendlich dazu, dass die aus datenschutzrechtlichen Gründen vorgesehenen Einschränkungen bei Mitteilungen nach Nr. 12 MiStra konterkariert werden.

Auch für den Sonderfall der Prüfung von Wahlrechtsausschlüssen bei den Wahlen in den neuen Bundesländern im Jahre 1994 hatte der Gesetzgeber Regelungen geschaffen, wonach die Meldebehörden aus datenschutzrechtlichen Erwägungen lediglich die Daten erhielten, die sie benötigten, um einen Wahlrechtsausschluss festzustellen (§§ 69, 70 BZRG).

§ 13 Abs. 1 Nr. 5 EGGVG sieht vor, dass Gerichte und Staatsanwaltschaften Daten übermitteln dürfen, wenn der Empfänger die Daten zur Aufgabenerfüllung benötigt, weil aufgrund der Entscheidung bestimmte Rechtsfolgen, unter anderem der Verlust des Wahlrechtes oder der Wählbarkeit, eingetreten sind. Die Meldebehörde darf jedoch Wahlrechtsausschlüsse nur so lange speichern, wie die Voraussetzungen hierfür vorliegen. Dafür ist ebenfalls der maßgebliche Zeitpunkt zu übermitteln, von dem an die Dauer des Verlustes berechnet wird. Darüber hinaus sieht auch § 20 EGGVG eine Unterrichtungspflicht vor, die notwendigerweise Folgemitteilungen erfordert.

Die Erstmitteilung erfolgt vor Beendigung des Strafverfahrens, und zu diesem Zeitpunkt steht die Dauer der Nebenfolge noch nicht fest. Zu den Verfahren im Sinne von § 20 Abs. 1 EGGVG zählt auch das Strafvollstreckungsverfahren, welches das aus Ermittlungs-, Zwischen-, Haupt- und Vollstreckungsverfahren bestehende Strafverfahren abschließt. Aus diesem Grund ist eine Folgemitteilung über den tatsächlichen Ausgang des Verfahrens, nämlich über den Zeitpunkt, zu dem die Vollstreckung der Freiheitsstrafe beendet ist, erforderlich und auch zulässig.

Ich habe das Justizministerium nochmals darauf hingewiesen, dass ich aus diesen Gründen eine entsprechende Verfahrensweise für geboten halte, und empfohlen, Folgemitteilungen landesweit verbindlich einzuführen. Die Antwort des Ministeriums steht noch aus.

3.1.13 Datenschutz bei laufenden Ermittlungsverfahren?

Im Rahmen einer Petition - der Petent vermutete, sein Telefon werde abgehört - vertrat das Justizministerium die Auffassung, dass meine Kontrollkompetenz zwar hinsichtlich abgeschlossener Ermittlungsverfahren gegeben sei. Dementsprechend wurde mir auch Einsicht in die betreffende Akte gewährt. Hinsichtlich aktueller Telefonüberwachungsmaßnahmen im laufenden Ermittlungsverfahren bestünde meine Kontrollkompetenz nach den einschlägigen Vorschriften des DSG MV jedoch nicht.

Diese Auffassung entspricht nicht dem geltenden Recht. Nach § 26 DSG MV kontrolliert der Landesbeauftragte für den Datenschutz die Einhaltung der datenschutzrechtlichen Bestimmungen bei allen öffentlichen Stellen des Landes. § 2 Abs. 3 DSG MV sieht lediglich Einschränkungen bei den Gerichten des Landes vor, wenn diese keine Verwaltungsaufgaben wahrnehmen. Dagegen unterliegt die Staatsanwaltschaft gemäß § 2 Abs. 3 Satz 3 DSG MV ausdrücklich der Kontrolle des Landesdatenschutzbeauftragten. Eine Vorschrift, die dem entgegensteht, existiert nicht. Dies betrifft grundsätzlich auch laufende Ermittlungsverfahren, in denen Telefonanschlüsse überwacht werden. Dabei ist allerdings strikt zwischen dem Kontrollrecht des Datenschutzbeauftragten und Mitteilungen an den Petenten zu differenzieren. Zweifelsohne wird dem Petenten in Fällen laufender Telefonüberwachungsmaßnahmen zu Recht keine Auskunft gegeben. Unabhängig davon muss jedoch der Landesbeauftragte für den Datenschutz auch bei laufenden Verfahren prüfen können, ob die Verfahrensvorschriften nach §§ 100 a, b Strafprozessordnung (StPO), die grundrechtssichernden Charakter für das Recht auf informationelle Selbstbestimmung haben, eingehalten wurden.

Das Justizministerium hat sich inhaltlich zur Sache noch nicht geäußert. Es stellte jedoch für später eine Antwort in Aussicht und verwies in diesem Zusammenhang auf die anstehende Novellierung des Landesdatenschutzgesetzes. Eine etwas eigenartige Auffassung. Normalerweise kommt bei der Bewertung von Sachverhalten das geltende Recht zur Anwendung.

Im Interesse der Betroffenen werde ich auch weiterhin im Bereich der laufenden Ermittlungsverfahren kontrollieren, wenn es erforderlich sein sollte. Dies habe ich dem Justizministerium so mitgeteilt.

3.2 Polizei

3.2.1 INPOL-Neu

Bereits in den ersten beiden Tätigkeitsberichten hatte ich mich zu INPOL-neu geäußert (siehe Erster Tätigkeitsbericht, Punkt 2.4.2; Zweiter Tätigkeitsbericht, Punkt 2.3.2). Der Echtbetrieb soll nach aktuellem Zeitplan schrittweise im Jahr 2000 aufgenommen werden. Ab Mai 2000 sollen zunächst Fahndungsabfragen aller Verbundteilnehmer aus dem System möglich sein.

Neu gegenüber dem Speicherkonzept des alten INPOL-Systems ist das Prinzip der Einmalerfassung. Alle personenbezogenen Daten werden nur noch einmal in einem „integrierten Datenpool“ gespeichert. Ein komplexes Berechtigungssystem soll den Teilnehmern (Länderpolizei, BKA, BGS und Zoll) und individuellen Nutzern unterschiedlich eingeschränkte Bereiche dieses Datenpools zur Verfügung stellen.

Aus datenschutzrechtlicher Sicht sind folgende Aspekte zu kritisieren:

Kriminalaktennachweis

Einen erweiterten Informationsumfang in INPOL-neu sieht die so genannte Fallkurzauskunft vor, die auch die Abfrage im Kriminalaktennachweis (KAN) umfasst. Nach § 8 Abs. 1 des neugefassten Bundeskriminalamtsgesetzes (BKAG) können innerhalb des KAN in Zukunft auch Informationen zu Tatverlauf, Tatzeit und -ort von Beschuldigten bundesweit gespeichert werden, soweit es sich um Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung handelt. Der neue KAN wird damit weit über die ursprüngliche Funktion des Aktennachweissystems hinausgehen. Die Projektgruppe INPOL-neu des BKA ist zusätzlich bestrebt, den gesamten kriminellen Werdegang einer „INPOL-relevanten Person“ im Rahmen des KAN abzubilden. Eine solche Erweiterung des KAN auf nicht INPOL-relevante Staftaten einer Person wäre nach dem geltenden Recht nicht zulässig. Die bundesweite Verfügbarkeit personenbezogener Fallinformationen hat der Gesetzgeber nur bei Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung zugelassen. Gesetzlicher Ausgangspunkt ist somit die einzelne begangene Straftat und nicht etwa die Person. Hinzu kommt, dass die Kriterien der Überregionalität und Erheblichkeit von Delikten bereits in der bisherigen Praxis sehr weit ausgelegt wurden.

Anzuwendendes Recht: Landespolizeirecht oder BKA-Gesetz?

Die INPOL-Verbunddateien sind gemeinsame Dateien des Bundes und der Länder. In verschiedenen Unterlagen zum INPOL-Projekt wird jedoch die alleinige Geltung des BKAG vorausgesetzt; Landespolizeigesetze finden dort keine Erwähnung. Da es sich aber vorwiegend um Daten der Länder handelt, die in den Dateien gespeichert werden, muss nach meiner Auffassung hinsichtlich der Speicher-, Prüf- und Löschungsfristen das jeweilige Landespolizeirecht gelten. Dies wird relevant bei den künftigen Errichtungsanordnungen für die INPOL-neu-Dateien, insbesondere dort, wo das jeweilige Landespolizeirecht kürzere Fristen vorsieht.

Auf diese wichtigen Aspekte des INPOL-neu-Projektes habe ich das Innenministerium unseres Landes hingewiesen. Die Landespolizei hat sich mit anderen Bundesländern zur Arbeitsgruppe INPOL-Land (AGIL) zusammengeschlossen, um die technischen Voraussetzungen der Umsetzung von INPOL-neu auf Landesebene vorzubereiten. Die Datenschutzbeauftragten begleiten das Projekt. Es bleibt abzuwarten, ob die datenschutzrechtlichen Anforderungen in ausreichendem Maße umgesetzt werden.

3.2.2 Verfassungsgericht stoppt Schleierfahndung

Es war von Anfang an nicht ganz unumstritten, im Rahmen der Novellierung des Gesetzes über die öffentliche Sicherheit und Ordnung (SOG M-V) im Februar 1999 auch die Schleierfahndung einzuführen. Die Regelung sah vor, dass die Polizei ohne irgendeinen Anlass bei Bürgern, die sich im Grenzgebiet bis zu einer Tiefe von 30 Kilometern sowie auf Durchgangsstraßen, in öffentlichen Einrichtungen des internationalen Verkehrs und im Küstenmeer aufhalten, sehr weitgehende Kontrollen vornehmen darf.

Der Innen- und der Rechtsausschuss unseres Landtages führten während des Gesetzgebungsverfahrens gemeinsam eine Expertenanhörung durch. Zu den Sachverständigen zählten unter anderem ein ehemaliger Polizeipräsident, der sich auf dem Gebiet des polizeilichen Datenschutzrechts bereits einen Namen gemacht hatte, mehrere im Themenbereich versierte Professoren, ein wissenschaftlicher Mitarbeiter des Bundesverfassungsgerichts und der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern. Alle Genannten hatten verfassungsrechtliche Bedenken gegen diese Regelung geäußert und sich gegen eine Einführung von verdachts- und ereignisunabhängigen Kontrollen ausgesprochen. Im Einzelnen wurde dabei vor allem Folgendes kritisiert:

- Die im Gesetzentwurf geplante sehr weitgehende Regelung setzt die im Rechtsstaatsprinzip verankerte Schwelle der konkreten Gefahr als Voraussetzung für polizeiliches Handeln erheblich herab; sie gibt zudem die bewährte polizeirechtliche Unterscheidung zwischen Störer und Nichtstörer völlig auf. Es ist ein allgemeiner Grundsatz des Polizeirechts, dass gegen den Nichtstörer nur ausnahmsweise bei Vorliegen der Voraussetzungen des polizeilichen Notstandes Maßnahmen ergriffen werden dürfen.

- Durch diese Maßnahme würde eine Vielzahl von unbescholtenen Bürgern in das Visier polizeilicher Maßnahmen geraten. Für Bürger, die sich im Grenzgebiet bis zu einer Tiefe von 30 Kilometern sowie auf Durchgangsstraßen (Bundesautobahnen, Europastraßen und anderen Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr), in öffentlichen Einrichtungen des internationalen Verkehrs und im Küstenmeer aufhalten, wäre nicht mehr vorhersehbar, wann sie sich einer Identitätsfeststellung durch die Polizei unterziehen müssten.

- Bereits nach geltendem Recht dürfen Personen mit Hilfe elektronischer Systeme, zum Beispiel durch Fahndungsabfrage in INPOL, überprüft werden. Anlassfreie Kontrollen würden dazu führen, dass eine unüberschaubare Anzahl von Personen nicht nachvollziehen könnte, welche ihrer Daten erhoben, gespeichert und genutzt werden.

Trotz der massiven verfassungsrechtlichen und datenschutzrechtlichen Kritik wurde die Schleierfahndung entsprechend dem ursprünglichen Entwurf vom Parlament verabschiedet und damit geltendes Recht.

Daraufhin legten einige Bürger unseres Landes beim Landesverfassungsgericht Mecklenburg-Vorpommern Verfassungsbeschwerde gegen die Schleierfahnung ein und und bekamen weitgehend Recht. Das Gericht hat in seinem am 21. Oktober 1999 verkündeten Urteil festgestellt, dass das in unserer Landesverfassung garantierte Grundrecht auf informationelle Selbstbestimmung verletzt worden ist, und hat die polizeiliche Befugnis für verdachts- und ereignisunabhängige Kontrollen erheblich eingeschränkt:

- Auf Durchgangsstraßen außerhalb des 30 Kilometer tiefen Grenzgebietes sind ereignis- und verdachtslose Identitätsfeststellungen von jedermann nicht mehr ohne weiteres zulässig. Vielmehr ist verfassungsrechtlich ein hinreichender Grund dafür erforderlich, dass der Einzelne zur vorbeugenden Bekämpfung grenzüberschreitender Kriminalität kontrolliert wird. Dabei muss der Gesetzgeber einen spezifisch auf die organisierte Kriminalität zugeschnittenen Straftatenkatalog aufstellen.

- Im Grenzgebiet bis zu einer Tiefe von 30 Kilometern, in Einrichtungen des internationalen Verkehrs und im Küstenmeer darf die Polizei künftig Personen lediglich anhalten und nach den Ausweispapieren fragen. Weitergehenden Zwangsmaßnahmen, wie das Verbringen zur Dienststelle, die Durchsuchung einer Person und ihrer Sachen sowie die Verarbeitung und Nutzung der dabei anfallenden personenbezogenen Daten, hat das Gericht eine deutliche Absage erteilt.

- Soll künftig auch auf Durchgangsstraßen kontrolliert werden, muss der Gesetzgeber Eingriffsschwellen festlegen, etwa indem er darauf abstellt, dass nach Lageerkenntnissen und polizeilicher Erfahrung sich auf einer Durchgangsstraße grenzüberschreitende organisierte Kriminalität abzeichnet.

- Für die Verarbeitung und Nutzung der bei einer Identitätsfeststellung zur Unterbindung des unerlaubten Aufenthalts oder zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität gewonnenen personenbezogenen Daten müssen bereichsspezifische gesetzliche Regelungen geschaffen werden.

An diese vorgegebenen Rahmenbedingungen wird sich der Landesgesetzgeber halten müssen, sofern er beabsichtigt, ein neues Gesetz zu verabschieden. Zur weiteren datenschutzrechtlichen Beratung im Gesetzgebungsverfahren bin ich gern bereit.

3.2.3 Polizeiliche Zusammenarbeit mit der Russischen Föderation

Das Bundesministerium des Innern (BMI) plante im Sommer 1999, das Deutsch-Russische Regierungsabkommen über die Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung kurzfristig in Kraft zu setzen.

Das Abkommen sieht einen umfangreichen polizeilichen Datenaustausch zwischen der Bundesrepublik Deutschland und der Russischen Föderation vor. Eine Voraussetzung für Datenübermittlungen an Stellen außerhalb des Geltungsbereichs des Grundgesetzes ist allerdings ein angemessener Datenschutzstandard im Empfängerland. Davon ist insbesondere bei solchen Staaten auszugehen, die die Europarat-Konvention Nr. 108 zum Schutz personenbezogener Daten ratifiziert haben. Da die Russische Föderation nicht zu diesen Staaten gehört und weitere Prüfungen bisher nicht erfolgt sind, ist ihr Datenschutzstandard zu hinterfragen.

Vorwiegend ist zu befürchten, dass nach der Übermittlung von Daten an die Russische Föderation die strengen Zweckbindungsregelungen, die das BKAG (§ 14 Abs. 7) und das SOG M-V (§ 41 Abs. 2 und 3) vorsehen, dort durchbrochen würden. Weitere Unsicherheiten resultieren aus der Tatsache, dass im Abkommen nicht geklärt ist, wer auf russischer Seite für die Einhaltung datenschutzrechtlicher Vorschriften sorgen soll.

Aus diesen Gründen habe ich unserem Innenministerium empfohlen, dem Abkommen in der vorliegenden Fassung nicht zuzustimmen. Das Innenministerium ist meiner Empfehlung jedoch nicht gefolgt. Gleichwohl ist das Abkommen bisher nicht in Kraft gesetzt worden, da Innenministerien anderer Länder datenschutzrechtliche Bedenken geäußert haben.

3.2.4 Täter-Lichtbild-System

Die Landespolizei plant die Einführung eines elektronischen Täterlichtbildsystems (TLBS). Mit dem TLBS sollen im erkennungsdienstlichen Bereich unter anderem Lichtbildaufnahmen gefertigt, die Lichtbildsammlung geführt und verschiedene Funktionen, wie Lichtbildvorzeigedatei, Wahllichtbildvorlage, Täterübersicht und Zeugeneinsichtnahme, unterstützt werden. Nachdem bei der ersten Ausschreibung keiner der Teilnehmer die Anforderungen erfüllen konnte, bedurfte es einer Änderung der Ausschreibungsunterlagen. Neu ist nun, dass das TLBS nicht mehr unmittelbar an die Polizeiliche Erkenntnisdatei Mecklenburg-Vorpommern (PED M-V) gekoppelt ist, sondern eine separate Datenbank eingerichtet wird, in die Teile aus der PED M-V übernommen werden sollen. Die Daten werden zentral auf einem Server des Landeskriminalamtes Mecklenburg-Vorpommern (LKA M-V) vorgehalten. Darüber hinaus soll der vollständige Datenbestand des TLBS tagaktuell auf separaten Servern in den Polizeidirektionen und in einem Kriminalkommissariat geführt werden, so dass die Abfragen nicht über das Landesnetz laufen. Nur innerhalb dieser Einheiten können Abrufe aus dem TLBS erfolgen. Möglicherweise sollen auch die anderen Kriminalkommissariate Daten erfassen und auf elektronischem Wege an das LKA M-V zum Einstellen der Daten in das TLBS übermitteln.

In ersten Empfehlungen zur Realisierung des Vorhabens bin ich im Wesentlichen auf folgende Bereiche eingegangen:

- rückwirkende Datenerfassung,
- Inhalte einzelner Datenfelder,
- Vernichtung von Ausdrucken,
- Vergabe differenzierter Zugriffsrechte sowie
- lückenlose Protokollierung der unterschiedlichen Zugriffe im Verfahren.

Für die Maßnahmen der erkennungsdienstlichen Behandlung durch die Polizei, hier das Anfertigen der Lichtbilder, sind die jeweiligen Rechtsgrundlagen konkret zu benennen und der Zweck sowie die Speicherfristen präzise zu beschreiben.

Klärungsbedarf besteht noch hinsichtlich der Aufnahme zusätzlicher Felder für die künftige Aufgabenerfüllung der Polizei. Soweit dies im Verfahren bereits berücksichtigt wird, könnten nach Auffassung des Innenministeriums Softwareanpassungskosten gespart werden. Dazu habe ich empfohlen, das zu entwickelnde Verfahren grundsätzlich am aktuellen Stand der Gesetze zu orientieren und keine unbestimmten Datenfelder auf Vorrat für eventuell künftig zu erfüllende Aufgaben einzurichten.

Ich werde die Umsetzung des Verfahrens weiter begleiten.

3.2.5 Erkennungsdienstliche Behandlung eines Zeugen - volles Programm

Erkennungsdienstliche Behandlung eines Zeugen

Ein Bürger hatte von der Polizei in einer Strafsache eine Vorladung als Zeuge erhalten. Zu Beginn der Vernehmung erläuterte der Polizist ihm den Sachverhalt und belehrte ihn über seine Rechte und Pflichten als Zeuge. Darüber hinaus erklärte ihm der Polizeibeamte, dass es für das Verfahren notwendig sei, Lichtbilder von ihm anzufertigen. Obwohl der Bürger nur als Zeuge geladen war, wurde ein Lichtbild von ihm in die Wahllichtbildkarte aufgenommen, die dem Geschädigten vorgelegt werden sollte. Ich habe den Sachverhalt aus datenschutzrechtlicher Sicht geprüft.

Die Polizei teilte mir mit, dass sie aufgrund der Verfügung der Staatsanwaltschaft so gehandelt habe und der Zeuge sich mündlich mit der Durchführung dieser Maßnahme einverstanden erklärt hatte. Die Kriterien der Einwilligung nach § 7 DSG MV wurden ihm erläutert. Darüber hinaus seien in diesem Fall für das Anfertigen der Lichtbilder für die Wahllichtbildkarte nicht die Vorschriften der Strafprozessordnung, sondern die materiellen Rechtsvorschriften des Nutzungs- und Urheberrechts maßgeblich. Der Betroffene ist Zeuge im Strafverfahren. Damit könne er auch das Nutzungs- und Urheberrecht zum Anfertigen und Verwenden seines Lichtbildes auf die Polizei übertragen.

Diese rechtlichen Ausführungen sind erstaunlich. Zwar kann jeder Bürger selbstverständlich auf seinen Wunsch hin Dritten Lichtbilder überlassen und auch entsprechende Rechte an diesen Unterlagen einräumen. Jedoch hätte ich eine solche Argumentation nicht im Zusammenhang mit der Tätigkeit der Polizei in einem Ermittlungsverfahren erwartet.

Ich habe daraufhin Einsicht in die Ermittlungsakte genommen sowie Rücksprache mit der Staatsanwaltschaft gehalten und im Ergebnis Folgendes festgestellt:

Die Staatsanwaltschaft hatte keine erkennungsdienstliche Behandlung des Zeugen angeordnet. Nach ihrer Verfügung sollten zwei Zeugen geladen werden, die, falls ihr Äußeres der vorliegenden Personenbeschreibung in etwa entspräche, erkennungsdienstlich behandelt und als Beschuldigte vernommen werden sollten. Eine Ähnlichkeit konnte beim Betroffenen allerdings nicht festgestellt werden, und er wurde in der Sache folgerichtig auch als Zeuge vernommen. Das Anfertigen von Lichtbildern war somit keinesfalls erforderlich. Darüber hinaus enthielten weder die Vorladung noch das Protokoll zur Zeugenvernehmung des Betroffenen Aussagen zur erkennungsdienstlichen Behandlung. Äußerst bedenklich war in diesem Zusammenhang auch, dass im Vorblatt zur Wahllichtbildvorlage der Punkt „Anforderung einer Täterübersicht“ angekreuzt und der Zeuge hier als Tatverdächtiger bezeichnet worden war.

Öffentliche Stellen haben bei Eingriffen in das Grundrecht auf informationelle Selbstbestimmung immer den Grundsatz der Verhältnismäßigkeit zu beachten. Wegen der mangelnden Erforderlichkeit konnte die Maßnahme auch nicht auf § 7 DSG MV und urheberrechtliche Vorschriften gestützt werden. Darüber hinaus war die mündliche Einwilligungserklärung zu kritisieren, da hierfür grundsätzlich die Schriftform vorgesehen ist. Davon darf nur in Ausnahmefällen abgewichen werden. Eine solche Ausnahme lag in diesem Fall gerade auch im Hinblick auf die Art des Eingriffes nicht vor. Es fehlte daher sowohl an der Erforderlichkeit für eine derartige Maßnahme als auch an einer rechtswirksamen Einwilligung.

Erfreulicherweise hat die Polizeibehörde letztendlich doch noch ihre Rechtsauffassung revidiert und kam ebenfalls zu dem Ergebnis, dass das Anfertigen des Lichtbildes nicht zulässig war. Der bestehende Widerspruch in der Akte konnte allerdings nicht geklärt werden. Nach Aussage der Polizei zeuge dies davon, dass sich der Mitarbeiter nicht ausreichend mit der Sachlage auseinandergesetzt und den datenschutzrechtlichen Bestimmungen nicht die erforderliche Bedeutung beigemessen habe. Dabei sei es zu dem Verstoß gegen die Strafprozessordnung und das Landesdatenschutzgesetz gekommen.

Die Polizei hat mitgeteilt, dass sämtliche Negative und Fotos des Zeugen sowohl bei der Polizei als auch in der Wahllichtbildvorlage in der Ermittlungsakte der Staatsanwaltschaft gelöscht wurden. Sie hat den Betroffenen über die Vernichtung der Unterlagen unterrichtet.

Umfang erkennungsdienstlicher Maßnahmen nach § 81 b StPO

In einem weiteren Fall hat sich ein Petent an mich gewandt, der in einem Ermittlungsverfahren als Beschuldigter erkennungsdienstlich behandelt worden war. Die Polizei hatte ein dreiteiliges Täterlichtbild, Abdrücke vom rechten Zeigefinger und eine Personenbeschreibung angefertigt. Meine Prüfung hat Folgendes ergeben:

Der Staatsanwalt hatte es für notwendig erachtet, dass dem Geschädigten Lichtbilder des Beschuldigten vorgelegt werden, und daher eine erkennungsdienstliche Behandlung in Form von Lichtbildern durch die Kriminalpolizei verfügt. Die Polizei stützte ihre Vorgehensweise auf diese Verfügung der Staatsanwaltschaft.

Sie hat mitgeteilt, dass alle Maßnahmen gemäß § 81 b StPO getroffen werden durften und auch die Anordnung der Staatsanwaltschaft nicht erweitert wurde. Vielmehr habe sich der durchführende Beamte für die Variante entschieden, mit der am wenigsten in die Rechte des Betroffenen eingegriffen werde.

Nach den Ausführungen der Polizei erfolgen in Mecklenburg-Vorpommern scheinbar in allen Fällen des § 81 b StPO mindestens die beim Petenten durchgeführten Maßnahmen. § 81 b 1. Alt. StPO lässt aber erkennungsdienstliche Maßnahmen gegen Beschuldigte nur zu, soweit es für den Zweck des Strafverfahrens notwendig ist. Der Umfang erkennungsdienstlicher Behandlungen hat sich daher am Grundsatz der Verhältnismäßigkeit zu orientieren. Der Verfügung der Staatsanwaltschaft nach waren lediglich Lichtbilder erforderlich. Die Antwort darauf, warum in diesem Fall eine weitergehende erkennungsdienstliche Behandlung des Beschuldigten erforderlich war, ist die Polizei schuldig geblieben.

Ich halte diese Verfahrensweise für bedenklich, da sie gegen den auch im Ermittlungsverfahren geltenden Grundsatz der Verhältnismäßigkeit verstößt. Da im vorliegenden Fall keine Einigung erzielt werden konnte, hatte ich mich an das Innenministerium unseres Landes mit der Bitte um Stellungnahme gewandt. Das Ministerium teilt meine Rechtsauffassung und hat mitgeteilt, dass es sich hierbei um einen Einzelfall handelt. Es hat die Polizeidienststelle inzwischen angewiesen, künftig bei der Durchführung erkennungsdienstlicher Maßnahmen die Vorschriften genau zu beachten. Die erkennungsdienstlichen Unterlagen des Petenten sind vernichtet worden.

3.2.6 Unschuldig - aber mehrfach verdächtigt

Ein Petent bat mich Ende 1997 um Unterstützung, da er in den vergangenen Jahren in drei Fällen von strafrechtlichen Ermittlungen betroffen war. Dabei handelte es sich um so schwerwiegende Delikte wie sexuellen Mißbrauch, Mord und Tötung. Der Leiter der beteiligten Polizeidirektion hatte bereits im November 1996 gegenüber dem Petenten bestätigt, dass er in den beiden ersten Fällen zu keinem Zeitpunkt Verdächtiger oder gar Beschuldigter gewesen war. Ein Amtsgericht eines anderen Bundeslandes hatte im dritten Fall im Juli 1997 einen Beschluss erlassen, mit dem es die Entnahme einer Speichelprobe und die molekulargenetische Untersuchung des Materials beim Petenten anordnete, um festzustellen, ob die am Tatort gefundenen Spuren von ihm stammen. Das Amtsgericht begründete den Beschluss unter anderem damit, dass der Beschuldigte bereits strafrechtlich in Erscheinung getreten und erhebliche Übereinstimmung in der Vorgehensweise bei der dem Beschuldigten damals vorgeworfenen Tat festzustellen sei. Der Petent war über diese Aussage äußerst empört, da sie nicht den Tatsachen entsprach. Darüber hinaus teilte er mit, dass die im Zusammenhang mit der Aufklärung der Straftaten in seinem Umfeld durchgeführten Ermittlungen zu Beeinträchtigungen seiner Person geführt haben. Dies könnten nach seiner Auffassung möglicherweise Folgen des nicht ordnungsgemäßen Umgangs mit seinen personenbezogenen Daten durch die Landespolizei sein. Er hat mich daher um eine datenschutzrechtliche Prüfung der Angelegenheit gebeten.

Ich habe mich an die Landespolizei gewandt, um Auskünfte zu den einzelnen Verfahren einzuholen. Meine Fragen wurden zunächst jedoch nur teilweise und unvollständig beantwortet. Dies habe ich gegenüber dem Innenministerium als oberste Aufsichtsbehörde wegen des Verstoßes gegen die Mitwirkungspflicht beanstandet und daraufhin bei der Landespolizei eine Kontrolle durchgeführt. Ich stellte fest, dass in allen drei Fällen ausreichend Anhaltspunkte für polizeiliche Ermittlungen vorlagen. Allerdings war der Umgang mit den personenbezogenen Daten des Betroffenen zu kritisieren.

Für den Ablauf eines Ermittlungsverfahrens gibt es kein starres Schema, da in Abhängigkeit vom Einzelfall bestimmte polizeitaktische Maßnahmen erforderlich sein können. Im Rahmen von strafrechtlichen Ermittlungen nach §§ 161, 163 StPO haben die Polizeibehörden auch den Grundsatz der Verhältnismäßigkeit zu wahren. Befragungen Dritter in der Nachbarschaft und in der Familie können bei derartigen Delikten schnell zu einer erheblichen Schädigung des Ansehens des Betroffenen führen. Insbesondere in diesen Fällen sind die für die Ermittlung des Sachverhaltes notwendigen Maßnahmen im Einzelnen genau abzuwägen. In dem einen geprüften Fall war nicht zu erkennen, warum der Petent zunächst nicht selbst befragt worden war, bevor Dritte einbezogen wurden.

Für die Ermittlungen im dritten Fall hatte unsere Landespolizei einer Dienststelle eines Nachbarbundeslandes Daten aus anderen Fällen übermittelt. Dabei war auch mitgeteilt worden, dass Hinweise gegen den Petenten in einem Verbrechen mit ähnlicher Vorgehensweise vorlagen. Allerdings war die Überprüfung zum Zeitpunkt der Übermittlung bereits abgeschlossen und hatte keine Anhaltspunkte beziehungsweise Verdachtsmomente für eine Täterschaft ergeben. Dies hatte der Leiter der Polizeidirektion dem Petenten auch schriftlich bestätigt. Darüber hinaus waren auch Informationen aus einem strafrechtlichen Ermittlungsverfahren weitergegeben worden, das die Staatsanwaltschaft anderthalb Jahre zuvor wegen Geringfügigkeit nach § 153 Abs. 1 StPO eingestellt hatte. Vor diesem Hintergrund habe ich gegen die Übermittlung dieser Daten unter dem Aspekt der Erforderlichkeit datenschutzrechtliche Bedenken geäußert.

In den Ermittlungsverfahren wurde der Begriff „Verdächtiger“ unterschiedlich verwandt. Im Gegensatz zur Aussage des Leiters der Polizeidirektion, dass der Petent zu keinem Zeitpunkt Verdächtiger war, wurde er durch die Kriminalpolizeiinspektion als solcher während der Ermittlungen geführt. Der Begriff „Verdächtiger“ wurde durch die beteiligten Stellen unterschiedlich ausgelegt. Es handelt sich dabei nicht nur um eine rechtstheoretische Frage, sondern um eine Frage mit ganz konkreten Auswirkungen. So werden beispielsweise Maßnahmen nach § 163 b StPO bei Verdächtigen und Unverdächtigen an unterschiedliche Voraussetzungen geknüpft. Maßgeblich ist, wie der Betroffene in dem Verfahren durch die ermittelnde Polizeidienststelle klassifiziert wurde. Insofern entsprach die Mitteilung des Leiters der Polizeidirektion nicht den Tatsachen.

Den geprüften Unterlagen war nicht zu entnehmen, dass die Aussage in der Begründung des Amtsgerichtsbeschlusses auf einer Datenübermittlung der Polizei unseres Landes beruht. Auch der Landesbeauftragte für den Datenschutz des Bundeslandes, der im dritten Fall weitgehend zuständig war, hat im Rahmen seiner Prüfung keine Anhaltspunkte dafür gefunden.

Die Polizeidirektion hat in ihrer Stellungnahme ebenfalls die Auffassung vertreten, dass bei den Ermittlungen in dem einen Fall zweckmäßigerweise zunächst der Petent hätte befragt werden sollen und falls dann noch erforderlich auch Personen aus der Nachbarschaft. Zum Umfang der Datenübermittlung konnte unter dem Gesichtspunkt der Verhältnismäßigkeit teilweise Übereinstimmung erzielt werden. Die Polizei äußerte ebenfalls Bedenken, dass gegenüber der ermittelnden Dienststelle im dritten Fall nicht mitgeteilt worden war, dass der Petent bei den anderen zwei Verfahren als Verdächtiger ausgeschlossen werden konnte.

Aufgrund meiner Bewertung habe ich empfohlen, die einzelnen Punkte mit den zuständigen Mitarbeitern auszuwerten. Der Leiter der Polizeidirektion ist dieser Empfehlung gefolgt und hat dies zum Anlass genommen, die zuständigen Polizeibeamten nochmals auf die konsequente Beachtung datenschutzrechtlicher Aspekte hinzuweisen.

3.2.7 Leichtfertiger Umgang mit DDR-Flüchlingsakten

Im Mai 1999 erhielten Meldebehörden von unserer Landespolizei 1.101 Akten mit Unterlagen über Rückkehrer und Zuzieher in die DDR. Die Polizei hatte die Akten zuständigkeitshalber den Meldebehörden überlassen, damit diese unter anderem die Historiedaten des Melderegisters ergänzen können.

Ein Landkreis machte mich auf dieses Vorgehen aufmerksam. Ich habe den Sachverhalt geprüft und dazu Einsicht in einzelne Akten genommen. Unter anderem sind folgende Unterlagen aus den 50er, 60er und 70er Jahren enthalten:

- Fragebogen für Rückkehrer/Erstzuzug - Vordruck PM 8 - (Personalien, Wohnanschriften seit Geburt, Arbeitsstellen, Zugehörigkeit zu Parteien, Vorstrafen, laufende Strafverfahren, Aufenthalte 1933 bis 1945, Kreditverpflichtungen, Unterhaltsverpflichtungen, Vermögen, Auslandsaufenthalte, Angaben zu Familienangehörigen, Verwandten, Bekannten, Freunden und Arbeitskollegen, Gründe für das Verlassen der DDR, Aufenthalt in Westdeutschland/Westberlin, Namen und Anschriften von Republiksflüchtlingen, Gründe für die Rückkehr, Zeugen);
- Personalbogen des Aufnahmeheimes (Angaben zur Person einschließlich medizinischer Daten);
- Ermittlungsberichte (zum Teil über mehrere Jahre, mit den Entscheidungen über das Fortführen der Personenkontrolle des Betroffenen bei fehlender Systemtreue);
- Mitteilungen über Zuchthausverurteilungen, Aufnahme-, Führungs- und Abschlussberichte der Strafvollzugsanstalt;
- Strafnachricht (A) des Wehrkreiskommandos;
- Mitteilung des Betriebes (Beurteilung des Betroffenen, Bericht);
- Lebenslauf/Mitteilung über Eheschließungen;
- Protokoll über die Kommissionssitzung im Volkspolizeikreisamt (VPKA) (Auswertung der persönlichen Verhältnisse des Betroffenen/Entscheidung über weitere Maßnahmen);
- Zuzugsgenehmigung/Einweisungsschein für Rückkehrer/Anmeldebestätigungen;
- Meldekarteikarte (zum Beispiel aus dem Jahre 1956);
- Maßnahmeplan des VPKA (zur jeweiligen Person);
- Erkennungsdienstliche Unterlagen (Lichtbild)/Personalausweisanträge;
- Strafanzeigen (unter anderem wegen des Verlassens der DDR)/Auszug aus dem Strafregister der DDR.

Der Inhalt der Akten zeigt deutlich die Sensibilität der Daten und lässt die Sammelleidenschaft der VPKA der DDR hinsichtlich personenbezogener Daten zu bestimmten Personengruppen erahnen.

Für die Übergabe dieser polizeilichen Akten an die Meldebehörden existiert keine Rechtsgrundlage. Dies habe ich gegenüber dem Innenminister unseres Landes beanstandet. Die Meldebehörden erhielten durch diese Datenübermittlung viele sensible personenbezogene Daten der Betroffenen zur Kenntnis, die in keinem sachlichen Zusammenhang mit ihren Aufgaben stehen.

Das Innenministerium hielt dem entgegen, dass es sich hierbei um Meldedaten handelte und die Unterlagen daher nach § 34 Abs. 1 Satz 1 DSG MV an die kommunalen Meldebehörden hätten übergeben werden müssen, da die Aufgaben der Abteilung Pass- und Meldewesen der ehemaligen VPKA an diese übergegangen seien.

Bei seiner Bewertung hat das Innenministerium jedoch die besonderen Strukturen des Pass- und Meldewesen der DDR und die enge Verknüpfung mit der Tätigkeit der Volkspolizei nicht hinreichend berücksichtigt. In der DDR existierte ein polizeiliches Meldewesen, dessen Aufgaben in der Verordnung über das Meldewesen in der DDR - Meldeordnung - und in Dienstvorschriften des Ministers des Innern und Chefs der Deutschen Volkspolizei über das polizeiliche Meldewesen geregelt waren. Hiernach wurden besondere Personengruppen, wie Ausländer, Personen, die im Sperrgebiet lebten, sowie auch die Gruppe der Rückkehrer und Zuzieher, nicht von der „normalen“ Sachbearbeitung Meldewesen erfasst. Die Vielzahl von personenbezogenen Daten, die ganz überwiegend nicht für die Aufgaben des Meldewesens erforderlich war, wurde für andere Zwecke verwendet. Die Polizei bewertete zum Beispiel aufgrund dieses umfangreichen Datenmaterials die Systemtreue des Betroffenen in regelmäßigen Abständen, bis dies nicht mehr notwendig erschien. In diesem Zusammenhang wurde auch die strafrechtliche Relevanz des Verlassens der DDR geprüft. Darüber hinaus gingen in bestimmten Fällen Mitteilungen an das Ministerium für Staatssicherheit (MfS) der DDR, damit dort gegebenenfalls über weitere Maßnahmen entschieden werden konnte. Das MfS hat für den Bereich des Ministerium des Innern und der Deutschen Volkspolizei der DDR zu diesem Zweck spezielle Dateien, wie VII/3 Zentrale Aufnahme (Aufnahme, Wiederaufnahme, Zurückgewiesene, Lebenslauf, Verbindungen, Verhalten) oder VII DDR-Ausreißer (ungesetzliches Verlassen: Gründe, Daten), geführt. Es ist daher festzuhalten, dass die umfangreichen Daten nicht vorrangig für melderechtliche Zwecke, sondern zur Überwachung und Strafverfolgung genutzt wurden. Das Meldewesen hat lediglich einzelne Ergebnisse dieser primär polizeilichen Tätigkeit auf den Kreismeldekarteien vermerkt. So finden sich beispielsweise auf einigen Karteien Hinweise wie „Rückkehrer“ oder „Republiksflucht“. Darüber hinaus ist auch die „weitere Bearbeitung“ des Personenkreises der Rückkehrer und Zuzieher nach den Vorschriften über das Meldewesen in der DDR nicht dem Bereich Meldewesen übertragen worden.

§ 34 DSG MV setzt voraus, dass die Aufgaben der alten Stelle auf die neue verantwortliche Stelle übergegangen sind. Dafür ist eine differenzierte Betrachtungsweise erforderlich, die nicht auf die bloße Funktionsbezeichnung, sondern auf die konkrete Aufgabe abstellt. Da es sich hier um eine „DDR-spezifische Aufgabe“ handelte, die von den Meldebehörden nach geltender Rechtslage nicht wahrgenommen wird, war die Datenübermittlung auch aus diesem Grunde nicht zulässig. Bei der Einrichtung der kommunalen Meldebehörden wurden die vom Zentralen Einwohnerregister (ZER) übernommenen Meldedaten erheblich reduziert und Meldealtdaten-bestände (Meldekarteien, Kreismeldekarteien) zum Teil geschwärzt oder vernichtet. Nach den Überleitungsbestimmungen des Landesmeldegesetzes (§§ 40, 44 LMG), die spezielle Regelungen zur Schaffung eines kommunalen Meldewesens aus den Altdatenbeständen der DDR beinhalten, war der Aufbau des neuen Meldewesens lediglich anhand der Daten des ZER sowie der örtlichen Meldekarteien und Kreismeldekarteien vorzunehmen. Daher waren diese Altakten auch nicht für den Verwaltungsvollzug der Meldebehörden erforderlich. Demzufolge hätten die Unterlagen der Volkspolizeikreisämter nicht an die Meldebehörden, sondern direkt an ein Archiv übergeben werden müssen. Dies gilt, nicht zuletzt auch vor dem zeitlichen Hintergrund, in besonderem Maße für Unterlagen, die in der heutigen Zeit noch aufgefunden werden.

Inzwischen hat es Gespräche mit dem Innenministerium gegeben. Bei der Einschätzung der Unterlagen sowie der Bewertung der Rechtslage besteht nach wie vor ein Dissens, der nicht ausgeräumt werden konnte. Annäherung wurde jedoch in folgenden Punkten erreicht:

- Die Unterlagen sind für die Landespolizei nicht zur Aufgabenerfüllung erforderlich und daher abzugeben.

- Die in den Unterlagen enthaltenen Daten können im Einzelfall für den Betroffenen bei rehabilitierungsrechtlichen Verfahren von Bedeutung sein.

- Künftige Funde von Altdaten im Polizeibereich werden dem Landeshauptarchiv übergeben.

Die Gemeinden und Landkreise haben die Unterlagen inzwischen an die kommunalen Archive übergeben. Für künftige Fälle ist sichergestellt, dass derart sensible Akten unmittelbar an das Archiv gehen und somit bei einer Nutzung den archivrechtlichen Schutzvorschriften unterliegen.

3.3 Das Nachrichtendienstliche Informationssystem der Verfassungsschutzbehörden

Im August 1998 habe ich beim Verfassungsschutz unseres Landes den Umgang mit Daten im Nachrichtendienstlichen Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder (NADIS) geprüft. In der Personenzentraldatei von NADIS werden Daten gespeichert, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind.

Von besonderer Bedeutung im NADIS ist das „Datum der letzten Erkenntnis/Information“ (EK-Datum). Das EK-Datum ist neben dem Wiedervorlagedatum (WV-Datum) maßgebliches Kriterium für die IT-gestützte listenmäßige Aufbereitung zur Unterrichtung der eingebenden Stellen über die von ihnen zu überprüfenden Daten. Prüf- und Löschfristen orientieren sich insbesondere an diesem Datum.

Die Kontrolle hat im Wesentlichen Folgendes ergeben:

- Lediglich in einem Fall stimmte das EK-Datum tatsächlich mit dem Datum der letzten relevanten Information überein. Auf entsprechende Nachfrage hin wurde bestätigt, dass es offensichtlich jedem einzelnen Mitarbeiter überlassen war, welches Datum als EK-Datum verwendet wird. Die eindeutigen Vorgaben der NADIS-Richtlinien waren völlig außer Acht gelassen worden.

- Für die Mehrzahl der kontrollierten Akten konnte der jeweilige Bearbeitungsstand erst nach Einsicht in die Personenarbeitsdatei Mecklenburg-Vorpommern (PAD-MV) herausgefunden werden. Verfügungen, die aus der Arbeit mit den Akten resultierten, waren nur in wenigen Fällen in den Akten selbst zu finden. Daher war nur schwer nachvollziehbar, aufgrund welcher Ereignisse welche Fristen vergeben worden sind.

- In mehreren Akten waren die Daten Unbeteiligter nicht gesperrt.

Aufgrund der Verstöße gegen datenschutzrechtliche Bestimmungen habe ich dem Innenminister eine förmliche Beanstandung ausgesprochen und folgende Empfehlungen gegeben:

- Das EK-Datum ist gemäß den Vorgaben der NADIS-Richtlinien festzulegen und dem jeweiligen aktuellen Erkenntnisstand anzupassen. Durch entsprechende organisatorische Hilfsmittel (zum Beispiel Dienstanweisung) ist sicherzustellen, dass alle Mitarbeiter einheitliche Kriterien bei der Vergabe des EK-Datums zugrunde legen. Das betrifft ebenfalls die Festlegung der Prüf- und Löschfristen (WV-Datum).

- Mit besonderer Sorgfalt ist zu prüfen, ob die gespeicherten personenbezogenen Daten erforderlich sind. Daten Betroffener dürfen nicht zu lange oder ohne Rechtsgrundlage gespeichert werden.

- Besonders sensibel ist mit Daten Unbeteiligter umzugehen. Hier muss äußerst sorgfältig geprüft werden, ob diese personenbezogenen Daten jeweils erforderlich sind.

- Es ist sicherzustellen, dass Verfügungen zur Löschung von Datensätzen umgehend umgesetzt werden. Die Prüflisten sind entsprechend zeitnah abzuarbeiten.

- Sind personenbezogene Daten nicht mehr für die Aufgabenerfüllung erforderlich, muss unverzüglich die Löschung in der PAD-MV, im NADIS und in den dazugehörigen Akten erfolgen. Daten sind mit Hilfe eines geeigneten Verfahrens zu sperren, wenn diese in Akten mit anderen - noch zur Aufgabenerfüllung notwendigen - Daten derart verbunden sind, dass eine Trennung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

- Wird festgestellt, dass gespeicherte personenbezogene Daten nicht richtig sind, so sind diese unverzüglich zu berichtigen.

Das Innenministerium ist diesen Empfehlungen gefolgt.

3.4 Einwohnerwesen

3.4.1 Elektronische Überwachung von Asylbewerbern geplant

Für Asylbewerber ist eine multifunktionale Chipkarte geplant. Sie soll Daten aus sämtlichen Lebensbereichen zusammenführen. Schon im Zweiten Tätigkeitsbericht habe ich mich dazu kritisch geäußert. Trotz dieser Bedenken hat sich das Land Mecklenburg-Vorpommern an der so genannten Machbarkeitsstudie zur Einführung der AsylCard beteiligt. Die dazu beauftragte Firma ORGA Consult GmbH hat dem Bundesministerium des Innern (BMI) im Juni 1998 den Abschlussbericht vorgelegt. Die Karte bietet eine Basisanwendung (Pflichtfunktion) - diese umfasst die eindeutige Identifizierung und die Ausweisfunktion - und so genannte zweckgebundene Anwendungen (optionale Funktionen). Letztere sollen öffentlichen Stellen wie Aufnahmeeinrichtungen, Ausländer-, Sozial- und Meldebehörden oder Arbeitsämtern Zugriff auf einen Teil der in der Basisanwendung gespeicherten Daten ermöglichen. Kritikwürdig sind insbesondere folgende Punkte:

- Der datenschutzrechtlich gebotene Vorrang der Erhebung beim Betroffenen wird durch den Technikeinsatz verdrängt. Die Daten werden nicht mehr beim Karteninhaber erhoben, sondern aus seiner AsylCard ausgelesen. Für ihn ist nicht mehr erkennbar, welche Daten die leseberechtigte Stelle zur Kenntnis nimmt. Dies führt zu einem Verlust von Transparenz für den Betroffenen.

- Der Zweckbindungsgrundsatz steht nicht mehr im Vordergrund. Vielmehr ist die vorgesehene Menge der zu übermittelnden Daten wesentlich geprägt vom Informationsbedürfnis einzelner Verwaltungsbereiche und nicht vom Grundsatz der Erforderlichkeit und Verhältnismäßigkeit im Sinne des Verfassungsrechts. So ist unter anderem nicht erkennbar, weshalb zum Beispiel die Polizei einen umfassenden Datenzugriff erhalten soll.

- Es gibt keine rechtlichen Vorgaben, die eine praktisch totale Aufenthaltskontrolle aller Asylsuchenden zulassen würden. Mit Hilfe der Technik soll ein Überwachungssystem realisiert werden, mit dem mehrmals am Tage der Meldepflicht durch einen Aufenthaltsnachweis nachgekommen werden soll.

Diese Bedenken habe ich dem Innenministerium unseres Landes mitgeteilt. Trotzdem hat es dem BMI auf eine Länderumfrage hin erklärt, dass Mecklenburg-Vorpommern weiterhin am Einsatz der AsylCard interessiert sei und sich auch an einem auf das Land begrenzten Pilotversuch beteiligen würde. Ob das Projekt weitergeführt wird, hängt von den Entscheidungen der anderen Bundesländer und letztendlich von der Entscheidung des BMI ab.

3.4.2 Automatisierte Abrufverfahren in Gemeinden und Ämtern

Der zunehmende Einsatz von Computern und der Aufbau von Verwaltungsnetzen führen dazu, dass es immer einfacher wird, Informationen auszutauschen. In letzter Zeit erhalte ich immer häufiger Anfragen, ob und unter welchen Voraussetzungen Verwaltungseinheiten innerhalb einer Gemeinde oder eines Amtes zum Beispiel Meldedaten im automatisierten Verfahren abrufen dürfen, um die Daten aus dem Melderegister schnell und auf direktem Wege zu erhalten, ohne die Meldebehörde einzuschalten.

Das Landesmeldegesetz (LMG) enthält Regelungen zur Weitergabe von Daten innerhalb von Gemeinden und Ämtern (§ 31 Absatz 8). Hiernach dürfen Daten aus dem Melderegister weitergegeben werden, wenn diese zur Erfüllung einer Aufgabe der Meldebehörde oder des Datenempfängers erforderlich sind. Eine spezielle Regelung für die Einrichtung automatisierter Abrufverfahren in diesem Bereich existiert jedoch nicht.

Teilweise wird nun die Auffassung vertreten, dass die allgemeine Vorschrift zur Datenweitergabe auch für das automatisierte Abrufverfahren anzuwenden ist. Die Vorschrift genügt jedoch nicht dem Gebot der Normenklarheit. Sie berücksichtigt darüber hinaus auch nicht hinreichend die mit einem automatisierten Abrufverfahren verbundenen Besonderheiten und Risiken.

Das automatisierte Abrufverfahren ermöglicht den direkten Zugriff auf die Daten des Melderegisters. Da nicht von vornherein zu überschauen ist, welche Daten im Einzelfall tatsächlich benötigt werden, wäre beim Abrufverfahren ein umfangreicher Datenbestand für die abrufende Stelle bereitzuhalten. Die abrufende Stelle hätte somit grundsätzlich die Möglichkeit, eine Vielzahl von Daten zur Kenntnis zu nehmen. Sie darf diese Zugriffsrechte jedoch nur nutzen, soweit dies für ihre Aufgabenerfüllung im Einzelfall tatsächlich erforderlich ist. Insofern kommen der Vergabe differenzierter Zugriffsrechte und dem Umfang des bereitzustellenden Datenbestandes eine besondere Bedeutung zu.

Die Meldebehörde erhält beim automatisierten Abrufverfahren - im Gegensatz zu der über sie direkt laufenden Anfrage - zunächst keine Kenntnis davon, von wem auf welche Daten zugegriffen wird. Sie kann somit nicht Umfang und Zweck der Abrufe vorab prüfen. Daher sind geeignete technische Maßnahmen zu treffen, um gegebenenfalls unzulässige Abrufe künftig auszuschließen.

Es ist erforderlich, dass der Landesgesetzgeber die rechtlichen Rahmenbedingungen für die Zulassung eines solchen Verfahrens und die hierfür notwendigen technischen und organisatorischen Maßnahmen normenklar regelt.

Weiterhin wird sehr genau zu prüfen sein, welche Stellen an einem solchen Verfahren teilnehmen dürfen. Bevor eine Verwaltungseinheit am Abrufverfahren beteiligt wird, sind die schutzwürdigen Belange der von dieser Maßnahme betroffenen Personen und die Erforderlichkeit des Abrufverfahrens für die Aufgabenerfüllung der abrufenden Stelle abzuwägen. Dabei ist zu untersuchen, ob die benötigten Daten eine derartige Zugriffsmöglichkeit auf das Melderegister rechtfertigen. Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit ist zu beachten. Falsche oder unvollständige Adressen, wie sie in Einzelfällen in allen Bereichen der öffentlichen Verwaltung auftreten, sind allein kein ausreichendes Argument, um als öffentliche Stelle an einem solchen Verfahren teilzunehmen.

Im Zuge der Anpassung des Landesmeldegesetzes an die Vorschriften des Melderechtsrahmengesetzes ist nach Mitteilung des Innenministeriums eine Novellierung vorgesehen. Die zu erwartenden Änderungen des Landesdatenschutzgesetzes (siehe auch Punkt 2.1) sollen dabei ebenfalls berücksichtigt werden. Es bleibt nur zu hoffen, dass dies endlich auch geschieht.

3.4.3 Widerspruchsrecht bei Übermittlung von Meldedaten unzureichend

Widerspruchsrecht gegen Datenübermittlungen aus dem Melderegister

Nach § 35 Abs. 1 Landesmeldegesetz (LMG) darf die Meldebehörde die Daten von Wahlberechtigten an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen für Zwecke der Wahlwerbung übermitteln. Für die Auswahl der Wählerdaten ist es zulässig, das Lebensalter zugrunde zu legen, und es können Vor- und Familiennamen, Doktorgrad und Anschriften weitergegeben werden. Der Wahlberechtigte hat die Möglichkeit, dieser Datenweitergabe zu widersprechen. Der Widerspruch kann ohne Begründung eingelegt werden und ist für den Betroffenen kostenfrei. Einzelnen Meldebehörden und interessierten Bürgern habe ich einen Vordruck zum Widerspruchsrecht zur Verfügung gestellt (siehe 24. Anlage).

Anfragen von Bürgern zeigen, dass vielen Wahlberechtigten ihr Widerspruchsrecht nicht bekannt ist. Veröffentlichungen, in denen regelmäßig auf das Widerspruchsrecht hingewiesen wird, werden oftmals nicht zur Kenntnis genommen.

Aber auch bei den Meldebehörden traten bei der Umsetzung des geltenden Rechts Probleme auf. So hatten beispielsweise einige Meldebehörden es bisher versäumt, ihrer jährlichen Bekanntmachungspflicht nach § 36 LMG nachzukommen und die Betroffenen auf die Widerspruchsrechte hinzuweisen.

Eine Stadt sah davon ab, die Widersprüche einzutragen, die für minderjährige Personen vorlagen, da sie noch nicht von den Datenübermittlungen betroffen seien. Beim Eintritt in die Volljährigkeit wurde der Widerspruch jedoch nicht nachgetragen. Diese Vorgehensweise entspricht nicht der Rechtslage. Aufgrund bestehender Unsicherheiten hat das Innenministerium hierzu klargestellt, dass Eltern für ihre minderjährigen Kinder widerspruchsbefugt sind, Jugendliche ab dem vollendeten 16. Lebensjahr jedoch selbst dieses Recht haben.

Eine Amtsverwaltung hatte von einem Betroffenen aufgrund einer kommunalen Satzung sogar Gebühren für den Widerspruch erhoben. Diese Verfahrensweise war unzulässig, da nach der hier anzuwendenden Verordnung über Kosten im Geschäftsbereich des Innenministeriums keine Gebühr vorgesehen ist und eine Ausweitung der Gebührenvorschriften durch eine örtliche Satzung in diesem Bereich nicht in Betracht kommt. Auf meine Empfehlung hin hat die Amtsverwaltung dem Petenten die widerrechtlich erhobenen Gebühren erstattet und die kommunale Gebührensatzung geändert.

In einem anderen Fall hatte es die Amtsverwaltung unterlassen, den Empfänger der Adressen von Erstwählern auf die Zweckbindung der Daten sowie auf die Pflicht, die Daten spätestens eine Woche nach der Wahl zu löschen, hinzuweisen. Auch die Veröffentlichung über das Widerspruchsrecht entsprach nicht den gesetzlichen Vorgaben, so dass die Betroffenen nicht ausreichend über ihre Rechte aufgeklärt wurden.

Im Zusammenhang mit der Anfrage einer Partei nach den Daten der Erstwähler für die Landtagswahlen erkundigten sich viele Meldebehörden zu den datenschutzrechtlichen Anforderungen. Vielfach wurde der Wunsch geäußert, dass aufgrund der politischen Ausrichtung dieser Partei eine Melderegisterauskunft für Wahlwerbungszwecke unterbleiben sollte. Ich habe die anfragenden Stellen darauf hingewiesen, dass § 35 Abs. 1 LMG eine Übermittlung von Wählerdaten grundsätzlich zulässt. Dabei ist das Gebot der Gleichbehandlung hinsichtlich der antragstellenden Parteien zu beachten. Jedoch räumt diese Vorschrift den Antragstellern keinen Rechtsanspruch auf Auskunft ein. Vielmehr handelt es sich um eine Ermessensentscheidung der einzelnen Meldebehörde.

Das Innenministerium unseres Landes hat die Meldebehörden ebenfalls mehrfach auf die Rechtslage sowie die Einhaltung der melderechtlichen Bestimmungen hingewiesen.

Das Oberverwaltungsgericht Mecklenburg-Vorpommern hat in diesem Zusammenhang eine Entscheidung des Verwaltungsgerichtes Schwerin bestätigt, mit der das Gericht die Entscheidung einer Meldebehörde, keine Auskunft zu erteilen, für zulässig erachtet hat (Beschluss vom 27. August 1998, 1 M 102/98). Die Meldebehörde war aufgrund der bereits vorliegenden zahlreichen Widersprüche davon ausgegangen, dass eine Vielzahl von Betroffenen sich gegen eine Weitergabe der personenbezogenen Daten an politische Parteien wenden würde. Mit der Entscheidung der Meldebehörde würden auch die Bürgerinnen und Bürger geschützt, die mangels Kenntnis der Rechtslage keinen Widerspruch haben eintragen lassen.

Diese Entscheidung ist aus datenschutzrechtlicher Sicht zu begrüßen, macht jedoch auf das entscheidende Dilemma aufmerksam. Vielfach nehmen die Betroffenen ihre Rechte nicht wahr, weil sie ihnen nicht bekannt sind. Entsprechende Hinweise der Meldebehörde bei der Anmeldung sowie durch die jährliche Veröffentlichung genügen offensichtlich nicht. Somit wird es den Meldebehörden überlassen, wie sie die Lage aufgrund ihrer Erfahrungen einschätzen und zu welcher Entscheidung sie im Einzelfall gelangen.

Diese Verfahrensweise trägt dem Recht des Betroffenen auf informationelle Selbstbestimmung nicht genügend Rechnung. Bereits in meinem Ersten Tätigkeitsbericht habe ich unter Punkt 2.3.1 auf die damit im Zusammenhang stehenden Schwierigkeiten hingewiesen.

Ich hatte mich an den Innenminister unseres Landes gewandt und vorgeschlagen, bei einer Novellierung des Landesmeldegesetzes eine Einwilligungslösung vorzusehen. Bürger sollten nicht erst von sich aus aktiv werden müssen, um eine unerwünschte Übermittlung ihrer Daten zu unterbinden. Es wäre besser, sie vorher zu fragen, ob sie damit einverstanden sind, dass ihre Daten übermittelt werden. In einem umfangreichen Schriftwechsel hat sich der Innenminister hiergegen ausgesprochen, insbesondere weil nach seiner Auffassung eine solche Regelung in § 35 LMG nicht mit § 22 Abs. 1 Melderechtsrahmengesetz zu vereinbaren sei. Ich teile diese Ansicht nicht, da die Rahmengesetzgebung einer entsprechenden Umsetzung durch Landesrecht nach meinem Dafürhalten nicht entgegensteht. Der Innenminister vertritt hingegen die Meinung, dass zuvor die entsprechende Vorschrift des Rahmengesetzes geändert werden müsste und hat im Ergebnis zugesagt, meine Anregung bei der nächsten Novellierung des Melderechtsrahmengesetzes aufzugreifen und beim Bundesminister des Innern vorzutragen.

Die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 hat in einer Entschließung zur Weitergabe von Meldedaten an Adressbuchverlage und Parteien gefordert, anstelle der Widerspruchsregelung künftig eine Einwilligungslösung vorzusehen (siehe 7. Anlage). Ich halte es nach wie vor für notwendig, diese Einwilligungslösung zu realisieren.

Gebührenpflichtige Auskunftssperre

Besteht eine Gefahr für Leben, Gesundheit und persönliche Freiheit eines Betroffenen, so kann er im Melderegister zu seinem Schutz eine Auskunftssperre nach § 35 Abs. 5 LMG eintragen lassen. In diesen Fällen dürfen an Privatpersonen und andere nicht-öffentliche Stellen keine Auskünfte aus dem Melderegister erteilt werden. Im Zweiten Tätigkeitsbericht, Punkt 2.7.3, habe ich über verschiedene Aspekte hierzu informiert. Neu ist nunmehr, dass der Betroffene hierfür eine Gebühr in Höhe von 20,- DM zu entrichten hat.

Wie das Innenministerium dargelegt hat, soll mit der Gebühr zumindest teilweise der erhebliche Verwaltungsaufwand gedeckt werden, der den Meldebehörden im Verfahren entsteht. Dabei sei auch zu berücksichtigen, dass die Gebühr gering und eine entsprechende Härtefallklausel vorgesehen sei. Darüber hinaus sei seit Einführung der Gebühr die Anzahl der Auskunftssperren bei einigen Meldebehörden deutlich zurückgegangen, was insofern eine positive Wirkung habe, da bei einer tatsächlichen Gefährdung Betroffene auch bereit sein dürften, die entsprechende Gebühr zu entrichten. Eine Änderung der Kostenverordnung sei daher nicht vorgesehen.

Ich halte es aus datenschutzrechtlicher Sicht für nicht akzeptabel, wenn die Wahrnehmung des Grundrechtes auf informationelle Selbstbestimmung durch den Betroffenen mit einer Gebühr verknüpft wird. Der Betroffene hat seine allgemeine Meldepflicht zu erfüllen und dabei die erforderlichen Daten der Meldebehörde mitzuteilen. Es ist ihm somit nicht freigestellt, über den Umgang mit seinen Daten frei zu entscheiden. Das Melderecht ist so konzipiert, dass der Aufenthalt eines Einwohners im Grundsatz für jeden feststellbar sein soll. Insofern hat das Recht auf informationelle Selbstbestimmung des Einzelnen eine Einschränkung erfahren.

Eine Auskunftssperre nach § 34 Abs. 5 LMG wird nur eingerichtet, wenn hochrangige Rechtsgüter betroffen sind. Dabei ist auch zu berücksichtigen, dass eine solche Gefahrensituation regelmäßig nicht durch den Betroffenen verschuldet worden ist und für ihn schon generell Mehraufwendungen entstehen, um die notwendigen Schutzmaßnahmen zu treffen. Ich halte es deshalb für unangemessen, dem Betroffenen für die Einrichtung einer Auskunftssperre darüber hinaus noch eine Gebühr aufzuerlegen. Auch die in der Gebührenverordnung vorgenommene Einschränkung der Gebührenpflicht bei Bedürftigkeit oder bei Vorliegen eines öffentlichen Interesses stellt insoweit kein ausreichendes Korrektiv dar.

In den meisten Bundesländern existieren gesetzliche Vorschriften, wonach die Einrichtung dieser Sperren für den Betroffenen gebührenfrei ist. Ich hoffe, dass unser Landesgesetzgeber die Erforderlichkeit hierzu erkennt und auch in Mecklenburg-Vorpommern eine entsprechende gesetzliche Regelung geschaffen wird.

3.4.4 Wohnsitzwechsel - Kopie des Mietvertrages zu den Akten der Meldebehörde?

Ein Petent hatte der Meldebehörde bei der Ummeldung seines Wohnsitzes zum Nachweis seinen Mietvertrag vorgelegt. Dieser wurde im Amt kopiert und die Kopie zu den Akten genommen. Im Nachhinein wunderte sich der Petent über diese Verfahrensweise und hat sich an mich gewandt.

Die Behörde begründete das Verfahren damit, dass bei der Aufklärung von melderechtlichen Verhältnissen zur Fortschreibung des Melderegisters zumeist der Vermieter befragt werden muss. Liegt keine Bestätigung des Wohnungsgebers vor, so muss die Meldebehörde in diesen Fällen auf die Daten des Mietvertrages zurückgreifen können. Ein Vermerk „Mietvertrag lag vor“ reicht daher nicht. Diese Verfahrensweise sei auch im Hinblick auf eine saubere und übersichtliche Aktenführung festgelegt worden. Die Kopien werden nach der Erfassung der relevanten Daten in das Melderegister vernichtet.

Ich habe mit der Meldebehörde die Rechtslage erörtert. Der Einwohner ist verpflichtet, bei der An- oder Abmeldung auch eine Bestätigung des Wohnungsgebers vorzulegen. Damit sollen Scheinmeldungen verhindert werden. Anerkannt ist, dass der Ein- oder Auszug auch durch Vorlage des Miet- oder Kaufvertrages nachgewiesen werden kann. Es ist jedoch nicht notwendig, den vollständigen Vertrag einzusehen oder eine Kopie des Vertrages zu den Unterlagen zu nehmen. Dieses Verfahren würde dazu führen, dass die Meldebehörde Einzelheiten des Vertrages, wenn auch nur auszugsweise, zur Kenntnis nehmen und gegebenenfalls speichern würde, obwohl diese nicht zur Aufgabenerfüllung erforderlich sind. Diesem Verfahren steht der Grundsatz der Verhältnismäßigkeit entgegen. In diesen Fällen genügt bei der Anmeldung die Kenntnisnahme der erforderlichen Daten aus dem Vertrag, die der Mitarbeiter sogleich erfassen kann.

Ich habe der Meldebehörde daher empfohlen, die benötigten Daten aus dem Mietvertrag auf der Ein- bzw. Auszugsbestätigung zu vermerken. Dadurch ist sichergestellt, dass der Umfang der Daten nicht über das erforderliche Maß hinausgeht und auch eine ordnungsgemäße Aktenführung gewährleistet ist. Die Meldebehörde ist meiner Empfehlung gefolgt.

3.5 Bürgerbüro

In einigen Gemeinden unseres Landes sind so genannte Bürgerbüros oder Bürgerämter eingerichtet worden. Diese sollen es den Einwohnern ermöglichen, ihre Verwaltungsgeschäfte schnell und umfassend an einem zentralen Ort zu erledigen. Bereits in meinem Dritten Tätigkeitsbericht bin ich unter Punkt 3.19.3 auf diese neue Organisationsform in der öffentlichen Verwaltung eingegangen. Im Berichtszeitraum haben mich eine Amtsverwaltung sowie der Städte- und Gemeindetag unseres Landes um eine datenschutzrechtliche Beratung gebeten.

Eine moderne bürgerfreundliche Verwaltung sollte unter anderem auch dadurch gekennzeichnet sein, dass sie beim Umgang mit personenbezogenen Daten dem Grundrecht des Betroffenen auf informationelle Selbstbestimmung ausreichend Beachtung schenkt. Bereits bei den Planungen für ein Bürgerbüro sind daher einige grundsätzliche datenschutzrechtliche Anforderungen umzusetzen.

Der Gesetzgeber hat den unterschiedlichen Stellen innerhalb der Verwaltung verschiedene Aufgaben zugewiesen. Auch innerhalb der Gemeindeverwaltung gilt der Grundsatz der informationellen Gewaltenteilung. Aus der Einheit der Gemeindeverwaltung folgt daher keineswegs eine informationelle Einheit. Nimmt ein Behördenmitarbeiter unterschiedliche Verwaltungsaufgaben wahr - so schon jetzt in den Amtsverwaltungen - , erhält er personenbezogene Daten aus verschiedenen Lebensbereichen des Betroffenen zur Kenntnis. Die umfassende Bearbeitung vieler unterschiedlicher Aufgaben durch einen einzelnen Behördenmitarbeiter birgt die Gefahr in sich, dass der Betroffene zum „gläsernen Menschen“ wird.

Beim Umgang mit den Daten ist im Rahmen der gesetzlichen Aufgabenerfüllung der Grundsatz der Zweckbindung zu beachten. Dementsprechend muss der Mitarbeiter zwischen den einzelnen Aufgaben trennen, für die er die Daten erhebt, verarbeitet und nutzt. In den Fällen, in denen Mitarbeiter verschiedene Aufgaben in Personalunion erledigen, ist dies kaum zu realisieren.

Daher sollten insbesondere verschiedene Aufgabenbereiche, die zu Interessenkonflikten führen können, nicht einem einzelnen Mitarbeiter übertragen werden. Um zu verhindern, dass der Grundsatz der Zweckbindung ausgehöhlt wird, sind eine getrennte Akten- und Dateienführung sowie die Vergabe differenzierter Zugriffsrechte vorzusehen. Darüber hinaus ist eine ordnungsgemäße Protokollierung die Voraussetzung für eine wirksame Datenschutzkontrolle.

Sensible Bereiche, wie steuerrechtliche und soziale Angelegenheiten, sollten grundsätzlich nicht in das Bürgerbüro integriert werden, da diese Daten einem besonderen Schutz unterliegen. Aus diesen Bereichen kommen lediglich Aufgaben in Betracht, die ohne personenbezogene Daten zu erledigen sind oder bei denen weniger sensible Daten anfallen. Dazu zählen unter anderem auch Auskünfte zu allgemeinen sozialen Fragen - ohne die konkrete Einzelfallbearbeitung - sowie das Bereithalten von Antragsformularen.

Das Bürgerbüro sollte über eine Diskretionszone sowie einen Wartebereich, der deutlich vom Servicebereich abgegrenzt ist, verfügen. Es ist sicherzustellen, dass Dritte keine Gespräche mithören und auch keine personenbezogenen Daten zur Kenntnis nehmen können. Geeignet dazu wäre unter anderem eine besondere Akustikgestaltung. Aber auch Stellwände oder Raumteiler kämen in Frage. Obwohl die vorgenannten sensibleren Bereiche grundsätzlich nicht im Bürgerbüro bearbeitet werden sollen, sollten auch Zimmer für Einzelgespräche zur Verfügung stehen, weil solche in Ruhe und besonders geschützter Atmosphäre erforderlich sein können.

Die Bürger sollten durch einen gut sichtbaren Aushang darauf hingewiesen werden, dass sie zwischen der Bearbeitung im Fachamt und einer Beratung im Bürgerbüro, gegebenenfalls auch im Einzelzimmer, wählen können.

Vor der Einrichtung eines Bürgerbüros ist in jedem Fall eine Konzeption zu erarbeiten, auf deren Grundlage die anstehenden datenschutzrechtlichen Fragestellungen sachgerecht gelöst werden müssen. Dabei ist darauf zu achten, dass die Einrichtung des Bürgerbüros zu keiner datenschutzrechtlichen Verschlechterung für den Betroffenen im Vergleich zur bisherigen Verwaltungsorganisation führt.

3.6 Datenübermittlung in Planfeststellungsverfahren

Zum Planfeststellungsverfahren für die Magnetschwebebahn von Hamburg nach Berlin erhielt ich von mehreren Bürgern Anfragen. Ein Amt hatte ein Formblatt für Einwendungen erstellt, mit dem neben der Art der Bedenken auch der Beruf des Einwenders sowie sein Status (Eigentümer/Bewohner/Nutzer) im Hinblick auf das betroffene Grundstück erfragt wurden. Darüber hinaus äußerten Bürger Bedenken gegen die Übermittlung personenbezogener Daten an den Vorhabenträger.

Der Vordruck des Amtes entsprach tatsächlich nur teilweise den datenschutzrechtlichen Bestimmungen. Auch im Planfeststellungsverfahren dürfen nur die Daten erhoben, verarbeitet und genutzt werden, die zu dessen Durchführung erforderlich sind. Angaben zum Beruf einzelner Einwender gehören nicht dazu. Nur in Fällen, in denen gleichförmige Einwendungen von mehr als 50 Personen erhoben werden, ist ein Vertreter nach § 17 Verwaltungsverfahrensgesetz mit Namen, Beruf und Anschrift zu benennen. Angaben zum Status des Betroffenen sind nur dann erforderlich, wenn diese im weiteren Verfahren relevant werden, weil sich beispielsweise an die Eigentümerstellung bestimmte Rechte knüpfen. Hierauf habe ich die Anhörungsbehörde, die zu dieser Frage Informationen herausgegeben hat, hingewiesen.

In Vorbereitung des Erörterungstermins werden dem Vorhabenträger die Einwendungen übermittelt, damit dieser hierzu Stellung nehmen und bestehende Bedenken ausräumen oder gegebenenfalls berücksichtigen kann. Mangels bereichsspezifischer Regelungen ist die Zulässigkeit der Datenübermittlung nach den allgemeinen datenschutzrechtlichen Bestimmungen zu beurteilen. Dabei ist zu prüfen, ob die Übermittlung personenbezogener Daten für die Stellungnahme des Vorhabenträgers erforderlich ist.

In den Fällen, in denen die Beeinträchtigung einer individuellen Rechtsposition vorgetragen wird, lässt sich eine sachgerechte Erörterung nur realisieren, wenn der Vorhabenträger auf die persönlichen Belange der Einwender eingeht. Daher ist in diesen Fällen eine Übermittlung personenbezogener Daten an den Vorhabenträger erforderlich. Werden hingegen allgemeine Bedenken formuliert, etwa „aus Gründen des Naturschutzes“, ist dies nicht notwendig. Im Ergebnis ist somit eine Übermittlung personenbezogener Daten im Planfeststellungsverfahren nur zulässig, wenn der Vorhabenträger die Einwendungen personenbezogen kennen muss, um die konkret betroffenen individuellen Belange des Einwenders zu berücksichtigen. Dies ist in jedem Einzelfall durch die Anhörungsbehörde zu prüfen.

Ich habe der Anhörungsbehörde daher eine differenzierte Verfahrensweise empfohlen, die den datenschutzrechtlichen Belangen des Einzelnen Rechnung trägt.

Das Wirtschaftsministerium unseres Landes hat zu den Empfehlungen Stellung genommen und ausgeführt, dass eine differenzierte Verfahrensweise zu einem unverhältnismäßig hohen Aufwand führen würde. Die Anonymisierung der personenbezogenen Daten in den Einzelfällen sei der Anhörungsbehörde nicht zuzumuten. Daher wäre nach Auffassung des Wirtschaftsministeriums die konkludente Einwilligung des Einwenders in eine Übermittlung seiner personenbezogenen Daten angemessen. Dazu sollte in der öffentlichen Bekanntmachung zum Planfeststellungsverfahren auf die datenschutzrechtlichen Bestimmungen hingewiesen werden. Die Einwendung wäre dann gleichzeitig als Einwilligung in die Datenübermittlung zu sehen. In der Veröffentlichung müsste auch hierüber sowie über die Möglichkeit des Widerspruches gegen die personenbezogene Übermittlung der Daten informiert werden.

Das entscheidende Kriterium bei der Datenübermittlung ist jedoch die Erforderlichkeit. Der Vorhabenträger muss beurteilen können, in welcher Weise individuelle Rechtsgüter des Einwenders betroffen sind. In allen anderen Fällen scheidet eine Datenübermittlung mangels Erforderlichkeit aus. Ein Rückgriff auf die Einwilligung kommt nur ausnahmsweise in Frage, wenn es an einer entsprechenden Regelung mangelt. Hier scheidet jedoch eine Datenübermittlung bereits nach den allgemeinen datenschutzrechtlichen Bestimmungen aus, so dass kein Raum für die Anwendung einer Einwilligung bleibt. Zu prüfen wäre in diesem Zusammenhang auch, ob diese Frage nicht bereichsspezifisch im Verwaltungsverfahrensgesetz geregelt werden sollte.

Ich habe das Wirtschaftsministerium daher gebeten, seine Rechtsauffassung nochmals zu überdenken. Eine Antwort ist das Ministerium bis heute leider schuldig geblieben.

3.7 Volkszählung

In der Europäischen Union (EU) soll im Jahre 2001 eine Volks- und Wohnungszählung stattfinden (siehe dazu ausführlich Dritter Tätigkeitsbericht, Punkt 3.9.1). Dazu existiert eine Leitlinie der EU, die jedoch im Gegensatz zu der ursprünglich geplanten EG-Verordnung lediglich empfehlenden Charakter hat. Deutschland wird für diesen Zensus weder eine aufwendige Bevölkerungsbefragung durchführen noch ein neues Verfahren entwickeln, sondern der EU Daten aus vorhandenen Statistiken und einem zeitnahen Mikrozensus liefern.

In Deutschland ist eine Volkszählung im Zeitraum 2004 bis 2006 geplant. Auch für diesen Zensus ist - anders als bei der letzten Zählung im Jahre 1987 - keine Bevölkerungsbefragung, sondern die Auswertung von Registern der Verwaltung, insbesondere der Melderegister, vorgesehen. Um festzustellen, ob die Fehlerquote bei den Registern nicht zu hoch ist und ob das Verfahren hinreichend genaue Ergebnisse liefern kann, soll es jedoch Testerhebungen geben. Es ist vorgesehen, für diesen Test im Jahr 2000 ein eigenes Gesetz zu verabschieden.

Nach den bisher bekannt gewordenen Einzelheiten sind Vorgehensweisen geplant, die in das Recht auf informationelle Selbstbestimmung eingreifen und daher einer eingehenden Prüfung ihrer verfassungsrechtlichen Zulässigkeit bedürfen:

- Speziell für die Volkszählung soll ein Teil der Register auf eventuell vorhandene Fehler überprüft werden. Dafür sind die in diesen Registern enthaltenen personenbezogenen Daten mit Angaben aus anderen Quellen zu vergleichen und gegebenenfalls zu ändern. Dieser Umgang mit personenbezogenen Daten ist kritisch zu hinterfragen, weil die Register ausschließlich für den Zweck des Verwaltungsvollzugs angelegt worden sind.

- Die verschiedenen Register sollen anhand der in ihnen enthaltenen personenbezogenen Daten gegeneinander abgeglichen werden. Dadurch könnten aussagekräftige Persönlichkeitsprofile entstehen. Auch hier ist zu untersuchen, ob die vorgesehenen Abgleiche durch den statistischen Zweck gerechtfertigt sind.

- Der Abgleich soll zentral im Statistischen Bundesamt erfolgen, wozu alle Registerdaten dorthin übermittelt und anschließend zusammengeführt werden. So entsteht für einen bestimmten Zeitraum in einer Stelle eine einmalige, sämtliche Einwohner der Bundesrepublik Deutschland umfassende Datensammlung. Diese Vollständigkeit und die unbegrenzten Möglichkeiten zur Verknüpfung und Auswertung der Daten rufen starke Bedenken gegen diese Sammlung hervor, auch wenn sie in dem vom Verwaltungsvollzug abgeschotteten und durch ein besonderes Amtsgeheimnis geschützten Bereich der Statistik vorgehalten wird. Es ist daher zu prüfen, ob nicht eine weniger einschneidende, abgestufte Vorgehensweise verbunden mit einer dezentralen Datenhaltung möglich ist. Im Hinblick auf den Grundsatz der Verhältnismäßigkeit sind unter Umständen auch Abstriche an den Auswertungsmöglichkeiten hinzunehmen.

- Bei der Zusammenführung der verschiedenen Register wird es aufgrund der vorhandenen Fehler sehr wahrscheinlich zu Widersprüchlichkeiten kommen. Ob eine Klärung durch Rückfragen bei den entsprechenden Stellen in Betracht kommt, ist fraglich, da dies das strikte Gebot zur Trennung von Statistik und Verwaltungsvollzug berühren würde.

Sobald konkrete und verbindliche Angaben zum Verfahren und zum Inhalt des Entwurfs für ein Testgesetz vorliegen, werden sich die Datenschutzbeauftragten des Bundes und der Länder eingehend mit dieser Materie befassen.

3.8 Telekommunikation und Medien

3.8.1 Telekommunikations-Datenschutzverordnung

Das Telekommunikationsgesetz (TKG) (siehe Dritter Tätigkeitsbericht, Punkt 3.10.2) verpflichtet die Bundesregierung zum Erlass einer Rechtsverordnung zum Schutz personenbezogener Daten der an der Telekommunikation Beteiligten. Die Vorschrift richtet sich an Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen. Diese neue Telekommunikations-Datenschutzverordnung **(**TDSV**)** soll die gegenwärtig geltende TDSV ablösen. Zwischen dieser Norm und dem TKG bestehen teilweise Unterschiede im Anwendungsbereich und in den Regelungen (siehe Dritter Tätigkeitsbericht, Punkt 3.10.4). Außerdem berücksichtigt die noch geltende TDSV nicht hinreichend die Telekommunikationsrichtlinie (ISDN-Richtlinie) der EG, die bis zum 24. Oktober 1998 hätte umgesetzt werden müssen (siehe Dritter Tätigkeitsbericht, Punkt 3.10.1).

Aufgrund dieser Sachlage besteht ein dringender Bedarf für eine neue TDSV. Das Bundesministerium für Wirtschaft und Technologie hat dazu verschiedene Referentenentwürfe vorgestellt. Der letzte Entwurf stammt vom 21. Oktober 1999. Er übernimmt viele Vorschriften der geltenden TDSV, passt den Anwendungsbereich sowie die Rechtsfolgen an das TKG an und beinhaltet auch neue Normen zur Verbesserung des Datenschutzes im Telekommunikationsbereich, wozu insbesondere die folgenden Regelungen gehören:

- Es wird klargestellt, dass Ausweiskopien nach Durchführung der für den Vertragsschluss erforderlichen Identitätsprüfung zu vernichten sind.

- Der Angerufene muss die Möglichkeit haben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den Anrufenden unterdrückt wurde, auf einfache Weise und unentgeltlich abzuweisen (so genanntes „Block-Blocking“).

- Die Vorschriften über die Rufnummernanzeige und deren Unterdrückung gelten auch für Verbindungen mit dem Ausland.

- Einwilligungen können auch elektronisch erklärt werden.

- Es werden Ordnungswidrigkeitentatbestände zur Durchsetzung einzelner Datenschutzregelungen aufgenommen.

Leider enthält der Entwurf auch viele aus Sicht des Datenschutzes bedenkliche Regelungen und sogar Vorschriften, die eine deutliche Verschlechterung des Datenschutzniveaus im Vergleich zur geltenden TDSV bedeuten. Gegenüber unserem Wirtschaftsministerium habe ich zum Entwurf der TDSV Stellung genommen und dabei vor allem folgende Regelungen kritisiert:

- Die in der geltenden TDSV enthaltene Hinweispflicht auf etwaige Gefährdungen der Netzsicherheit ist gestrichen worden. Der Nutzer hat somit keine Möglichkeit, sein Telekommunikationsverhalten einer realistischen Einschätzung der Netzsicherheit anzupassen und entsprechende eigene Vorkehrungen zum Schutz seiner Daten zu treffen. Die Hinweispflicht sollte daher wieder aufgenommen werden.

– Es fehlt ein ausdrücklicher Erforderlichkeitsvorbehalt für die Befugnis zur Verarbeitung von personenbezogenen Daten bei der Ermittlung und Abrechnung der Entgelte durch die Anbieter von Telekommunikationsdienstleistungen. So könnte etwa die Standortkennung im Mobilfunk selbst dann verarbeitet werden, wenn sie für die Entgeltberechnung nicht benötigt würde.

– Mit Nachdruck empfehlen die Datenschutzbeauftragten die Realisierung des so genannten Holländischen Modells, bei dem niemand ohne seine ausdrückliche Einwilligung in Einzelverbindungsnachweise aufgenommen wird. Dies würde auch wesentlich einfacher und effektiver als das im Entwurf vorgesehene aufwendige Antragsverfahren verhindern, dass Anrufer bei Beratungsstellen in deren Einzelverbindungsnachweisen aufgeführt werden.

– Im Gegensatz zur aktuellen Regelung (ein Monat) dürfen nun alle Verbindungsdaten der letzten sechs Monate für die Missbrauchsbekämpfung - beispielsweise zur Verhinderung einer illegalen kostenlosen Leitungsnutzung - verarbeitet werden. Dies ist viel zu weitgehend und ebensowenig akzeptabel wie die Tatsache, dass hiervon Betroffene nicht mehr benachrichtigt werden müssen.

– Wenn ein Anschlussinhaber schlüssig vorträgt, dass er bedrohende oder belästigende Anrufe erhält, dürfen ihm bestimmte Verbindungsdaten der bei ihm eingegangenen Anrufe mitgeteilt werden. Nach dem Entwurf soll dies sogar für Anrufe gelten, die zeitlich vor seiner Meldung lagen. Diese so genannte rückwirkende Fangschaltung stellt einen schweren Eingriff in das Fernmeldegeheimnis der Anrufer dar und sollte daher generell ausgeschlossen werden.

– Nach der aktuellen TDSV ist dem Anrufer anzuzeigen, wenn sein Anruf an einen anderen Anschluss weiter geschaltet wird. Der Entwurf sieht eine solche Regelung nicht mehr vor. Diese Streichung stellt für die Anrufer eine nicht hinnehmbare Gefährdung ihrer Persönlichkeitsrechte dar. Die Signalisierungspflicht muss deshalb auch in der neuen TDSV enthalten sein.

Ich habe unser Wirtschaftsministerium gebeten, meine Änderungsvorschläge bei der Bund-Länder-Abstimmung des Entwurfs einzubringen. Die Antwort des Ministeriums steht noch aus.

3.8.2 Datenschutzbestimmungen im Rundfunkrecht

Dem Landtag liegt ein Gesetzentwurf zur Änderung rundfunkrechtlicher Vorschriften im Land Mecklenburg-Vorpommern vor. Es soll am 1. April 2000 in Kraft treten. Der Entwurf hat die Form eines Artikelgesetzes und beinhaltet als Artikel 1 das Zustimmungsgesetz zum Vierten Rundfunkänderungsstaatsvertrag (4. RfÄndStV), über den die Regierungschefs der Länder Einvernehmen erzielt haben, und als Artikel 2 die Novellierung und Neubekanntmachung des Landesrundfunkgesetzes (RundfG M-V). Der 4. RfÄndStV ändert den Rundfunkstaatsvertrag über den öffentlichen Rundfunk, das RundfG M-V regelt den privaten Rundfunk in Mecklenburg-Vorpommern und die Weiterverbreitung vorhandener Rundfunkprogramme in Kabelanlagen.

Ein wesentlicher Bestandteil der Änderungen ist die Einführung von Datenschutzbestimmungen in das Rundfunkrecht, die unter anderem folgende wichtige Regelungen beinhalten:

- Der Nutzer ist ausführlich über den Umgang mit seinen Daten zu unterrichten.

- Technische Einrichtungen sind so zu gestalten, dass nur die für die Dienstleistung unbedingt erforderlichen personenbezogenen Daten anfallen können.

- Soweit möglich, ist auch ein anonymes oder pseudonymes Nutzungs- und Bezahlungsverfahren anzubieten.

- Nutzungsprofile sind nur in pseudonymisierter Form zulässig.

Die Vorschriften stimmen - bis auf die notwendigen Anpassungen für den Rundfunkbereich - meist wörtlich mit den Datenschutznormen im Mediendienstestaatsvertrag und im Teledienstedatenschutzgesetz überein. Im Dritten Tätigkeitsbericht unter Punkt 2.2 habe ich diese Regelungen ausführlich dargestellt. Ihnen liegen entsprechende Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahre 1996 zu Grunde.

Wenn der Entwurf so verabschiedet wird, würde er einen großen Fortschritt für den Datenschutz im Rundfunkbereich in unserem Lande bedeuten.

3.9 Finanzwesen

3.9.1 Detektiv verfolgt Hund

Viele Kommunen versuchen, vorhandene Steuerquellen intensiver zu nutzen, so auch die Hundesteuer. Private Unternehmer haben darauf mit dem Angebot einer neuen Dienstleistung reagiert - der Durchführung von so genannten Hundebestandsaufnahmen. Dabei fragen Mitarbeiter der Privatunternehmen im Auftrag der Kommune „an der Haustür“ nach, ob im jeweiligen Haushalt Hunde gehalten werden. Die Ergebnisse werden mit den Listen der gemeldeten Hundesteuerpflichtigen bei der Kommune verglichen. Ergibt sich dabei, dass einzelne Bürger ihre Hunde nicht angemeldet haben, kann die Steuerverwaltung der Kommune gezielt tätig werden.

Kommunen und Dienstleister haben mich gebeten, dieses Vorgehen aus datenschutzrechtlicher Sicht zu prüfen. Zunächst einmal habe ich festgestellt, dass nach den geltenden Hundesteuersatzungen nicht einmal die Mitarbeiter der Kommunen berechtigt sind, solche Befragungen durchzuführen. Hierzu ist eine ausdrückliche Erlaubnis erforderlich, da die allgemeinen abgabenrechtlichen Regelungen keine hinreichende Grundlage bieten.

Wie weit die Beauftragung Privater mit Tätigkeiten für die Verwaltung zulässig ist, ist eine grundsätzliche Frage, zu der ich mich bereits im Zusammenhang mit der Frage der Geschwindigkeitsmessung durch Private geäußert habe (siehe Zweiter Tätigkeitsbericht, Punkt 2.4.3 und Dritter Tätigkeitsbericht, Punkt 3.3.1).

Entsprechend den dort dargestellten Grundsätzen dürfen Privatunternehmen bei einer Befragung von Bürgern, die im Rahmen der Steuerverwaltung erfolgt, nur Hilfstätigkeiten ausüben und nicht im Kernbereich der Steuerverwaltung tätig werden.

So ist zum Beispiel der Abgleich der Befragungsergebnisse mit den Listen der Hundesteuerpflichtigen nur durch die Kommune selbst vorzunehmen. Die Mitarbeiter der Unternehmen müssen sich darauf beschränken, die einzelnen Bürger - und zwar nur Erwachsene - anzusprechen und um Auskunft darüber zu bitten, ob sie Eigentümer eines Hundes sind. Die Bürger sind jedoch ihnen gegenüber nicht zu Auskünften verpflichtet.

Darauf müssen die Befragenden selbst und ungefragt hinweisen. Sie haben auch keinesfalls ein Zutrittsrecht zur Wohnung des Befragten und dürfen im Übrigen auch nicht gezielt nach Anzeichen für das Vorhandensein von Hunden suchen. Den Mitarbeitern der Privatunternehmen ist es auch nicht erlaubt, eigene „detektivische Ermittlungen“ anzustellen oder Bußgelder festzusetzen.

Soll ein Dienstleister den Hundebestand aufnehmen, so ist dafür eine ausdrückliche Ermächtigung in der Hundesteuersatzung erforderlich. Außerdem ist ein schriftlicher Auftrag zu erteilen, der den Voraussetzungen des § 4 DSG MV entspricht. Die Mitarbeiter des Auftragnehmers sind auf das Datengeheimnis zu verpflichten.

Eine der betroffenen Kommunen hat den mit dem Dienstleister abzuschließenden Vertrag meinen Hinweisen folgend geändert. Gegenüber dem Innenministerium habe ich eine Überarbeitung des Musterentwurfes zur Hundesteuer entsprechend den oben genannten Empfehlungen angeregt und gebeten, die Hinweise bei der künftigen Genehmigung von Hundesteuersatzungen zu beachten.

3.9.2 Pfändungsverfügung ins Blaue

Ein Petent hat mich gebeten, das Vollstreckungsverfahren von Geldforderungen einer Amtsverwaltung zu prüfen.

Die Verwaltung hatte Pfändungsverfügungen an in der Umgebung ansässige Kreditinstitute versandt, ohne zu wissen, ob der Vollstreckungsschuldner überhaupt in Beziehung zu diesen stand.

Diese Verfahrensweise ist unzulässig. § 309 (AO) lässt die Pfändung von Geldforderungen durch Pfändungsverfügungen zu und ist auch für die Vollstreckung öffentlich-rechtlicher Geldforderungen im kommunalen Bereich anzuwenden. Die Pfändungsverfügung verbietet dem Kreditinstitut dann, Zahlungen an den Vollstreckungsschuldner zu leisten. Das Kreditinstitut ist verpflichtet, binnen zwei Wochen eine Erklärung abzugeben, ob und inwieweit die in der Verfügung bezeichnete Forderung durch das Kreditinstitut als begründet anerkannt wird und ob gegebenenfalls andere Personen oder Stellen Anspruch auf diese Forderung erhoben oder diese bereits gepfändet haben.

Beim Versenden der Pfändungsverfügungen war in diesem Fall jedoch nicht bekannt, mit welchem Kreditinstitut der Vollstreckungsschuldner in Geschäftsbeziehung steht. Das sollte mit diesem Vorgehen unter anderem überhaupt erst geprüft werden. Allerdings führt dieses Verfahren im Ergebnis dazu, dass mehrere Stellen von der Pfändung Kenntnis erhalten, obwohl dies nicht erforderlich ist. Der Grundsatz der Verhältnismäßigkeit sowie das Verbot der zwecklosen Pfändung stehen einem solchen Verfahren entgegen. Der damit verbundene Eingriff in das Recht auf informationelle Selbstbestimmung ist durch keine Rechtsgrundlage gedeckt. Darauf habe ich hingewiesen.

Die Amtsverwaltung wird künftig nur noch Pfändungsverfügungen zustellen, wenn Anhaltspunkte vorliegen, die auf eine Geschäftsbeziehung zwischen Vollstreckungsschuldner und Kreditinstitut schließen lassen.

3.9.3 Haushalts-, Kassen- und Rechnungswesen

Verantwortlich für den Einsatz des Softwareprodukts PROfiskal im Haushalts-, Kassen- und Rechnungswesen ist das Finanzministerium. Es bedient sich der Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) als Auftragnehmerin. Zu den verschiedenen datenschutzrechtlich relevanten Aspekten, die sich bei einem solchen Vorhaben zwangsläufig ergeben, habe ich schon vor einiger Zeit Empfehlungen gegeben (siehe Dritter Tätigkeitsbericht, Punkt 3.11.3).

Schwerpunkte im Berichtszeitraum waren das Datenschutz- und IT-Sicherheitskonzept, die Echtdatentests sowie die Einführung der elektronischen Kassenanordnung.

Datenschutz- und IT-Sicherheitskonzept

Im Jahr 1999 gab es Gespräche mit dem Finanzministerium und der DVZ M-V GmbH sowie detaillierte Hinweise zur Änderung und Ergänzung der aktuellen Version des Handbuches für das Datenschutz- und IT-Sicherheitskonzept.

So wurde mit Mitarbeitern der DVZ M-V GmbH eingehend über den Änderungsbedarf im Handbuch gesprochen. Trotz teilweise verschiedener Ansichten im Einzelnen wurde dabei deutlich, dass die von der DVZ M-V GmbH in ihrem Bereich getroffenen technischen und organisatorischen Maßnahmen einen Schutzstandard gewährleisten, der der Sensibilität der verarbeiteten personenbezogenen Daten angemessen ist. Hier geht es im Wesentlichen darum, die Funktion des Handbuches als Grundlage der in den Räumen der DVZ M-V GmbH realisierten Schutzmaßnahmen deutlicher zu machen und dabei die Linie von den Grundsätzen und Anforderungen des Datenschutzes über die Gefährdungsanalyse und das Sicherheitskonzept bis hin zur Umsetzung und Kontrolle der Maßnahmen schlüssiger und nachvollziehbarer zu gestalten.

Die Gewährleistung von Sicherheit ist ein dynamischer Prozess. Deshalb ist es auch möglich, dass die vorgeschlagenen Änderungen zu Neubewertungen einzelner Szenarien führen und dann auch andere Maßnahmen erforderlich machen. Angesichts des hohen Schutzniveaus, das die DVZ M-V GmbH in technischer und organisatorischer Hinsicht erfahrungsgemäß bietet, dürften aber Änderungen der Sicherheitsvorkehrungen in absehbarer Zeit nur in geringem Maße nötig sein.

Schwieriger ist die Situation bei den PROfiskal-Arbeitsplätzen in der Finanzverwaltung. Ursprünglich war vorgesehen, auf den entsprechenden Endgeräten keine anderen Anwendungen zu betreiben. Tatsächlich laufen aber auf den eigentlich PROfiskal vorbehaltenen Rechnern auch andere Anwendungsprogramme. Auf diesen Computern können teilweise Administrationsaufgaben für PROfiskal und sogar für andere Anwendungen durchgeführt werden, die Auswirkungen auf PROfiskal haben. Das Handbuch selbst macht aber fast keine konkreten Aussagen zur Netz- und Endgerätesicherheit. Insofern besteht dringender Handlungsbedarf.

Test mit Echtdaten

Im Dezember 1999 teilte mir das Finanzministerium mit, dass die DVZ M-V GmbH bei den verschiedenen Versionsänderungen der Software PROfiskal Laufzeittests mit Echtdaten plant. Sie sollen unabhängig von den Ergebnissen der Prüfungen auf der Testdatenbank und parallel zu diesen laufen.

Tests mit Echtdaten sind nur im Einzelfall und in engen Grenzen zulässig, insbesondere sollten sie nur dann erfolgen, wenn alle übrigen Prüfungen positiv verlaufen sind (siehe Dritter Tätigkeitsbericht, Punkt 3.11.3). Außerdem sind Vorabprüfungen mit Testdaten auch aus anderem Grunde wichtig. Nur mit ihnen können konkrete vielschichtige Fallkonstellationen erzeugt und komplexe Fehlermuster analysiert werden, die in der Echtdatenbank in der Regel so nicht verfügbar sind.

Ich habe daher empfohlen, von den geplanten parallelen Laufzeittests abzusehen und generell erst dann mit Echtdaten zu arbeiten, wenn aufgrund der umfassenden Prüfung mit Testdaten von einer im Wesentlichen fehlerfreien Funktion des einzusetzenden Programmes ausgegangen werden kann.

Das Finanzministerium unterrichtete mich darüber, dass die Tests zur Vorbereitung der nächsten PROfiskal-Version in folgender Reihenfolge durchgeführt werden:

1. Prüfung mit Testdatenbank,
2. Test des Laufzeitverhaltens mit Echtdatenbank,
3. Prüfung der Funktionalitäten, die auf der Testdatenbank nicht geprüft werden können, mit den vorhandenen Echtdaten.

Einführung der elektronischen Kassenanordnung

Das Finanzministerium hat im Jahr 1998 über eine Ausschreibung für eine Machbarkeitsstudie zur Einführung der elektronischen Kassenanordnung berichtet. Bei dem Verfahren sollen auch Methoden der digitalen Signatur (siehe Dritter Tätigkeitsbericht, Punkt 2.2) und moderne Techniken der Nutzeridentifikation eingesetzt werden. Des Weiteren weist das Ministerium in der Ausschreibung auf die Forderung der Datenschutzbeauftragten nach dem Einsatz kryptographischer Verfahren beim elektronischen Datentransport hin. Die DVZ MV GmbH betont in ihrer Studie die entscheidende Wichtigkeit von Authentizität (Feststellbarkeit des Urhebers) und Integrität (Unverfälschtheit) der Daten und gelangt unter anderem zu folgenden Ergebnissen:

- Erst der Einsatz von Mitteln, die dem Signaturgesetz entsprechen, gewährleistet langfristig die Anforderung an Datenschutz und Datensicherheit.

- Die Anwendung von Verfahren, die nicht signaturgesetzkonform sind, wird nicht empfohlen. Dies ist zunächst aus rechtlichen, aber auch zunehmend aus wirtschaftlichen Gesichtspunkten begründbar.

Diese Bewertung der DVZ M-V GmbH teile ich. Daher habe ich das Finanzministerium gebeten, die elektronische Kassenanordnung nicht einzuführen, ohne Methoden der digitalen Signatur und kryptographische Verfahren zur Gewährleistung des Datenschutzes und der Datensicherheit zu verwenden. Das Ministerium teilte mir mit, dass elektronische Kassenanordnungen noch nicht erfolgen, da die technischen Voraussetzungen nicht bestehen.

Ich habe das Finanzministerium gebeten, mich über die Planungen und Entwicklungen für PROfiskal in unserem Lande auf dem Laufenden zu halten und mich insbesondere vor der Einführung von Informations- und Kommunikationstechniken, mit denen personenbezogene Daten verarbeitet werden, rechtzeitig zu unterrichten.

3.9.4 Muss man bei Sterbefällen Vermögensangaben machen?

Ein Standesamt verlangte von einem Bestattungsunternehmen, das Formular „Ergänzende Angaben zum Sterbefall“ auszufüllen, in dem unter anderem auch Angaben zu Inhalt und Umfang des Nachlasses gefordert wurden. Andernfalls könne keine Sterbeurkunde ausgestellt werden.

Die relevanten Vorschriften hierfür sind §§ 34 und 36 Erbschaftsteuer- und Schenkungsteuergesetz in Verbindung mit der Erbschaftsteuer-Durchführungsverordnung.

Nach diesen Bestimmungen können die Daten über den Nachlass prinzipiell zu Steuerzwecken erhoben werden. Zuvor sind die Betroffenen aber über den Zweck der Angaben aufzuklären. Außerdem sind sie nicht verpflichtet, die in dem Ergänzungsbogen vorgesehenen sensiblen Angaben zu machen. Dies habe ich unserem Innenministerium als oberster Standesamtaufsicht mitgeteilt.

Das Ministerium hat die Ausführungen zum Anlass genommen, die unteren Standesamtaufsichtsbehörden darauf hinzuweisen, dass

- die Standesbeamten die „Ergänzenden Angaben zum Sterbefall“ von den den Sterbefall anzeigenden Personen nicht verlangen dürfen,

- sie keine eigenen Ermittlungen durchführen dürfen, sondern dies der Finanzverwaltung vorbehalten ist und

- sie die betroffenen Personen vor Beantwortung der Fragen darüber zu unterrichten haben, dass solche Angaben auch an die Finanzverwaltung übermittelt werden.

Somit wird gewährleistet, dass Angehörige nicht gegen ihren Willen gegenüber Standesbeamten Angaben zu Sterbefällen machen, die mehr Daten umfassen, als für standesamtliche Aufgaben benötigt werden.

3.9.5 Kein Konto ohne Ausweiskopie?

Bei einer Kontoeröffnung halten Kreditinstitute Angaben über die Identität des künftigen Kontoinhabers fest. Dieses Vorgehen folgt aus § 154 Abs. 2 Satz 1 der Abgabenordnung (AO). Die Bank oder Sparkasse kann sich dazu den Personalausweis oder den Reisepass des Antragstellers vorlegen lassen und daraus den vollständigen Namen, das Geburtsdatum und den Wohnsitz erfassen und speichern. Mit Einwilligung des Antragstellers kann sie statt dessen auch eine Kopie des Ausweises zu den Akten nehmen.

Die obersten Finanzbehörden des Bundes und der Länder meinen aber, § 154 Abs. 2 Satz 1 AO sei so zu verstehen, dass die Kreditinstitute verpflichtet seien, Kopien von den Ausweisen der Kontoinhaber vorzuhalten. Dies würde dazu führen, dass Banken und Sparkassen über die oben genannten Daten hinaus auch Daten erheben, die sie zur Erfüllung ihrer Aufgaben nicht benötigen.

Auf meine Anfrage hin hat das Finanzministerium Mecklenburg-Vorpommern erklärt, eine Überprüfung der Identität des Kontoinhabers wäre ohne Ausweiskopie wesentlich erschwert beziehungsweise nicht mehr möglich. Eine andere Auslegung würde zudem gegen Artikel 4 der so genannten Geldwäscherichtlinie der EG (zu EG-Richtlinien allgemein siehe Punkt 2.4) verstoßen, da diese Bestimmung zwingend vorschreibe, dass vor jeder Kontoeröffnung ein Ausweis des Kunden zu kopieren sei.

Nicht ersichtlich ist allerdings, warum eine Personenüberprüfung wesentlich erschwert oder gar unmöglich sein soll, wenn keine Ausweiskopie vorliegt, aber Namen, Geburtsdatum und Wohnsitz erfasst wurden. Mit diesen Daten kann eine Person in nahezu allen Fällen eindeutig identifiziert werden. Unverständlich ist die Behauptung des Ministeriums, die Geldwäscherichtlinie fordere das Anfertigen von Ausweiskopien, denn in deren Artikel 4 heißt es: „Die Mitgliedstaaten [der EG] sorgen dafür, dass die Kredit- und Finanzinstitute ... von den zur Feststellung der Identität verlangten Dokumenten eine Kopie oder Referenzangaben ... aufbewahren.“ Dem eindeutigen Wortlaut nach sind die Mitgliedstaaten somit keineswegs verpflichtet, von den Kreditinstituten das Anfertigen von Kopien zu verlangen. Sie müssen lediglich veranlassen, dass die die Person identifizierenden Angaben erfasst werden.

Das Bundesfinanzministerium wirkt auf eine Neufassung des § 154 Abs. 2 AO hin, wonach die Kreditinstitute ausdrücklich verpflichtet werden sollen, soweit möglich Ausweiskopien von den Kontoinhabern anzufertigen. Diese „verschärfte Identifizierungspflicht“ ist bisher in bestimmten Fällen - etwa bei Finanztransaktionen ab 30.000,- DM - im Geldwäschegesetz, das die EG-Geldwäscherichtlinie umsetzt, vorgesehen. Eine Übernahme dieser Regelung in die Abgabenordnung ist mit deren ausschließlich steuerlicher Zielsetzung nicht zu vereinbaren. So hat nach höchstrichterlicher Rechtsprechung § 154 AO aufgrund seiner systematischen Stellung lediglich die Aufgabe, die formale Kontenwahrheit zu gewährleisten. Die beabsichtigte Ausweitung der Identifizierungspflicht für sämtliche Kontoeröffnungen führt zu einer nicht erforderlichen und damit unzulässigen Speicherung auf Vorrat, weil damit Daten erhoben und gespeichert werden, die zur Sicherung der Kontenwahrheit nicht benötigt werden. Die Anknüpfung der erweiterten Identifizierungspflicht zur Bekämpfung der Geldwäsche an eine Kontoeröffnung ist - gerade im Vergleich zu Finanztransaktionen von 30.000 DM und mehr - offensichtlich zu weitgehend und somit auch unverhältnismäßig, da die weit überwiegende Mehrzahl der Kontoinhaber nie eine Tat begehen wird, die als strafbare Geldwäsche beurteilt werden kann. Die angestrebte Gesetzesänderung ist deshalb insgesamt als unerlaubter Eingriff in das Recht auf informationelle Selbstbestimmung zu werten.

Ich habe unser Finanzministerium gebeten, sich im Rahmen der Bund-Länder-Abstimmung für eine Regelung einzusetzen, die klarstellt, dass die Kreditinstitute nur mit Einwilligung der Kontoinhaber deren Ausweise kopieren und ansonsten lediglich deren Namen, Geburtsdatum und Wohnsitz erfassen dürfen. Das Ministerium hat mitgeteilt, dass meine Bedenken im Rahmen des Gesetzgebungsverfahren zu § 154 AO erörtert werden.

3.9.6 Zweitwohnungssteuer

Gemeinden in Mecklenburg-Vorpommern haben, ebenso wie eine Vielzahl weiterer Kommunen im Bundesgebiet, Satzungen zur Erhebung einer Zweitwohnungssteuer erlassen. In der Öffentlichkeit haben diese Satzungen insbesondere deshalb Beachtung gefunden, weil sie zum Teil auch Gartenhäuser, Bootsschuppen und ähnliche Bauten in den Kreis der steuerpflichtigen Zweitwohnungen einbeziehen. Im Zusammenhang damit hat sich eine Kommune mit der Frage an mich gewandt, ob das Amt für Liegenschaften Daten über den Abschluss von Verträgen zur kleingärtnerischen Nutzung von Grund und Boden an das Steueramt der Stadt übermitteln darf. Diese Übermittlung sollte das Steueramt in die Lage versetzen, mögliche Steuerschuldner festzustellen.

Grundsätzlich sind auf eine Übermittlung personenbezogener Daten zur Steuererhebung die Regelungen der Abgabenordnung anzuwenden. Im vorliegenden Fall bieten diese jedoch keine Rechtsgrundlage. Weder ist ein Fall einer Auskunftspflicht nach der Abgabenordnung gegeben, da sich diese lediglich auf Verfahren in Sachen bestimmter (bekannter) Beteiligter bezieht. Noch kann auf die Grundsätze der Amtshilfe zurückgegriffen werden, da mit der Übermittlung eine Zweckentfremdung der ursprünglich für andere Zwecke erhobenenen Daten einhergeht und das Bundesverfassungsgericht bereits im Volkszählungsurteil einen amtshilfefesten Schutz gegen Zweckenfremdung gefordert hat.

Auch handelt es sich nicht um einen Fall einer zulässigen Zweckänderung personenbezogener Daten nach dem Landesdatenschutzgesetz von Mecklenburg-Vorpommern. Daher habe ich empfohlen, eine Bestimmung in die Satzung aufzunehmen, die die zu ermittelnden Daten sowie den Kreis derjenigen Personen, deren Daten übermittelt werden sollen, hinreichend bestimmt und somit eine Rechtsgrundlage für die beabsichtigte Datenübermittlung schafft.

Die mir später übermittelten Entwürfe für eine Änderung der Satzung über die Zweitwohnungssteuer enthalten eine ausführliche Regelung über die Erhebung personenbezogener Daten zur Ermittlung Steuerpflichtiger. Allerdings sollen danach neben kommunalen Behörden beispielsweise auch das Kraftfahrtbundesamt und das Bundeszentralregister Daten erhalten können. Sowohl das Straßenverkehrsgesetz wie auch das Bundeszentralregistergesetz enthalten jedoch abschließende Regelungen, die Zwecke und Adressaten von Datenübermittlungen der genannten Stellen festlegen. Diese Regelungen stehen nicht zur Disposition eines kommunalen Satzungsgebers.

Die geplante Satzung enthält noch eine Reihe weiterer zu kritisierender Regelungen. So ist beabsichtigt, die durch die Übermittlung gewonnenen Daten zur Berichtigung des Melderegisters zu verwenden. Dies wäre jedoch eine unzulässige Zweckdurchbrechung der Datenerhebung und ein Verstoß gegen das Steuergeheimnis, da die Voraussetzungen für eine Offenbarung dieser Steuerdaten nach der Abgabenordnung nicht gegeben sind. Vorgesehen sind außerdem umfangreiche Mitwirkungspflichten Dritter (insbesondere für Wohnungseigentümer, Hauptmieter, Kleingartenvereine) für den Fall, dass der Inhaber einer Zweitwohnung selbst seiner Verpflichtung zur Abgabe von Erklärungen über seine Steuerpflicht nicht nachkommt oder nicht zu ermitteln ist. Im Ergebnis würde dies dazu führen, dass sämtliche Eigentümer von Wohnungen in der Stadt die Daten aller Mieter übermitteln müssten, da eine vollständige Ermittlung eventuell Steuerpflichtiger anders nicht zu erreichen wäre. Dies ist auch deshalb bedenklich, weil es zum Entstehen eines zweiten Melderegisters führen und die im Landesmeldegesetz abschließend geregelte Mitwirkungspflicht des Wohnungsgebers ausdehnen würde. Ferner soll durch die neugefasste Satzung der Einsatz Privater zur Ermittlung von steuerrechtlich relevanten Daten erlaubt werden. Dagegen habe ich grundsätzliche Bedenken. Denn anders als im Fall der Hundebestandsaufnahme (siehe Punkt 3.9.1) würden sensible Daten in erheblichem Umfang erhoben und damit eine in den Kernbereich der kommunalen Steuerverwaltung hineinreichende Tätigkeit an Private übertragen werden.

Diese Hinweise habe ich der Stadt und dem Innenministerium übermittelt.
Nachdem die Stadt die Satzungsänderung dennoch unverändert beschlossen und dem Innenministerium zur Genehmigung vorgelegt hat, bleibt abzuwarten, ob dieses den Empfehlungen im Rahmen des Genehmigungsverfahrens Rechnung tragen wird. Eine Entscheidung war mir bis Redaktionsschluss nicht bekannt.

3.9.7 Elektronische Steuererklärung

Im Januar 1999 informierte mich unser Finanzministerium über die Absicht, Steuerpflichtigen und Steuerberatern in Mecklenburg-Vorpommern die Möglichkeit zu eröffnen, Steuererklärungen künftig in elektronischer Form zu erstellen und dem Finanzamt per Datenleitungen zu übermitteln. Basis hierfür ist das Softwareprojekt ELSTER (ELektronische STeuerERklärung), das von der EDV-Stelle des Finanzamtes München entwickelt wurde und bundesweit eingesetzt werden soll. Über eine eigene Homepage (www.elster.de) informiert die EDV-Stelle sehr ausführlich über das Projekt. Vom Finanzministerium erhielt ich einige Projektunterlagen und den Entwurf eines Sicherheitskonzeptes als Information zur vorgesehenen Einführung von ELSTER in Mecklenburg-Vorpommern.

Softwarepakete, mit denen die Steuererklärung beispielsweise zu Hause am eigenen Computer erstellt werden kann, existieren seit einigen Jahren. Um ELSTER möglichst einfach in diese bestehenden Verfahren verschiedener Anbieter zu integrieren, hat die EDV-Stelle München den Softwarebaustein „Telemodul“ entwickelt und für den bundesweiten Einsatz freigegeben. Verwendet nun eine Softwarefirma in ihrer Steuersoftware das kostenlos zur Verfügung stehende Telemodul, erübrigt sich das vom Landesdatenschutzgesetz geforderte Freigabeverfahren (vgl. § 17 Abs. 2 Nr. 10 DSG MV - Organisationskontrolle), und eine gesonderte Abnahme durch die Finanzverwaltung ist nicht mehr erforderlich.

Um die Vertraulichkeit der elektronisch übermittelten Steuerdaten zu gewährleisten, ist eine Verschlüsselung mit einem Verfahren vorgesehen, das die anerkannten kryptographischen Algorithmen Triple-DES und RSA nutzt. Die Oberfinanzdirektion Rostock (OFD) soll das Schlüsselpaar (geheimer und öffentlicher Schlüssel) für den RSA-Algorithmus erzeugen. Das hierfür entwickelte vertrauenswürdige Verfahren stellt sicher, dass der geheime Schlüssel, der zur Entschlüsselung der übermittelten Steuerdaten erforderlich ist, ausschließlich den zuständigen Stellen der Finanzverwaltung zugänglich ist. Der öffentliche Schlüssel wird an die EDV-Stelle München auf einem besonders gesicherten Weg übermittelt und in das Telemodul eingebunden. Somit steht er jedem Steuerpflichtigen zur Verschlüsselung seiner Daten zur Verfügung, nachdem er eine Steuersoftware mit integriertem Telemodul gekauft hat. Das gesamte Verfahren entspricht weitgehend den datenschutzrechtlichen Anforderungen. Ich habe lediglich noch empfohlen, für die Schlüsselerzeugung bei der OFD einen Personalcomputer zu verwenden, der nicht vernetzt ist und insbesondere über keinen Internetzugang verfügt. Der besonders sicherheitsrelevante Vorgang der Schlüsselerzeugung (siehe auch Punkt 3.16.3) könnte sonst möglicherweise nicht mehr ausreichend gegen Manipulationen geschützt werden.

Zusätzlich zu den elektronisch übermittelten Steuerdaten ist zurzeit noch eine papiergebundene, so genannte komprimierte Steuererklärung abzugeben, die auf dem Computer des Steuerpflichtigen automatisch erzeugt wird, wenn dieser die elektronischen Daten absendet. Das Finanzamt bearbeitet die Steuererklärung erst dann, wenn sowohl die elektronischen Daten als auch die komprimierte Steuererklärung vorliegen und wenn es die zusätzlich notwendigen Unterlagen (Lohnsteuerkarte, Belege, usw.) wie bisher auf konventionellem Weg erhalten hat.

Ziel der Finanzverwaltung ist die vollständig elektronische Steuererklärung. Da dann die komprimierte Steuererklärung entfällt, sind zusätzliche Sicherungsmaßnahmen nötig. Dazu ist vorgesehen, die Übermittung der elektronischen Steuerdaten mit einer elektronischen Unterschrift abzusichern.

Darüber hinaus wird erwogen, künftig auf die Zusendung der Lohnsteuerkarte zu verzichten und statt dessen die erforderlichen Lohnsteuerbescheinigungsdaten elektronisch vom Arbeitgeber übermitteln zu lassen. Die sicherheitstechnischen Rahmenbedingungen hierfür sind noch festzulegen. Beispielsweise müssen die Daten dem entsprechenden Steuerfall sicher zugeordnet werden können. Dazu wird ein eindeutiger und unveränderlicher Ordnungsbegriff benötigt. Da nach der Auffassung der Steuerverwaltung solche persönlichen Angaben wie Name und Geburtsdatum oder die Lohnsteuernummer dazu nicht geeignet sind, wurde vorgeschlagen, die Sozialversicherungsnummer jedes Steuerpflichtigen zu verwenden.

Gegen diese zweckentfremdete Verwendung der Sozialversicherungsnummer gibt es grundsätzliche rechtliche Bedenken. Die derzeitige Rechtslage lässt nur zu, diese Nummer im Zusammenhang mit der Erfüllung der gesetzlichen Aufgabe der Sozialversicherungsträger oder ihnen gleichgestellter Einrichtungen zu verwenden (§§ 18f, 18g Sozialgesetzbuch Viertes Buch - SGB IV). Auch von einer Änderung der Rechtslage ist hier meines Erachtens abzuraten, denn dieser Weg impliziert die Gefahr, dass die Sozialversicherungsnummer zu einem allgemeinen Personenkennzeichen wird. Das Bundesverfassungsgericht hat jedoch im Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65,1) klargestellt, dass ein solches Personenkennzeichen, das die Zusammenführung aller personenbezogenen Daten zu einem Gesamtbild ermöglichen könnte, mit dem Grundgesetz nicht zu vereinbaren wäre. Auch Zweckmäßigkeitserwägungen der Finanzverwaltung müssen demgegenüber zurückstehen, zumal auch Alternativen zur Verwendung der Sozialversicherungsnummer als Ordnungsbegriff existieren.

Weiterhin ist für das Projekt ELSTER zu klären, welche Rechtsgrundlage für das Verfahren maßgeblich ist. Es hält sich zwar an den durch § 150 Abs. 6 AO vorgegebenen Rahmen, die nach dieser Vorschrift erforderliche Rechtsverordnung fehlt bisher jedoch. Die Steueranmeldungs-Datenübermittlungs-Verordnung (StADÜV) genügt den Anforderungen jedenfalls nicht, unter anderem, weil sie weder Inhalt, Verarbeitung noch die Sicherung der zu übermittelnden Daten festlegt. Die Rechtsgrundlage für Steuererklärungen mit dem Verfahren ELSTER wäre also noch zu schaffen.

3.10 Soziales

3.10.1 Gesundheitsreform (GKV 2000) - neuer Ansatz für den Datenschutz

In der ersten Hälfte des Jahres 1999 hat die Bundesregierung den Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreform 2000) beschlossen. Der Gesetzentwurf sah vor, dass die Krankenkassen nun generell versichertenbezogene Daten verarbeiten und nutzen, um kontrollieren zu können, ob Leistungen wirtschaftlich sinnvoll erbracht werden. Dadurch wären die Krankenkassen in die Lage versetzt worden, Versichertenprofile anzulegen und den Patienten „gläsern“ zu machen. Der Bundesbeauftragte für den Datenschutz hat daher angeregt, eine gemeinsame Position der Datenschutzbeauftragten des Bundes und der Länder zu diesem Entwurf zu erarbeiten.

Eine wesentliche gemeinsame Forderung war, dass die Krankenkassen statt versichertenbezogener Daten über medizinische Behandlungen pseudonymisierte verarbeiten und nutzen sollen. Diese Forderung und weitere Empfehlungen der Datenschutzbeauftragten habe ich der Sozialministerin unseres Landes zugesandt und darum gebeten, diese Auffassung in die Beratungen zur Gesundheitsreform einzubringen. Darüber hinaus haben die Datenschutzbeauftragten in einer Entschließung vom 25. August 1999 (siehe 22. Anlage) den Gesetzgeber dringend gebeten zu prüfen, ob die gegenüber der bisherigen Datenverarbeitung bei den Krankenkassen weiterreichenden Bestimmungen des Gesetzentwurfes erforderlich und verhältnismäßig sind. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 7. und 8. Oktober 1999 in Rostock in einer weiteren Entschließung (siehe 17. Anlage) gefordert, die gesetzlichen Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung der Daten durchzusetzen, um die Wirksamkeit der Pseudonymisierung zu sichern.

Die Position der Datenschutzbeauftragten hat breite Zustimmung gefunden, so dass der datenschutzrechtliche Teil des Gesetzentwurfes überarbeitet wurde. Von den Krankenkassen unabhängige Datenannahmestellen sollen nun die von den Leistungserbringern übermittelten versichertenbezogenen Daten pseudonymisieren. Die Krankenkassen können mit den so bearbeiteten Informationen keine Profile ihrer Versicherten über deren Krankheiten erstellen, aber ihre Kontrollaufgaben im vollen Umfang wahrnehmen. Auch die Gefahr „gläserner Patienten“ ist damit gebannt.

In wenigen Fällen soll es für die Krankenkasse jedoch nach wie vor zulässig sein, Leistungen mit versichertenbezogenen Daten stichprobenartig zu prüfen. Mit der nur in der jeweiligen Datenannahmestelle vorhandenen Zuordnungsfunktion können zu diesem Zweck versichertenbezogene Datensätze generiert werden. Die Krankenkassen dürfen diese Daten nur für stichprobenartige Prüfungen verwenden und müssen sie nach der Prüfung löschen.

Im weiteren Gesetzgebungsverfahren zur GKV-Gesundheitsreform 2000 zeichnet sich ab, dass der Entwurf in einen vom Bundesrat zustimmungspflichtigen und einen nicht zustimmungspflichtigen Teil getrennt wird. Vor diesem Hintergrund haben sich die Datenschutzbeauftragten des Bundes und der Länder (außer Thüringen) mit einem gemeinsamen Appell an den Gesetzgeber gewandt (siehe 23. Anlage), um sicherzustellen, dass die in einem breiten Konsens erreichten guten Datenschutzregelungen des Entwurfes nicht wieder in Frage gestellt werden.

3.10.2 Risiken eines neuen Datenmodells bei den Betriebskrankenkassen

Der Landesverband Nord der Betriebskrankenkassen informierte zu Beginn des Jahres 1999 über ein bundesweites Projekt zum Datenaustausch mit Leistungserbringern - zum Beispiel Physiotherapeuten, Optikern, Sanitätshäusern, aber auch Ärzten - über eine Datenannahmestelle. Von dort könnte jede einzelne Betriebskrankenkasse (BKK) ihre Daten mit einem automatischen Verfahren abrufen, und es könnten auch allgemeine Informationen von den Krankenkassen über diese Stelle an Leistungserbringer übermittelt werden. Der Landesverband beantragte eine Genehmigung für ein automatisches Datenabrufverfahren bei der zuständigen Aufsichtsbehörde, die bei mir anfragte, ob datenschutzrechtliche Bedenken dagegen bestehen. Wegen der bundesweiten Bedeutung habe ich meine Kollegen über dieses Projekt informiert.

Der BKK-Landesverband Nord hat das geplante Verfahren damit begründet, dass bundesweit geschätzte 280.000 Leistungserbringer an circa 380 Betriebskrankenkassen Daten übermitteln müssen, wenn ihre Versicherten deren Leistungen in Anspruch genommen haben. Außerdem müssten für Prüfungen (§ 297 Sozialgesetzbuch Fünftes Buch - SGB V) eine bestimmte Zahl von Abrechnungsdatensätzen der circa 110.000 Kassenärzte über 23 Kassenärztliche Vereinigungen an die jeweilige Betriebskrankenkasse übermittelt werden. Mit dem BKK-InfoNet, einem weiteren Teil des Projektes, sollten diese hohe Anzahl von Datenübermittlungen reduziert und gleichzeitig die Prüfungen besser vorbereitet werden. Die Datenannahmestelle sollte dafür anonymisierte und pseudonymisierte Abrechnungsdaten für die Datenbank des BKK-InfoNet bereitstellen. Soweit die Daten in der Annahmestelle nicht bereits anonymisiert vorliegen, würden sie hier pseudonymisiert und an die zentrale Datenbank weitergegeben. Ein Versicherter könnte dann nur mit Kenntnis des Zuordnungsmerkmals oder der Zuordnungsfunktion wieder identifiziert werden. Die Datenbank wiederum wäre die Basis für ein Data-Warehouse-System (siehe auch Punkt 3.16.5).

Eine Arbeitsgruppe von Datenschutzbeauftragten, der auch ich angehörte, hat gegenüber dem Bundesverband der Betriebskrankenkassen zu dem Vorhaben Stellung genommen. Insbesondere haben wir auf Folgendes hingewiesen:

Die Krankenkassen können stichprobenartig Prüfungen über die Wirtschaftlichkeit von ambulanten ärztlichen Behandlungen über die zuständige Kassenärztliche Vereinigung des Arztes veranlassen. Die Prüfungen haben folglich immer einen regionalen Bezug. Deshalb ist fraglich, warum anstelle mehrerer regionaler Dateien eine zentrale Datei beim BKK-Bundesverband eingerichtet werden soll.

Die einzelnen Teile des Projektes, also die Aufgaben der Datenannahmestelle, des InfoNet, des BKK-Bundesverbandes und jeder einzelnen Krankenkasse müssen auch entsprechend den jeweils geltenden Rechtsvorschriften voneinander abgegrenzt werden. Beispielsweise ist unklar, ob mit den Auswertungsmöglichkeiten eines Data-Warehouses der zentrale Datenbestand des InfoNet überhaupt verarbeitet werden darf. Bei einer solchen Vorgehensweise besteht die Gefahr, dass mit den entsprechenden Softwarewerkzeugen aus dieser Datenbank medizinische Leistungen für viele Versicherte personenbezogen ermittelt werden könnten. Eine Krankenkasse darf nur ausnahmsweise anhand von Stichproben medizinische Leistungen versichertenbezogen auswerten (§ 297 SGB V). Bei jeder Stichprobe werden aus einer bestimmten Anzahl von pseudonymisierten Datensätzen versichertenbezogene Datensätze erstellt. Dies erfolgt mit Hilfe des oben erwähnten Zuordnungsmerkmals oder der Zuordnungsfunktion, die nur der Datenannahmestelle bekannt ist. Werden nun versichertenbezogene Daten mehrerer Stichproben gespeichert, so kann damit die gesamte Pseudonymisierung wirkungslos werden. Deshalb muss der Bundesverband besondere Maßnahmen treffen, um dies auszuschließen.

Schließlich sind in einem Datenschutz- und Datensicherheitskonzept konkrete Maßnahmen zum rechtmäßigen Umgang mit den Daten in den einzelnen Teilen des Projektes festzulegen.

Der BKK-Bundesverband hat auf die Stellungnahme der Datenschutzbeauftragten bisher noch nicht reagiert. Ohnehin ist gegenwärtig nicht klar, ob und wie das Gesamtprojekt - auch vor dem Hintergrund der Gesundheitsstrukturreform (siehe auch Punkt 3.10.1) - umgesetzt wird.

Das Sozialministerium hat mir im November 1999 mitgeteilt, dass die beantragte Genehmigung nicht erteilt wurde, weil die einzige ihm bislang unterstehende BKK durch eine Fusion nun nicht mehr seiner Aufsicht untersteht.

3.10.3 Kindschaftsrecht datenschutzgerecht umgesetzt

Der Bundesgesetzgeber hat im Dezember 1997 das Gesetz zur Reform des Kindschaftsrechts (Kindschaftsrechtsreformgesetz -KindRG) beschlossen, das am 1. Juli 1998 in Kraft getreten ist. Mit diesem Gesetz sind zahlreiche Rechtsvorschriften in anderen Gesetzen geändert worden. Ein Mitglied des Landtages hat mich um eine datenschutzrechtliche Stellungnahme gebeten.

Das durch das KindRG novellierte Sozialgesetzbuch Achtes Buch (SGB VIII) enthält nunmehr eine Norm zur Datenübermittlung für den Fall, dass ein Scheidungsverfahren anhängig ist und die Eheleute gemeinsame minderjährige Kinder haben. Das Gericht teilt dem Jugendamt dann Namen und Anschriften der Parteien mit, damit die Jugendhilfe die Betroffenen über ihre Leistungsangebote direkt unterrichten kann.

Des Weiteren ist geregelt, dass das Jugendamt einen Vater über seine Rechte beraten soll, wenn Eltern bei der Geburt eines Kindes nicht miteinander verheiratet sind. Auch dazu benötigt es personenbezogene Daten.

Der Gesetzgeber hat sich bei diesen Bestimmungen davon leiten lassen, dass das Kindeswohl diesen Eingriff in das Recht auf informationelle Selbstbestimmung erforderlich macht.

Nähere Bestimmungen zur weiteren Nutzung beziehungsweise Löschung der an das Jugendamt übermittelten Daten sind im Kindschaftsrechtsreformgesetz nicht enthalten, so dass die allgemeinen sozialdatenschutzrechtlichen Grundsätze anzuwenden sind. Das Landesjugendamt hatte bereits eine Arbeitsgruppe „Kindschaftsrecht“ gebildet, der ich Empfehlungen gegeben habe, wie sie diese Grundsätze umsetzen kann. So sollten die Betroffenen aus dem Anschreiben zum Beratungsangebot erfahren, woher und auf welcher Rechtsgrundlage die personenbezogenen Daten dem Jugendamt zugegangen sind. Außerdem sollte festgelegt und die Betroffenen sollten darüber informiert werden, wie das Jugendamt die Daten verarbeitet und nutzt und wann es sie löscht. Das Landesjugendamt hat dies beispielsweise im Musteranschreiben an Eltern bei einer Scheidung folgendermaßen umgesetzt:

„Sehr geehrte Eltern, das zuständige Familiengericht hat uns im Rahmen seiner Mitteilungspflicht gem. § 622 Abs. 2 ZPO (Zivilprozessordnung) darüber informiert*, daß Sie die Scheidung eingereicht haben.“

In der Fußnote wird weiter erklärt:

„*Die vom Amtsgericht übermittelten Daten dienen ausschließlich dieser Information und werden nach Zweckerfüllung (vgl. § 17 Abs. 3 KJHG) binnen 6 Monaten vernichtet.“

Das Landesjugendamt hat meine Empfehlungen auch vollständig in die weiteren Mustervordrucke und Arbeitsanleitungen eingearbeitet. So konnten die Jugendämter die Bestimmungen des Kindschaftsrechtsreformgesetzes gleich zum Zeitpunkt seines In-Kraft-Tretens unter Berücksichtigung sozialdatenschutzrechtlicher Grundsätze umsetzen.

Dem Mitglied des Landtages habe ich dieses Ergebnis mitgeteilt.

3.10.4 Was das BAföG-Amt dem Antragsteller mitteilen darf

Wenn ein Auszubildender (Schüler oder Student) Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) beantragt, muss das zuständige BAföG-Amt zunächst prüfen, ob und in welchem Umfang die Eltern des Antragstellers zum Unterhalt verpflichtet sind. Dazu benötigt das Amt Einkommensdaten und Angaben über die Familienverhältnisse der Eltern, zum Beispiel die Anzahl der weiteren unterhaltsberechtigten Personen.

Ein Vater hat sich an mich gewandt, weil er vermeiden wollte, dass sein studierender Sohn, zu dem er seit langer Zeit keinen Kontakt mehr hatte, die Angaben über sein Einkommen zur Kenntnis erhält.

Das BAföG enthält eine Bestimmung, nach der ein Elternteil oder der Ehegatte eines Auszubildenden verlangen kann, dass die Angaben zum Einkommen im Bescheid mit Ausnahme des für die Leistung angerechneten Einkommensbetrages entfallen (§ 50 Abs. 2 Satz 3 BAföG). Dies gilt aber nicht, wenn der Antragsteller ein berechtigtes Interesse an der Kenntnis der Einkommensdaten hat und dafür förderungsrechtliche Gründe nennt. In diesem Fall kann das Amt auch die relevanten Daten mitteilen. Das BAföG-Amt muss bei der Entscheidung, ob die Daten über das Einkommen eines Elternteils oder des Ehegatten dem Auszubildenden mitgeteilt werden, zwischen den jeweiligen Interessen abwägen. In der Regel sollte das Datenschutzinteresse des zum Unterhalt Verpflichteten Vorrang haben.

Den Vater habe ich darüber informiert, dass das BAföG-Amt auch in seinem Fall alle entscheidungserheblichen Belange bei der Abwägung berücksichtigt.

In diesem Zusammenhang habe ich dem BAföG-Amt in einem ähnlichen Fall auch mitgeteilt, dass das Auskunftsinteresse des Auszubildenden an den Einkommensdaten gegenüber dem Interesse der Eltern, diese Daten zu unterdrücken, dann subsidiär ist, wenn er bloße Zweifel an der materiellen Rechtmäßigkeit des Bescheides hat. Aus dem Vergleich zwischen der Höhe des Einkommens der Eltern oder des Ehegatten und des für die Leistung angerechneten Einkommens kann der Auszubildende gerade keine förderungsrechtlichen Schlüsse ziehen. Dazu müsste er die genauen Einkommensnachweise kennen, die aber das Amt nicht mitteilen darf.

Andererseits hat aber ein Unterhaltsberechtigter gegenüber einem Unterhaltspflichtigen einen gesetzlichen Anspruch, über das Einkommen und Vermögen Auskunft zu erhalten, soweit dies erforderlich ist, um Unterhaltsleistungen festzustellen (§ 1605 Bürgerliches Gesetzbuch - BGB). Dieser Anspruch, der zivilrechtlich durchsetzbar ist, kann nicht gegen das BAföG-Amt geltend gemacht werden, sondern immer nur gegenüber dem Unterhaltspflichtigen. Ein Gericht müsste jedoch auch prüfen, ob die Auskunft erforderlich ist.

Insoweit werden sowohl im BAföG-Verfahren als auch bei dem zivilrechtlichen Auskunftsanspruch die Interessen zwischen Unterhaltsberechtigten und Unterhaltspflichtigen interessengerecht abgewogen.

3.10.5 Datenverarbeitung im Auftrag von Wohngeldstellen - was ist zu beachten?

Bei der Kontrolle eines Sozialhilfeträgers hat sich herausgestellt, dass Sozialdaten für Wohngeldleistungen durch eine nicht-öffentliche Stelle verarbeitet wurden. Die Wohngeldstelle als Teil dieses Trägers nahm von den Antragstellern die Anträge entgegen und speicherte die Daten auf einer Diskette. Diese Diskette wurde dann einem privaten Rechenzentrum durch einen Botendienst übermittelt. Das Rechenzentrum berechnete das Wohngeld, druckte die Bescheide aus und übermittelte sie dem Sozialamt. Von dort wurden sie an die Betroffenen versandt.

Zunächst war zu prüfen, ob es sich hierbei noch um eine Verarbeitung der Daten im Auftrag der Wohngeldstelle handelt oder ob das Rechenzentrum die Funktion der öffentlichen Stelle übernommen hat. Aus den Gesprächen mit beiden Seiten ergab sich, dass eine Datenverarbeitung im Auftrag vorliegt, denn das Rechenzentrum verarbeitet die Daten lediglich nach einem vorgegebenen Algorithmus und hat dabei keinen Ermessensspielraum. Außerdem obliegt allein der Wohngeldstelle die Entscheidung, ob der Bescheid so zugestellt oder überarbeitet wird.

Bei der Verarbeitung von Sozialdaten im Auftrag eines Sozialleistungsträgers sind die Vorschriften des Sozialgesetzbuches Zehntes Buch (SGB X), hier insbesondere des § 80 Abs. 5 SGB X, zu beachten. Demnach müssen vor allem zwei Voraussetzungen erfüllt sein:

- der Auftragnehmer kann die übertragenen Arbeiten erheblich kostengünstiger besorgen und

- der Auftrag darf nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfassen.

Die Wohngeldstelle hat nachgewiesen, dass das Rechenzentrum die Daten tatsächlich erheblich kostengünstiger verarbeiten kann. Auch die zweite Bedingung war erfüllt, da bei jeder monatlichen Berechnung immer nur Daten über Neu- oder Änderungsanträge verarbeitet werden. Darüber hinaus werden die Daten nach der Übergabe an die Wohngeldstelle und der Auftragsbestätigung gelöscht. Es wird somit nur ein Teil des Datenbestandes über Wohngeldempfänger und dieser nur kurzzeitig gespeichert.

Da das Sozialamt für die Rechtmäßigkeit dieser Datenverarbeitung verantwortlich bleibt, habe ich folgende weitere Empfehlungen gegeben:

Der Sozialleistungsträger muss prüfen, ob mit den beim Auftragnehmer getroffenen datenschutzrechtlichen Regelungen der Schutz des Sozialgeheimnisses gewahrt bleibt. Vertraglich sollte beispielsweise festgelegt werden, in welcher Form das Rechenzentrum die Daten erhält, wo der Verantwortungsübergang stattfindet (Datenannahme und Datenübergabe) oder welche Leistungen konkret zu erbringen sind. Ebenso sollten die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Wahrung des Sozialgeheimnisses Vertragsbestandteil sein. So ist unter anderem zu bestimmen, wer Zugang zu den Datenverarbeitungsanlagen für Wohngelddaten hat und wie sichergestellt und kontrolliert wird, dass es sich hierbei tatsächlich um Berechtigte handelt. Der Auftragnehmer ist zu verpflichten, die Sozialdaten ausschließlich zweckentsprechend und nur im vertraglich vereinbarten Umfang zu verarbeiten und nutzen. Zur Gewährleistung eines einheitlichen Datenschutzes sollte außerdem in den Vertrag aufgenommen werden, dass sich der Auftragnehmer hinsichtlich der Verarbeitung dieser Sozialdaten der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

Meine Hinweise wurden durch Überarbeitung der bestehenden Verträge berücksichtigt.

3.10.6 Hausbesuch vom Sozialamt

Ein Abgeordneter hat mir mitgeteilt, dass er bei Veranstaltungen in seinem Heimatwahlkreis häufig gefragt wird, ob ein Sozialhilfeempfänger verpflichtet sei, Hausbesuche von Mitarbeitern des Sozialamtes zu dulden. Nach seinen Informationen nutzen die Sozialämter diese Möglichkeit, um zu prüfen, ob der Hilfeempfänger in einer eheähnlichen Gemeinschaft lebt.

Nach § 20 Sozialgesetzbuch Zehntes Buch (SGB X) gilt im Sozialleistungsrecht der Amtsermittlungsgrundsatz. Danach ist das Sozialamt verpflichtet, alle für die Entscheidung des Sozialhilfeantrages erheblichen Tatsachen zu ermitteln. Dazu gehört auch die Feststellung, ob ein Sozialhilfeempfänger in einer eheähnlichen Gemeinschaft lebt.

Der Antragsteller hat dabei Mitwirkungspflichten, die sich vor allem aus §§ 60 ff Sozialgesetzbuch Erstes Buch (SGB I) ergeben. So hat der Hilfeempfänger alle Tatsachen anzugeben, die für die Leistungsgewährung wichtig sind. Bevor jedoch ein Hausbesuch durchgeführt wird, sind zunächst Ermittlungsmaßnahmen vorzuziehen, die weniger intensiv in die Privatsphäre des Antragstellers eingreifen. So muss dem Antragsteller ermöglicht werden, anderweitig nachzuweisen, dass keine eheähnliche Gemeinschaft besteht, indem er zum Beispiel einen Untermietvertrag vorlegt. Im Einzelfall kann aber auch der Hausbesuch berechtigt sein. Beispielsweise wenn der konkrete Verdacht besteht, dass die Angaben des Antragstellers unwahr sind und der Hausbesuch in einem angemessenen Verhältnis zur beantragten Leistung steht.

Über diese Rechtslage hat der Abgeordnete in einer Pressemitteilung informiert.

3.10.7 Wie stellt das Sozialamt Vermögen oder Einkommen fest?

Ein Bürger wollte wissen, ob er verpflichtet sei, dem Sozialamt im Zusammenhang mit seinem Sozialhilfeantrag eine Befreiung vom Bankgeheimnis für insgesamt neun Banken seines Wohnortes zu erteilen. Er hatte dies abgelehnt, da er befürchtete, dass seine Geschäftsbeziehungen mit den Banken erschwert werden, wenn dort seine vorübergehende Sozialhilfebedürftigkeit bekannt wird. Er ist als Selbständiger tätig und daher auf Kredite angewiesen, wenn seine Notlage überstanden ist.

Sozialhilfe sollen nur Personen erhalten, die sich nicht selbst helfen können oder die erforderliche Hilfe von anderen nicht bekommen. Das Sozialamt muss prüfen, ob diese Voraussetzungen vorliegen, und kann dazu Art und Umfang seiner Ermittlungen bestimmen. Die betroffene Person hat dabei mitzuwirken. Sie hat insbesondere alle leistungserheblichen Tatsachen anzugeben und auf Verlangen des Sozialleistungsträgers die erforderlichen Auskünfte zu erteilen oder zuzustimmen, dass Dritte sie erteilen. Im Einzelfall kann auch mit Einwilligung der betroffenen Person eine Auskunft bei einer Bank eingeholt werden, um festzustellen, ob Vermögen oder Einkommen vorhanden sind. Den Kreditinstituten wird dann jedoch bekannt, dass ein Kunde oder potentieller Kunde Sozialleistungen beantragt hat oder erhält. Deshalb sind vorher alle anderen Mittel, die weniger tief in das Persönlichkeitsrecht eingreifen, auszuschöpfen.

Ein milderes Mittel ist beispielsweise eine Anfrage beim Bundesamt für Finanzen, ob die betroffene Person einen Freistellungsauftrag von der Zinsbesteuerung für ein Konto (oder Aufträge für mehrere Konten) gestellt hat. Durch die Steuerreformgesetze 1999/2000 ist das Bundesamt berechtigt, den Sozialleistungsträgern Daten über Freistellungsaufträge mitzuteilen, soweit dies zur Überprüfung des bei der Sozialleistung zu berücksichtigenden Einkommens oder Vermögens erforderlich ist oder die betroffene Person zustimmt. Ein Sozialleistungsträger erhält so die Information, bei welchen Banken die betroffene Person Konten besitzt, und kann sie daraufhin auffordern, aktuelle Auszüge dieser Konten vorzulegen. Der Vorteil dieses Verfahrens ist, dass einer Bank keine weiteren personenbezogenen Daten des Betroffenen übermittelt werden müssen. Die im Einzelfall erforderlichen Daten kann die betroffene Person im Rahmen ihrer Mitwirkungspflicht dann selbst vorlegen.

Allerdings ist es auch denkbar, dass ein Sozialhilfeantragsteller über ein Konto mit Vermögen oder Einkommen verfügt, für das er aus unterschiedlichen Gründen keinen Freistellungsantrag gestellt hat. Ist dies aus Sicht des Sozialamtes wahrscheinlich, kann es die betroffene Person bitten, einer Bankauskunft zuzustimmen.

Die in dem konkreten Fall vom Betroffenen erbetene weitreichende Zustimmung ist meines Erachtens unverhältnismäßig. Ich habe dem Sozialamt empfohlen, in Zukunft zunächst in der oben beschriebenen Weise zu verfahren. Wenn danach noch Zweifel über die finanzielle Situation eines Betroffenen bestehen, kann im Einzelfall mit seiner Einwilligung bei einer Bank die entsprechende Auskunft eingeholt werden.

Das Sozialamt hat zugesichert, entsprechend meiner Empfehlung zu verfahren.

3.11 Gesundheitswesen

3.11.1 Meldungen an das Krebsregister

Die Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt und Thüringen hatten durch einen im November 1997 unterzeichneten Staatsvertrag beschlossen, ein gemeinsames Krebsregister mit Sitz in Berlin zu bilden, um damit auch die Registrierung der Krebserkrankungen in der ehemaligen DDR fortzuführen. Das wissenschaftliche und gesundheitspolitische Interesse an diesem Register ist sehr groß. Unsere wesentlichen Empfehlungen hierzu hatte ich bereits im Zweiten Tätigkeitsbericht unter Punkt 2.12.2 vorgestellt.

Zu Beginn des Jahres 1998 hat der Landtag das Gesetz zur Ausführung des Krebsregistergesetzes (Krebsregisterausführungsgesetz - KrebsRAG M-V) beraten und beschlossen. Mit diesem Gesetz wurde auch dem Staatsvertrag zugestimmt, und er wurde in Kraft gesetzt.

Nach dem Krebsregisterausführungsgesetz sind Ärzte und Zahnärzte verpflichtet, Daten über Krebserkrankungen, die sie bei Patienten mit Hauptwohnsitz in Mecklenburg-Vorpommern feststellen, innerhalb eines vorgegebenen Zeitraumes mit Name und Anschrift an die Vertrauensstelle des Gemeinsamen Krebsregisters zu übermitteln. Der Unterrichtungsanspruch der Patienten über die Meldung bleibt durch die landesrechtliche Regelung unberührt. Ein Widerspruchsrecht haben die Patienten in diesem Fall nicht.

In der Gesetzesberatung habe ich empfohlen, die Meldepflicht der Ärzte bestehen zu lassen, aber den Patienten ein Widerspruchsrecht einzuräumen. Sofern ein Patient dieses Recht beansprucht, dürfte der Arzt dessen personenbezogene Daten an die Vertrauensstelle des Krebsregisters nicht übermitteln.

Im Referentenentwurf des Krebsregisterausführungsgesetzes wird die Meldepflicht der Ärzte damit begründet, dass ohne sie der Erfassungsgrad der Erkrankungen unter 90 % falle. Ein hoher Erfassungsgrad wäre insbesondere auch dann nicht zu erreichen, wenn der Arzt den Patienten zuvor überzeugen müsse, dass die Meldung für die Krebsforschung notwendig sei. Des Weiteren ist darauf hingewiesen worden, dass durch die Meldepflicht an das Nationale Krebsregister der ehemaligen DDR etwa 95 % aller Krebserkrankungen erfasst worden sind. Es sei damit eines der international größten Register und weltweit anerkannt. Die hohe Erfassungsquote sei nach 1989 in Mecklenburg-Vorpommern drastisch zurückgegangen und habe in den Jahren 1995/1996 nur etwa 60 % betragen.

Meines Erachtens ist die Ursache für den Rückgang der Meldungen im Wesentlichen in dem erforderlichen Aufwand zu suchen. Dieser Aufwand wurde den Ärzten nur zu einem geringen Teil honoriert, so dass wohl viele davon abgesehen haben, das entsprechende Formular auszufüllen und an das Krebsregister zu senden. Es konnte jedenfalls nicht belegt werden, dass viele Betroffene seit 1995/1996 ihr Widerspruchsrecht genutzt haben und deshalb die Erfassungsquote so gering war.

Der Bundesgesetzgeber hat im Übrigen das Widerspruchsrecht im Krebsregistergesetz, das die wesentlichen landesrechtlichen Regelungen vorgegeben hat, folgendermaßen begründet: „Gemäß früheren Umfragen bei der Bevölkerung und bei Patienten, gerade auch bei Krebskranken, muß nicht damit gerechnet werden, daß eine nennenswerte Zahl von Patienten, die über Art und Ausmaß ihrer Erkrankung aufklärbar sind, von ihrem Recht auf Widerspruch Gebrauch machen. Daher ist auch bei einer Melderechtslösung mit Widerspruchsrecht derzeit von einer ausreichenden Vollständigkeit auszugehen.“ (BR-Drs. 669/93 S. 20/21)

Der Gesetzgeber des Landes hat meine Empfehlung nicht umgesetzt und seinen Regelungsspielraum nach dem Krebsregistergesetz des Bundes ausgenutzt. Die Patienten haben nach dem Krebsregisterausführungsgesetz somit kein Widerspruchsrecht gegen die Meldung an das Krebsregister.

Gegen den weiteren Umgang mit den Daten im Krebsregister habe ich grundsätzlich keine Bedenken. Es sind viele Maßnahmen realisiert, die die Vertraulichkeit sichern. Beispielsweise können ohne Einwilligung des Betroffenen nur pseudonymisierte Daten für die wissenschaftliche Forschung genutzt werden. Mit diesen Daten kann ein Krankheitsfall nicht beziehungsweise nur mit einem unverhältnismäßigen Aufwand einer konkreten Person zugeordnet werden.

Die Landesregierung sollte dennoch auf der Grundlage der in Ländern mit einem Widerspruchsrecht gesammelten Erfahrungen prüfen, ob nicht auch in Mecklenburg-Vorpommern dieses Recht den Bürgern mittelfristig wieder eingeräumt werden kann.

Als Beispiel sei hier auf die Erfahrungen der Wissenschaftler mit dem Deutschen Kinderkrebsregister verwiesen. In diesem Register dürfen nur Daten verarbeitet und genutzt werden, wenn die Eltern krebskranker Kinder einwilligen. Nach den Angaben der Literatur lehnen deutlich weniger als ein Prozent der Eltern dies ab. Offensichtlich ist also auch mit einer Einwilligungslösung eine sehr hohe Erfassungsquote erreichbar.

3.11.2 Ärztliche Schweigepflicht im Bestattungsgesetz

Im Januar 1998 wurde mir der Referentenentwurf eines Gesetzes über das Leichen-, Bestattungs- und Friedhofswesen im Land Mecklenburg-Vorpommern (Bestattungsgesetz Mecklenburg-Vorpommern) zur Stellungnahme übersandt.

Der Umgang mit Daten, die der ärztlichen Schweigepflicht unterliegen, ist in § 6 geregelt. Hier war vorgesehen, dass der die Leichenschau durchführende Arzt die Todesbescheinigung ausstellt. Offen blieb jedoch, an welche Stelle der Arzt diese zu senden hat. Ich habe daher empfohlen, dies ebenfalls im Gesetz zu regeln.

Weiterhin war festgelegt, unter welchen Voraussetzungen das Gesundheitsamt Angehörigen Einsicht in sowie Auskunft über den Inhalt der Todesbescheinigung gewähren kann beziehungsweise in welchen Fällen Ablichtungen ausgehändigt werden dürfen.

Angehörige von Verstorbenen sollten sich in der Regel an den behandelnden Arzt wenden, da dieser am besten einschätzen kann, ob das dargelegte Interesse es rechtfertigt, die ärztliche Schweigepflicht zu durchbrechen. Da es jedoch sein kann, dass die Angehörigen nicht wissen, welcher Arzt den Verstorbenen behandelt hat, sollten auch in diesem Fall Auskunfts- bzw. Einsichtsrechte im erforderlichen Umfang gegeben sein. Allen anderen, beispielsweise Versicherungsträgern, sollte nur Auskunft oder Einsicht in Todesbescheinigungen gewährt werden, wenn sie ein rechtliches Interesse glaubhaft darlegen. Nach dem Entwurf war es möglich, Ablichtungen von Todesbescheinigungen zu erhalten. Dies sollte aus datenschutzrechtlicher Sicht ersatzlos gestrichen werden, da damit Daten offenbart werden könnten, die für den Einzelfall nicht erforderlich sind.

Vorgesehen war weiter, dass die Daten der Todesbescheinigung für wissenschaftliche Forschungsvorhaben genutzt werden dürfen, wenn durch sofortige Anonymisierung sichergestellt ist, dass schutzwürdige Belange des Verstorbenen nicht beeinträchtigt werden oder aber das öffentliche Interesse gegenüber dem Geheimhaltungsinteresse überwiegt. Hier blieb jedoch die Frage offen, wer die vorgeschriebene Anonymisierung vornehmen soll. Auch war nicht geregelt, wer die Entscheidung trifft, in welchem Fall das öffentliche Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen erheblich überwiegt. Letzteres entscheidet in der Regel die oberste Aufsichtsbehörde - in diesem Fall das Sozialministerium. Daher habe ich empfohlen, den Entwurf entsprechend zu ergänzen.

Die Hinweise wurden weitgehend umgesetzt. Unberücksichtigt blieb jedoch der Vorschlag, dass niemand Ablichtungen von Todesbescheinigungen erhält.

3.11.3 Krankenhaus informiert Ordnungsamt über fahruntüchtigen Patienten

Ein in einer Klinik beschäftigter Arzt hat das Ordnungsamt darüber informiert, dass einer seiner Patienten aus gesundheitlichen Gründen nicht in der Lage ist, ein Kraftfahrzeug zu führen. Der Führerschein des Betroffenen war jedoch schon vorher eingezogen worden. Er zweifelte, ob sein Arzt rechtmäßig gehandelt hat, und bat mich, den Sachverhalt zu prüfen.

Die Mitteilung des Arztes an das Ordnungsamt, er halte seinen Patienten aus gesundheitlichen Gründen für fahruntüchtig, ist unter zwei Aspekten zu beurteilen. Einerseits hat eine solche Information in der Regel erhebliche Konsequenzen für den Betroffenen. Das Ordnungsamt entzieht befristet oder unbefristet die Fahrerlaubnis, wenn nachgewiesen wird, dass jemand vorübergehend oder dauernd ungeeignet ist, ein Fahrzeug zu führen. Andererseits gefährdet ein untüchtiger Fahrzeugführer sich selbst und seine Mitmenschen, so dass die entsprechende Nachricht an das Amt erforderlich sein kann, um dies zu verhindern.

Bricht ein Arzt seine Schweigepflicht, weil dies zur Abwehr einer gegenwärtigen Gefahr für Leben, körperliche Unversehrtheit oder persönliche Freiheit des Patienten oder Dritter erforderlich ist (§ 34 Strafgesetzbuch - StGB), so handelt er nicht rechtswidrig. Er muss dabei jedoch abwägen, ob die zu schützenden Interessen des Patienten den Verstoß gegen die ärztliche Geheimhaltungsvorschrift (§ 203 Abs. 1 Nr. 1 StGB) rechtfertigen und detailliert prüfen, ob von dem Patienten eine gegenwärtige Gefahr ausgeht. Das ist beispielsweise der Fall, wenn der Patient noch im Besitz einer Fahrerlaubnis ist oder wenn er sie unmittelbar nach der Entlassung aus der Klinik zurückerhalten soll.

Im vorliegenden Fall war dem Petenten die Fahrerlaubnis bereits entzogen, und es war nicht zu erwarten, dass er sie kurz nach der Entlassung aus der Klinik zurückerhalten würde. Es bestand also keine gegenwärtige Gefahr für andere. Die Mitteilung an die Ordnungsbehörde war damit nicht durch § 34 StGB gedeckt.

Ich habe dem Ärztlichen Direktor der Klinik empfohlen, bei Informationen an die Ordnungsbehörde in ähnlichen Fällen ein abgestuftes Verfahren zu wählen. Eine Mitteilung der Ordnungsbehörde oder der Führerscheinstelle über die Fahruntüchtigkeit eines Partienten kommt ohnehin nur in Betracht, wenn der Arzt weiß, dass derjenige einen Führerschein besitzt. Doch auch dann sollte der Patient zunächst in einem klärenden Gespräch bewogen werden, seinen Führerschein selbst abzugeben. Zeichnet sich jedoch ab, dass er dem ärztlichen Rat nicht folgen wird, kann der Arzt prüfen, ob eine unmittelbare Gefahr für den Patienten oder Dritte besteht. Nur dann darf er seine Schweigepflicht brechen und die Behörde entsprechend benachrichtigen. Der Patient sollte auf diese Vorgehensweise hingewiesen werden. Er sollte weiter darauf aufmerksam gemacht werden, dass die Mitteilung auch dann ergeht, wenn der Patient den Führerschein nicht freiwillig abgibt oder eine Schweigepflicht-Entbindungserklärung nicht erteilt.

Künftig wollen die Ärzte der Klinik entsprechend dieser Empfehlung verfahren.

In einem weiteren Fall hat mich eine Ärztin gefragt, ob sie die Ordnungsbehörde benachrichtigen darf, wenn sie in einem Fahrzeugführer einen Patienten erkennt, der aus gesundheitlichen Gründen fahruntüchtig und deshalb nicht im Besitz einer Fahrerlaubnis ist.

Das Fahren ohne Fahrerlaubnis ist eine Straftat und wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe geahndet. Liegen konkrete Anhaltspunkte für diese Tat vor, kann jede Person, so auch der behandelnde Arzt, Strafanzeige stellen. Die Strafverfolgungsorgane prüfen dann, ob die Voraussetzungen zur Einleitung eines Ermittlungsverfahrens vorliegen. Diese Handlungsweise stellt keinen Verstoß gegen die Geheimhaltungspflicht des Arztes dar. Wenn ein Patient aus gesundheitlichen Gründen nicht geeignet ist, mit einem Fahrzeug am öffentlichen Straßenverkehr teilzunehmen, so geht von ihm eine konkrete Gefahr aus. Die Voraussetzungen des rechtfertigenden Notstandes gemäß § 34 StGB liegen vor.

3.11.4 Notrufe werden aufgezeichnet

Rettungsleitstellen zeichnen automatisch die Gespräche auf, die über Notrufnummern bei ihnen eingehen. Ein Bürger wollte wissen, ob das zulässig sei.

Elektronische Aufzeichnungen von Telefongesprächen sind wegen des grundgesetzlich geschützten Fernmeldegeheimnisses nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die Gesprächsteilnehmer einwilligen. Aus nahe liegenden Gründen kann für diesen Zweck eine Einwilligung nicht eingeholt werden. Sie würde die Hilfe verzögern und den Anrufer in einer schwierigen Situation zusätzlich belasten. Das entsprechende bereichsspezifische Gesetz, das Gesetz über den Rettungsdienst für das Land Mecklenburg-Vorpommern, enthält keine Regelung zur Aufzeichnung von Gesprächen über die Notrufnummer.

Deshalb habe ich die zuständige oberste Aufsichtsbehörde, das Sozialministerium, gebeten zu klären, auf welcher rechtlichen Grundlage eingehende Notrufe von den Rettungsleitstellen aufgezeichnet und dort gespeichert werden. Eine Rechtsvorschrift müsste auch festlegen, durch welche technischen und organisatorischen Maßnahmen der rechtmäßige Umgang mit den aufgezeichneten Daten sicherzustellen ist und wann die Aufzeichnungen zu löschen sind.

Der Landkreistag Mecklenburg-Vorpommern hat mich daraufhin zu einer Beratung der Arbeitsgemeinschaft der Ordnungsämter eingeladen, in der die Vertreter der Rettungsleitstellen erläuterten, warum es notwendig sei, die Gespräche aufzuzeichnen. Unter anderem gäbe dies den Beschäftigten in den Leitstellen mehr Sicherheit. Bei Unklarheiten könne die Meldung noch einmal gehört und geprüft werden, ob die eingeleiteten Maßnahmen richtig sind. Dies sei vor allem deshalb von Bedeutung, weil Anrufer beispielsweise unter dem Eindruck eines Unfalls oftmals sehr erregt seien. Bei Gefahr für Leib und Leben sei es außerdem angemessen, dass dokumentiert wird, wann welche Maßnahmen veranlasst worden sind. Schließlich spiele hier auch eine Rolle, dass die Aufzeichnungen verfügbar sein sollen, um solche Fälle verfolgen zu können, bei denen ein Anrufer die Notrufnummer vorsätzlich zweckwidrig benutzte. Einerseits sind diese Argumente nachvollziehbar, andererseits ist aber für die Aufzeichnung auch Rechtssicherheit für Anrufer und Beschäftigte in den Leitstellen zu schaffen.

Da es sich bei diesem Sachverhalt nicht um eine landesspezifische Besonderheit handelt - denn Notrufe werden bundesweit in den Rettungsleitstellen aufgezeichnet und gespeichert - , habe ich bei meinen Kollegen in den Ländern nachgefragt, welche gesetzlichen Regelungen dort existieren. Außerdem habe ich den Bundesbeauftragten für den Datenschutz gebeten zu prüfen, ob eine bundesweit einheitliche Bestimmung im Telekommunikationsrecht in Betracht kommt. Die Umfrage hat ergeben, dass bereits in mehreren Ländern in den Rettungsdienstgesetzen oder den Sicherheits- und Ordnungsgesetzen entsprechende Normen vorhanden sind und eine bundeseinheitliche Regelung nicht vorhanden, aber auch nicht erforderlich ist. Aus diesem Grund habe ich dem Innenministerium unseres Landes empfohlen, dem Landesgesetzgeber vorzuschlagen, die elektronische Aufzeichnung von Notrufgesprächen gesetzlich zu regeln. Eine Regelung im Sicherheits- und Ordnungsgesetz hätte den Vorteil, dass hier eine Aufzeichnungsbefugnis für den Polizeinotruf und den Rettungsnotruf aufgenommen werden könnte.

Das Innenministerium hat mir dazu mitgeteilt, dass eine gesetzliche Regelung nicht als notwendig erachtet wird und dies auf folgende Argumente gestützt: Nach dem Grundgesetz und dem Strafgesetzbuch würden nur solche Worte geschützt, die nicht öffentlich gesprochen werden. Bei der Benutzung eines Notrufes handele es sich aber um öffentlich gesprochene Worte, die keinem besonderen Schutz unterlägen. Darüber hinaus sei der Intimbereich des Sprechenden nicht betroffen. Im Übrigen seien die Regelungen zur Datenerhebung, -verarbeitung und -nutzung im Sicherheits- und Ordnungsgesetz (SOG M-V) die Grundlage für eine kurzfristige Speicherung.

Diese Argumente gegen eine gesetzliche Regelung zur Aufzeichnung von Notrufen erscheinen nicht überzeugend. Ein Hilferufender wendet sich gerade nicht an die Öffentlichkeit, wenn er eine Notrufnummer nutzt, sondern an eine für die Abwehr von Notfällen kompetente und dafür zuständige Behörde. Ein Notruf unterscheidet sich insofern nicht von einem anderen Anruf bei einer Behörde. Die besondere Eilbedürftigkeit für eine Hilfe kann auch kein Maßstab dafür sein, ein solches Gespräch als öffentlich zu betrachten. Ferner kann auch der Intimbereich des Anrufenden sehr wohl betroffen sein, insbesondere wenn es sich dabei um einen Beteiligten eines Notfalles handelt. Die im Schreiben des Innenministeriums zitierten Regelungen des SOG M-V betreffen nur die allgemeine Datenerhebung und -verarbeitung und sind daher kaum als Rechtsgrundlage für das Aufzeichnen von Telefongesprächen geeignet. Ich habe deshalb nochmals eine gesetzliche Regelung empfohlen. Eine Antwort hierauf liegt mir bisher nicht vor.

3.11.5 Prüfaufträge an den Medizinischen Dienst müssen konkret sein

Der Medizinische Dienst der Krankenversicherung (MDK) wird im Auftrag gesetzlicher Krankenkassen tätig, wenn für eine Entscheidung medizinischer Sachverstand vonnöten ist.

Ein Krankenhaus machte mich darauf aufmerksam, dass eine Krankenkasse den MDK beauftragte, Krankenhausbehandlungen zu prüfen, ohne den Grund dafür näher zu bezeichnen. Das Ankündigungsschreiben der Krankenkasse trug die Überschrift: „Namentliche Aufstellung für die MDK-Krankenhausbegehung am ...“. Weiter heißt es dort: „Sehr geehrte Damen und Herren, nachfolgend aufgeführte Versicherte werden am o. g. Termin durch Akteneinsicht in Ihrem Haus begutachtet.“ Die anschließende Tabelle enthielt die Merkmale: laufende Nummer, Versicherter, Station, Aufnahmenummer, Aufnahmetag.

Das Sozialgesetzbuch Fünftes Buch (SGB V) regelt konkret, in welchen Fällen die Krankenkasse den MDK beauftragen kann. Beispielsweise wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, die Leistungsart oder den Umfang der Leistung zu begutachten (§ 275 Abs. 1 SGB V). Dafür sind jedoch nur bestimmte Unterlagen der Krankenakte erforderlich, zum Beispiel der Operationsbericht. Sollen hingegen die Notwendigkeit und die Dauer der stationären Behandlung geprüft werden (§ 276 Abs. 4 SGB V), so ist dies ein umfassenderer Auftrag, der es erforderlich machen kann, dass der MDK die gesamten Unterlagen des Behandlungsfalles einsehen muss. Allein aufgrund der unterschiedlichen Rechtsvorschriften ist es notwendig, dass die Aufträge hinreichend konkret sind.

Ein konkreter Prüfauftrag ist jedoch ebenso für das Krankenhaus erforderlich, weil es verpflichtet ist, die Patientendaten nach Abschluss der Behandlung zu sperren (§ 19 Abs. 1 Satz 1 Landeskrankenhausgesetz für das Land Mecklenburg-Vorpommern - LKHG M-V). Die Sperrung darf nur aufgrund einer Rechtsvorschrift, so auch zur Erfüllung der gesetzlichen Aufgaben des MDK, oder mit Einwilligung des Patienten aufgehoben werden. Dies ist in der Krankenakte zu begründen und zu vermerken (§ 19 Abs. 2 Satz 6 LKHG M-V).

Es ist außerdem ein datenschutzrechtliches Prinzip, dass insbesondere unregelmäßige Datenübermittlungen oder die Einsichtnahme, bei der es sich in der datenschutzrechtlichen Terminologie ebenfalls um eine Übermittlung handelt, im Einzelfall zu dokumentieren sind. Es muss nachvollziehbar sein, welche Stelle zur Erfüllung welcher Aufgaben wann und welche Daten erhalten hat, weil der Patient ein entsprechendes Recht auf Auskunft hat.

Die Krankenkasse stimmte dieser Auffassung zu und wollte daraufhin dem MDK nur noch differenzierte und auf den Einzelfall bezogene Prüfaufträge erteilen.

Mehrere Monate später erfuhr ich jedoch von einem anderen Krankenhaus, dass die Aufträge der Kasse immer noch nicht den datenschutzrechtlichen Ansprüchen genügen. Deshalb habe ich dem MDK empfohlen, auf die Krankenkassen einzuwirken und nur solche Aufträge auszuführen, die hinreichend konkret sind. Der MDK hat mir mitgeteilt, dass aus dortiger Sicht die bisherige Vorgehensweise ebenfalls nicht befriedigend sei. Im Übrigen liege zu dieser Frage inzwischen ein Vermittlungsvorschlag der Landesschiedsstelle vor, der am 1. April 1999 in Kraft gesetzt worden ist und Näheres zur Überprüfung der Notwendigkeit und der Dauer von Krankenhausbehandlungen regelt. Zu diesem Vertrag hat der MDK ein Ankündigungsschreiben entworfen, das der Krankenkasse anhand von 25 vorgegebenen Gründen ermöglicht, das Prüfungsersuchen zu konkretisieren. Weitere Erläuterungen oder Gründe können auf dem Schreiben frei eingetragen werden. Abschließend wird das Krankenhaus darin gebeten, seine Stellungnahme dem MDK innerhalb von zehn Tagen zuzusenden.

Diese Vorgehensweise ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

3.11.6 Patientenakten aus dem Krankenhaus gestohlen

Ein Journalist hat mich informiert, dass auf einer illegalen Müllkippe Unterlagen aus einem Krankenhaus gefunden worden sind. Aus einer Patientenakte war beispielsweise das Schicksal einer im Krankenhaus nach einer Operation verstorbenen Patientin zu entnehmen. Außerdem befanden sich darin ein Gutachten eines rechtsmedizinischen Instituts und ein Obduktionsbefund, aus dem hervorging, dass bei richtigen medizinischen Maßnahmen die Patientin nicht verstorben wäre. Der Name des Arztes, der für die medizinische Versorgung der Patientin verantwortlich war, war ebenfalls in den Unterlagen genannt.

Patientendaten unterliegen dem besonderen Schutz der ärztlichen Schweigepflicht (§ 203 Strafgesetzbuch). Diesem Schutzbedürfnis müssen Krankenhäuser beim Umgang mit Patientenakten durch angemessene technische und organisatorische Maßnahmen gerecht werden. Gelangen solche Unterlagen unbefugten Dritten in die Hände, werden Patienten und unter Umständen auch Personal in ihren Persönlichkeitsrechten verletzt, und ihnen können darüber hinaus materielle Schäden entstehen.

In diesem Fall hatte die Krankenhausverwaltung geprüft, ob ein ärztlicher Behandlungsfehler vorlag. Deshalb waren die Unterlagen nicht - wie sonst üblich - im Krankenhausarchiv, sondern im Panzerschrank der Verwaltung aufbewahrt worden. Der Verwaltungsdirektor hat auf meine Anfrage hin mitgeteilt, dass in diese Räume eingebrochen wurde und die Aktenschränke sowie ein darin befindlicher festmontierter Stahlschrank aufgebrochen worden sind. Die Täter haben nach seiner Meinung dann offensichtlich die für sie nicht nützlichen Unterlagen auf der Müllkippe entsorgt.

Obwohl die Verwaltungsräume durch eine funktionstüchtige Alarmanlage gesichert waren, konnten weder das Krankenhauspersonal noch die Polizei die Einbrecher stellen. Meine weitere Kontrolle ergab allerdings, dass die Polizei erst eine Stunde nach dem Ansprechen der Alarmanlage über den Alarm informiert worden ist. Sie ist dann zwar unverzüglich am Tatort erschienen, doch verliefen ihre Ermittlungen nun erfolglos.

Der Verwaltungsdirektor teilte darüber hinaus mit, dass es in der Vergangenheit öfter Fehlalarme gab. Deshalb habe der zuständige Mitarbeiter dieser Alarmierung keine Bedeutung beigemessen und ist zu spät der Ursache nachgegangen.

Es zeigte sich hier, dass zwar angemessene technische Einrichtungen zum Schutz der Unterlagen vorhanden waren, organisatorische Mängel im Krankenhaus jedoch den Umfang des Schadens nicht begrenzen konnten. Eine Alarmanlage ist natürlich nutzlos, wenn nicht sichergestellt ist, dass sofort geeignete Maßnahmen eingeleitet werden, wenn sie anspricht.

In Auswertung des Vorfalls wurde eine neue Dienstanweisung erarbeitet. Demzufolge sind die Mitarbeiter verpflichtet, bei jedem Alarm sofort die Polizei zu verständigen.

3.11.7 Diktate nicht gelöscht, Patientendaten auf dem Müll

Ein Bürger fand im Sperrmüll einen Anrufbeantworter, für den er Verwendung hatte. Zu Hause stellte er fest, dass sich in dem Gerät noch eine Magnetbandkassette befand, auf der Diktate mit Patientendaten gespeichert waren. Er informierte eine Zeitung, die über den sorglosen Umgang mit diesen Daten im November 1999 berichtete.

Ich habe mich mit dem Bürger in Verbindung gesetzt und die Tonbandkassette erhalten, um den Inhalt auszuwerten. Das Band enthielt mehrere Diktate über stationäre Behandlungen namentlich genannter Patienten aus den Jahren 1992 und 1993, insbesondere Epikrisen und Röntgenbefunde.

Darüber hinaus nannte am Ende vieler Diktate der Diktierende seinen Namen. Auf meine Nachfrage hat mir die Ärztekammer mitgeteilt, in welchem Krankenhaus ein Arzt mit diesem Namen tätig gewesen ist. Bei einer Kontrolle des Krankenhauses hat mir der leitende Chefarzt bestätigt, dass dieser Arzt in der fraglichen Zeit dort angestellt war und auch die Patienten dort behandelt worden sind. Der genaue Hergang des Verlustes dieser Kassette konnte im Krankenhaus nicht mehr festgestellt werden. Möglicherweise sind bei einem Umtausch der Diktiertechnik nicht gelöschte Bänder an Dritte gelangt.

Ich habe den sorglosen Umgang mit Patientendaten beanstandet, insbesondere weil keine ausreichenden technischen und organisatorischen Maßnahmen zum Schutz der gespeicherten Patientendaten vorgesehen waren.

Das Krankenhaus hatte bereits kurz nach meinem Besuch eine Dienstanweisung zum Umgang mit auf Tonträgern gespeicherten Patientendaten erlassen. Nunmehr sollen die Tonträger registriert und gegen den Zugriff durch Dritte beziehungsweise vor Verlust geschützt werden. Unmittelbar nach dem Abschreiben der Diktate sind die Daten auf den Magnetbandkassetten zu löschen. Dazu werden die Kassetten kurzzeitig einem Magnetfeld ausgesetzt. Entsprechende Löschmagnete stehen seit dem Tausch der Diktiertechnik zur Verfügung. Die eingeleiteten Maßnahmen (§ 17 Abs. 2 Nrn. 1, 2 und 6 DSG MV) erscheinen geeignet, um ähnliche Vorfälle für die Zukunft weitgehend auszuschließen.

3.12 Personalwesen

3.12.1 Was die Polizei von Bewerbern wissen will

Ein Bewerber für den Polizeidienst in Mecklenburg-Vorpommern hat mich um eine datenschutzrechtliche Prüfung der von ihm auszufüllenden Datenerhebungsbogen gebeten. Er sollte unter anderem Fragen zur Person, zu den familiären Verhältnissen sowie zum Gesundheitszustand beantworten.

Nach dem Landesbeamtengesetz dürfen Daten über Bewerber erhoben werden, soweit dies zur Begründung des Dienstverhältnisses erforderlich ist oder eine Rechtsvorschrift dies erlaubt (§ 100 Abs. 4 Landesbeamtengesetz - LBG M-V). Bei einigen Daten bestanden jedoch Zweifel, ob sie für diesen Zweck tatsächlich notwendig sind.

Im allgemeinen Teil des Erhebungsbogens wurde im Zusammenhang mit der Adresse danach gefragt, bei welcher Person der Bewerber Untermieter ist. Um den Bewerber für mögliche Rückfragen zu erreichen, sind die Angaben des Vermieters nicht erforderlich. Keine Einwände bestehen gegen Auskünfte über eine Haupt- oder Nebenwohnung. Ferner sollte er auch die Telefonnummer angeben. Dies ist ein Datum, das nur auf freiwilliger Basis erhoben werden kann, denn es ist nicht zwingend für die Bearbeitung einer Bewerbung erforderlich. Ich habe vorgeschlagen, die Bewerber darauf hinzuweisen, welche Fragen freiwillig beantwortet werden können.

Nicht zu erkennen ist, zu welchem Zweck Daten wie der Geburtsname und das Geburtsdatum des Ehepartners oder Name, Vorname sowie Beruf und Wohnung der Eltern notwendig sein sollen. Sofern diese Angaben für eine Sicherheitsüberprüfung benötigt werden, ist der Bewerber nach den Vorschriften des Sicherheitsüberprüfungsgesetzes auf den Zweck dieser Erhebung hinzuweisen. In diesem Fall wären die Daten gesondert zu erheben.

Darüber hinaus waren meines Erachtens einige Fragen des Erhebungsbogens zu weitgehend. Beispielsweise ist bei geforderten Angaben über Strafen zu prüfen, ob eine zeitliche Eingrenzung (wie Strafen der letzten xx Jahre) entsprechend der Speicherdauer im Bundeszentralregister den Zweck erfüllt. Auch die Erhebung über finanzielle Verpflichtungen oder Schulden war zu weitgehend beziehungsweise nicht klar formuliert. Zulässig wäre jedoch die Frage, ob der Bewerber finanzielle Verpflichtungen hat, die er aus dem bisherigen oder zu erwartenden Einkommen nicht bedienen kann.

Bei einzelnen Fragen zur gesundheitlichen Vorgeschichte des Bewerbers hatte ich Zweifel, ob sie überhaupt im Vorfeld der ohnehin noch durchzuführenden ärztlichen Untersuchung und damit ohne ärztliche Beratung beantwortet werden sollten. Dies betraf insbesondere die Angaben zur Familienanamnese. So sollte unter anderem angegeben werden, ob bei einem nahen Verwandten bestimmte Krankheiten vorgekommen sind oder ob ein naher Verwandter Selbstmord begangen hat. Da der Bewerber nicht abschätzen kann, wieweit er Krankheiten seiner Angehörigen offenbaren soll, wird er meines Erachtens einem Konflikt ausgesetzt. Er steht hier möglicherweise unter dem Druck, „alle Umstände zu offenbaren“, und wird deshalb dazu neigen, Angaben zu machen, die ein Arzt später als nicht relevant für die gesundheitliche Disposition einstuft. Beispielsweise ist fraglich, ob der Selbstmord eines Onkels zur Beurteilung der gesundheitlichen Eignung erforderlich ist. Für den Bewerber ist dies ein naher Verwandter. Ein Arzt mag aber zu der Einschätzung kommen, dass dieser Selbstmord keine Schlussfolgerungen auf den Gesundheitszustand des Betroffenen zulässt, und würde dieses Datum nicht in die ärztliche Dokumentation aufnehmen. Dem Betroffenen sind aber in der Regel medizinische Zusammenhänge nicht bekannt und somit wäre möglicherweise ein nicht erforderliches Datum Bestandteil der über einen langen Zeitraum aufzubewahrenden polizeiärztlichen Dokumentation.

Damit der Bewerber nicht im Vorfeld einer Untersuchung Eintragungen vornimmt, die nicht notwendig sind, habe ich empfohlen, ihm die Wahl zu überlassen, ob er die Daten zur gesundheitlichen Vorgeschichte vor der Untersuchung oder im Beisein des untersuchenden Arztes beantwortet.

Das Innenministerium unseres Landes hat zugesagt, meine Empfehlungen bei der Überarbeitung des Formulars zu berücksichtigen.

Auf die Frage nach dem Selbstmord von nahen Verwandten wird angesichts ihrer geringen Aussagekraft für die Beurteilung der gesundheitlichen Eignung eines Bewerbers künftig verzichtet.

3.12.2 Praxis der Stasi-Überprüfung noch zeitgemäß?

Mit Blick auf den 10. Jahrestag der Wiedervereinigung im Jahr 2000 wird von unterschiedlichen Kräften vor allem aus dem Bereich der Politik vorgeschlagen, die Überprüfungen bei Mandatsträgern und Mitarbeitern im öffentlichen Dienst anhand von Stasi-Unterlagen zu überdenken und möglicherweise neu zu gestalten.

Seit dem In-Kraft-Treten des Stasi-Unterlagen-Gesetzes (StUG), das wesentliche rechtliche Grundlagen für eine Überprüfung von Beschäftigten des öffentlichen Dienstes, von Abgeordneten sowie Angehörigen kommunaler Vertretungskörperschaften enthält, beschäftigt diese Thematik insbesondere auch die Datenschutzbeauftragten in den neuen Bundesländern.

Eine Arbeitsgruppe von Datenschutzbeauftragten des Bundes und der Länder, der auch ich angehörte, hat sich 1999 intensiv mit der Überprüfungspraxis befasst. Im Ergebnis konnte keine einheitliche Auffassung zu Papier gebracht werden. Folgende Überlegungen standen zur Diskussion:

Ein datenschutzrechtlicher Grundsatz besagt unter anderem, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn sie rechtmäßig erhoben worden sind. Deshalb dürfen öffentliche Stellen Datensammlungen, die auf rechtswidrige Weise und unter Verstoß gegen Menschenrechte zu Stande gekommen sind, grundsätzlich nicht verwenden. Die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR sind derartige Datensammlungen. Die letzte, frei gewählte Volkskammer und anschließend der Bundesgesetzgeber sind aber der seinerzeit stark diskutierten Forderung, diese Aktensammlungen unbesehen zu vernichten, aus guten Gründen nicht gefolgt.

Inzwischen sind allerdings die Überlegungen und Zielsetzungen, die zu einer Legitimation der weiteren Verwendung der Informationen aus diesen Datensammlungen geführt haben, differenziert und mit etwas mehr Abstand zu betrachten. So ist fraglich, ob Daten aus diesen Sammlungen bei Personalmaßnahmen im öffentlichen Dienst der neuen Bundesländer weiterhin als prägendes Element für das Kriterium der persönlichen Eignung und damit der Zuverlässigkeit herangezogen werden können, während in den alten Bundesländern eine solche Regelüberprüfung schon lange nicht mehr stattfindet beziehungsweise überhaupt nie stattgefunden hat. Angesichts der latenten Fluktuation ganzer Bevölkerungsteile zwischen den alten und den neuen Bundesländern dürfte eine solch unterschiedliche Handhabung ohnehin nicht zu rechtfertigen sein. Bezweifelt werden muss auch, ob bei den heute weit über zehn Jahre zurückliegenden Ereignissen der Wahrheitsgehalt einzelner Daten noch in ausreichendem Maße überprüft werden kann und eine gerechte Bewertung der Ergebnisse in jedem Einzelfall noch möglich ist.

Es darf aber gerade das in weiten Teilen der Bevölkerung der neuen Bundesländer ausgeprägte Bedürfnis nach nunmehr gerechtem Handeln ihres Staates nicht einer formalen Rechtsstaatlichkeit untergeordnet werden. Insbesondere die in der Bevölkerung verbreitete Sorge, dass alte Spitzel und Denunzianten in neuen öffentlichen Ämtern wieder Entscheidungen über sie treffen, darf man nicht ignorieren.

Daher ist eine möglichst breite und weitgehend offene Diskussion über dieses Thema geboten.

Umfang der Überprüfungen

Einer kritischen Betrachtung bedarf beispielsweise die Frage, welche Personengruppen zehn Jahre nach Auflösung des Ministeriums für Staatssicherheit noch in die Überprüfung einbezogen werden:

Die Überprüfung öffentlich Bediensteter sowie von Bewerbern für den öffentlichen Dienst zielt darauf ab festzustellen, ob die Betroffenen die hierfür erforderliche persönliche Zuverlässigkeit besitzen oder ob ein Festhalten am Arbeitsverhältnis unzumutbar erscheint (vgl. Einigungsvertrag Anlage I, Kapitel XIX, Sachgebiet A, Abschnitt III, Nr. 1, Abs. 5).

Sind von vornherein keine Ergebnisse zu erwarten, die unter diesen Gesichtspunkten für eine Kündigung oder einen Ausschluss des Bewerbers zu verwerten sind, hat die Überprüfung zu unterbleiben. Dies ist nach der höchstrichterlichen Rechtsprechung schon jetzt der Fall, wenn

- ein nach der Wiedervereinigung begonnenes Arbeitsverhältnis jahrelang unbeanstandet geblieben ist, der/die Bedienstete sich mithin bewährt hat;
- eine einzelfallbezogene Würdigung der gesamten Persönlichkeit ohnehin dazu führen würde, dass eine eventuell entdeckte Stasi-Verstrickung keine besonderen Maßnahmen rechtfertigen würde oder
- wegen des Alters der Person eine Verstrickung ausgeschlossen ist oder wegen des Zeitablaufs nicht mehr berücksichtigt werden könnte.

Zugrunde zu legen ist darüber hinaus auch die Wertigkeit der konkret besetzten oder zu besetzenden Positionen; grundsätzlich sollten die Überprüfungen auf Personen beschränkt werden, die eine herausragende Stellung einnehmen oder einnehmen sollen. Dies muss auch für Personengruppen gelten, denen die Bevölkerung ein besonderes Vertrauen entgegenbringt (Polizei, Justiz, Bildungswesen). Von Überprüfungen aller Personen des öffentlichen Dienstes wäre deshalb abzusehen.

Hingegen können und sollten diese Überprüfungen weiterhin erfolgen, wenn der konkrete Verdacht besteht, dass ein Sachverhalt vorliegt, der personelle Maßnahmen rechtfertigen würde.

Die Landesregierung Mecklenburg-Vorpommern hat im Februar 1999 beschlossen, dass bei Bewerbungen für den öffentlichen Dienst nicht mehr regelmäßig beim BStU (Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR) nachgefragt wird. Anfragen erfolgen nur, wenn tatsächliche Anhaltspunkte für eine Zusammenarbeit mit dem Ministerium für Staatssicherheit (MfS)/dem Amt für Nationale Sicherheit (AfNS) vorliegen, wenn sich jemand für eine herausgehobene Position bewirbt oder wenn einem Bewerber sicherheitsempfindliche Aufgaben übertragen werden sollen. Außerdem ist der Zeitraum für solche Anfragen auf Tätigkeiten begrenzt worden, die am 31. Dezember 1980 oder danach begannen oder die davor begannen, aber über diesen Zeitpunkt hinaus andauerten.

Besondere Probleme wirft die Überprüfung von Abgeordneten und Angehörigen kommunaler Vertretungskörperschaften auf. Zwar gilt sie noch immer als vertrauensbildende Maßnahme, gleichwohl zeigt sich aber gerade hier, dass das Aufdecken einer früheren Verbindung zum Ministerium für Staatssicherheit nicht zwangsläufig zu Konsequenzen führt. Darüber hinaus sind einige der Betroffenen heute schon bis zu sechsmal überprüft worden. Deshalb sollte auch bei diesen Personen die Überprüfung in absehbarer Zeit ein Ende finden. In Mecklenburg-Vorpommern findet die Prüfung der Landtagsabgeordneten nach einer Änderung des Abgeordnetengesetzes zu Beginn der 3. Wahlperiode auf freiwilliger Basis statt.

Nutzung von Daten im Rahmen der Überprüfungen

Die Nutzung von Daten für Überprüfungen muss sowohl dem Anliegen des Stasi-Unterlagen-Gesetzes, die historische, politische und juristische Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes zu gewährleisten und zu fördern, als auch dem Recht der Betroffenen auf informationelle Selbstbestimmung Rechnung tragen.

Es lässt sich nicht vermeiden, dass Mitarbeiter des Bundesbeauftragten für die Stasi-Unterlagen bei Recherchen auch Unterlagen von Opfern des Staatssicherheitsdienstes einsehen. Dieser tiefe Eingriff in die Privatsphäre von Betroffenen ist aber so gering wie möglich zu halten. Es sollte daher bereits in der Behörde des Bundesbeauftragten sichergestellt werden, dass Akten über Betroffene der Stasitätigkeit in eine erneute Überprüfung nicht wiederholt einbezogen werden, insbesondere dann nicht, wenn diese Unterlagen Daten aus der Intimsphäre der Betroffenen enthalten.

Das StUG selbst sieht für Mitarbeiter des öffentlichen Dienstes ein Mitteilungsverbot über eine inoffizielle Tätigkeit für das Ministerium für Staatssicherheit vor dem 31. Dezember 1975 vor (§ 19 Abs. 1 Satz 2 StUG). Dieses Mitteilungsverbot gilt aber nicht für Abgeordnete und Angehörige kommunaler Vertretungskörperschaften. Der Rechtsgedanke, dass eine weit zurückliegende inoffizielle Tätigkeit für den Staatssicherheitsdienst nicht grundsätzlich die Eignung des Betreffenden für eine Tätigkeit im öffentlichen Dienst in Frage stellt, sollte durch eine angemessene Dynamisierung des Mitteilungsverbotes über eine Mitarbeit, die länger als 20 Jahre zurückliegt, fortgeführt werden.

Die Verwendung der Stasi-Unterlagen ist auf den Zweck der Überprüfung beschränkt. Eine Zweckentfremdung von Überprüfungsergebnissen ist in jedem Fall auszuschließen. Insbesondere dürfen Informationen, die im Rahmen einer Überprüfung erlangt wurden, nicht zur öffentlichen Anprangerung, zur politischen Rechtfertigung, zur Titelaberkennung oder bei Beförderungsentscheidungen genutzt werden. Die Strafvorschrift des § 44 StUG sollte dahingehend erweitert werden, dass jedes unbefugte, zweckfremde Mitteilen von Informationen auch über eine inoffizielle Tätigkeit strafbar ist.

Rechte der Betroffenen

Die ursprüngliche Fassung des Stasi-Unterlagen-Gesetzes räumte Betroffenen und Dritten ein Antragsrecht auf Anonymisierung der sie betreffenden Daten ab dem 1. Januar 1997 ein. Der Gesetzgeber hat diesen Termin zweimal, nunmehr auf den 1. Januar 2003, verschoben. Den Betroffenen und Dritten sollte aber bereits jetzt zumindest ein Widerspruchsrecht gegen die Verarbeitung ihrer personenbezogenen Daten durch den Bundesbeauftragten für die Stasi-Unterlagen eingeräumt werden, wenn sie aufgrund ihrer besonderen Situation überwiegende schutzwürdige Gründe gegen diese Verarbeitung anführen können. Eine solche Regelung würde auch dem Rechtsgedanken des Art. 14 lit a) der Europäischen Datenschutzrichtlinie Rechnung tragen, die jedem ein Widerspruchsrecht gegen die prinzipiell rechtmäßige Verarbeitung seiner Daten aus überwiegenden, schutzwürdigen, sich aus seiner besonderen Situation ergebenden Gründen einräumt.

Weiterhin sollten im Zusammenhang mit der Weitergabe von personenbezogenen Daten für Zwecke der Forschung, der politischen Bildung und der Berichterstattung durch die Medien (§§ 32, 34 StUG) die Informationsrechte der betroffenen Personen gestärkt werden. Dabei kann es nicht darum gehen, den Amtsträgern bzw. Personen der Zeitgeschichte, Mitarbeitern und Begünstigten des Staatssicherheitsdienstes generell die Möglichkeit zu eröffnen, diese Übermittlung zu unterbinden. Sie sollten aber vorab beziehungsweise zeitgleich zumindest über die Weitergabe informiert werden.

Schließlich sind Fälle bekannt geworden, in denen Dienstherren ehemaligen Mitarbeitern des Ministeriums für Staatssicherheit, die bei ihnen beschäftigt waren, Einsicht in die sie betreffenden Bescheide des Bundesbeauftragten für die Stasi-Unterlagen unter Hinweis auf das Stasi-Unterlagen-Gesetz generell verweigert haben. Auch eine Abwägung der berechtigten Interessen der betroffenen Opfer und Dritter am Schutz ihrer personenbezogenen Daten mit dem rechtlichen Interesse ehemaliger Mitarbeiter der Staatssicherheit kann jedoch nicht dazu führen, dass einem ehemaligen Mitarbeiter des Staatssicherheitsdienstes die Möglichkeit der Rechtsverteidigung derart verkürzt wird.

Aufbewahrung der personenbezogenen Unterlagen

Die Unterlagen sind sicher und vor unbefugtem Zugang geschützt aufzubewahren. Darüber hinaus sind differenzierte Aufbewahrungsfristen festzulegen, die dem Grundsatz der Erforderlichkeit Rechnung tragen und sich am zeitlichen Rahmen der Überprüfung hinsichtlich des Mitteilungsverbotes über eine lang zurückliegende inoffizielle Tätigkeit für den Staatssicherheitssdienst (§ 19 StUG) und dem Ende des Überprüfungsprozesses im Jahre 2006 (§ 20 Abs. 3 StUG) orientieren.

Es ist sicherzustellen, dass personenbezogene Daten, die der Bundesbeauftragte für die Stasi-Unterlagen an andere Stellen herausgegeben hat, nach Erledigung der Aufgaben an den Bundesbeauftragten zurückgegeben bzw. vernichtet werden, soweit nicht gesonderte Archivgesetzbestimmungen etwas anderes regeln. Neben den Archiven des Bundesbeauftragten sollten grundsätzlich keine weiteren Archive personenbezogene Unterlagen des Staatssicherheitsdienstes oder Kopien davon aufbewahren.

3.12.3 Was darf in die Personalakte aufgenommen werden?

In vielen Anfragen wollten Bürger von mir wissen, welche Daten von Beschäftigten des öffentlichen Dienstes für die Personalakte erhoben werden dürfen.

Personalakten müssen ein möglichst vollständiges Bild über den Werdegang des Beschäftigten geben, um zu einem sachgemäßen Personaleinsatz und zu einer effektiven Personalplanung beizutragen. Da es sich bei den Personalakten um so genannte zahlungsbegründende Unterlagen handelt, müssen sie außerdem Daten enthalten, die zur Zahlung von Besoldung, Vergütung oder Lohn erforderlich sind.

Ein Petent hat mir mitgeteilt, dass eine Gemeinde bei einer Scheidung vollständige Scheidungsurteile von ihren Beschäftigten für die Personalakten anfordert. Es war für ihn nicht nachvollziehbar, zu welchem Zweck das vollständige Urteil benötigt wird.

Die Beschäftigungsbehörde muss wissen, ob ein Beschäftigter ledig, verheiratet oder geschieden ist, weil unter anderem die Höhe des zu zahlenden Familienzuschlages davon abhängig ist. Diese Daten sind auch durch entsprechende Unterlagen nachzuweisen. Dafür ist es jedoch nicht erforderlich, das vollständige Scheidungsurteil in die Personalakte aufzunehmen. In den Verwaltungsvorschriften des Innenministeriums zum Landesbeamtengesetz Mecklenburg-Vorpommern (LBG MV), deren Anwendung das Ministerium im Übrigen auch den Gemeinden empfiehlt, ist daher geregelt, dass ein Beschäftigter die Scheidung durch Vorlage des Richterspruchs (Tenor des Urteils) oder durch eine beglaubigte Abschrift des Familienbuches mit dem Scheidungsvermerk nachweisen kann. Nicht zulässig ist es dagegen, das vollständige Scheidungsurteil einschließlich der Scheidungsgründe zu verlangen.

Darauf habe ich die zuständige Personalstelle hingewiesen. Sie hat meine Empfehlung berücksichtigt und wird künftig nur die entsprechenden Unterlagen zur Personalakte nehmen.

Durch eine andere Petition wurde ich darüber informiert, dass die Personalabteilung eines Ministeriums von den Beamten Mitgliedsbescheinigungen der Krankenkassen verlangt, um sie zu den Unterlagen zu nehmen.

Auf meine Frage, zur Erfüllung welcher Aufgaben die Angaben zur Krankenversicherung in der Personalakte erhoben werden, teilte mir das Ministerium mit, dass der Dienstherr eine Meldepflicht gegenüber der Krankenkasse habe. Eine solche Pflicht bestehe beispielsweise, wenn Gehaltszahlungen wegen Langzeiterkrankungen eingestellt werden sollen.

Entsprechend der Vorschriften des Sozialgesetzbuches existieren Meldepflichten nur für Sozialversicherungspflichtige beziehungsweise für Beschäftigte, die freiwillig gesetzlich krankenversichert sind. Für Beamte, die privatversichert sind, fehlt es an einer Rechtsgrundlage, nach der die Beschäftigungsbehörde zu dieser Mitteilung verpflichtet ist. Insoweit dürfen Mitgliedsbescheinigungen von Beamten für Personalunterlagen auch nicht gefordert werden.

Ich habe dem Ministerium empfohlen, künftig auf die Erhebung dieser Bescheinigungen zu verzichten und bereits angeforderte Nachweise aus den Akten zu entfernen und zu vernichten.

Die Empfehlung wurde umgesetzt. Ergänzend sei jedoch erwähnt, dass die Beihilfestelle wissen muss, ob ein Beamter privat oder freiwillig in der gesetzlichen Krankenversicherung versichert ist, um die entsprechenden Kosten für ärztliche Leistungen, Heil- oder medizinische Hilfsmittel auf der Grundlage des jeweiligen Versicherungsschutzes erstatten zu können. Die Beihilfestelle fordert daher vor der erstmaligen Kostenerstattung zu Recht einen Krankenversicherungsnachweis an.

3.13 Bildung, Kultur, Wissenschaft und Forschung

3.13.1 Chipkarte als Studentenausweis

Eine Tageszeitung berichtete über das Vorhaben einer Hochschule unseres Landes, einen elektronischen Studentenausweis (Chipkarte) einzuführen. Dieser sollte nicht nur als Studenten- und Bibliotheksausweis sowie als Meldekarte genutzt werden, sondern auch als Geldkarte für bargeldlose Zahlungen an Kopiergeräten und in der Mensa.

So interessant das Vorhaben auch erscheint - der obligatorische Einsatz einer „Hochschulchipkarte“ bedarf einer Rechtsgrundlage, und an dieser fehlt es im Landeshochschulgesetz (LHG M-V). Daher kann eine solche Chipkarte nur mit Einwilligung der Studenten eingeführt werden. In diesem Fall sind die Studenten umfassend über Art, Umfang, Zweck und Beteiligte der Datenverarbeitung zu informieren. Von einer wirksamen Einwilligung kann aber nur dann ausgegangen werden, wenn die Studierenden auch ohne Nutzung der Chipkarte gleiche Leistungen in Anspruch nehmen können. Für den Einzelnen darf ein Kartenverzicht also nicht mit gravierenden Nachteilen verbunden sein.

Aufgrund der vielfältigen Nutzungsmöglichkeiten ist auch durch technische Maßnahmen sicherzustellen, dass nur die jeweils berechtigte Stelle die erforderlichen Daten lesen kann. Die auf einem Chip gespeicherten Daten müssen einer strengen Zweckbindung unterliegen. Identifizierende Angaben wie Name und Adresse können in der Regel von allen berechtigten Stellen der Universität gelesen werden. Anders verhält es sich jedoch bei Angaben wie Matrikelnummer, Studienfach oder Semester. Diese sind an einen eingeschränkten Verwendungszweck gebunden.

Die Projektunterlagen sahen aber beispielsweise vor, dass die Matrikelnummer auf den Kartenkörper gedruckt werden sollte. Damit würde die Trennung von Matrikelnummer und Person aufgehoben. Die Matrikelnummer ist ein hochschulinternes personenbezogenes Datum und darf deshalb nur für hochschulinterne Anwendungen und auch in diesem Rahmen nur für berechtigte Mitarbeiter zugänglich sein. Um den erforderlichen Zugriffschutz zu realisieren, muss die Matrikelnummer im Chip sicher gegen einen Zugriff durch Dritte gespeichert werden, beispielsweise in Zusammenhang mit einer PIN (Persönliche Identifikations-Nummer).

Mit der Einführung des Chipkartenprojektes sind auch technische und organisatorische Maßnahmen zu treffen, die eine datenschutzgerechte Verarbeitung der Daten sicherstellen. Vor allem betrifft dies die fälschungssichere Authentifizierung der Karteninhaber, die Steuerung der Zugriffs- und Nutzungsberechtigungen sowie die Vertraulichkeit und Integrität der gespeicherten Daten. Insbesondere ist es nicht zulässig, personenbezogene Nutzungsprofile zu erstellen.

Gegen eine Einführung von Chipkarten an Hochschulen bestehen im Grunde keine Bedenken, sofern die oben genannten datenschutzrechtlichen und technisch-organisatorischen Aspekte berücksichtigt werden.

3.13.2 Anfrage bei der Sekteninformationsstelle - nicht vertraulich?

Ein Bürger hatte Fragen zu einer in unserem Land ansässigen religiösen Gruppe und wandte sich an die Sekteninformationsstelle im (damaligen) Kultusministerium. In diesem Zusammenhang teilte er dem Ministerium mit, dass seine Frau Mitglied dieser Gruppe sei. Er befürchtete, dass es sich bei der religiösen Gruppe um eine Sekte handelt, die auch seine beiden gegenwärtig bei der Mutter lebenden minderjährigen Kinder beeinflussen könnte. Der Brief enthielt eine Reihe sehr sensibler Informationen aus dem unmittelbaren persönlichen und familiären Bereich. Unter anderem war dem Kultusministerium nunmehr bekannt, dass in einem Sorgerechtsstreit um die beiden Kinder ein Jugendamt eingeschaltet war. Auch war man dort der Auffassung, die Anfrage des Petenten und die Antwort des Ministeriums dem Jugendamt zur Erfüllung seiner Aufgaben übermitteln zu müssen. Von dieser Übermittlung erhielt der Petent bei einer Akteneinsicht im Jugendamt Kenntnis. Er hat mich gebeten, den Sachverhalt aus datenschutzrechtlicher Sicht zu prüfen.

Der zuständige Mitarbeiter des Kultusministeriums erklärte, dass die Übermittlung dieser Daten aufgrund von datenschutzrechtlichen Bestimmungen zulässig sei. Außerdem seien die persönlichen Angaben aus dem Brief dem Jugendamt ohnehin bekannt, da es mit der Familiensache befasst sei.

Eine Rechtsvorschrift, die die Vorgehensweise des Kultusministeriums rechtfertigt, existiert nicht. Die Datenübermittlung war weder erforderlich, um Aufgaben der Sekteninformationsstelle, noch um solche des Jugendamtes zu erfüllen. Es konnten keine konkreten Aufgaben genannt werden, nach denen der Sachverhalt datenschutzrechtlich anders bewertet werden müsste. Auch der Hinweis, die übermittelten Daten wären dem Jugendamt bekannt, lässt keine andere Bewertung zu, denn zumindest die Tatsache, dass sich der Petent an die Sekteninformationsstelle gewandt hat, war dem Jugendamt nicht bekannt. Da die Behörde die Daten von sich aus, also ohne Anforderung, an das Jugendamt übermittelte, konnte sie keine Kenntnisse darüber haben, ob und gegebenenfalls welche Daten das Jugendamt tatsächlich benötigte.

Wegen des Verstoßes gegen die gesetzlichen Bestimmungen zur Datenübermittlung habe ich dem (jetzigen) Minister für Bildung, Wissenschaft und Kultur eine förmliche Beanstandung ausgesprochen und um eine Stellungnahme gebeten.

Die betreffenden Mitarbeiter wurden über die zu beachtenden datenschutzrechtlichen Bestimmungen belehrt, und es ist davon auszugehen, dass sich ein solcher Vorgang in dieser Behörde nicht wiederholt.

3.13.3 Schüler im Fokus der Forschung

Anfang 1999 wurde ich darüber informiert, dass die Organisation für wissenschaftliche Zusammenarbeit und Entwicklung (OECD) in rund 30 Ländern eine Untersuchung zur Qualität des Schulwesens durchführt. Sie trägt den Titel „Programm for International Students Assessment“ (PISA). Den deutschen Teil der Schulleistungsuntersuchung hat im Auftrag der Kultusministerkonferenz das Max-Planck-Institut für Bildungsforschung (MPI) in Berlin betreut.

Auf meine Nachfrage hin hat unser Bildungsministerium mitgeteilt, dass auch Mecklenburg-Vorpommern sich an der Untersuchung beteiligt, und einige Unterlagen zur datenschutzrechtlichen Bewertung zur Verfügung gestellt. Wegen des kurz bevorstehenden Starts in mehreren Bundesländern und der nur unvollständigen Unterlagen war das allerdings nur noch bedingt möglich. In Zusammenarbeit aller Datenschutzbeauftragten der beteiligten Länder wurden jedoch Verbesserungen erreicht.

So sollten beispielsweise die Eltern der zufällig ausgewählten Schüler eine Einwilligungserklärung unterschreiben, ohne zu wissen, welche Fragen im Einzelnen von ihren Kindern zu beantworten sind. Diese Einwilligung ist jedoch nur dann wirksam, wenn den Eltern und Schülern zum Zeitpunkt der Einwilligung der genaue Inhalt der Fragebögen bekannt ist. Das MPI hat den Eltern nach dem Hinweis der Datenschutzbeauftragten die Möglichkeit eingeräumt, die Fragebögen in der Schule einzusehen. Darüber hinaus wurden sie darauf hingewiesen, dass sie ihre Einwilligung jeder Zeit und ohne Angabe von Gründen widerrufen können.

In einem Anschreiben wurde den Teilnehmern ferner „vollständige Anonymität“ zugesichert. Davon konnte jedoch keine Rede sein, da in dem Erhebungsbogen das Geburtsdatum anzugeben war. Mit diesem Datum und weiteren Angaben wäre es durchaus möglich, eine Person zu bestimmen, auch wenn ihr Name nicht angegeben ist. Um zu gewährleisten, dass die Daten auch mit Zusatzwissen keiner Person zugeordnet werden können, haben die Datenschutzbeauftragten empfohlen, lediglich den Geburtsmonat und das -jahr zu erheben.

Die Hinweise wurden bei der Überarbeitung der Unterlagen berücksichtigt. Ich habe das Bildungsministerium gebeten, bei ähnlichen bundesweiten Forschungsprojekten darauf zu dringen, für eine datenschutzrechtliche Abstimmung eine angemessene Zeit vorzusehen.

Im April 1999 wurde ich über ein weiteres Forschungsprojekt in Kenntnis gesetzt. Das MPI ist danach an einer internationalen Studie zur politischen Bildung von Schülern und Schülerinnen beteiligt, die wieder in mehreren Bundesländern durchgeführt wird. Auch hier habe ich ähnliche datenschutzrechtliche Defizite festgestellt wie bei dem Forschungsprojekt PISA. Vor allem die Anschreiben an die Eltern und Lehrkräfte sowie die Einwilligungserklärungen genügten wieder nicht den datenschutzrechtlichen Bestimmungen.

Das Bildungsministerium unseres Landes hat mitgeteilt, dass bei einer ersten Präsentation der Daten im MPI auch über die datenschutzrechtlichen Mängel gesprochen worden ist. Es wurde dort vereinbart, dass die Datenschutzbeauftragten künftig bereits in der Planungsphase entsprechender Untersuchungen einbezogen werden sollen.

3.13.4 Forschungsprojekt über Hausarztpraxen

Die Kassenärztliche Vereinigung Mecklenburg-Vorpommern wollte das Projekt „Hausarztpraxen mit psychosomatischer Besonderheit“ einführen und zuvor von mir wissen, welche datenschutzrechtlichen Bestimmungen dabei zu berücksichtigen sind.

Ziel dieses Projektes ist es, die so genannte Gesprächsmedizin zu fördern. Durch neue ärztlich präventive und therapeutische Möglichkeiten soll die Beratung bedürftiger Patienten verbessert und darüber hinaus die Qualität und Wirtschaftlichkeit dieser Praxen ermittelt werden. Ein privates Forschungsinstitut sollte die Ergebnisse auswerten. Um die Aufgaben erfüllen zu können, war es unter anderem erforderlich, Patienten und Praxisinhaber zu befragen.

Die Zulässigkeit von Forschungsvorhaben mit Sozialdaten aus der gesetzlichen Krankenversicherung richtet sich nach § 287 Abs. 1 Sozialgesetzbuch Fünftes Buch (SGB V). Danach dürfen die Krankenkassen und die Kassenärztliche Vereinigung Datenbestände für Forschungszwecke auswerten. Da aber diese Aufgabe dem Institut übertragen werden sollte, habe ich den Abschluss einer Datenschutzvereinbarung zwischen der Kassenärztlichen Vereinigung und dem Institut empfohlen. Diese sollte unter anderem Folgendes regeln:

Dem Institut dürfen nur Daten übermittelt werden, die eine Identifizierung von Patienten und Praxisinhabern ausschließen (pseudonymisierte Daten).

Die Kassenärztliche Vereinigung als Auftraggeber des Forschungsvorhabens ist in diesem Rahmen gegenüber dem Institut weisungsberechtigt und darf die Räumlichkeiten des Auftragnehmers betreten, um die Datenverarbeitung und -nutzung zu kontrollieren.

Das Institut hat technische und organisatorische Maßnahmen zu treffen, um einen unberechtigten Zugriff auf Computer, Datenträger und Datenspeicher zu verhindern. Insbesondere ist festzulegen, wie der sichere Transport beziehungsweise der Versand von Datenträgern erfolgt, in welcher Form Datenträger beim Institut aufbewahrt und wie nicht mehr benötigte Daten gelöscht werden.

Unter Berücksichtigung dieser Empfehlungen wurde ein datenschutzgerechtes Konzept erarbeitet, so dass der Durchführung des Projektes nichts mehr im Wege stand.

3.14 Wirtschaft und Gewerbe

3.14.1 Kontrolle einer Handwerkskammer

Im Berichtszeitraum habe ich in einer Handwerkskammer den Umgang mit personenbezogenen Daten der Handwerker sowie ihrer Gesellen und Lehrlinge kontrolliert.

Die Handwerkskammer ist nach der Handwerksordnung verpflichtet, eine Handwerksrolle sowie eine Lehrlingsrolle zu führen. Welche Daten für die jeweilige Rolle erforderlich sind, ist in einer Anlage zur Handwerksordnung geregelt. Dort ist auch festgelegt, dass Eintragungen auf Antrag oder von Amts wegen gelöscht werden, wenn die Voraussetzungen dafür nicht mehr vorliegen, beispielsweise weil der Betrieb nicht mehr existiert oder der Lehrling seine Ausbildung beendet hat. Darüber hinaus ist bestimmt, dass die aus den Rollen entfernten Daten in einer gesonderten Datei zu speichern sind. Dies ist unter anderem erforderlich, um gegebenenfalls Fragen zu Firmennachfolgen klären oder eine Ausbildung nachweisen zu können.

Bei dem Kontroll- und Informationsbesuch habe ich insbesondere festgestellt, dass die Handwerkskammer im Antrag auf Eintragung in die Handwerksrolle auch solche Daten erhoben hat, die der Datenkatalog der Handwerksordnung nicht vorsah. Dazu gehörten unter anderem Telefon- und Faxnummern sowie der Geburtsort des Handwerkers. Telefon- bzw. Faxnummern können für die Aufgabenerfüllung der Handwerkskammer, beispielsweise für Rückfragen, durchaus nützlich sein. Im Antrag ist allerdings darauf hinzuweisen, dass deren Angabe freiwillig ist. Das Datum “Geburtsort“ war demgegenüber für die Aufgabenerfüllung der Handwerkskammer weder erforderlich noch nützlich. Daher sollte es künftig nicht mehr erhoben werden.

Auch waren die rechtlichen Vorgaben zur gesonderten Speicherung der aus den Rollen entfernten Daten nicht realisiert. Ich habe empfohlen, diese Vorgaben unverzüglich umzusetzen. Darüber hinaus sollte in einer Dienstanweisung geregelt werden, welche Mitarbeiter mit den archivierten Daten für welche Zwecke umgehen dürfen.

Die mit personenbezogenen Daten umgehende Stelle hat durch entsprechende technische und organisatorische Maßnahmen dafür zu sorgen, dass die Daten nicht Dritten zugänglich sind. Hierzu gehört auch, dass der Zugriff auf Dateien durch ein persönliches Passwort gesichert ist. Ein Passwort ist jedoch nur dann wirksam, wenn es vertraulich behandelt wird. In der Handwerkskammer hat der Systemadministrator die Passworte ausgewählt und eingerichtet. Bei dieser Verfahrensweise ist ein sicherer Nachweis, wer wann welche Daten verarbeitet hat, nicht gewährleistet. Deshalb sollte jeder Anwender sein persönliches Passwort künftig selbst wählen.

Um bei einem Diebstahl oder Brand möglichst schnell reagieren und Datenverluste abwenden zu können, ist es notwendig, dass der Server sicher untergebracht ist. Ich habe der Handwerkskammer empfohlen, den Raum mit Bewegungs- und Rauch-/Brandmeldern nachzurüsten.

Eine weitere Aufgabe der Handwerkskammer ist die Beitragsfestsetzung ihrer Mitglieder. Zu diesem Zweck übermittelt die Oberfinanzdirektion (OFD) Anschrift, Steuernummer und Messbeträge (Gewerbeertrag/Gewinn) aller im Bereich der OFD ansässigen Handwerksbetriebe an die Arbeitsgemeinschaft Kammerleitstelle Messbeträge (AKG). Die AKG teilt der Handwerkskammer zunächst einen verkürzten Datensatz mit, der im Wesentlichen die Betriebsbezeichnung, die Anschrift und die Steuernummer enthält. Die Handwerkskammer gleicht diesen Datensatz mit den Betrieben ab, die in ihre Rolle eingetragen sind, und vervollständigt ihn mit der entsprechenden Betriebsnummer. Der so bearbeitete Datensatz wird wieder an die AKG übermittelt und dort mit den Daten zum Gewerbeertrag/Gewinn vervollständigt sowie an die Handwerkskammer zurückgeschickt. Dieser Datensatz wird dann schließlich zur Beitragsfestsetzung genutzt. Bei diesem Verfahren ist es möglich, dass eine Handwerkskammer von der AKG auch Daten von Betrieben erhält, die nicht in ihrer Handwerksrolle eingetragen sind und die zur Aufgabenerfüllung der Handwerkskammer somit nicht erforderlich sind. Deshalb habe ich vorgeschlagen, wie folgt zu verfahren:

Die Handwerkskammer sollte der AKG die Betriebsbezeichnungen, Anschriften und Betriebsnummern der bei ihr eingetragenen Handwerksbetriebe übermitteln. Die AKG vervollständigt den Datensatz mit den von der Oberfinanzdirektion übermittelten und für die Beitragsfestsetzung erforderlichen Daten und sendet ihn der Kammer zurück. Bei diesem Verfahren erhält die Handwerkskammer nur die Daten der in ihrem Bereich ansässigen Betriebe, und es entfallen überflüssige Datenübermittlungen.

Die Handwerkskammer hat mir hierzu mitgeteilt, dass bereits in einem Pilotprojekt ein Verfahren getestet wird, das dem vorgeschlagenen Verfahren entspricht. Meine weiteren Empfehlungen hat sie ebenfalls berücksichtigt.

3.14.2 Falscher Zeitungsausschnitt in der Akte eines Schornsteinfegers

Im Frühjahr 1999 hat mich ein Petent darüber informiert, dass im Wirtschaftsministerium unseres Landes seine Daten mit denen des Vorsitzenden einer Partei mit rechtsextremistischer Tendenz wegen zufälliger Übereinstimmung der Familiennamen in Zusammenhang gebracht würden.

Der Petent ist Schornsteinfegermeister und hatte sich beim Wirtschaftsministerium um einen Kehrbezirk beworben. Die Beteiligten vertraten jedoch zum Verwaltungsverfahren unterschiedliche Auffassungen, deshalb entschloss sich der Petent, seine Interessen gerichtlich durchzusetzen. Seine Anwältin nahm Einsicht in die Gerichtsakte und stellte fest, dass das Ministerium Daten übermittelt hatte, die in keinem Zusammenhang zu dem Betroffenen standen. Es handelte sich dabei um die Kopie eines Zeitungsausschnittes, in dem über den Vorsitzenden einer politischen Partei berichtet wird, der denselben Familiennamen hat. Allerdings war unter dem Artikel handschriftlich der Vorname des Politikers vermerkt, der ganz offensichtlich nicht mit dem Vornamen des Petenten übereinstimmt.

Vor diesem Hintergrund habe ich im Wirtschaftsministerium die dort geführten Akten von Schornsteinfegermeistern kontrolliert.

Die Akte des Petenten hatte das Gericht inzwischen wieder an das Ministerium zurückgesandt. Der oben genannte Zeitungsausschnitt befand sich immer noch darin. Der zuständige Mitarbeiter erklärte, dass dieser Artikel dem Ministerium anonym per Telefax zugesendet worden war. Er bestätigte auch, dass der Zeitungsausschnitt für das Bewerbungsverfahren nicht relevant wäre und es deshalb nicht erforderlich war, ihn zu der Akte des Petenten zu nehmen.

Des Weiteren enthielt die Akte mehrere Faxsendeberichte sowie einen handschriftlichen Vermerk über ein Gespräch von Mitarbeitern des Ministeriums mit dem Petenten. Der Vermerk enthält Äußerungen des Petenten, von denen nicht nachvollziehbar war, für welchen Zweck sie aufgezeichnet worden waren. Allgemein gilt, dass personenbezogene Daten nur verarbeitet, also auch aufbewahrt oder gespeichert werden dürfen, wenn dies erforderlich ist, um eine in der Zuständigkeit der verarbeitenden Stelle liegenden Aufgabe zu erfüllen.

Aufgabe des Wirtschaftsministeriums in diesem Fall ist es zu prüfen, ob der Bewerber geeignet ist, einen Kehrbezirk zu übernehmen. Zu diesem Zweck sind Angaben zur beruflichen Qualifikation und zur Berufserfahrung notwendig. Die Kenntnis der Daten aus dem Zeitungsausschnitt war für diese Aufgabe jedoch entbehrlich. Darüber hinaus stand der Artikel in keinem Zusammenhang mit der Person des Petenten. Durch die Speicherung der Kopie des Zeitungsausschnittes in der Akte wurde sogar ein falscher Anschein erweckt. Diese Speicherung und somit auch die Übermittlung des Ausschnittes an das Gericht waren nicht zulässig.

Im Ergebnis der Kontrolle habe ich diesen Verstoß gegen datenschutzrechtliche Bestimmungen beanstandet. Der Wirtschaftsminister hat zugesichert, die unzulässig gespeicherten Daten zu sperren beziehungsweise zu löschen und dafür zu sorgen, dass nur noch solche Daten verarbeitet werden, die zur Aufgabenerfüllung tatsächlich erforderlich sind.

Um künftig einen datenschutzgerechten Umgang mit personenbezogenen Daten zu gewährleisten, habe ich darüber hinaus Folgendes empfohlen:

Per Telefax sollten personenbezogene Daten aufgrund der damit verbundenen Risiken (siehe Dritter Tätigkeitsbericht, Punkt 3.18.3) nur übermittelt werden, wenn dies besonders eilbedürftig ist und wenn zusätzliche Maßnahmen die Vertraulichkeit der Sendung sichern.

Aktenvermerke, wie die oben genannte Gesprächsnotiz, dürfen nur solche Daten enthalten, die zur Aufgabenerfüllung erforderlich sind. Bereits bevor ein Vermerk über ein Gespräch angefertigt wird, muss deshalb klar sein, zu welchem Zweck die Daten benötigt werden. Dem Betroffenen ist der Zweck zu erläutern. Beispielsweise könnte ihm auch eine Abschrift des Vermerks zugeschickt werden.

Das Wirtschaftsministerium hat die Empfehlungen umgesetzt.

3.15 Land-, Forst- und Wasserwirtschaft

3.15.1 Daten für Abwasseranschluss an privates Unternehmen

Ein Petent wollte seine Abgaben stunden lassen. In einem schriftlichen Antrag sollte er dazu einem privaten Unternehmen, das von einem kommunalen Zweckverband mit der Betriebsführung beauftragt worden war, personenbezogene Daten mitteilen. Neben den Angaben zur Person, zum Grundstück, zum Nettoerwerbseinkommen und zu den Vermögensverhältnissen sollten das auch Angaben zu den Gründen vorübergehender Abwesenheit weiterer im Haushalt lebender Personen, zur Art ihres Einkommens und Namen sowie Geburtsdaten der Kinder sein. Überdies sollte der Antragsteller detaillierte Angaben zur genauen Lage eventuell vorhandener Grundstücke machen. Der Petent hatte Bedenken zum Umgang mit seinen Daten durch das Unternehmen und hat mich gebeten, das Antragsformular zu prüfen.

Abgabenerhebung ist Hoheitsrecht. Danach ist der Zweckverband für die Beitrags- und Gebührenerhebung zuständig. Er darf seine Aufgaben nur dann auf private Dritte übertragen, wenn hierfür eine Rechtsgrundlage existiert. Der Umfang einer solchen Funktionsübertragung ist aber weder in der Kommunalverfassung Mecklenburg-Vorpommern (KV M-V) noch im Wassergesetz des Landes Mecklenburg-Vorpommern (LWaG) ausdrücklich geregelt. Die Gesetze bestimmen lediglich, dass sich der Zweckverband Dritter bedienen kann. „Bedienen“ bedeutet, dass die Hilfe Dritter für Vorarbeiten, untergeordnete oder unterstützende Tätigkeiten in Anspruch genommen werden kann. Die Befugnis, über wichtige Sachverhalte verbindlich zu entscheiden, muss beim Verband bleiben.

Ich habe meine Auffassung dem Zweckverband, der zuständigen Kommunalaufsicht und dem Innenministerium unseres Landes mitgeteilt. Im Ergebnis haben sich alle Beteiligten dieser Rechtsauffassung vorbehaltlos angeschlossen. Nunmehr werden Entscheidungen über den Abschluss von Ratenzahlungs- und Stundungsverträgen, entsprechend meiner Empfehlung, von der Verbandsversammlung oder dem Verbandsvorsteher beziehungsweise dem Verbandsvorstand getroffen.

Die Prüfung des Antragsformulars ergab des Weiteren, dass nicht alle der geforderten Daten für die Entscheidung erforderlich waren.

Ich habe dem Zweckverband daher Folgendes empfohlen:

- Bei der Darlegung der Vermögensverhältnisse ist eine Differenzierung nach der Art der Einnahmen nicht notwendig. Ausreichend sind Angaben zur Höhe des verfügbaren Einkommens. Soweit der Antragsteller auch Eigentümer weiterer Grundstücke ist, sind Daten zur Höhe der hieraus erzielten Nettoeinnahmen anzugeben. Konkrete Einzelheiten über Lage und Nutzungsart der Grundstücke werden in diesem Zusammenhang nicht benötigt und sollten daher nicht abgefragt werden.

- Bei Angaben zu Familienverhältnissen ist nur die Zahl der unterhaltsberechtigten Kinder relevant. Auf Namen, Vornamen und Geburtsdaten der Kinder sollte verzichtet werden.

Der Verband hat diese Empfehlungen umgesetzt.

3.15.2 Braucht der Wasser- und Abwasserzweckverband einen vollständigen Grundbuchauszug?

Ein Bürger hat angefragt, ob ein Zweckverband für Wasserversorgung und Abwasserbehandlung zur Ermittlung der Daten für Anschlussbeiträge vollständige Grundbuchauszüge von den Beitragspflichtigen anfordern darf.

Der Zweckverband darf personenbezogene Daten nur im erforderlichen Umfang erheben, beispielsweise um zu manifestieren, wer der tatsächliche Eigentümer eines Grundstückes ist. Hierzu kann er vom Grundbuchamt einen Grundbuchauszug anfordern. Das Grundbuchblatt ist in verschiedene Abteilungen gegliedert. In Abteilung 1 ist der jeweilige Eigentümer vermerkt. Die Abteilungen 2 und 3 enthalten Eintragungen zu Belastungen, Verfügungsbeschränkungen oder einstweiligen Sicherungen.

Auf meine Empfehlung hin wird der Verband künftig das Grundbuchamt darauf hinweisen, dass lediglich die Daten der Abteilung 1 für seinen Zweck erforderlich sind. Die Daten der Abteilung 2 und 3 werden im Grundbuchamt vor der Fertigung der Kopie abgedeckt und so nicht mehr übermittelt.

3.16 Technik und Organisation

3.16.1 Sichere Vernetzung der Landesverwaltung noch in den Kinderschuhen

Bei fast jeder Anwendung von moderner Informations- und Kommunikationstechnik in der Verwaltung werden personenbezogene Daten verarbeitet. Auch bei einer ressort- und behördenübergreifenden Netzplanung sind deshalb die Anforderungen des § 17 DSG MV umzusetzen. Dies gilt selbstverständlich und insbesondere auch dann, wenn die Nutzung des Internet beabsichtigt ist (siehe Zweiter Tätigkeitsbericht, Punkt 2.18.3).

Solche landesweiten und ressortübergreifenden technischen und organisatorischen Maßnahmen zu koordinieren, ist in Mecklenburg-Vorpommern Aufgabe der Koordinierungs- und Beratungsstelle der Landesregierung für Informations- und Telekommunikationstechnik in der Landesverwaltung (LKSt). Ihr ist durch die IT-Richtlinien des Landes auferlegt worden, insbesondere auch die Bestimmungen des Datenschutzrechts zu beachten (Nr. 1.3 der IT-Richtlinien vom 14. April 1999). Der Interministerielle Ausschuss für Informationstechnik (IMA-IT) hat die LKSt hierbei zu unterstützen (Nr. 2.2.2 derselben Vorschrift).

Als Weitverkehrsnetz steht für Landesbehörden seit längerer Zeit das von der Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) betriebene Landesverwaltungs- und Informationsnetz (LAVINE) zur Verfügung. Es unterstützt vor allem anwendungsbezogene Netze, zum Beispiel für die Polizei (Landesweites Polizeiinformations-System LAPIS) oder für das Haushalts-, Kassen-, Rechnungswesen (PROfiskal, siehe Punkt 3.9.3). Für eine Reihe dieser Anwendungen wäre es dringend notwendig, kryptographische Verfahren einzusetzen, um Integrität, Vertraulichkeit und Zurechenbarkeit der Daten zu sichern (siehe Punkt 3.16.2).

Um auch den zentralen TK-Anlagenverbund der Landesregierung für den Datenaustausch zu nutzen, haben das Innen- und das Kultusministerium bereits Mitte 1997 vorgeschlagen, ein Ressortverbundnetz zwischen den Ministerien aufzubauen. Für die zu übertragenden Daten wurde kein Schutzbedarf festgestellt und auf eine Risikoanalyse für das Netz verzichtet. Auch wurden zunächst keine organisatorischen Regelungen geplant, um die neue Kommunikationsform in den Geschäftsgang einzubinden. Der Vorschlag enthielt lediglich technische Details auf funktioneller Ebene; sicherheitstechnische oder gar datenschutzrechtliche Erwägungen fehlten vollständig. Dahingegen hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Stellungnahme zu diesem Vorschlag schon für die Übertragung von gering bis mittel schutzbedürftigen Daten mehrere technische Zusatzanforderungen, wie den Einsatz von D-Kanalfiltern und einer zentralen Firewall, gestellt und die ausschließlich verschlüsselte Übertragung von Daten empfohlen. Ende 1999 wurde damit begonnen, einige Empfehlungen des BSI umzusetzen. So ist beispielsweise der Einsatz von D-Kanal-Filtern vorgesehen. Solange jedoch die vom BSI empfohlenen Maßnahmen nicht vollständig realisiert sind, dürfen meines Erachtens auch weiterhin keine personenbezogenen Daten in diesem Netz übertragen werden.

Im Oktober 1999 hat die LKSt in Zusammenarbeit mit der DVZ M-V GmbH ein Grobkonzept zum Aufbau eines Corporate Network für Mecklenburg-Vorpommern vorgelegt. Darin finden sich auch Vorgaben und Optionen, die sich zu datenschutzgerechten Lösungen ausbauen lassen. So ist festgelegt, unter welchen Bedingungen Netzübergänge zum Internet und zu anderen Netzen zulässig sind und wer für bestimmte Maßnahmen zur Netzwerksicherheit verantwortlich ist. Ferner werden einige Teilnetze, die im Corporate Network aufgehen sollen, besser verfügbar sein, da eine durchgängig vermaschte Architektur gewählt wurde. Darüber hinaus ist daran gedacht, den Nutzern Möglichkeiten zur Implementierung kryptographischer Verfahren zu geben. Der IMA-IT hat bereits beschlossen, ein Feinkonzept zu erarbeiten, in dem dann mehrere Optionen wie Leitungsverschlüsselung als Netzwerkdienst und auch Schlüsselverwaltungsdienste genauer auszuführen sind.

Das bereits vorliegende Grobkonzept weist zwar in die richtige Richtung, der LKSt gelang es bisher allerdings nicht, den Anforderungen aus den Ressorts zu genügen. Einige Anwender haben nun selbst die Initiative ergriffen. Ende 1998 hat das Justizministerium beispielsweise die DVZ M-V GmbH beauftragt, eine Firewall aufzubauen und zu betreiben, um das eigene lokale Netz und die Netze der Gerichte, Staatsanwaltschaften und Justizbehörden abzusichern. Diese Stellen nutzen neben den justizinternen Anwendungen vor allem das juristische Informationssystem JURIS sowie die elektronische Post. Ausgewählte Benutzer benötigen weitere Internetdienste. Bei Konzeption und Realisierung hat sich das Justizministerium sowohl von der LKSt als auch von mir beraten lassen. Die so entstandene Firewall ist ein mehrstufiges System aus Komponenten verschiedener Hersteller, welches auch einen Virenscanner für eingehende Daten enthält. Durch diese Maßnahmen konnte ein wirkungsvoller Grundschutz realisiert werden, der den Anforderungen an Datensicherheit und Datenschutz weitgehend gerecht wird. Es ist beabsichtigt, die Sicherheit der Firewall durch das BSI überprüfen zu lassen.

Die Firewall ist durchaus geeignet, auch die sicherheits- und datenschutztechnischen Ansprüche der anderen Ressorts zu erfüllen. Deshalb ist die Entscheidung der LKSt zu begrüßen, das gesamte System als zentrale Sicherheitskomponente in das Corporate Network zu übernehmen.

Das vorliegende Grobkonzept sollte aber auch Anlass dazu sein, einige bisher unabhängig voneinander betriebene Projekte neu zu konzipieren. So war die bisher in der Staatskanzlei betriebene Kopfstelle für elektronische Post (X.400) nicht zur Übermittlung personenbezogener Daten vorgesehen (siehe Zweiter Tätigkeitsbericht, Punkt 2.18.2 sowie Dritter Tätigkeitsbericht, Punkt 3.18.2); Verschlüsselung und Signatur fehlen hier völlig. Da über das Corporate Network auch das Netz TESTA (siehe Punkt 3.16.13) und somit X.400-E-Mail angeboten wird, sollte man darüber nachdenken, X.400 über die zentralen Komponenten des Corporate Network einzubinden. Auf diese Weise lässt sich bereits mit dem bisher vorhandenen Firewallsystem das Datensicherheitsniveau deutlich heben. Des Weiteren sollte auch das Ressortverbundnetz auf der Basis des TK-Anlagenverbundes nicht ohne sicherheitstechnische Verbesserungen in das Corporate Network integriert werden. Um künftig auch personenbezogene Daten übertragen zu dürfen, sind zuvor der Schutzbedarf festzustellen, das Risiko zu analysieren und die daraus resultierenden, vom BSI bereits angesprochenen Maßnahmen unverzüglich zu realisieren.

3.16.2 Verschlüsselung künftig ein Standardmerkmal?

Die Bundesregierung hat sich lange mit der Frage befasst, ob der Einsatz von Verschlüsselungsverfahren rechtlich geregelt werden sollte (siehe Dritter Tätigkeitsbericht, Punkt 2.3). Unter dem Begriff „Kryptokontroverse“ haben Politiker, Wissenschaftler, Wirtschaftsfachleute und Datenschützer in der Vergangenheit darüber debattiert, ob das Verbot oder die Einschränkung der Verschlüsselung verfassungsrechtlich zulässig, technisch durchsetzbar, wirtschaftlich vertretbar und überhaupt sinnvoll möglich wäre.

Im Sommer 1999 wurde diese Diskussion auf eine neue Basis gestellt. Am 2. Juni veröffentlichte die Bundesregierung die Eckpunkte der deutschen Kryptopolitik. Darin wird die Kryptographie als eine entscheidende Voraussetzung für den Datenschutz besonders hervorgehoben. Nun ist nicht mehr vorgesehen, die freie Verfügbarkeit von Verschlüsselungsprodukten einzuschränken. Die Bundesregierung strebt an, das Vertrauen der Nutzer in die Sicherheit der Verschlüsselung zu stärken, und will die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützen. Dazu will sie Maßnahmen ergreifen, um deutsche Hersteller bei der Entwicklung und der Produktion von sicheren und leistungsfähigen Verschlüsselungsprodukten zu fördern und die internationale Wettbewerbsfähigkeit dieses Sektors zu unterstützen.

Die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 8. Oktober 1999 die Position der Bundesregierung ausdrücklich begrüßt (siehe 15. Anlage). Damit werde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssten. Die Datenschutzbeauftragten fordern deshalb die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen und kryptographische Verfahren häufiger als bisher einzusetzen. Kryptographie müsse künftig zum Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet werden sollte, wenn wichtige Gründe dagegen sprächen.

Selbstverständlich wirken sich die Eckpunkte der deutschen Kryptopolitik auch auf die IT-Landschaft unseres Landes aus. Im Rahmen meiner Beratungstätigkeit habe ich in der Vergangenheit häufig darauf hingewiesen, dass es notwendig ist, elektronisch gespeicherte und übermittelte personenbezogene Daten durch Verschlüsselung vor Missbrauch zu schützen. Meines Erachtens ist insbesondere die Koordinierungs- und Beratungsstelle der Landesregierung für Informations- und Telekommunikationstechnik in der Landesverwaltung (LKSt) in der Pflicht, möglichst landeseinheitliche Empfehlungen für den Einsatz kryptographischer Verfahren zu geben. Noch fehlen solche Vorgaben jedoch, was Anwender, die mit Verschlüsselungsverfahren sensible Daten schützen möchten, erheblich verunsichert.

Schon 1994 habe ich gefordert, die Daten des Landesweiten Polizeiinformations-Systems LAPIS im Landesdatennetz LAVINE verschlüsselt zu übertragen. Nach Umstellungen der Netzstruktur wird mittlerweile zwar verschlüsselt, jedoch entspricht die Länge der verwendeten Schlüssel immer noch nicht den sicherheitstechnischen Anforderungen.

Auch die Planungen zum Elektronischen Grundbuch (siehe Punkt 3.1.8) wären meines Erachtens zügiger verlaufen, wenn die elektronische Unterschrift mit kryptographischen Verfahren auf der Basis von Landesstandards hätte realisiert werden können. Möglicherweise hätten sich dadurch auch kostenintensive Gutachten erübrigt.

Im Bereich der automatisierten Personaldatenverarbeitung ist mir nicht eine Anwendung in unserem Land bekannt, bei der die sensiblen Daten verschlüsselt gespeichert und übertragen werden. Meine Empfehlungen beispielsweise im Rahmen der Beratungen zum Landesstandardsystem PERSYS wurden zwar grundsätzlich akzeptiert, während der gesamten Nutzungszeit aber nicht umgesetzt. Auch bei den Planungen zum neuen Landesstandard EPOS (Elektronisches Personal-, Organisations- und Stellenverwaltungssystem) spielen Fragen der Verschlüsselung bisher nur eine untergeordnete Rolle.

Diese drei Beispiele sollen deutlich machen, welcher Handlungsbedarf hier besteht. Verschlüsselung sollte im Sinne der Eckpunkte der deutschen Kryptopolitik auch bei IT-Verfahren unseres Landes zu einem Standardmerkmal werden. Es ist dringend nötig, endlich damit zu beginnen und die entsprechenden Rahmenbedingungen zu schaffen, die eine einfache und weitgehend einheitliche Nutzung von kryptographischen Verfahren in der gesamten Landesverwaltung ermöglichen (siehe auch Punkt 3.16.3).

3.16.3 Braucht das Land ein eigenes Trustcenter?

Für Wirtschaft und Verwaltung wird die Verfügbarkeit unverfälschter elektronischer Daten und deren Schutz vor Missbrauch immer wichtiger. Die Bundesregierung hat inzwischen erkannt, dass kryptographischen Verfahren hierbei künftig eine besondere Bedeutung zukommt (siehe Punkt 3.16.2). Dieser Bedeutung werden sie jedoch nur gerecht, wenn technische und personelle Rahmenbedingungen geschaffen werden, die dem Stand der Entwicklung entsprechen.

In diesem Zusammenhang ist der ordnungsgemäße Umgang mit kryptographischen Schlüsseln von besonderer Bedeutung. Das Signaturgesetz (SigG) und die Signaturverordung (SigV) enthalten beispielsweise detaillierte Regelungen zum Umgang mit solchen Schlüsseln und zur hierfür erforderlichen Infrastruktur (siehe Dritter Tätigkeitsbericht, Punkt 2.2). Dort ist festgelegt, dass unabhängige, vertrauenswürdige Stellen („Zertifizierungsstellen“ oder „Trustcenter“ genannt) einzurichten sind, die unter anderem die Zuordnung von Schlüsseln zu Personen durch ein elektronisches Zertifikat bestätigen, bestimmte Schlüssel und deren Zertifikate zum elektronischen Abruf bereithalten oder ungültige Schlüssel sperren. Alle technischen Komponenten müssen einem detaillierten Anforderungskatalog genügen (§§ 12, 16 SigV). Das Personal muss besonders zuverlässig sein (§ 10 SigV) und über die erforderlichen Fachkenntnisse verfügen (§ 4 Abs. 3 SigG). Die Einrichtung solcher Trustcenter erfordert deshalb einen hohen materiellen und personellen Aufwand.

Auch die öffentlichen Stellen Mecklenburg-Vorpommerns werden in zunehmendem Maße kryptographische Verfahren einsetzen (siehe Punkt 3.16.2). Dafür sind technisch ausgereifte und wirtschaftlich vertretbare Rahmenbedingungen zu schaffen, die den Forderungen des SigG und der SigV genügen oder sich für bestimmte, weniger sensible Bereiche zumindest an sie anlehnen. Die dort beschriebenen Mechanismen zielen zwar vorwiegend darauf ab, Fälschungen digitaler Signaturen oder digital signierter Daten zuverlässig festzustellen, zur Wahrung der Vertraulichkeit elektronisch übermittelter oder gespeicherter Daten sind jedoch ähnliche Verfahren anwendbar.

Für eine behördeninterne Anwendung, bei der bestimmte Daten durch Verschlüsselung lediglich vor „neugierigen Blicken“ geschützt werden sollen und deren Nutzerkreis überschaubar ist, wäre es sicher wirtschaftlich sinnvoll und aus datenschutzrechtlicher Sicht auch vertretbar, dass diese Behörde selbst die erforderlichen Schlüssel verwaltet, sofern dort entsprechend fachkundiges IT-Personal beschäftigt ist.

Sollen jedoch kryptographische Verfahren in landesweiten Anwendungen oder in Einzelverfahren mit sensiblen Daten und einer großen Zahl von Nutzern eingesetzt werden, steigen die Anforderungen an die technische Infrastruktur und an die Fachkunde der Mitarbeiter, so dass auf eine übergeordnete Schlüsselverwaltung kaum noch verzichtet werden kann. Für diese Fälle wäre es denkbar, die Angebote eines Dienstleisters in Anspruch zu nehmen. Zurzeit existiert allerdings nur eine Firma in Deutschland, die von der Regulierungsbehörde für Telekommunikation und Post (RegTP) die Genehmigung erhalten hat, eine signaturgesetzkonforme Zertifizierungsstelle zu betreiben. Schlüsselverwaltung wäre nach § 4 DSG MV prinzipiell auch zulässig als Umgang mit personenbezogenen Daten im Auftrag. Allerdings wird eine derartige Auftragsdatenverarbeitung für bestimmte Bereiche der Verwaltung eingeschränkt. Das betrifft beispielsweise den Umgang mit Patientendaten (§ 21 LKHG M-V), mit Daten des Grundbuches (§ 126 Abs. 3 GBO - siehe Punkt 3.1.8), mit Meldedaten (§ 38 LMG) oder mit Daten, die dem Steuergeheimnis unterliegen (§ 30 AO). Sollen nun externe Dienstleister die Aufgaben einer Zertifizierungsstelle wahrnehmen, ist insbesondere zu bedenken, dass der besonders schutzwürdige Teil der Datenverarbeitung des Landes, die Verwaltung der Schlüssel, Dritten überlassen würde. Das Land würde technisches Know-how aus der Hand geben, das für das Funktionieren der Verwaltung unerlässlich ist. Auch mit Blick auf die schon vorhandenen Einschränkungen halte ich es deshalb für nicht vertretbar, den gesamten Bereich der Schlüsselverwaltung Dritten zu überlassen.

Kryptographische Schlüssel sollten vorzugsweise durch Stellen des Landes verwaltet werden. Mecklenburg-Vorpommern wäre deshalb gut beraten, künftig ein eigenes Trustcenter zu betreiben, das mit den Vorschriften des Signaturgesetzes konform geht und dann der Landes- und Kommunalverwaltung als Dienstleister zur Verfügung steht. Die sehr hohen Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität könnte möglicherweise das Landesrechenzentrum, das von der Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) betrieben wird, erfüllen, so dass weitere Investitionen kaum erforderlich wären. Zu klären wären hierzu allerdings noch Fragen, die den Rechtsstatus der DVZ M-V GmbH betreffen (siehe auch Punkt 3.1.8). Das DVZ-Gesetz, das sich zurzeit in der Ressortabstimmung befindet, könnte möglicherweise auch für diesen Bereich Rechtssicherheit schaffen.

3.16.4 Neues zur Internetnutzung

Über die Risiken, die mit dem Anschluss von Behördennetzen an das weltweite Internet verbunden sind, habe ich ausführlich im Zweiten Tätigkeitsbericht unter Punkt 2.18.3 berichtet und Empfehlungen zur Minimierung dieser Risiken gegeben.

Bei Beratungsgesprächen und Kontrollen in Behörden des Landes habe ich jedoch auch in diesem Berichtszeitraum festgestellt, dass einige Verantwortliche noch immer unsicher sind, wenn es um Datenschutzfragen im Zusammenhang mit dem Internet geht (siehe auch Punkt 3.16.4). Erfreulich ist jedoch, dass ich jetzt häufiger bereits in der Planungsphase solcher Vorhaben um Beratung gebeten werde.

In diesem Zusammenhang hat sich unser schriftliches Informationsmaterial bewährt. In einer Orientierungshilfe des AK Technik (siehe Punkt 4) zum Thema Internet wurden bereits 1996 die Anforderungen an eine datenschutzgerechte Internetanbindung ausführlich erläutert. 1998 wurde dieses Dokument in wesentlichen Teilen überarbeitet und ergänzt. Auch meine Dienststelle hat diese Broschüre kostenlos abgegeben und den Text zum Herunterladen aus unserem Internetangebot (siehe Punkt 4) bereitgestellt.

In der Orientierungshilfe werden Sicherheitslücken erläutert, die in Internet-Software und -Protokollen auftreten, und konkrete Lösungsvorschläge zur Reduzierung der daraus resultierenden Datensicherheitsrisiken unterbreitet. Insbesondere werden die Vor- und Nachteile verschiedener Firewall-Technologien und -Konfigurationen beschrieben, die die Verbindung zwischen lokalen Netzen (LAN) und Weitverkehrsnetzen (WAN) absichern.

Neben technischen Details werden auch organisatorische Maßnahmen erläutert und methodische Hinweise gegeben. Damit eine Firewall ihre Schutzwirkung entfalten kann, sind viele Arbeiten notwendig, die über die Beschaffung und Einrichtung der Technik hinausgehen. So müssen beispielsweise der Kommunikationsbedarf der Mitarbeiter und die Risiken für die im lokalen Netz verarbeiteten Daten ermittelt werden. Dazu sind detaillierte Kenntnisse über die Struktur und mögliche Angriffspunkte innerhalb des lokalen Netzes erforderlich. Die Ergebnisse dieser Untersuchungen sind in einem Sicherheitskonzept niederzulegen. Hieraus ergeben sich dann wesentliche Anforderungen an die auszuwählende Architektur und Konfiguration der Firewall.

Auch der Betrieb einer Firewall erfordert einen nicht zu unterschätzenden Zeit- und Personalaufwand. So ist die Software regelmäßig zu aktualisieren, damit sie ihre Schutzwirkung auch gegenüber neu entdeckten Sicherheitsproblemen behält. Die von der Firewall erzeugten Protokolle müssen regelmäßig auf mögliche Angriffe (und Versuche) ausgewertet werden. Außerdem ist laufend zu kontrollieren, ob die Rechte der Benutzer mit den jeweiligen Fachaufgaben übereinstimmen. Gegebenenfalls sind die Rechte entsprechend anzupassen.

Im Bereich der Weitverkehrsvernetzung (WAN) entwickelt sich die Technik besonders schnell. Hinzu kommt, dass die Verarbeitung personenbezogener Daten in diesem Bereich durch neue Rechtsvorschriften wie dem Mediendienstestaatsvertrag (MDStV), dem Teledienstedatenschutzgesetz (TDDSG) und der neuen Telekommunikations-Datenschutzverordnung (TDSV) neu geregelt worden ist (siehe auch Punkt 3.8.1). Unsere Empfehlungen mussten also dem Stand der Technik und der Gesetzgebung angepasst werden. Die Orientierungshilfe wird deshalb zurzeit gemeinsam von den Arbeitskreisen „Technische und organisatorische Datenschutzfragen“ und „Medien“ der Datenschutzbeauftragten des Bundes und der Länder ein weiteres Mal überarbeitet. Die aktualisierte Fassung wird voraussichtlich im zweiten Quartal 2000 veröffentlicht. Sie ist dann wieder als Broschüre in meiner Dienststelle kostenlos erhältlich und wird im Internet zum Herunterladen bereitstehen.

3.16.5 Data Warehouse

Mit der ständig zunehmenden Leistungsfähigkeit der in Wirtschaft und Verwaltung eingesetzten Informations- und Telekommunikationstechnik nimmt die Menge der gespeicherten personenbezogenen Daten scheinbar unaufhaltsam zu. Wer beispielsweise Chipkartensysteme oder neue Kommunikationsmedien nutzt, muss damit rechnen, dass er aus vielen Lebensbereichen Daten preisgibt, die sowohl Privatunternehmen als auch die öffentliche Verwaltung speichern. Datensparsamkeit und Datenvermeidung spielen noch immer - und zum Teil ganz bewusst - eine untergeordnete Rolle.

In Unternehmen und Behörden wächst das Interesse, das gesammelte Datenmaterial effektiver als bisher zu nutzen. Wir müssen zunehmend mit „gläsernen Bürgern“ rechnen, wenn die Gesamtheit aller so verfügbaren Daten einer Person analysiert und die Beziehungen dieser Daten zueinander beurteilt werden.

Das Data Warehouse (DWH) ermöglicht eben gerade diese neue Betrachtungsweise, indem es alle gesammelten Daten nach bestimmten Kriterien sortiert, speichert und zur Analyse und Auswertung bereithält. Bisher nicht offenkundig gewordene Zusammenhänge zwischen Einzeldaten sollen aus der Gesamtheit erkannt werden, um beispielsweise wirtschaftliche Vorteile für ein Unternehmen erzielen zu können. Dabei soll der Manager - und künftig wohl auch der Behördenleiter - aus der Fülle des Datenmaterials nur die strategisch wichtigen Daten, möglichst in ansprechender und visuell einprägsamer Weise, erhalten, ohne dass er den Ballast der täglich anfallenden operativen Daten wahrnimmt und dabei auf die ständige Mitwirkung von Informatikern und Statistikern angewiesen ist.

Auch wenn DWH-Konzepte bisher fast nur im Bereich der Privatwirtschaft und auch dort zunächst nur ansatzweise anzutreffen und die Ergebnisse noch recht bescheiden sind, halte ich die frühzeitige Betrachtung dieser neuen Technologie aus datenschutzrechtlicher und -technischer Sicht für notwendig. Künftige Anwender sollen den möglichen Nutzen für Wirtschaft und Verwaltung sorgfältig gegenüber dem gebotenen Schutz der Privatsphäre des Einzelnen abwägen können und im Ergebnis dieses Prozesses die jeweils erforderlichen datenschutzfreundlichen Technologien einsetzen. Zu diesem Zweck sind die Arbeitskreise „Technische und organisatorische Datenschutzfragen“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gegenwärtig damit befasst, eine Orientierungshilfe zu erarbeiten, die Hinweise zum datenschutzgerechten Betrieb von DWH geben und eine rechtliche Bewertung derartiger Konzepte ermöglichen soll.

Was demnächst in Deutschland erwartet werden kann und wie wichtig deshalb solche Hilfsmittel werden, sollen die folgenden Beispiele zeigen.

Nach Versandhäusern und Warenhausketten erkennen zunehmend auch staatliche Stellen den Nutzen dieser neuen Technologie. So ist das Bundesaufsichtsamt für den Wertpapierhandel dabei, für die Börsenaufsicht so genannte Softwareagenten einzuführen, die aus den täglichen Meldungen über Käufe und Verkäufe von Aktien und Optionsscheinen verdächtige Transaktionen herausfiltern sollen, um unerlaubte Insidergeschäfte aufzudecken.

Als eine weitere Anwendung dieser Technologie wird im Zusammenhang mit der Verbreitung bestimmter verbotener Inhalte über das Internet beispielsweise derzeit erwogen, mit speziellen Internetsuchmaschinen rund um die Uhr systematisch danach zu suchen. Eine Datenbank mit den so gewonnenen Informationen entspräche praktisch einem aus dem Internet gespeisten DWH, das nach verschiedenen, jederzeit den Bedürfnissen des Fragestellers anpassbaren Kriterien durchsucht werden kann. Nicht erwähnt wird in diesem Zusammenhang zumeist, dass mit solchen Werkzeugen auch sämtliche im Internet veröffentlichten Äußerungen von Einzelnen systematisch erkundet und dokumentiert werden können.

Ob ein DWH, das ohne Restriktionen diese und weitere Möglichkeiten der modernen Technik nutzt, noch mit den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts aus dem Jahre 1983 und mit den Zweckbindungsgrundsätzen der Datenschutzgesetze von Bund und Ländern vereinbar ist, muss sicher hinterfragt werden.

Ein DWH, das sich datenschutzfreundlicher Technologien bedient (siehe Dritter Tätigkeitsbericht, Punkt 2.1) und beispielsweise für vorher nicht definierbare Zwecke lediglich anonymisierte oder unter bestimmten Voraussetzungen pseudonymisierte Daten verwendet, genügt möglicherweise datenschutzrechtlichen Anforderungen. Natürlich sind dann technische und organisatorische Maßnahmen erforderlich, die eine Deanonymisierung verhindern oder die Zuordnung eines Pseudonyms zu einer Person nur unter vorher festgelegten, rechtlich zulässigen Bedingungen ermöglichen.

Die Entwicklung in diesem Bereich wird weiterhin kritisch zu beobachten und zu begleiten sein, um möglichst rechtzeitig eine datenschutzgerechte Gestaltung und Nutzung von DWH zu erreichen.

3.16.6 Prüfkriterien für datenschutzfreundliche Produkte (Common Criteria 2.0)

Ohne den Einsatz sicherer Informationstechnik (IT) ist heute ein reibungsloses Funktionieren von Wirtschaft und Verwaltung nicht mehr vorstellbar. Sicherheit bedeutet in diesem Zusammenhang, dass die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Zurechenbarkeit automatisiert verarbeiteter Daten jederzeit gewährleistet sind. Die Nutzer der IT müssen darauf vertrauen können, dass die hierfür notwendigen Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden.

Um nun die Sicherheitseigenschaften von IT-Produkten vergleichen und das Maß der Vertrauenswürdigkeit einschätzen zu können, haben verschiedene Länder Europas und Nordamerikas zunächst unabhängig voneinander entsprechende Prüfkriterien entwickelt. In den USA enthält beispielsweise das so genannte Orange Book seit 1985 derartige Kriterien. Für Deutschland entwickelte das Bundesamt für Sicherheit in der Informationstechnik (BSI) solche IT-Sicherheitskriterien.

Um Handelshemmnisse aufgrund unterschiedlicher Sicherheitsstandards zu vermeiden, entschlossen sich 1989 einige europäische Regierungen, ihre nationalen Kriterien zu harmonisieren. Auf diese Weise entstanden die so genannten Information Technology Security Evaluation Criteria (ITSEC) - die Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik. Seit 1993 wird daran gearbeitet, die gemeinsamen Kriterienkataloge der USA und Kanada und die europäischen anzugleichen. Als Ergebnis dieser Bemühungen wurde 1998 die Version 2.0 der so genannten Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik) fertiggestellt. Damit steht erstmals ein international gültiger Kriterienkatalog zur Verfügung, der demnächst von der Internationalen Standardisierungsorganisation (ISO) unter der Nummer 15 408 zum internationalen Standard erklärt werden soll.

Für den Datenschutz sind die Common Criteria 2.0 von besonderer Bedeutung. Erstmals in der Geschichte derartiger Kriterienkataloge sind Anforderungen zum Schutz der Privatsphäre enthalten. Im Teil „Funktionale Sicherheitsanforderungen“ werden im Abschnitt „Datenschutz“ Grundsätze zur Anonymität, Pseudonymität, Unverkettbarkeit und Unbeobachtbarkeit formuliert. Mit Hilfe der in den Common Criteria beschriebenen „Protection Profiles“ können unter anderem auch datenschutzspezifische Anforderungen für bestimmte Produkttypen definiert werden. Dadurch ist es einerseits möglich, Herstellern von IT-Produkten international vergleichbare und - insbesondere für die Produktzertifizierung - prüffähige Vorgaben für die Entwicklung datenschutzfreundlicher Produkte zu machen. Andererseits können Zertifizierungsstellen solche Produkte evaluieren und prüfen. Künftige Nutzer werden in die Lage versetzt, das Maß an Datenschutzfreundlichkeit eines Produktes bereits vor dem Einsatz objektiv einzuschätzen.

Die Datenschutzbeauftragten von Bund und Ländern könnten ihre Beratungstätigkeit weiter in das Vorfeld des Einsatzes konkreter IT-Produkte oder -Verfahren verlagern, indem sie auf der Basis dieser Kriterienkataloge datenschutzrelevante Empfehlungen und Forderungen formulieren. Der AK Technik hat vor diesem Hintergrund eine Arbeitsgruppe gebildet, in der auch meine Dienststelle vertreten ist. Diese Gruppe will zunächst ein Protection Profile zu den Themen Verschlüsselung und Pseudonymisierung erstellen (siehe auch Punkt 4). Damit könnten beispielsweise wichtige Voraussetzungen geschaffen werden, um die Forderungen der Gesundheitsreform 2000 zur Datenübermittlung der Leistungserbringer an die Krankenkassen umzusetzen (siehe auch Punkt 3.10.1). Den Leistungserbringern können möglicherweise nach den Common Criteria geprüfte und zertifizierte Hard- und Softwareprodukte zur Verfügung gestellt werden, mit denen sie Patientendaten sicher speichern können und die zu übermittelnden Daten pseudonymisieren, bevor sie diese an die Krankenkassen weiterleiten.

Um möglichst schnell zu nutzbaren Ergebnissen zu kommen, wurden das BSI und der Technische Überwachungsverein Informationstechnik (TÜViT) Essen gebeten, in der Arbeitsgruppe mitzuarbeiten. Erfreulicherweise haben sie dieser Bitte entsprochen. Die ersten beiden Sitzungen fanden beim BSI in Bonn in einer angenehm konstruktiven Atmosphäre statt. Der erste Entwurf eines Protection Profiles zum Thema Pseudonymisierung und Verschlüsselung liegt bereits vor. Über den Fortgang der Arbeiten werde ich weiter berichten.

3.16.7 Wer weiß schon noch, was in seinem Rechner passiert?

Im Frühjahr 1999 berichteten die Medien über das Vorhaben des weltweit führenden Chipherstellers Intel, seinen neuesten Prozessor Pentium III mit einer eindeutigen, auslesbaren und nicht veränderbaren Prozessorseriennummer (PSN) zu versehen, um vernetzt arbeitende Personalcomputer zu identifizieren. Die PSN sollte nach Intels Vorstellungen beispielsweise als zusätzliches Authentifikationsmerkmal genutzt werden, um internetbasierte Transaktions- oder Kommunikationsvorgänge besser als bisher abzusichern. Auch für eine effektive und manipulationssichere Bestandsverwaltung von Personalcomputern in Firmen und Behörden sollte die PSN von Nutzen sein.

Intels Pläne lösten weltweit eine heftige Debatte über Datenschutzfragen bei der Nutzung des Pentium III aus. Es wurde befürchtet, dass die Privatsphäre der Nutzer dieses Prozessors erheblich beeinträchtigt würde, wenn das Auslesen der PSN durch sie selbst nicht verhindert werden kann. Weil die PSN und der Nutzername verknüpft werden können, wäre nicht auszuschließen, dass beispielsweise alle Internetaktivitäten eines Pentium III-Nutzers lückenlos nachvollziehbar sind.

Intel stellte daraufhin in Medienveröffentlichungen und auf Informationsveranstaltungen, zu denen auch die Datenschutzbeauftragten eingeladen waren, verschiedene Softwarekomponenten vor, mit denen die PSN durch den Nutzer ein- und ausgeschaltet werden konnte. Die Fachöffentlichkeit wies jedoch nach, dass keines der angebotenen Produkte das Auslesen auf sichere und für den Nutzer transparente Weise wirksam verhinderte. Da reine Softwarekomponenten offensichtlich nicht das geforderte Ergebnis bringen konnten, appellierte Intel an die PC-Hersteller, die PSN-Abschaltung in das BIOS (Basic Input Output System) ihrer Rechner zu integrieren.

Versierte Computerspezialisten deckten aber auch beim Abschalten der PSN im BIOS-Setup Schwachstellen auf. Auch diese Lösungen garantierten also nicht, dass die Seriennummer nur mit Zustimmung des Anwenders auslesbar ist. Im Ergebnis bleibt für Nutzer des Pentium III auch weiterhin das Unbehagen, nie mit Sicherheit zu wissen, wann und von wem gerade die PSN gelesen wird.

Durch die öffentliche Debatte um eindeutige Kennungen wurde nebenbei auch bekannt, dass selbst einige Softwarehersteller den Nutzern ihrer Produkte derartige Kennungen zuordnen. Ein Beispiel hierfür war die Online-Registrierung des Betriebssystems Windows 98 der Firma Microsoft. Jedem Anwender wurde eine eindeutige Identifizierungsnummer (GUID - Globally - Globally Unique Identifier) zugeordnet, die zusammen mit weiteren Systemdaten nicht nur in der Registrierdatenbank des Betriebssystems gespeichert, sondern unter bestimmten Voraussetzungen von Microsoft abgerufen und auch in der Kundendatenbank des Unternehmens abgelegt werden kann. Die GUID fanden Spezialisten dann sogar in Dokumenten wieder, die von Textverarbeitungsprogrammen (Word 97) und Tabellenkalkulationssoftware (Excel 97) erzeugt wurden.

Nach massiven Protesten von Anwendern und Datenschützern bestätigte Microsoft, dass tatsächlich Informationen von Rechnern ihrer Kunden ohne deren Wissen abgerufen werden konnten. Microsoft-Manager versicherten jedoch, dass es sich dabei lediglich um einen Softwarefehler handele, der umgehend behoben würde. Die zweite Ausgabe von Windows 98 übertrug dann diese Identifizierungsnummer tatsächlich nicht mehr. Nach wie vor werden jedoch bei der Online-Registrierung Daten übertragen. Ob aber alle Nutzer wissen, dass man auf seinem Rechner eine bestimmte Datei (Cookie) löschen muss, um diese Übermittlung zu verhindern, ist zu bezweifeln.

Datenschützer fordern schon seit Jahren, transparente und damit datenschutzfreundliche Hard- und Softwareprodukte zu entwickeln und herzustellen. Die beiden Beispiele lassen jedoch befürchten, dass es vielfach noch an der erforderlichen Transparenz für den Nutzer fehlt und von Datenschutzfreundlichkeit deshalb oftmals nicht die Rede sein kann. Die weltweiten Diskussionen um die Seriennummer des Pentium III und um die Online-Registrierung von Softwareprodukten haben die Datenschutzbeauftragten von Bund und Ländern zum Anlass genommen, in einer gemeinsamen Entschließung die Hersteller von Informations- und Kommunikationstechnik aufzufordern, Hard- und Software so zu entwickeln, dass sich Anwender und unabhängige Dritte jederzeit von der Wirksamkeit der Sicherheitsvorkehrungen überzeugen können (siehe 11. Anlage). Insbesondere ist zu verhindern, dass Daten von Nutzern übermittelt werden, ohne dass diese es bemerken.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, die auch eine Transparenz der Verfahrensabläufe gewährleisten. Ein Mittel zur Gewährleistung dieser Transparenz ist beispielsweise die Zertifizierung von informationstechnischen Produkten und Verfahren durch unabhängige Stellen. Unter Punkt 3.16.6 ist beschrieben, auf welche Weise international einheitliche Prüf- und Bewertungskriterien dazu beitragen können, dass Nutzer moderner Technik auf die korrekte und transparente Funktion der notwendigen Sicherheitsfunktionen von Hard- und Software vertrauen können.

3.16.8 Orten von Mobiltelefonen

In meinem Dritten Tätigkeitsbericht habe ich im Punkt 3.18.1 unter anderem erläutert, warum vertrauliches Telefonieren mit dem Mobiltelefon nicht immer gewährleistet ist. Neben den dort beschriebenen Möglichkeiten des Missbrauchs darf man aber auch andere Gefahren, die von dieser Technik ausgehen, nicht unterschätzen. Mobiltelefone sind kleine Funkgeräte, die beim Senden durch ihre hochfrequente Abstrahlung andere empfindliche elektronische Geräte stören können. Deshalb ist die Benutzung beispielsweise in Flugzeugen und in vielen Bereichen von Krankenhäusern verboten. Hier besteht die Gefahr, dass lebensnotwendige Systeme in ihrer Funktion beeinträchtigt werden.

Seit einiger Zeit sind Geräte auf dem Markt, mit deren Hilfe festgestellt werden kann, ob in einem bestimmten Umkreis Mobiltelefone in Betrieb sind. Nachdem ich die Abhörmöglichkeiten von Mobiltelefonen bereits untersucht hatte, lag es nahe zu prüfen, ob diese Ortungsgeräte mehr können, als nur die Existenz eines eingeschalteten Telefons zu ermitteln.

Auf meine Anfrage hin stellte mir eine Firma freundlicherweise ein Exemplar aus ihrer Produktion leihweise zur Verfügung, um es auf datenschutzrelevante Aspekte zu überprüfen.

Der „Mobifinder“ signalisiert optisch oder akustisch die Empfangsfeldstärke mit Datum und Uhrzeit von sendenden Mobiltelefonen. Jedes Gerät sendet beim Einbuchen oder beim Zellenwechsel, während des Wählvorganges, im Gesprächszustand und bei der Antwort auf eine so genannte Paging-Request-Anfrage im Stand-by-Modus. Der Mobifinder kann die Empfangspegel sowie das Datum und die Uhrzeit der letzten 200 Meldungen speichern. Zur Auswertung können diese Meldungen auf dem Display angezeigt oder mit einer speziellen Übertragungseinrichtung auf einen Personalcomputer überspielt werden.

Die gemessene Empfangsfeldstärke wird als Maß für die Entfernung des Mobiltelefons vom Mobifinder angenommen. Die Rufnummern oder die Gerätekennung (IMSI) werden nicht erkannt und damit nicht angezeigt oder gespeichert. Der Mobifinder speichert also keine personenbezogenen Daten. Lediglich die Ortung eines Mobiltelefons durch Nutzung mehrerer unterschiedlich positionierter Mobifinder ist unter bestimmten Voraussetzungen möglich.

Man könnte also mit dem Mobifinder feststellen, ob Funktelefone missbräuchlich benutzt werden, um beispielsweise heimlich Gespräche abzuhören. Somit könnte durch Nutzung des Mobifinders prinzipiell sogar den Risiken begegnet werden, die ich unter dem Stichwort „Handy als Abhörgerät“ im Dritten Tätigkeitsbericht beschrieben habe.

Vor diesem Hintergrund habe ich empfohlen, auf Hersteller von Mobilfunkgeräten Einfluss zu nehmen, um einige Grundfunktionen des Mobifinders in Mobiltelefone zu übernehmen. Es wäre beispielsweise sinnvoll, den Sendevorgang am Gerät selbst optisch anzuzeigen, um ein unbemerktes Abhören weitgehend auszuschließen.

3.16.9 Videoüberwachung

Videotechnik wird ständig kleiner, billiger und leistungsfähiger. Nicht zuletzt deshalb finden wir diese Technik immer häufiger sowohl im privaten Bereich als auch im öffentlichen Leben. Im Straßenverkehr, im Kaufhaus, an der Tankstelle, in der Bank, im Schulbus, am Einfamilienhaus und an vielen anderen Stellen werden wir zunehmend mit Videokameras konfrontiert. An die Überwachung auf Privatgrundstücken haben wir uns schon fast gewöhnt. Die Rechtsprechung hat den Einsatz dieser Technik zur Ausübung des Hausrechts als grundsätzlich zulässig erklärt. Die Grenzen zum öffentlichen Bereich verschwimmen jedoch immer mehr. Sowohl diese Tatsache als auch die rasante technische Entwicklung in diesem Bereich zwingen auch die Datenschutzbeauftragten, sich mit dieser Entwicklung zu befassen.

Videoüberwachung und -aufzeichnung berühren Kernfragen des Persönlichkeitsrechts in besonderer Weise. Während bei der konventionellen Verarbeitung personenbezogener Daten in der Regel immer nur Einzelaspekte aus dem Leben eines Menschen relativ transparent an einem bestimmten Ort gespeichert und verarbeitet werden, erfasst die Videotechnik den Menschen und sein Verhalten als Ganzes. Videodaten stehen dabei nicht mehr nur lokal zur Verfügung, sondern können durch die rasant entwickelten Möglichkeiten der Bildübertragung praktisch ohne merkliche Zeitverzögerung beispielsweise über das Internet in alle Welt übertragen werden. Jeder technische Laie kann sich auf einfache Weise die Bilder so genannter Web-Cams, die eine belebte Straßenkreuzung New Yorks oder das Badezimmer eines extrovertierten Bürgers beobachten, auf seinem heimischen Personalcomputer ansehen. Darüber hinaus dürfen in diesem Zusammenhang die Fortschritte der Biometrie nicht außer Acht gelassen werden. Denn leistungsfähige Überwachungssysteme stellen nicht nur fest, dass sich jemand in einem überwachten Bereich aufhält, sondern sind bereits in der Lage, durch hochentwickelte Bild- und Mustererkennungssysteme aus der Menge beobachteter Personen einzelne Menschen zu identifizieren.

Gegenwärtig wird verstärkt der Einsatz der Videotechnik zur Kriminalitätsbekämpfung diskutiert. Ein Blick nach England, wo derartige Überwachungssysteme bereits häufig eingesetzt werden, zeigt jedoch, wohin die Entwicklung tatsächlich führen kann. Im Rahmen des Wiesbadener Datenschutzforums 1999, das mein hessischer Kollege Professor Dr. Friedrich von Zezschwitz unter das Motto Videoüberwachung gestellt hatte, berichtete eine britische Juristin über die Situation in ihrem Heimatland. Große Teile von Städten werden bereits flächendeckend überwacht. Von einigen Teilen der Bevölkerung wird diese Erscheinung positiv aufgenommen und führt zum Teil sogar dazu, dass viele Bürger vorzugsweise in Geschäften einkaufen wollen, die videoüberwacht werden.

Mein schleswig-holsteinischer Kollege Dr. Helmut Bäumler zeigte in seinem Vortrag im Rahmen des Wiesbadener Datenschutzforums auf, welche Entwicklung zu befürchten ist, wenn sich der in England und den USA zu beobachtende Trend ungehindert auch in Deutschland fortsetzt. Zunächst wird nur beobachtet, dann wird versucht, kriminelles Verhalten zu erkennen, und am Ende steht die Kontrolle des Sozialverhaltens. Angesichts dieser Entwicklung müsse man sich schon einige Fragen stellen: Wird man künftig immer erklären müssen, warum man sich im Einzelfall anders als die meisten verhält? Werden Kinder künftig in ihrer Entwicklung dadurch geprägt, dass sie ständig von Kameras beobachtet werden und jedes angebliche Fehlverhalten sofort offenkundig wird? Kann sich unter den Augen der Videotechnik noch demokratisches Selbstbewußtsein und konstruktive Kritik gegen die Staatsmacht entwickeln?

Da einzelne Videoanwendungen für sich gesehen durchaus sinnvoll erscheinen und jedenfalls in Deutschland noch genug Platz ist, sich unbeobachtet zu bewegen, muss die Kritik aus datenschutzrechtlicher Sicht aus sehr grundsätzlichen Positionen heraus geführt werden. Sicher ist nachvollziehbar, dass angesichts des schleichenden Prozesses zunehmender Überwachung mit videotechnischen Mitteln gesetzliche Normen längst überfällig sind. Die im Referentenentwurf zur Novellierung des Bundesdatenschutzgesetzes vorgesehenen Regelungen beispielsweise werden der Problematik meines Erachtens nicht gerecht. Angesichts der technischen Möglichkeiten, die moderne Videotechnik bietet, und der daraus resultierenden hohen Eingiffsintensität in das Persönlichkeitsrecht des Einzelnen sind vielmehr klare bereichsspezifische Befugnisnormen sowie eindeutige Festlegungen zur Speicherung und Löschung erforderlich. Weiterhin müssen auch für die Verarbeitung von Bilddaten die Grundsätze der Erforderlichkeit und Zweckbindung gelten. Darüber hinaus müssen Betroffene immer erkennen können, wer zu welchem Zweck Bilder aufnimmt und verarbeitet. Klare Regelungen zur Dauer der Aufbewahrung und zu Verwendungsverboten müssen definiert werden, und entsprechende Widerspruchs- bzw. Löschungsrechte sind den Betroffenen einzuräumen.

3.16.10 Orientierungshilfe für den Einsatz von Verzeichnisdiensten

Im öffentlichen Bereich sind zunehmend Verzeichnisdienste zu finden. Vorreiter in unserem Land sind die Universitäten und Hochschulen.

In Verzeichnisdiensten werden vor allem personenbezogene Daten wie Namen, Adressen, Telefonnummern, E-Mail-Adressen oder öffentliche Schlüssel für Verschlüsselung und Signatur, aber auch Daten über Organisationen, Rechner und Peripheriegeräte gespeichert und zum Abruf bereitgestellt. Systeme wie Network Directory System (NDS) von Novell oder Produkte nach dem internationalen Standard X.500 machen diese Informationen dann prinzipiell einem beliebigen Benutzerkreis verfügbar. Die Daten sind hierarchisch aufbereitet (in der Regel nach der Organisationsstruktur) und verwenden eindeutige Namen. Sie lassen sich dadurch sehr gut recherchieren und mit anderen Datenbeständen verknüpfen.

Um das Missbrauchspotential und mögliche Gegenmaßnahmen dieser Technik zu untersuchen, hat der AK Technik der Konferenz der Datenschutzbeauftragten von Bund und Ländern (siehe auch Punkt 4) eine Arbeitsgruppe eingesetzt, welche im Berichtszeitraum den ersten Teil einer Orientierungshilfe erstellt hat. Einen zweiten Teil, in dem es vorrangig um Rechtsfragen geht, erarbeitet zurzeit der AK Medien der Konferenz.

Zwei Aspekte sind für die Einrichtung und Nutzung von Verzeichnisdiensten in Behörden von besonderer Bedeutung:

- Welche Daten in ein Verzeichnis aufgenommen werden, muss unter anderem davon abhängen, ob der Dienst nur in der eigenen Behörde, behördenübergreifend oder auch öffentlich zur Verfügung stehen soll.

- Ein Verzeichnisdienst wird üblicherweise auf einem Rechner oder mittels einer verteilten Datenbank auf mehreren Rechnern realisiert. Die Sicherheit des Gesamtsystems lässt sich deshalb nur beurteilen, wenn man auch die anderen Teile (Netzwerkverbindungen, Betriebssysteme usw.) mit betrachtet.

Bei der Erarbeitung der Orientierungshilfe, die sich vorwiegend mit behördeninternen Verzeichnissen befasst, wurden bisher vor allem folgende Probleme identifiziert:

- Der Betreiber verantwortet, welcher Benutzerkreis welche Daten abrufen kann. Vor allem bei öffentlichen Verzeichnissen ist hier die Zulässigkeit zu prüfen; schon die Veröffentlichung des Arbeitsgebietes kann für den Betroffenen von Nachteil sein.

- Bisher getrennt gespeicherte Daten lassen sich einfacher zusammenführen, da Personen eindeutige Identifikationen zugewiesen werden, zu denen man beliebige Informationen speichern kann. Zusammen mit Adress- und Telefonbüchern auf CD-ROM und anderen Quellen lassen sich unter Umständen sehr detaillierte Profile erstellen, deren Umfang nicht absehbar ist.

- Von den verteilten Datenbeständen lassen sich Kopien (Repliken) erzeugen (mittels gezielter Abfrage oder Abgleichs). Diese Repliken sind nicht zwangsläufig in jedem Teilsystem aktuell. Löschung und Berichtigung sind nicht immer garantiert. Ferner kann nicht immer kontrolliert werden, nach welchen Kriterien die Repliken ausgewertet werden; dies gilt vor allem für öffentliche Verzeichnisse.

- Nicht jedes Produkt unterstützt ausreichende Authentifikations- und Zugriffsschutzverfahren. So wurden letztere erst im Jahre 1993 in der Norm X.509 festgelegt. Oft ist nicht sicher ausgeschlossen, dass Unberechtigte Daten lesen, verändern oder löschen oder den Dienst außer Betrieb setzen können.

Zur Lösung dieser Schwierigkeiten muss immer die Sicherheit des Netzwerks betrachtet werden, über das der Verzeichnisdienst betrieben wird. So sind bei einer Replikation über unsichere Leitungen etwa im WAN-Bereich kryptographische Mittel bereits unterhalb des Verzeichnisdienstes anwendbar; dies ist ein allgemeinerer Ansatz, der auch für andere Netzwerkdienste gilt. Speziell für Verzeichnisdienste empfiehlt die Orientierungshilfe bisher unter anderem:

- Der Verzeichniseintrag ist auf das Notwendige zu beschränken, wie E-Mail-Adresse, Telefonnummer, Faxnummer und öffentliche Schlüssel. Andere Informationen wie Tätigkeitsfelder oder Arbeitszeiten sollten nur in das Verzeichnis aufgenommen werden, soweit sie für die Aufgabenerledigung erforderlich sind.

- Zu klären ist, zu welchen Personen Angaben im Verzeichnisdienst veröffentlicht werden dürfen.

- Das Recht der Betroffenen auf einen korrekten Eintrag ist zu beachten. Hier bietet es sich an, dem Betroffenen die Daten vor der Eingabe in den Verzeichnisdienst vorzulegen. Mit Hilfe eines Filters sollte differenziert werden können, welche Attribute intern und welche auch extern abrufbar sind.

- Zugriffsregelungen sind möglichst eng zu fassen; es sollten starke Authentifikationsmechanismen verwendet werden (zum Beispiel digitale Signatur).

– Organisatorisch ist zu gewährleisten, dass der Verzeichnisdienst aktuell bleibt.

– Erstellung, Änderung und Löschung von Einträgen sowie Replikation von Verzeichnisteilen sind für Revisionszwecke zu protokollieren.

Die Orientierungshilfe wird voraussichtlich im ersten Quartal 2000 veröffentlicht. Sie ist dann in meiner Dienststelle kostenlos erhältlich und wird im Internet zum Herunterladen bereitstehen.

3.16.11 Kfz-Zulassung via Internet

Der Bundesbeauftragte für den Datenschutz hat über das Projekt eines erweiterten Kfz-Zulassungsverfahrens informiert, das die Nutzung des Internet bei der Datenübermittlung zwischen Kfz-Händler und Zulassungsstelle einschließt. Ziel dieses Verfahrens ist es einerseits, die Wartezeit der Bürger bei der Zulassung eines Kfz zu verkürzen und eine einfachere Reservierung von so genannten Wunschkennzeichen zu realisieren. Andererseits sollen Kfz-Händler die Möglichkeit erhalten, Zulassungen auch außerhalb der Öffnungszeiten von Zulassungsstellen vorzubereiten. Darüber hinaus sollen Erfassungsfehler vermieden werden, indem die bisher doppelte Erfassung von Antragsdaten durch Antragsteller und Zulassungsstelle entfällt.

Da die datenschutzrechtlichen Aspekte des Kfz-Zulassungsverfahrens in den Zuständigkeitsbereich der jeweiligen Landesdatenschutzbeauftragten fallen, habe auch ich mich mit dieser Thematik befasst. Es wurden zwei Verfahren diskutiert.

Das erste Verfahren sah vor, dass beispielsweise Autohäuser als „beliehene Unternehmer“ den überwiegenden Teil des Zulassungsverfahrens selbst durchführen sollen. Der Behörde bliebe lediglich die Registrierung der Zulassung und die Aufbewahrung der Originalunterlagen. In diesem Fall müssten die Autohäuser selbst personenbezogene Daten im Rahmen des Zulassungsverfahrens speichern und Blankoformulare, Siegel und Plaketten für die Hauptuntersuchung aufbewahren. Hierfür fehlt jedoch die gesetzliche Grundlage. Darüber hinaus wäre für die vorgelagerten Prüfungen (etwa die Identitätsprüfung des Halters) ein Zugriff auf die Melderegister und die Halterdaten nötig. Bei der Vielzahl der Beteiligten wäre die rechtliche Zulässigkeit einzelner Abrufe nur schwer zu kontrollieren, und der Missbrauch würde erleichtert. Deshalb habe ich mich gegen dieses Verfahren ausgesprochen.

Das zweite Verfahren sieht hingegen vor, dass der Kfz-Händler lediglich die für die Zulassung erforderlichen Daten auf elektronischem Wege an die Zulassungsstelle übermittelt. Diese Daten könnten beispielsweise unter Verwendung entsprechender Sicherheitseinrichtungen über das Internet in einen gesonderten Bereich des Behördencomputers eingegeben werden. Die Übernahme in den Echtdatenbestand zur abschließenden Bearbeitung der Zulassung erfolgt dann erst nach der anschließenden Prüfung durch Mitarbeiter der Zulassungsstelle. Die Antragsteller müssen dann nur noch in der Zulassungsstelle erscheinen, um die Unterlagen dort gegen Unterschrift in Empfang zu nehmen.

Dieses Verfahren halte ich für datenschutzrechtlich unbedenklich, wenn folgende Sicherheitsmaßnahmen umgesetzt werden:

- Kfz-Händler dürfen keinen Zugang zum Echtdatenbestand der Zulassungsbehörden haben.

- In den Zulassungsstellen sind dazu entsprechende Sicherheitsvorkehrungen zu treffen (Trennung des Eingaberechners vom Behördennetz oder Einsatz einer Firewall, Protokollierung usw.).

- Die Eingabebereiche verschiedener Autohändler müssen voneinander getrennt sein.

- Zugangsberechtigte müssen sich zweifelsfrei identifizieren und authentifizieren. Dazu sind dem Stand der Technik entsprechende Maßnahmen zu treffen (beispielsweise digitale Signatur, Chipkarten, Rufnummernprüfung, IP-Adressüberprüfung).

- Der Kreis der zugangsberechtigten Mitarbeiter aller am Verfahren beteiligten Stellen ist auf das für die Aufgabenerfüllumg erforderliche Maß zu beschränken

- Die Antragsdaten sollten vor der Übertragung verschlüsselt werden.

- Die Sicherungsfunktion des Kfz-Briefes muss erhalten bleiben.

Einige Bundesländer wenden dieses Verfahren bereits an. Der Landkreis Saarlouis hat beispielsweise die oben genannten Anforderungen im IT-Sicherheitskonzept vollständig berücksichtigt.

Sollten sich Zulassungsstellen unseres Landes für den Einsatz dieses Verfahrens entscheiden, werde ich gerne zu weiteren datenschutzrechtlichen Fragen beraten.

3.16.12 Neue Antragsverfahren für Ausweispapiere und Führerscheine

Alle deutschen Pässe und Personalausweise stellt die Bundesdruckerei GmbH in Berlin her. Seit dem 1. Dezember 1998 fertigt sie dort auch die neuen EU-Führerscheine im Scheckkartenformat. Auch Pass- und Melde- sowie Fahrerlaubnisbehörden aus Mecklenburg-Vorpommern erteilen Aufträge dazu.

In den letzten Jahren wurden das Antrags- und das Produktionsverfahren für Ausweispapiere umfassend modernisiert, um die Qualität zu verbessern und die Herstellungszeiten zu verkürzen. Die neuen Dienstleistungen und Produkte werden jetzt unter den Namen D-PASS (für Pässe), DIGANT (für Personalausweise) und DIGANT-FS (für Führerscheine) vertrieben. Die Bundesdruckerei hatte den Arbeitskreis Technik eingeladen, um über das neue Verfahren und die dazu geschaffene technische Infrastruktur zu informieren, damit die Datenschutzbeauftragten die Behörden in ihrem jeweiligen Zuständigkeitsbereich kompetent beraten können (siehe auch Punkt 4).

In den Behörden, die an dem neuen Verfahren teilnehmen, werden an einem speziell ausgestatteten Arbeitsplatz die Antragsdaten erfasst und die Passfotos der Antragsteller gescannt. Dadurch entfällt die sonst recht aufwändige Bildbearbeitung und Datenkorrektur in der Bundesdruckerei. Anschließend werden die Daten per elektronischer Post zur Bundesdruckerei übertragen, die sie zunächst auf Integrität und Plausibilität prüft und dann in den Produktionsprozess für die entsprechenden Ausweispapiere übernimmt. Gleichfalls auf elektronischem Wege informiert die Druckerei die Auftraggeber über den Fortgang von Produktion und Versand, und sie übermittelt auf diese Weise auch Ausweisnummern und Herstellungsdaten.

Die besondere Aufmerksamkeit der Entwickler galt der Sicherheit der Datenübertragung. Alle auftraggebenden Behörden kommunizieren ausschließlich verschlüsselt mit der Bundesdruckerei. Hierbei kommen anerkannte kryptographische Algorithmen zum Einsatz, die nach dem gegenwärtigen Stand der Technik als sicher gelten. Die Schlüssel werden bei den Auftraggebern auf Chipkarten gespeichert. Für D-PASS und DIGANT wurde die CCI GmbH, Meppen, beauftragt, die Schlüsselverwaltung einschließlich der Personalisierung der Chipkarten zu übernehmen. Bei DIGANT-FS bedient sich die Bundesdruckerei der gleichen Infrastruktur und auch der gleichen Schlüssel, die für die Kommunikation der Fahrerlaubnisbehörden mit dem Kraftfahrt-Bundesamt (KBA) eingesetzt werden.

In der Bundesdruckerei selbst schützen zwei Firewallsysteme aus Produkten verschiedener Hersteller die Produktionsdaten vor möglichen Manipulationen. Mitarbeiter aus getrennten Fachbereichen pflegen und überwachen jeweils eine der Firewalls.

Die neuen elektronischen Verfahren bieten sowohl für den Bürger als auch für die Verwaltung Vorteile. Ausweispapiere lassen sich jetzt schneller und mit geringerer Reklamationsrate herstellen. Darüber hinaus kann die Verwaltung Anfragen jetzt zügiger beantworten. Der bei diesem Verfahren realisierte Datenschutzstandard kann gegenwärtig als beispielgebend für andere Verfahren angesehen werden.

3.16.13 Bundesweite Behördenvernetzung mit TESTA

Seit September 1999 nimmt das Land Mecklenburg-Vorpommern die Dienste des Weitverkehrsnetzes TESTA-Deutschland in Anspruch. TESTA (Trans European Services for Telematics between Administrations) ist ein Projekt der Europäischen Union zur Vernetzung europäischer und nationaler Behörden. Die Deutsche Telekom AG als Betreiber von TESTA-Deutschland stellt jedem Bundesland einen Zugang zur Verfügung. Über das Netz werden Dienste wie elektronische Post (siehe Dritter Tätigkeitsbericht, Punkt 3.18.2), ein elektronischer Verzeichnisdienst (siehe auch Punkt 3.16.10) oder der Zugriff auf das juristische Informationssystem JURIS-Online angeboten.

Da TESTA auch zur Übertragung von personenbezogenen Daten verwendet wird, bin ich im Rahmen der Sitzungen des Interministeriellen Ausschusses für Informationstechnik (IMA-IT) um Beratung zu den Sicherheitsmechanismen gebeten worden. Ich habe darauf hingewiesen, dass für den Betrieb von TESTA öffentliche Leitungen genutzt werden. Die deshalb bereits auf Bundesebene geplanten Sicherheitsmaßnahmen wurden bisher jedoch nicht vollständig umgesetzt. Beispielsweise ist die als Grundsicherung erforderliche Leitungsverschlüsselung noch nicht realisiert. Darüber hinaus ist bereits jetzt absehbar, dass für einige der geplanten Anwendungen eine Ende-zu-Ende-Verschlüsselung und die Sicherung der übermittelten Daten durch eine digitale Signatur notwendig sein werden. Diese kryptographischen Verfahren erfordern ein effektives Schlüsselmanagement, das ohne ein Trustcenter kaum wirtschaftlich realisierbar ist (siehe dazu auch Punkt 3.16.3). Ich habe deshalb empfohlen, bereits jetzt ein Trustcenter für TESTA zu planen.

Auch andere Landesdatenschutzbeauftragte wurden bereits um Hinweise zu TESTA gebeten. Um bundesweit möglichst einheitliche Anforderungen an den datenschutzgerechten Betrieb dieses Netzes stellen zu können, hat hierzu auch der AK Technik beraten (siehe Punkt 4). Im Ergebnis werden die oben genannten Empfehlungen nun übereinstimmend von den Datenschutzbeauftragten des Bundes und der Länder gegeben.

Neben den bundesweit relevanten Themen, die unter anderem von der Koordinierungs- und Beratungsstelle Informationstechnik im Bundesinnenministerium (KBSt) bearbeitet werden, gibt es viele landesspezifische Fragen, für die die Koordinierungs- und Beratungsstelle der Landesregierung für Informations- und Telekommunikationstechnik in der Landesverwaltung (LKSt) zuständig ist. Da die Planung zur landesweiten Vernetzung noch in den Kinderschuhen steckt (siehe Punkt 3.16.1), konnten bisher die Anforderungen an die Schnittstelle zum Landesnetz LAVINE beziehungsweise zum TK-Anlagenverbund der Landesregierung von der LKSt noch nicht präzise genug definiert werden. Die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH), die den Netzzugang im Auftrag der LKSt aufbaut und pflegt, hat bisher nur einen Filter für bestimmte Protokolle und Adressen sowie die für TESTA erforderliche Adressübersetzung (Network Address Translation, NAT) eingerichtet. Ich habe gegenüber unserem Innenministerium zum Ausdruck gebracht, dass diese Maßnahmen zwar erforderlich, jedoch noch nicht ausreichend sind. Meines Erachtens kommt der Anschluss von TESTA nur über die zentrale Firewall (siehe Punkt 3.16.1) in Betracht, damit die übertragenen Daten zusätzlich auch auf Protokollfehler (und -manipulationen) und auf Computerviren gefiltert werden können. Um diese Forderung umzusetzen, müsste die DVZ M-V GmbH jedoch entsprechend präzisierte Anforderungen von der LKSt erhalten. Das ist bisher nicht geschehen.

4 Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik)

Im Berichtszeitraum fanden unter meiner Federführung fünf Sitzungen des Arbeitskreises in Berlin, Essen und Schwerin statt. Die gemeinsame Arbeit der Techniker aus den Dienststellen aller Datenschutzbeauftragten in diesem Gremium war insbesondere von der ständig zunehmenden - vielfach auch länderübergreifenden - Vernetzung der Behörden geprägt. Im Mittelpunkt unserer Beratungen standen deshalb unter anderem datenschutztechnische Aspekte der Nutzung des Internet durch Behörden, die Anwendung kryptographischer Verfahren zum Schutz von personenbezogenen Daten bei ihrer Speicherung oder Übermittlung und die Revisionssicherheit der verwendeten Hard- und Softwarekomponenten.

Bereits im Herbst 1996 hatte der Arbeitskreis in der Orientierungshilfe „Internet“ die Risiken bei der Nutzung dieses Mediums beschrieben und Empfehlungen gegeben, wie diese Risiken minimiert werden können. Die Technik entwickelt sich gerade in diesem Bereich jedoch so schnell, dass schon wenig später eine Überarbeitung des Textes erforderlich war. Im September 1998 legte der AK Technik deshalb eine zweite aktualisierte Auflage vor. Dank tatkräftiger Unterstützung einiger Sponsoren konnten die Texte in Form einer handlichen Broschüre veröffentlicht werden. Zurzeit ist die dritte Auflage der Orientierungshilfe in Vorbereitung. Hier wird ein Abschnitt hinzukommen, in dem insbesondere die Auswirkungen der neuen Gesetze im Medien- und Telekommunikationsbereich auf den Betrieb von Firewalls erläutert werden (siehe Punkt 3.16.4).

Auch im Rahmen des Arbeitskreises hat es sich bewährt, intensive Kontakte zu Fachleuten aus Wissenschaft, Wirtschaft und Verwaltung zu pflegen, damit deren Fachwissen in die Beratungstätigkeit der Datenschutzbeauftragten einfließen kann. Im Herbst 1998 und im Sommer 1999 war der AK Technik beispielsweise von der Bundesdruckerei nach Berlin eingeladen worden, um sich vor Ort über neue internetbasierte Verfahren im Zusammenhang mit der Beantragung und Herstellung von Personalausweisen und Führerscheinen zu informieren. Einerseits konnten dadurch schon in der Projektierungsphase Hinweise zur datenschutzgerechten Ausgestaltung dieser Verfahren berücksichtigt werden (siehe Punkt 3.16.12), andererseits hatten die Arbeitskreismitglieder die Möglichkeit, sich insbesondere im Hinblick auf eine effektive Beratungstätigkeit bei vergleichbaren Anwendungen über den Einsatz moderner kryptographischer Verfahren an einem praktischen Beispiel zu informieren.

Im Herbst 1999 tagte der AK Technik bei der TÜV Informationstechnik GmbH (TÜViT) in Essen. Die Gastgeber berichteten unter anderem ausführlich über die Prüfung und Zertifizierung von technischen Komponenten, die für die sichere Nutzung des Internet von Bedeutung sind (beispielsweise Firewall-Komponenten). Weiterhin erläuterten die Fachleute des TÜViT, welche Rolle dabei international gültige Sicherheitskriterien wie ITSEC und Common Criteria spielen (siehe Punkt 3.16.6). Erörtert wurde auch, auf welche Weise die Datenschutzbeauftragten bei ihren Beratungen und Kontrollen das beim TÜViT vorhandene Fachwissen nutzen können. Ein Ergebnis war beispielsweise die Gründung einer gemeinsamen Arbeitsgruppe, die einheitliche Prüfkriterien für datenschutzfreundliche Produkte entwickeln soll.

Im Zusammenhang mit Fragen der Transparenz und Revisionssicherheit von Hard- und Software befasste sich der AK Technik auch mit der Seriennummer des Pentium III und mit der Online-Registrierung von Softwareprodukten (siehe Punkt 3.16.7). Die Mitglieder bereiteten für die 57. Konferenz der Datenschutzbeauftragten einen entsprechenden Entschließungsentwurf vor. Unter anderem werden darin Hard- und Softwarehersteller aufgefordert, ihre Produkte so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können. Die Konferenz verabschiedete die Entschließung und empfahl den Anwendern moderner Technik, nur solche Produkte einzusetzen, die auch eine Transparenz der Verfahrensabläufe gewährleisten (siehe 11. Anlage).

Die technische Kompetenz der Arbeitskreismitglieder war auch im Zusammenhang mit der anstehenden Novellierung der Datenschutzgesetze von Bund und Ländern gefragt. Seit langem wird völlig zu Recht kritisiert, dass insbesondere die Vorschriften zu den technischen und organisatorischen Maßnahmen nicht mehr dem Entwicklungsstand entsprechen. Der AK Technik hatte 1998 von der Datenschutzkonferenz deshalb den Auftrag erhalten, Vorschläge für die Vereinheitlichung und Weiterentwicklung der bisher gültigen Technikregelungen zu unterbreiten sowie Empfehlungen für neue Regelungen zu speziellen technischen Komponenten wie Chipkarten oder Laptops zu erarbeiten. Der Arbeitskreis hat seine Arbeitsergebnisse im Frühjahr 1999 der 57. Konferenz vorgelegt. Die Konferenz war sich war sich einig, dass „...das Papier bei der Novellierung der Datenschutzgesetze von Bund und Ländern für alle Beteiligten als Hilfsmittel dienen und dazu beitragen soll, möglichst einheitliche, dem Stand der Technik entsprechende Regelungen zum technischen und organisatorischen Datenschutz zu finden.“

5 Öffentlichkeitsarbeit

Das Interesse der Bürger und der öffentlichen Stellen an Informationen zum Datenschutz hat im Berichtszeitraum deutlich zugenommen. Besonders erfreulich daran ist, dass Landes- und Kommunalbehörden mich in zunehmendem Maße bereits im Vorfeld datenschutzrelevanter Projekte um Beratung bitten. Auch bei den „Tagen der offenen Tür“ des Landtages Mecklenburg-Vorpommern, bei denen der Landesbeauftragte für den Datenschutz über seine Arbeit informiert, bekunden immer mehr Besucher Interesse an aktuellen Themen des Datenschutzes.

Darüber hinaus hatten zahlreiche Institutionen Vortragswünsche, so unter anderem Krankenhäuser und Kliniken, Hochschulen und Universitäten, der Arbeitslosenverband, der Militärische Abschirmdienst, das Landesjugendamt, der Bund der Juristinnen und eine Seniorengruppe der Volkshochschule. Bei den gewünschten Themen handelte es sich insbesondere um grundsätzliche Fragen des Datenschutzes, juristische Sachverhalte, den Sozialdatenschutz sowie datenschutztechnische Details.

Offensichtlich ist auch das von uns angebotene schriftliche Informationsmaterial für die Bürger, die Verwaltung und die Wirtschaft zu einer wichtigen Informationsquelle geworden. Vollständig überarbeitet haben wir die in Form einer Loseblattsammlung vorliegenden „Gesetze und Verordnungen zum Datenschutz“. Der AK Technik (siehe Punkt 4) hat Materialien zum Internet (siehe Punkt 3.16.1) und zu datenschutzfreundlichen Technologien (siehe Dritter Tätigkeitsbericht Punkt 2.1) herausgegeben. Durch Unterstützung einiger Sponsoren war es uns möglich, sie in Broschürenform zu veröffentlichen. Vielfältige Anfragen aus dem Bereich der Krankenhäuser und Kliniken waren Anlass für eine weitere Broschüre mit dem Titel „Datenschutz im Krankenhaus“.

Dank der tatkräftigen fachlichen Unterstützung des Fachbereiches Informatik der Universität Rostock unterhalten wir seit Anfang 1999 eine eigene Internet-Homepage. So können wir einen noch größeren Adressatenkreis erreichen, ohne unseren kleinen Haushalt zusätzlich zu belasten. Leserfreundlich stehen unter der Adresse www.lfd.m-v.de alle bisher veröffentlichten Materialien wie Tätigkeitsberichte, Gesetzessammlung oder Orientierungshilfen zum Abruf bereit. Außerdem wird mit so genannten Links auf die Internetangebote der Kollegen in Bund und Ländern verwiesen.

Seit 1998 sind wir unter der Adresse datenschutz@mvnet.de für Bürger und Behörden auch auf elektronischem Wege erreichbar. Wer möchte, kann seine Mitteilung verschlüsseln. Dafür steht der erforderliche öffentliche Schlüssel in unserem Internetangebot zum Abruf bereit. Dort sind auch detaillierte Hinweise zum Umgang mit der verwendeten Verschlüsselungssoftware PGP zu finden.

Die Zusammenarbeit mit den Vertretern der Medien in unserem Land hat sich gut entwickelt. Einerseits haben uns die Journalisten in unserer Tätigkeit unterstützt, indem sie die Bürger über aktuelle datenschutzrelevante Sachverhalte informiert haben. Andererseits gab es aber auch Fälle, wo Verstöße gegen den Datenschutz erst durch die journalistische Tätigkeit aufgedeckt wurden und Missstände beseitigt werden konnten. Ich würde mich freuen, wenn sich diese gute Zusammenarbeit auch in den kommenden Berichtszeiträumen fortsetzt.

6 Anlagen

1. Anlage: Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998

Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, dass bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, dass erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, dass auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen („Free TV“ und „Pay TV“) muss die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, dass die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muss sich an dem Ziel ausrichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;

- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;

- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;

- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d. h., Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

2. Anlage: Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998

Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten“ der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten“ noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluss der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, dass ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

3. Anlage: Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlass an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlass an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

4. Anlage: Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefassten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.

- Die anlassfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muss in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.

- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

5. Anlage: Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlass von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u. a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

6. Anlage: Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Fehlende bereichsspezifische Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz - bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern - im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, dass sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, dass die Rechtsprechung des Bundesverfassungsgerichts zum so genannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluss an ihren Beschluss der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien namentlich die

- Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen,

- Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden,

- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien,

- Datenübermittlung zu wissenschaftlichen Zwecken,

– Datenverarbeitung in der Zwangsvollstreckung,

– Datenverarbeitung im Jugendstrafvollzug,

– Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muss vorab unter datenschutzrechlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein „StVÄG 1996“ erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Zu kritisieren sind vor allem:

– Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung,

– Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte,

– Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen.

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

7. Anlage: Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

8. Anlage: Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z. B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

9. Anlage: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben

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

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

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

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

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

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

10. Anlage: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

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

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

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

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

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

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

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

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

11. Anlage: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Transparente Hard- und Software

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

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

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

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

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

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

12. Anlage: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98)

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

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

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

13. Anlage: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss vom 17.09.1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

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

14. Anlage: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Täter-Opfer-Ausgleich und Datenschutz

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

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

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

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

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

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

15. Anlage: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung

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

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

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

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

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

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,

- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,

– Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),

– Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,

– Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,

– Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

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

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

16. Anlage: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

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

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

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

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

17. Anlage: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Patientenschutz durch Pseudonymisierung

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

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

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

18. Anlage: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

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

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

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

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

19. Anlage: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

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

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

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

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

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

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

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

Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

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

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

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

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

Angemessener Datenschutz auch für Untersuchungsgefangene

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

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

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

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

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

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

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

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

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

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

„Gesundheitsreform 2000“

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes „Gesundheitsreform 2000“:
Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

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

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

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

Insbesondere klärungsbedürftig sind folgende Punkte:

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

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

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

– Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

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

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

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

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

23. Anlage: Appell der Datenschutzbeauftragten des Bundes und der Länder

Hoher Datenschutz für Versicherte bei Gesundheitsreform muss gehalten werden!

Das am 4. November 1999 vom Bundestag beschlossene Gesundheitsreformgesetz 2000 enthält mehrere datenschutzrechtliche Verbesserungen gegenüber der bisherigen Rechtslage. Durch das „Aufschnüren“ des Pakets und die Preisgabe der zustimmungspflichtigen Teile des Gesetzes droht nun, dass diese Verbesserungen nicht umgesetzt werden. Die Datenschutzbeauftragten des Bundes und der Länder Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein fordern die zuständigen gesetzgebenden Körperschaften auf, den entsprechenden - politisch bislang völlig unstreitigen - Gesetzesteil im Bundesrat passieren zu lassen:

Als Folge der Kritik der Datenschutzbeauftragten wurden vom Bundestag die Regelungen zum Umgang mit den Daten der Versicherten in der gesetzlichen Krankenversicherung erheblich verbessert, z. B. durch die Beschränkung der Datenzugriffsrechte innerhalb der Krankenkassen, die Einführung eines Beratungsgeheimnisses oder eine verbesserte Einbeziehung der Patientinnen und Patienten bei bestimmten ärztlichen Datenübermittlungen.

Wegweisend für die Zukunft im Umgang mit Patientendaten ist aber die vorgesehene Pseudonymisierung des gesamten Abrechnungsverfahrens. Damit können die politisch und ökonomisch angestrebten Auswertungen mit medizinischen Daten, die vor allem der Kostenkontrolle dienen, vorgenommen werden, ohne dass hierdurch die Belange des Patientengeheimnisses oder des Datenschutzes verletzt würden. Das bisherige Verfahren würde grundlegend verbessert, weil bei den Krankenkassen auch Krankenhaus- und Arzneimittelkosten nicht mehr personenbezogen abgerechnet werden müssten - die Gefahr des „gläsernen Patienten“ würde erheblich reduziert.

Dieser versichertenfreundliche Gesetzesteil ist jedoch im Bundesrat zustimmungspflichtig. Während der Beratungen in den Ausschüssen des Bundestages wurde er quer durch die Parteien befürwortet und so verabschiedet. Selbst die Kassen und die Pharmaindustrie begrüßten die Vorschläge weitgehend. Bedeutende zusätzliche Kosten würden durch das neue Verfahren nicht entstehen.

Es stünde allen politisch Handelnden gut zu Gesicht, den Datenschutz im besonders schützenswerten Bereich des Gesundheitswesens trotz aller politischer Kontroversen zu verbessern. Wir appellieren daher an die Bundesregierung bzw. das Gesundheitsministerium, die erreichten guten Datenschutzregelungen in den Bundesrat einzubringen, und an den Bundesrat, diesen zuzustimmen.

24. Anlage: Vordruck zum Widerspruchsrecht

Absender:

_____
Vorname, Name

_____
Geburtsdatum

_____
Straße / Postfach

_____ _____
Postleitzahl, Ort (Datum)

An
die Gemeinde*/die Stadt*/
das Amt* .....
- Meldebehörde -
_____

_____

Widerspruch gegen die Weitergabe meiner Daten gemäß §§ 32, 35 Meldegesetz für das Land Mecklenburg-Vorpommern (Landesmeldegesetz - LMG -)

Sehr geehrte Damen und Herren,

hiermit widerspreche ich der Weitergabe meiner Daten an

❒ Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Parlaments- und Kommunalwahlen sowie verfassungsrechtlich oder gesetzlich vorgesehenen Abstimmungen (§ 35 Abs. 1 LMG),

❒ Mandatsträger, Presse oder Rundfunk bei Anfragen nach Alters- oder Ehejubiläen (§ 35 Abs. 2 LMG),

❒ Adressbuchverlage zum Zwecke der Veröffentlichung in einem Adressbuch (§ 35 Abs. 3 LMG)

❒ öffentlich-rechtliche Religionsgesellschaften meiner Familienangehörigen (Ehegatte, minderjährige Kinder, Eltern minderjähriger Kinder), denen ich selbst nicht angehöre (§ 32 Abs. 2 LMG).

Mit freundlichen Grüßen

_____
(Unterschrift)

* Nicht Zutreffendes bitte streichen

7 Abkürzungsverzeichnis

AfNS	Amt für Nationale Sicherheit
AK Medien	Arbeitskreis „Medien“ der Datenschutzbeauftragten des Bundes und der Länder
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder
AKG	Arbeitsgemeinschaft Kammerleitstelle Messbeträge
AO	Abgabenordnung
ARGUS	Allgemeines Register- und Informationssystem für Gerichte und Staatsanwaltschaften
ARGUS-GB	Allgemeines Register- und Informationssystem für Gerichte und Staatsanwaltschaften - Bereich Grundbuch
ARGUS-StA	Allgemeines Register- und Informationssystem für Gerichte und Staatsanwaltschaften - Bereich Staatsanwaltschaft
AufbewBest	Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden
BAföG	Bundesausbildungsförderungsgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BIOS	Basic Input Output System
BKAG	Bundeskriminalamtsgesetz
BKK	Betriebskrankenkasse
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BNotO	Bundesnotarordnung
BR-Drs.	Bundesrats-Drucksache

BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BVerfGE	Entscheidung des Bundesverfassungsgerichts (Band ..., Seite ...)
BZRG	Bundeszentralregistergesetz
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EG	Europäische Gemeinschaft
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EK-Datum	Datum der letzten Erkenntnis/Information
ELSTER	Elektronische Steuererklärung
EPOS	Elektronisches Personal-, Organisations- und Stellenverwaltungssystem
EU	Europäische Union
GBO	Grundbuchordnung
GG	Grundgesetz
GKV-Gesundheits-reform 2000	Gesetz zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000
GStA	Generalstaatsanwaltschaft
GUID	Globally Unique Identifier
IHK	Industrie- und Handelskammer
IMA-IT	Interministerieller Ausschuss für Informationstechnik
ISO	Internationale Standardisierungsorganisation
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria
KAN	Kriminalaktennachweis

KBA	Kraftfahrt-Bundesamt
KBSt	Koordinierungs- und Beratungsstelle Informationstechnik im Bundesministerium des Innern
KindRG	Kindschaftsrechtsreformgesetz
KrebsRAG M-V	Krebsregisterausführungsgesetz Mecklenburg-Vorpommern
LAN	Lokal Area Network (lokales Netz)
LAPIS	Landesweites Polizeiinformations-System
LAVINE	Landesverwaltungs- und Informationsnetz
LBG M-V	Landesbeamtengesetz Mecklenburg-Vorpommern
LHG M-V	Landeshochschulgesetz Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LKSt	Koordinierungs- und Beratungsstelle der Landesregierung für Informations- und Telekommunikationstechnik in der Landesverwaltung
LMG	Landesmeldegesetz für das Land Mecklenburg-Vorpommern
MDK	Medizinischer Dienst der Krankenversicherung
MfS	Ministerium für Staatssicherheit
MiStra	Mitteilungen in Strafsachen
MPI	Max-Planck-Institut für Bildungsforschung
NAT	Network Address Translation
NDS	Network Directory System
OECD	Organisation für wissenschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
PAD-MV	Personenarbeitsdatei Mecklenburg-Vorpommern
PED M-V	Polizeiliche Erkenntnisdatei Mecklenburg-Vorpommern

PERSYS	Personal- und Stellenverwaltungssystem
PIN	Persönliche Identifikations-Nummer
PISA	Program for International Students Assessment
PSN	Processor Serial Number (Prozessorseriennummer)
RegTP	Regulierungsbehörde für Telekommunikation und Post
RfÄndStV	Rundfunkänderungsstaatsvertrag
RundfG M-V	Landesrundfunkgesetz Mecklenburg-Vorpommern
SGB I	Sozialgesetzbuch Erstes Buch
SGB IV	Sozialgesetzbuch Viertes Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SigG	Signaturgesetz
SigV	Signaturverordung
SOG M-V	Gesetz über die öffentliche Sicherheit und Ordnung Mecklenburg-Vorpommern
StADÜV	Steueranmeldungs-Datenübermittlungs-Verordnung
StUG	Stasi-Unterlagen-Gesetz
StVÄG	Strafverfahrensänderungsgesetz
TDSV	Telekommunikations-Datenschutzverordnung
TESTA	Trans European Services for Telematics between Administrations
TKG	Telekommunikationsgesetz
TLBS	Täterlichtbildsystem
TÜViT	Technischer Überwachungsverein Informationstechnik

VPKA	Volkspolizeikreisamt
WAN	Wide Area Network (Weitverkehrsnetz)
WV-Datum	Wiedervorlagedatum
ZPO	Zivilprozessordnung

8 Stichwortverzeichnis

A

Abgaben 100
Abgabenordnung 66
Abgleich 58
Abhörgerät 112
Abrufverfahren 50, 71, 116
Administrationsaufgaben 64
Adressbuch 131
AK Medien 107, 114
AK Technik 12, 106, 107, 110, 114, 117, 119, 120
Akten 15
Akteneinsichtsrecht 21
Amtsermittlungsgrundsatz 76
Amtshilfe 6
Amtsstellung 27
Anhörungsbehörde 56
Anonymisierung 9, 13, 80, 108
Anonymität 61, 109, 136
Anrufweiterschaltung 60
Anschlussbeitrag 101
Anwendungsprogramm 64
AO 66
Archiv 47
ARGUS 24
ARGUS-StA 30
Artikelgesetz 60
AsylCard 49
Aufbewahrung 138
Aufbewahrungsbestimmungen 31
Aufbewahrungsvorschriften 15
Aufgebot 21
Aufsichtsbehörde 6, 80
Auftragnehmer 63
Auftragsdatenverarbeitung 25, 75, 105
Auskunft 27
Auskunftsrecht 15, 21
Ausland 59
Ausschlussurteil 22
Ausweis 59
Authentizität 12, 65

B

BAföG 74
Bank 66
Beanstandung 33, 48, 95
Befragung 57
behördlicher Datenschutzbeauftragter 9
Beihilfestelle 93
Beitrags- und Gebührenerhebung 100
Beitragsfestsetzung 98
Bekanntmachungspflicht 51
beliehener Unternehmer 116
berechtigtes Interesse 27
bereichsspezifisch 13
Berufsgeheimnis 9, 28
Beschuldigter 20
Bestattungsunternehmen 65
Betäubungsmittel 18
Betriebskrankenkasse 71
Bevölkerungsbefragung 57
Bewerber 86
BfD 11, 29
Biometrie 113
BNotO 27
BSI 25, 109
Bundesamt für Sicherheit in der Informationstechnik 25, 109
Bundesausbildungsförderungsgesetz 74
Bundesbeauftragter für den Datenschutz 11, 29
Bundesdatenschutzgesetz 13, 114
Bundesfinanzministerium 67
Bundesnotarordnung 27
Bundesregierung 11
Bundesverfassungsgericht 10, 28
Bürgerbüro 55

C

Chipkarte 9, 11, 13, 24, 49, 93, 107, 117, 118, 133
Common Criteria 109, 120

D

Data-Warehouse 72
Dateibeschreibung 32
Datenannahmestelle 71, 72, 150
Datenschutz- und IT-Sicherheitskonzept 63
Datenschutzaudit 123
Datenschutzbeauftragter 9
datenschutzfreundliche Technologien 108, 136, 137, 140
Datenschutzfreundlichkeit 109, 111
Datenschutzgesetz 9, 12, 13
Datenschutzkontrolle 9, 15
Datenschutzrichtlinie 9, 11, 13
Datenschutzvereinbarung 96
Datensicherheit 9, 65
Datensicherung 15
Datensparsamkeit 13, 107, 134
Datentransport 65
Datenübermittlung 68, 94
Datenvermeidung 9, 11, 107, 127, 133
DDR 45
Deutscher Juristentag 127
Dienstanweisung 33
Dienstaufsicht 28
Dienstordnung 29
digitale Signatur 24, 65, 117, 119
digitales Fernsehen 123
Direktwirkung 7
DNA-Analyse 17, 144
Drogenkriminalität 19
DVZ M-V GmbH 25, 63, 106, 119
DVZ-Gesetz 106

E

Echtdaten 64
Echtdaten-Test 64
EG 14, 59, 66
EG-Datenschutzrichtlinie 7, 9, 11, 13, 127, 133
EG-Richtlinie 66
Eigentümer 101
Eingabekontrolle 30
Eingriffsbefugnis 132
Einsicht 27
Einwilligung 17, 18, 41, 53, 57, 59, 66, 131, 139, 144
elektronische Einwilligung 59
elektronische Kassenanordnung 65
Elektronische Post 118

Elektronische Steuererklärung 69
Elektronisches Grundbuch 104
ELSTER 69
Endgerät 64
Endgerätesicherheit 64
ENFOPOL 137
Entgeltberechnung 60
Entwurf 9
EPOS 104
Erbschaftsteuer- und Schenkungsteuergesetz 65
Erkennungsdienstliche Behandlung 40, 41
Ermittlungsverfahren 7, 36, 81
EU 13, 57
Europäische Gemeinschaft 14, 59, 66
Europäische Grundrechtscharta 142
Europäische Kommission 7
Europäische Union 13, 57
Europäischer Gerichtshof 7, 14

F

Fahrerlaubnis 80
Fahruntüchtigkeit 81
Fangschaltung 60
Fernmeldegeheimnis 60
Fernmess- und Fernwirkdienste 13
Finanzamt 69
Finanzbehörde 66
Finanzministerium 63, 66
Finanzverwaltung 64, 66, 69
Firewall 117, 119, 120
Formular 65
Forschung 20, 79, 91, 95, 96, 148
Free TV 123
Freigabeverfahren 10, 69
Freistellungsauftrag 77, 126
Führerschein 120

G

Gartenhaus 67
GBO 24
Geburtsdatum 66
Gefährdungsanalyse 63
Geheimhaltungsinteresse 80
Geldkarte 125
Geldwäsche 66
Geldwäschegesetz 67

Geldwäscherichtlinie 66
Generalstaatsanwaltschaft 30
Gericht 34, 128
Gesetzesvorbehalt 10
GKV-Gesundheitsreform 2000 ..... 8, 70, 110, 143, 149, 151
Großer Lauschangriff 146
Großrechner 12
Grundbuch 23, 27
Grundbuchakten 6
Grundbuchamt 27, 101
Grundbuchauszug 101
Grundbuchordnung 24
Grundstück 27

H

Handwerksrolle 97
Haushalt 63
Hinweispflicht 59
Hoheitsrecht 100
Holländisches Modell 60
Hundebestandsaufnahme 61

I

ICD-10-Schlüssel 150
Identifizierung 66
Identität 66
Identitätsfeststellungsgesetz 17
Identitätsprüfung 59
IMA-IT 119
Industrie- und Handelskammer 26
Informations- und Kommunikationsdienste-Gesetz 11
Informations- und Kommunikationstechnik 65
Innenministerium 9
INPOL-neu 37, 38
Integrität 12, 65
Internet 69, 101, 106, 108, 116, 120, 137
ISDN-Richtlinie 59
ISO 109
ITSEC 120
IT-Sicherheitskriterien 109

J

Jugendamt 73
JURIS 118
Justizminister 27

K

KAN 37
Kassenärztliche Vereinigung 96
KBSt 119
Kfz-Brief 117
kommunales Melderegister 131
Kontrollbefugnis 9
Kontrollkompetenz 36, 133
Krankenhaus 84
Krankenkasse 96
Krebsregister 78
Krebsregisterausführungsgesetz 78
Kreditinstitut 62, 66
Kriminalaktennachweis 37
Kriminalitätsbekämpfung 113
Kryptographie 103, 127, 140
kryptographischer Schlüssel 105
kryptographisches Verfahren 24, 65, 104, 120
Kryptokontroverse 103
Kryptopolitik 8, 103
Kultusministerium 94

L

LAN 106
Landesdatenschutzgesetz 7, 13
Landesjugendamt 74
Landesmeldegesetz 51
Landesrundfunkgesetz 60
Landesverfassungsgericht 8
Landesverfassungsschutzgesetz 11
Landesweites Polizeiinformations-System 101, 104
Landgericht 28
LAPIS 101, 104
Laufzeittest 64
Lauschangriff 146
LAVINE 104, 119
Lehrlingsrolle 97
LKSt 101, 104, 119
Lohnsteuerkarte 70
Löschung 31

M

Machbarkeitsstudie 65
Magnetbandkassette 85
Mediendienstestaatsvertrag 61
Mediennutzungsverhalten 123
Medizinischer Dienst der Krankenversicherung 83, 150
Meldebehörde 45
Meldedaten 46, 50, 105, 131
Meldepflicht 92
Melderegister 50, 54, 58, 68, 116
Melderegisterauskunft 52
Mietvertrag 54
Mikrozensus 57
Mindestfrist 10
Missbrauchsbekämpfung 60
Mitarbeiter im öffentlichen Dienst 88
Mitgliedstaat 13
Mitwirkungspflicht 68, 76
Mobifinder 112
Mobilfunk 60, 112

N

Nachlass 65
NADIS 47
Namen 66
NAT 119
Network Directory System 114
Netzsicherheit 59, 64
nicht-öffentlicher Bereich 10
Notar 6, 27
Notrufnummer 81
Novellierung 7, 13, 60, 121
Nutzeridentifikation 65
Nutzungsprofil 61

O

Offenbarungsversicherung 26
Online-Registrierung 111, 121
Orange Book 109
Ordnungswidrigkeit 59
Organisationskontrolle 33
Ortung 112

P

parlamentarische Kontrolle 21, 146
Parteien 51
Passwort 30
Patientendaten 83, 85, 105, 143, 149
Patientengeheimnis 151
Pay TV 123
PED M-V 40
Pentium III 110, 121, 136
Personalakte 92
Personalausweis 66, 120
Personaldaten 22, 32, 104
Persönlichkeitsprofil 58
PERSYS 104
Pfändung 62
Planfeststellungsverfahren 56
Polizei 45
Polizeikontrolle 8
Polizeiliche Erkenntnisdatei Mecklenburg-Vorpommern 40
Processor Serial Number 110, 136
PROfiskal-Handbuch 63
Protektion Profiles 109
Protokollierung 31, 41
Prüfkriterien 109
Pseudonym 61
pseudonymisierte Daten 8, 71
Pseudonymisierung 9, 13, 108, 110, 143, 151
Pseudonymität 109
PSN 110, 136

R

Rechenzentrum 12
Rechnernetz 12
rechtfertigender Notstand 81
Rechtsprechung 28
Rechtssicherheit 10, 12
Rechtsverordnung 10
Referentenentwurf 9, 59
Register 58
Registerverfahrensbeschleunigungsgesetz 23
RegTP 105
Regulierungsbehörde für Telekommunikation und Post 105
Reisepass 66
Rettungsleitstelle 81

Revisionsfähigkeit 12, 136
Revisionssicherheit 120
richterliche Anordnung 18
richterliche Unabhängigkeit 128
Richtlinie 13, 66
Rückkehrer 45
Rufnummernanzeige 59
Rundfunkänderungsstaatsvertrag 60
Rundfunkstaatsvertrag 60, 123

S

Schadensersatz 9
Schattenkonten 125
Schleierfahndung 38
Schlüsselerzeugung 69
Schuldnerlisten 26
Schweigepflicht 80
Schweigepflicht, ärztliche 80, 84
Schweigepflichtentbindungserklärung 81
Sekte 94
SGB I 76
SGB IV 70
SGB V 72, 83
SGB VIII 73
SGB X 75
Sicherheitskonzept 10, 63
Sicherheitsüberprüfung 29
Sicherheitsziele 12
Signalisierung 60
Signaturgesetz 24, 65, 105, 106
Signaturverordung 105
Sozialdaten 75
Sozialhilfeempfänger 76
Sozialversicherungsnummer 70
Sparkasse 66
Sparkassenverordnung 22
Staatsanwaltschaft 30, 34, 36, 41
Staatssicherheitsdienst 91
StADÜV 70
Standortkennung 60
Stasi-Unterlagen-Gesetz 88
Statistik 57
Statistisches Bundesamt 58
Sterbeurkunde 65
Steueramt 67
Steueranmeldungs-Datenübermittlungs-Verordnung 70
Strafakten 22, 138
Systemdatenschutz 9

T

Täterlichtbildsystem 40
Täter-Opfer-Ausgleich 16, 139
TDSV 59, 107
technische und organisatorische Maßnahmen 9, 12, 63
Technische und organisatorische Maßnahmen 23
Teledienstedatenschutzgesetz 61
Telefonüberwachung 18, 36, 132
Telekommunikation 12, 59
Telekommunikationsanlage 32
Telekommunikations-Datenschutzverordnung 59, 107
Telekommunikationsgesetz 59
Telekommunikationsrichtlinie 59
Test 10, 58, 64
TESTA 118
Testdaten 30
Testdatenbank 64
Textverarbeitungsprogramm 32
TKG 59
Transparenz 10, 12, 136
Trennung 58
Trustcenter 24, 105, 119

Ü

Übermittlungskontrolle 50
Überprüfung 89
Überwachungssystem 113
Unabhängigkeit 10
Unschuldsvermutung 21
Unterhalt 74
Unterstützungspflicht 27
Untersuchungshaft 20, 130, 147

V

Verbindungsdaten 60, 134, 145
Verfassungsschutzbehörde 11
Verfügbarkeit 12
Verhaltensprofil 145
Vernetzung 12
Verordnung 14
Verordnungsermächtigung 10
Verschlüsselung 8, 13, 69, 127, 140
Verschwiegenheitspflicht 22, 27
Verteidiger 20
Vertrauenswürdigkeit 109

Vertraulichkeit 12
Verwaltungsvollzug 58
Verzeichnisdienst 114, 118
Videokamera 113
Videoüberwachung 9, 11, 113, 133
Volkszählung 58
Volkszählungsurteil 11, 28, 67
Vollstreckung 26
Vollstreckungsschuldner 62
Vordruck 56

W

Wahlen 51
Wahllichtbildkarte 41
Wahlwerbung 131
WAN 106, 107
Web-Cam 113
Widerspruch 78
Widerspruchsrecht 16, 114
Windows 98 111
Wirtschaftsministerium 60
Wohngeld 75
Wohnraumüberwachung 146
Wohnsitz 66

X

X.500 114

Z

Zertifizierung 109, 111, 120
Zertifizierungsstelle 105
Zeugenvernehmung 42
Zugriffskontrolle 33
Zugriffsrecht 50
Zulassungsstelle 116
Zustimmungsgesetz 60
Zweckbindung 55
Zweckverband 101

9 Publikationen

Beim Landesbeauftragten für den Datenschutz sind derzeit folgende Publikationen kostenlos erhältlich und stehen im Internetangebot unter [www.lfd.m-v.de]zum Abruf bereit:

- **Gesetze und Verordnungen zum Datenschutz** - Stand 1998 -
  (Loseblattsammlung)

- **Technik und Datenschutz** - Stand 1996 -
  (Arbeitsergebnisse und Tagungsunterlagen des Arbeitskreises Technik in Broschürenform)

- **Datenschutzfreundliche Technologien** - Stand 1998 -

- **Orientierungshilfe Internet** - Stand 1998 -
  (Broschüre „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“)

- **Handys - Komfort nicht ohne Risiko** - Stand 1998 -
  (Faltblatt)

- **Informationen zum Datenschutz**
  (Faltblätter mit aktuellen Informationen)

  2. Datenschutz und Personalcomputer
     - Stand 1992 -
  4. Patientenakte
     - Stand 1992 -
  5. Datenschutz und Verfassungsschutz
     - Stand 1993 -
  6. Datenschutz und Personen-Identifikation
     - Stand 1993 -
  7. Datenschutz und Telefax
     - Stand 1993 -
  9. Datenmißbrauch
     - Stand 1993 -
  12. Das ISDN-Netz
      - Stand 1994 -
  13. Freiwillige Patienten-Chipkarten
      - Stand 1994 -
  15. Umgang mit Sozialdaten
      - Stand 1995 -
  16. Personenbezogene Daten in der Forschung
      - Stand 1995 -
  17. Technikfolgenabschätzung
      - Stand 1995 -
  18. Sicherheit der Informationstechnik
      - Stand 1995 -
  19. Personalakten und Personalaktendaten
      - Stand 1995 -
  20. Statistische Erhebungen
      - Stand 1995 -

Tätigkeitsberichte *(in Broschürenform)*

- Erster Tätigkeitsbericht für den Zeitraum 1992/93
- Zweiter Tätigkeitsbericht für den Zeitraum 1994/95
- Dritter Tätigkeitsbericht für den Zeitraum 1996/97
- Vierter Tätigkeitsbericht für den Zeitraum 1998/99

Informationen des Bundesbeauftragten für den Datenschutz *(in Broschürenform)*

- BfD - INFO 1 - Bundesdatenschutzgesetz - Stand 1996
- BfD - INFO 2 - Der Bürger und seine Daten - Stand 1993
- BfD - INFO 3 - Schutz der Sozialdaten - Stand 1994
- BfD - INFO 4 - Der behördliche Datenschutzbeauftragte - Stand 1996
- BfD - INFO 5 - Datenschutz und Telekommunikation - Stand 1998

Handreichungen *(in Form von Kopien)*

- Hinweise zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen - Stand 1992 -
- Orientierungshilfe „Forderung an Wartung und Fernwartung von DV-Anlagen“ - Stand 1993 -
- Hinweise zur Führung von Dateibeschreibung und Geräteverzeichnis - Stand 1993 -
- Organisationshilfe zur Vernichtung von Schriftgut - Stand 1996 -
- Orientierungshilfe „Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme)“ - Stand 1994 -
- Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung“ - Stand 1995 -
- Orientierungshilfe „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ - Stand 1996 -
- Musterdienstvereinbarung über die Nutzung der Telekommunikationsanlage - Stand 1998 -
- Empfehlungen zur Paßwortgestaltung und zum Sicherheitsmanagement - Stand 1991 -